Calypso
Networks Association

GUIDE

to drafting tenders for cards, NFC mobile ticketing and terminals based on the Calypso standard

February 2023

How to open up your ticketing system in calls for tenders?

TABLE OF CONTENTS

1 CONTEXT

Ticketing systems are a highly strategic issue for transit authorities and operators as they transform the mobility policy for their territory and also ensure it can generate revenue. These systems are designed to be sustainable and flexible, particularly with regards to fare changes, network extensions and the implementation of interoperability schemes.

To ensure the durability of a ticketing system, it is necessary to be able to integrate equipment, cards and software from different manufacturers during its lifecycle. Indeed, the original supplier of the system does not necessarily have the capacity or the desire to provide evolutions at a reasonable price. Having several potential suppliers avoids a monopoly situation for the networks, which could result in excessive costs, or the inability to carry out an upgrade.

To ensure compatibility and technical interoperability between different suppliers, it is important to move from a product logic (fixed and generally proprietary in essence) to a standards logic, provided that they are open and multisource. The client must then have requirements for compliance with these norms and standards, the proof of which must be provided by the supplier through the certification of its products.

The Calypso standard meets the requirements set by international bodies for open standard designation: "A standard is said to be open when **it is made available to all, developed, maintained and managed in a collaborative and consensual process. An open standard facilitates interoperability and data exchange between different products or services and is intended to be widely adopted**[1] ".

Calypso was created to be developed, maintained and managed by transport authorities and operators who together form the Calypso Networks Association (CNA). CNA is a non-profit association which operates with the objective to guarantee scalability, interoperability, and vendor independence for all users. Calypso is the only ticketing standard that is multisource at all levels, including the electronic components in cards.

It is a major provider of resilience in times of component shortages. It provides the industrial world with reference specifications and a certification process to attest product conformity. It is the standard adopted by many networks around the world. Many suppliers of different origins therefore offer Calypso products in a multisource scheme that has been successful for more than 20 years. This genuine competition guarantees that the buyer will be offered Calypso products at the right price.

The challenge of ticketing tenders, beyond the hardware purchase function, is to guarantee compatibility between the media (contactless cards, NFC smartphones, ...) and the ticketing terminals (validators, sales and control devices, kiosks, ...) already deployed and newly acquired. Without this prerequisite compatibility, it is impossible to deploy interoperable schemes.

[1] *According to the definition of open standard given by the International Telecommunication Union*

The document "Ticketing for MaaS: best practices for durable systems" presents all the best practices to follow when specifying a ticketing system. In particular, it reminds us that the data model must not be integrated into a ticketing system or terminal tender, but must be managed independently, under the control of the client, who must ensure the ownership of the data model.

2 PURPOSE OF THE DOCUMENT

The purpose of this document is to outline what is required in a **call for tenders for contactless cards, NFC mobile ticketing systems and terminals to guarantee compatibility and scalability**.

A public tender must allow open and fair competition for all manufacturers. This document has been written in compliance with the principles of French public procurement codes and can therefore be used as a guide to producing calls for tenders.

This document is written by CNA, free of copyright and can be replicated in whole or in part.

CNA offers support for the drafting of your call for tenders, in particular assistance in defining the configuration and personalisation of your Calypso cards.

A verification of the configuration and personalisation of Calypso cards delivered by the manufacturers is also proposed.

For more information, please contact us: contact@calypsonet.org

3 GENERAL PRINCIPLES

The general principles below are detailed in the chapters dedicated to cards, NFC smartphones and terminals respectively:

- Systematically refer to all norms and standards applicable to the field,
- Require certified products, proof of compliance with standards, or in the absence of existing certification, a declaration of compliance with standards applicable to the field,
- Refer to existing shared standards and best practices when available at national level (e.g. in France NF P99-405-1[2], NF P99-512 3[3], etc.),
- Preferably, ask to integrate the Calypso Hoplink application in Calypso Prime cards and security modules. This does not add cost and allows for future interoperability,
- Do not refer to a commercial product name specific to a given industry,
- Do not refer to technologies, specifications or solutions that have become obsolete, in particular through the emergence of shared repositories.

[2] *Transport sector computer ticketing - Interoperability and encoding rules of computer ticketing (INTERCODE) - Part 1 : codification of data elements and structures*

[3] *Transportation fare Management - Interoperable Fare Management System (Interoperable Fare Back Office) - INTERBOB – Dataflow*

4 SPECIFIC REQUIREMENTS **FOR CONTACTLESS CARDS**

A properly implemented Calypso system can accept all Calypso certified contactless cards

Calypso Networks Association has created three products:

Calypso PRIME Calypso LIGHT Calypso basic

All of them have the same security mechanisms and can be managed by the same terminal software, ensuring compatibility and easy integration.

- Calypso PRIME combines transport and multi-application/multiservice functionalities on a single card. It also permits the management of multiple ticketing contracts and interoperability between networks, including those on an international scale. Calypso Prime also allows card authentication without requiring additional security modules (SAM) in its PKI version.
- Calypso LIGHT is a refined version, more suitable for occasional users, with the same security level as Calypso Prime. It can be issued on ISO plastic or paper and two transport contracts from the same operator can coexist on one card. It is also a product specifically adapted to ABT (Account Based Ticketing) architectures.
- Calypso basic available since 2022, is a single-contract, contactless, reloadable paper ticket, suitable for single trips.

In the context of a call for tenders, a principal must require that the cards are certified both at the radio frequency level (hardware/hardware) and at the Calypso functional level (software/software), as described in the next two sub-chapters. Purchasing uncertified cards poses a serious risk of card-terminal incompatibility.

4.1. RADIO FREQUENCY (RF) REQUIREMENTS AND CERTIFICATIONS

The first requirement is that the **contactless card** must comply with the latest version of **ISO/IEC TS 24192** (formerly **CEN/TS 16794**), which is the transport application of **ISO/IEC 14443**.

Compliance with this standard ensures that the card is interoperable with terminals that comply with this standard. And also, with NFC smartphones that comply with the NFC Forum (https://nfc-forum.org/) requirements, especially when used to reload a ticket onto the contactless card.

Compliance with this standard must be demonstrated by obtaining a certificate from a certification body approved by the Smart Ticketing Alliance, which has developed and implemented the RF certification programme (https://www.smart-ticketing.org/certification/) for several years.

The RF certification process is carried out by Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), an independent certification body, which is the only one currently authorised to issue RF certification under the Smart Ticketing Alliance program.

The current list of cards certified to ISO/IEC TS 24192 (CEN/TS 16794) by PayCert is public and can be found on the PayCert website : https://www.cna-paycert-certification.eu/rf-interface/picc/.

! IMPORTANT : The RF certification of a card concerns the finished product, including the component with its software, the inlay with antenna and the card body, assembled.

We strongly advise against ordering cards using the B’ protocol (also called Innovatron). This protocol is obsolete because there is no certified product that complies with this protocol. As a reminder, the B’ protocol does not allow the integration of Hoplink. It does not allow either the treatment of NFC smartphones (Secure Element and Host Card Emulation) nor the implementation of interoperability. If the network operates only in B’, it is recommended to order dual-mode cards (and ISO 14443 A|B) in order to facilitate migration when the time comes.

See Section 6.1.2 Obsolescence Management for more details on the consequences of maintaining the B’ protocol.

4.2. CALYPSO FUNCTIONAL REQUIREMENTS AND CERTIFICATION

CNA has outlined both the reference specifications to which any Calypso card (Prime, Light, Basic) must conform and also a certification scheme to guarantee this conformity. This certification is managed by the certification body PayCert, the only entity authorised to issue certificates. There is a dedicated certification for each of the three cards (Prime, Light, Basic).
It should be noted that Calypso Prime can be configured in three versions. The tender must specify which configuration is requested:

- Regular mode, (formerly rev 3.1); this mode includes the basic functions of Calypso Prime with TDES and DESX cryptography.
- Extended mode (formerly rev 3.2), with AES cryptography and optional data encryption in addition to the normal mode features.
- PKI mode (formerly rev 3.3), which adds asymmetric PKI cryptography to the extended mode, allowing card authentication without a security module (SAM) in the terminal.

In a **call for tenders:**

- For Calypso Prime cards, compliance with Calypso Prime certification, at the same level (or higher) as the version (regular, extended or PKI) being requested, is required. It is recommended to require at least extended mode certification compliance. If you need card authentication without a security module, you should request PKI mode compliance.
- For Calypso Light cards, compliance with Calypso Light certification is required.
- For Calypso Basic cards, compliance with Calypso Basic certification is required.

A list of certified Calypso cards can be found at: https://www.cna-paycert-certification.eu/card/

4.3. CARDS CONFIGURATION

For all **Calypso** cards **(Prime, Light and Basic)**, the requested configuration must comply with the following rules:

- Use an application identifier (also called "AID" or "container") **standardised** by ISO and referenced by CNA, specific to the ticketing system operator. Do not use generic identifiers such as "1TIC.ICA" for which uniqueness is not guaranteed and which are incompatible with NFC smartphone ticketing solutions. CNA manages a list of registered Calypso AID values.To request a registered Calypso AID, please contact the Calypso technical support: support@calypsonet.org

- Use the identifier provided by CNA as is, without adding any additional 00.

For **Calypso Prime** cards, the configuration must also respect the following rules and recommendations:

- Always configure the applications in Regular, Extended or PKI mode, as needed (and not in Calypso Revision 2.4 or lower version).

- Integrate the Hoplink application (recommended because in most cases it does not add any cost and will enable the futur implementation of an interoperability scheme).

- Use the most recent file structures and avoid old file structures as much as possible.
  A list of file structures referenced by CNA is available in the "Calypso File Structure Registry" document (ref. 060709-CalypsoFiles).

- Use dedicated key sets for each application with recent cryptography: **TDES, AES or PKI**, and no longer use obsolete cryptographies, such as DES.

- If there is a need for compatibility with an older network (Calypso revision 2.4), a certified Prime card emulating revision 2.4 should be requested.

For **Calypso Light** cards, the configuration must also respect the following rules:

- Choose one of the two allowed file structures (Reference or Classic), depending on the existing structures and your future needs.
- Use, preferably, a dedicated key set for this product. Light cards use TDES cryptography only.

For **Calypso Basic** cards, the configuration must also:

- Use a dedicated key set for this product. Basic cards use TDES cryptography only.

Warning: Do not confuse the **file structure** of a Calypso card with the **contract structure**, also called "instantiation". These two structures do not cover the same notion. The file structure defines the organisation of the files in the card. The contract structure, "instantiation", is used to encode transport tickets.

CNA offers support for the drafting of your call for tenders, in particular assistance in defining the configuration and personalisation of your Calypso cards. A verification of the configuration and personalisation of Calypso cards delivered by manufacturers is also proposed.

For more information, please contact us: contact@calypsonet.org

4.4. TEXT FOR CALL FOR TENDERS

See how-to sheet n°1

5 SPECIFIC REQUIREMENTS **FOR NFC MOBILE TICKET**

5.1. SOLUTIONS: SE AND HCE

NFC mobile ticketing is the technology that allows the use of an NFC smartphone to purchase and/or validate tickets (i.e. reader mode) or to emulate a contactless card.

In this document we focus on the ability of the NFC smartphone to emulate a contactless card. NFC mobile ticketing is available in several modes depending on whether the security is based on a hardware security element in the NFC smartphone or not:

- NFC **SE** (Secure Element) mobile ticketing uses a microprocessor component identical to the one found in a card, and therefore has the same level of security: Common Criteria EAL4+ at least for the SE. SEs are present in recent models of NFC smartphones from several manufacturers, including Samsung and Apple

  A generic Calypso applet (software application) is provided by CNA to be loaded in the SE and thus fully emulate a Calypso Prime card.

  This solution has the advantage of not requiring any evolution of the existing ticketing terminals, just a few parameters, provided that the system is compliant with at least Calypso Prime revision 3, regular mode.

- NFC **HCE** (Host Card Emulation) mobile ticketing does not rely on the use of a SE stored in the NFC smartphone, but on software security. It is compatible with all Android NFC smartphones. To compensate for the lower innate security, due to the non-use of a Secure Element to protect sensitive data, a mechanism (called tokenisation) regularly updates the secret keys of the Calypso HCE application stored in the NFC smartphone, limiting the risk of fraud.

  As with the SE solution, the system must be compliant with at least Calypso Prime revision 3. It requires a slight software evolution of the validation ticketing terminals in order to implement security measures specific to the HCE solution.

Compliance with the terminal requirements, described later in this document, guarantees compliance with the specific requirements for NFC mobile solutions.

NFC mobile solutions, whether applet-based in an SE or HCE, are marketed by dedicated vendors in charge of installing and initialising the Calypso application in the NFC smartphone.

5.2. SECURE ELEMENTS (SE) SOLUTION REQUIREMENTS

The SE solution can be sourced directly from a dedicated supplier or indirectly through your ticketing integrator. In both cases, the customer must request that the supplier guarantees:

- The NFC mobile ticketing solution can work with any RF certified NFC smartphone, either based on the NFC Forum certification or on the ISO/IEC TS 24192 latest edition certification (or its CEN/TS 16794 version)

- The applet is loaded in Secure Elements (SE) only, which have been functionally certified as compliant with Calypso "Applet/SE" pairing. PayCert, an independent accredited organisation, manages this certification, and the list of certified products is available at https://www.cna-paycert-certification.eu/card/calypso-prime-applet/. If an "Applet/SE" pairing is not already certified, it is up to the supplier to request this certification.

5.3. CALYPSO HCE SOLUTION REQUIREMENTS

The HCE solution can be sourced directly from a dedicated supplier or indirectly via your ticketing integrator. In both cases, the customer must ensure that the following requirements are taken into account:

- The supplier guarantees that its NFC mobile ticketing solution can work with any Android NFC smartphone that has been RF certified, either on the basis of the NFC Forum certification, or on the basis of the ISO/IEC TS 24192 latest edition certification (or its CEN/TS 16794 version).

- **Functional certification of compliance with Calypso HCE specifications** will be required as soon as it becomes available (end of 2023).

- **Calypso HCE security certification** is based on a state-of-the-art standard for resistance to smartphone data hacking. CNA issues this certificate with the assistance of Internet of Trust (https://www.internetoftrust.com/) as an independent certification body. A list of vendors that have passed this certification is available at calypsonet.org. It is strongly recommended that this certification be required, even though it is not currently mandated by CNA.

- Compliance with the Calypso HCE specifications and guidelines established by CNA regarding the requirements applicable to the ticketing system infrastructure.

! The Calypso HCE solution is purely software based and cannot rely on the security classification of an electronic component in the NFC smartphone. To ensure a security level that complies with the Calypso standard, CNA has implemented a set of security measures specific to the HCE solution, which can be found **in the specifications and guidelines.**

All Calypso HCE vendors are contractually committed, as licensees, to comply with these specifications and guidelines.

5.4. TEXT FOR CALL FOR TENDERS

See how-to sheet n°2

6 SPECIFIC REQUIREMENTS **FOR TERMINALS AND TICKETING SOFTWARE**

For the purposes of this document, a terminal is a sales, validation, control or personalisation device. Ticketing software is that which enables a ticketing transaction, which in the CNA ecosystem includes the reader software, the Calypso library and the ticketing application, regardless of whether they are in the terminal or exported to a central server.

REMINDER: to guarantee interoperability between several items of ticketing infrastructure, especially cards and readers, it is crucial that each one is certified both at radio frequency and functional levels.

6.1. RADIO FREQUENCY (RF) REQUIREMENTS AND CERTIFICATION

The first requirement is that the **contactless terminal's radio frequency (RF)** complies with the latest version of **ISO/IEC TS 24192** (formerly named **CEN/TS 16794**), which is the transport application of **ISO/IEC 14443**.

Compliance with this standard ensures terminal interoperability with cards that comply with this standard. And also, NFC smartphones that comply with NFC Forum requirements, especially when used to emulate a contactless transport card.

Compliance with this standard must be demonstrated by obtaining a certificate from a certification body approved by the Smart Ticketing Alliance, which has developed and implemented the radio frequency certification programme (https://www.smart-ticketing.org/certification/) for several years.

The RF certification process is carried out by Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), an independent certification body and the only body currently authorised to issue RF certification according to the Smart Ticketing Alliance program.

The current list of ISO/IEC TS 24192 (CEN/TS 16794) certified terminals is public and can be found on the PayCert website at https://www.cna-paycert-certification.eu/rf-interface/pcd/.

! **IMPORTANT**: The RF certification of a terminal includes:

- The finished product, including the electronic hardware in its final packaging, with the software
- Or on a sub-assembly of the finished product, insofar as this sub-assembly has been integrated into the finished product according to the manufacturer's recommendations, which guarantee no loss of the certification.

6.1.1. COMPATIBILITY WITH EMV CONTACTLESS PAYMENT CARDS AND APPLICATIONS

If the implementation of an **Open Payment** service is envisaged in the short, medium or long term, it is advisable to request, in addition to the RF certification, that the terminals be EMVCo level 1 (L1) certified. **This certification process is done with EMVCo** (https://www.emvco.com/).

The updated list of EMVCo L1 certified terminals is public and can be found on the EMVCo website at: https://www.emvco.com/approved-registered/approved-products/

6.1.2. COMPATIBILITY WITH APPLE NFC PRODUCTS

If the implementation of **NFC mobile ticketing on the iPhone or Apple Watch** is envisaged in the short, medium or long term, it is necessary to request, in addition to the RF certification, that the terminals manage the Apple specific («ECP») protocol in order to support the Apple Express mode (https://support.apple.com/en-us/HT212171). **This certification process is done with Apple Inc.**

To date, there is no public list of terminals supporting the Apple Express mode.

6.1.3. OBSOLESCENCE MANAGEMENT

The first Calypso cards issued in the 2000s used the Innovatron protocol (also called B' or B prime). Today, the Calypso standard is based exclusively on ISO/IES 14443 (type A or B). But old cards using the B' protocol are still in the field because terminals are sometimes not updated to use ISO/IES 14443 type A or B protocols.

Only a few models of terminals still integrate the B' protocol in addition to the standard protocol, which leads to a significantly higher cost of this equipment compared to standard terminals. It is therefore necessary to question the relevance of maintaining the B' protocol rather than replacing the B' cards still in circulation.

On the other hand, the wide variety of terminals that comply with the ISO/IEC TS 24192 standard (formerly called CEN/TS 16794) guarantees an optimum price for this equipment. Finally, the B' protocol does not allow for the integration of Hoplink, nor for the handling of NFC smartphones (SE and HCE), nor for the management of MaaS.

The management of existing B' cards should only continue if it is imperative, and only in this case should a terminal supporting both the standard and B' protocols be specified.

6.2. SOFTWARE REQUIREMENTS

6.2.1. STRUCTURED IN THREE SOFTWARE LAYERS

CNA has defined a three-layer software structure to ensure scalability, modularity, and the ability of the terminal to handle all certified Calypso cards. These three layers are described on the website https://calypsonet.org/calypso-for-terminals/.

Each software layer has its own requirements document, written by CNA.

6.2.2. READER LAYER (SOFTWARE READER)

The software layer in charge of the exchanges between the card and the reader, called "Reader Layer", can manage all types of cards and SAMs, whatever their technology: Calypso, CIPURSE, MIFARE, etc. This software layer does not contain any Calypso specific elements. The application software layer accesses it via reference APIs (Reader API & Card API) defined by CNA.

To date, the client must ask the bidder to present the reader registration letter issued by CNA, which certifies, on a declarative basis, compliance with the requirements described in the "Reader Layer Requirements" document, established by CNA. At the end of 2023, a "Reader Layer" certification will replace the declarative one.

6.2.3. CALYPSO LAYER (CALYPSO FUNCTIONAL LIBRARY)

The "Calypso Layer" software layer enables the specific management of Calypso-specific cards and SAMs in strict compliance with the functional specifications of this standard. This layer corresponds to the Calypso library, the application software layer accesses it via a reference API (Application Programmable Interface) defined by CNA.

To date, the client must ask the bidder to present the Calypso library registration letter issued by CNA, which attests, on a declarative basis[4], to compliance with the requirements described in the "Calypso Layer Requirements" document. At the end of 2023, a "Calypso Layer" certification will replace the declarative one.

ℹ The declaration is a simple commitment document from the manufacturer to respect the requirements (Reader or Calypso layer). The certification verifies both the respect of the requirements and the conformity to the reference APIs defined by CNA; there is thus a guarantee of interoperability.

[4] *It is important to remember that this is a declaration made by the manufacturers on their honour and not the result of tests carried out by an independent laboratory. When the corresponding certification will exist (end of 2023), it should be required.*

6.2.4. TICKETING LAYER

The Ticketing Layer is the ticketing application (fare and business rules, access management, etc.) that is present in the terminal - or remote in a central server (ABT systems).

CNA has published a document called **"Ticketing Layer Requirements"**.

It is both a requirements document and a recommendation for the use of the reference APIs defined by CNA. It also contains best practices to follow in the implementation and management of a Calypso ticketing system.

The "Ticketing Layer Requirements" document does not require certification because the ticketing applications are specific to each network. It is up to each network to ask for its respect and use.

6.2.5. OPEN SOFTWARE: ECLIPSE KEYPLE

CNA recommends that the open source software Eclipse Keyple be included in the calls for tenders. Eclipse Keyple is free of rights (Eclipse Public License 2.0 (or EPL-2.0)).

Reliance on open source software creates a durable solution, as ensuring that the potential for evolution is independent from a specific supplier, prevents a monopoly and increases competition, especially with regards to cost. The use of Keyple guarantees that the terminal will be able to process all certified Calypso cards, including the most recent ones.

Keyple implements the reference APIs defined by CNA for Calypso terminals and complies with the Reader Layer and Calypso Layer requirements.

Keyple is composed of two software applications each associated with a specific layer:

- **Keyple Core** corresponds to the "Reader layer", here, the hardware (reader) integration is done via a plugin.

- **Keyple Calypso** corresponds to the "Calypso layer".

If Keyple Calypso is used, the bidder can provide the registration letter of the Keyple Calypso library directly.

If Keyple Core is used, the bidder must submit the reader registration letter, which attests, on a declarative basis, to compliance with the requirements described in the "Reader Layer Requirements" document. This registration letter ensures compliance of the "terminal hardware/Keyple Plugin/Keyple Core" package.

When available, the certification will replace the registration letter.

The use of Eclipse Keyple, as an open source software, guarantees a total independence between the terminal hardware and software :

- It is therefore possible to replace one hardware with another, while keeping the same software (Keyple Core, Keyple Calypso and application software) and by using (or developing) the Keyple Plugin ad hoc for the new hardware.
- It is possible to intervene on the software of a given terminal, without any involvement on the hardware, which avoids any proprietary issues for the global hardware/software solution.

6.3. CERTIFICATION AND DECLARATION OF CONFORMITY

The following table indicates the certifications and/or declarations to be required, according to the type of hardware, until certification is available.

Hardware/Software Type	Certification required	Registration letter to be required		Commitment letter to be required
	ISO/IEC TS 24192	Reader layer	Calypso layer	Ticketing layer
Hardware without Calypso library	√	√		
Hardware with Calypso library	√	√	√	
Equipment integrating the network ticketing application	√	√	√	√
Calypso library only			√	
Ticketing application only				√

The list of terminals and software that have been declared compliant is available at https://calypsonet.org/calypso-certification/.

Each layer must be compliant for a device to be **deemed compliant**.

6.4. TERMINAL REQUIREMENTS FOR SECURITY MODULES

Depending on the terminal, it may be necessary to provide slots for the integration of security modules (SAMs).

The number of slots depends on the context, the type of terminal and the type of Calypso card that will be used.

For all terminals, it is recommended to provide at least two slots, and preferably four, for possible system upgrades.

The current format of the security module (SAM) is the SIM format (ID-1/1FF) of which the mini SIM format (2FF) is detachable. For specific needs, it is possible to obtain the micro SIM (3FF), or nano SIM (4FF) formats.

6.5. TEXT FOR CALL FOR TENDERS

See how-to sheet n°3

“HOW-TO” SHEET N°1

SPECIFYING CALYPSO CARDS IN A CALL FOR TENDERS

We mention here only the text elements (in black), to be inserted in a call for tenders, concerning the conformity of Calypso cards, with explanatory comments (in italics). All other characteristics, physical, ergonomic, specific constraints, additional requirements must be added for the bidder to answer.

Concerning Calypso cards, compliance with all ISO/IEC 14443, ISO/IEC 7816, ISO/IEC TS 24192 (or CEN/TS 16794) reference standards is ensured by simply referring to the obligation of RF certification of the card, which is a first prerequisite to interoperability, by asking the bidder to submit the certificate of the proposed card:

"The card shall be certified to ISO/IEC TS 24192 latest edition (or by default CEN/TS 16794). The bidder will provide the certificate of the proposed card. As a reminder, the certificate provided relates to the finished product as it will be delivered, including the component with its software, the inlay with antenna and the card body, assembled. It cannot be a certificate issued for a different product, in case one of these elements has been modified after the certification. Nor can it be a certificate issued by the component supplier based on a different insert."

Compliance with the Calypso functional specifications, which is the second prerequisite for interoperability, is ensured by referencing the Calypso functional certification requirement, requiring the bidder to submit the certificate for the proposed card:

"The card must have undergone Calypso functional certification. The bidder shall submit the certificate for the card it proposes."

- *If the card is a Calypso Prime card, the requested mode must be specified: Regular, Extended (recommended as a minimum) or PKI if a Calypso Prime card implementing asymmetric cryptography is chosen.*

- *If it is a Calypso Light card or Calypso Basic, there is no need for further specification.*

- January 2023 -

Regarding the configuration and customisation aspects, the elements (described in paragraph 4.3) are to be included in the tender text.
For each application contained in the Calypso Prime card (local network application, Hoplink, AMC, ...):

"The cards provided must respect the application ***(mention the name of the application):***

- Use the network application identifier (also called AID or container) standardised by ISO and referenced by CNA: ***(mention the chosen identifier provided by CNA as is, without adding any additional 00s)***,

- Be configured in Regular / Extended / PKI mode ***(depending on the need, put the chosen application (Regular, Extended or PKI), or mention*** "emulation of Calypso revision 2.4" ***only if there is a need for compatibility with an old network)***.

- Use a dedicated TDES / AES key set, the key set will be provided a posteriori ***(choose one of the two cryptographies according to the existing key sets in the network and the future needs and do not use DES or DESX key sets anymore)***.

- Use the file structure: ***(choose a recent file structure depending on the need and avoid old file structures as much as possible. A list of file structures referenced by CNA is available in the "Calypso File Struture Registry" document (ref. 060709-CalypsoFiles)***."

CNA offers support for the drafting of your tenders, in particular assistance in defining the configuration and personalisation of your Calypso cards.

A verification of the configuration and personalisation of the Calypso cards delivered by the manufacturers is also proposed.

For more information, please contact us: contact@calypsonet.org

- January 2023 -

"The supplied cards must respect the following conditions for the Hoplink application ***(if the customer chooses, as there is no extra cost)***:

- Use the Hoplink identifier.
- Be configured in Regular/Extended mode ***(depending on the need, put the chosen mention between these two modes).***
- Use the Hoplink TDES key set.
- Use the Hoplink file structure: structure 0Ch.
- Initialise the environment file according to the Hoplink specification.
- Print the Hoplink logo (see Hoplink graphic charter)."

For a Calypso Light card:

"Supplied cards must:

- Use the network application identifier (also called AID or container) standardised by ISO and referenced by CNA, specific to the ticketing system operator: ***(mention the chosen identifier provided by CNA as it is, without adding any additional 00)***,
- Be configured according to the Reference / Classic file structure ***(choose one of the two depending on the existing structures in the network and future needs)***,
- Use a dedicated TDES key set for this product; the key set will be provided afterwards."

For a Calypso Basic card:

"Supplied cards must:

- Use the application identifier (also called AID or container) standardised by ISO and referenced by CNA, specific to the ticketing system operator: ***(mention the chosen identifier provided by CNA as it is, without adding any additional 00)***,
- Use a set of dedicated TDES keys for this product; the set of keys will be provided afterwards."

“HOW-TO” SHEET N°2

SPECIFYING A CALYPSO NFC MOBILE TICKETING SOLUTION IN A CALL FOR TENDERS

For Calypso NFC mobile ticketing solution on SE:

"The proposed Calypso NFC mobile ticketing solution on SE must have the ability to run on any RF certified NFC smartphone, either based on the NFC Forum certification or based on the ISO/IEC TS 24192 latest edition certification (or its CEN/TS 16794 version).

The applet must be loaded only in Secure Elements (SE) that have been functionally certified by PayCert, an independent accredited organisation, as being compliant with Calypso. The list of certified products is available at https://www.cna-paycert-certification.eu/card/calypso-prime-applet/. The supplier commits to regularly ensure during the contracted service period that all NFC smartphones in which the applet is loaded have obtained the Calypso functional certification of the Applet/SE pair. If an Applet/SE pair is not already certified, it will be up to the supplier to request this certification.

On the date of offer, the supplier will give the exhaustive list of NFC smartphones (supplier and product reference) eligible for the Calypso NFC mobile ticketing service it proposes. The supplier commits to keep an active watch on the NFC smartphones eligible for the Calypso SE solution and will regularly update this list throughout the duration of the service."

- January 2023 -

<u>For Calypso NFC HCE mobile ticketing solution:</u>

"The proposed Calypso NFC HCE mobile ticketing solution must have the ability to run on any NFC smartphone on Android operating system (OS) that has been RF certified, either based on NFC Forum certification or based on ISO/IEC TS 24192 latest edition certification (or its CEN/TS 16794 version).

The supplier must provide certificates proving that it has obtained:

- Calypso functional certification of the Calypso HCE SDK (to come)
- Calypso HCE SDK security certification.

The Calypso NFC HCE mobile ticketing solution must be based on Calypso HCE specifications and guidelines, and comply with all requirements. The supplier must provide a sworn statement that its Calypso NFC HCE mobile ticketing solution complies with the Calypso HCE specifications and guidelines in their entirety.

On the date of offer, the supplier will give the exhaustive list of NFC smartphones on Android operating system (OS) eligible for the Calypso NFC HCE mobile ticketing service it proposes. The supplier commits to keep an active watch on the NFC smartphones eligible for the Calypso HCE solution and will regularly update this list throughout the duration of the service."

“HOW-TO” SHEET N°3

SPECIFYING CALYPSO TERMINALS IN A CALL FOR TENDERS

The texts to be inserted in a call for tenders for terminals of a ticketing system only concern the correct implementation of the Calypso standard. A strict respect of the requirements defined by CNA and detailed in chapter 6 is necessary to guarantee the compatibility with all certified cards and NFC mobile ticketing solutions.

As a reminder and in accordance with the document «Ticketing for MaaS: best practices for durable systems», the data model must not be integrated in a terminal tender but managed independently under the control of the originator who ensures ownership.

With reference to the table in chapter 6.3, the text below corresponds to the line equipment integrating the network ticketing application.

"The proposed terminal must have received the certificate of conformity to the ISO/IEC TS 24192 standard (formerly named CEN/TS 16794), which the bidder will attach to its offer. It is reminded that this radio frequency certificate of the terminal must cover the finished product which includes the electronic hardware in its final packaging, with the software.

The terminal software will be structured in three software layers in order to ensure scalability, modularity and the ability of the terminal to handle all certified Calypso cards. These three layers are described at https://calypsonet.org/calypso-for-terminals/.

The bidder will have to prove its compliance with the requirements of these three software layers by providing:

- The registration letter of the terminal card reader, which attests, on a declarative basis, to compliance with the requirements described in the "Reader Layer Requirements".

- The registration letter for the Calypso library, which attests, on a declarative basis, to compliance with the requirements described in the "Calypso Layer Requirements" document.

- A letter of commitment, which attests, on a declarative basis, to compliance with the requirements, recommendations and good practices described in the "Ticketing Layer Requirements" document.

- January 2023 -

The first two paragraphs will be replaced by the two paragraphs below as soon as the certification is available and will therefore replace this registration on a declarative basis:

- The certificate of the terminal card reader, which attests to compliance with the requirements described in the "Reader Layer Requirements" document.

- The certificate of the Calypso library, which attests to compliance with the requirements described in the "Calypso Layer Requirements" document.

The proposed terminal will use the reference APIs defined by CNA: Reader API, Card API and Calypso API.

The proposed terminal will preferably use the open source software Eclipse Keyple.
Eclipse Keyple is free of rights (Eclipse Public License 2.0 (or EPL-2.0)).

When using the Keyple Core module, the bidder will be required to submit the Reader Registration Letter, which attests, on a declarative basis, to compliance with the requirements described in the "Reader Layer Requirements document". ***(To be replaced by the certificate as soon as the corresponding certification is available).***

If the Keyple Calypso module is used, the bidder shall provide the existing Keyple Calypso library registration letter directly ***(to be replaced by the certificate as soon as the corresponding certification is available)*****.**

The proposed terminal shall have a minimum of two, and preferably four, slots reserved for Security Module Integration (SAM) in the following format: ***(choose between SIM (ID-1/1FF), mini SIM (2FF), micro SIM (3FF), nano SIM (4FF)).***"

DEFINITIONS
AND ACRONYMS

- **ABT or Server-centric**

Account-based Ticketing system (ABT), also known as ID-centric, Server-centric, Cloud-based, Server-based (ISO name) or Security in System (ISO name). These terms refer to systems where the processing takes place in back-office and where cards are used merely for securely identifying holders and linking them to accounts.

- **AES**

Advanced Encryption Standard (as defined in ISO/IEC 18033-3). Symmetrical cryptographic algorithm using 128-bit data and key.

- **AID**

Application Identifier (also called «container»): value unique in a card, allowing to unambiguously identify a card application, as defined in ISO/IEC 7816-4 and ISO/IEC 7816-5.

- **AMC**

Multi-service Citizen Application: a standard whose objective is to allow the use of a single medium (card or mobile application) to access different services (transport, culture, waste disposal, parking, tourism, etc.). In France, the reference for the standards is NF 99-508.

- **API for Terminal**

An API (Application Programmable Interface) for a terminal defines a common interface for software application management. At the level of a ticketing terminal, several APIs can exist, from the management of the contactless reader to higher level ticketing applications

- **APPLET**

Application which may be loaded into a Secure Element (usually associated with the Java environment).

- **Card-based systems**

Card-based systems in public transport use smart cards, or NFC enabled mobile phones, to store travel value, travel products (for example a monthly pass), discount rights (for example for students or the elderly), and tickets. Tickets can be pre-paid or Pay-As-You-Go (check-in check-out, or check-in only). Tickets are stored so they can be inspected. In card-based systems the fare calculation and applicative software are located in the different field equipment (validators, sale machines, inspection readers, ...), i.e. the front office of the ticketing system.

- **CEN**

CEN (European Committee for Standardisation) is an association of the national standards bodies from 34 European countries. CEN is a standards body recognised by the European Union as being responsible for the development and definition of standards at European level in collaboration with ISO.

- **Chip**

An electronic chip or component, designed and manufactured by specialised silicon manufacturers. The chip is integrated into the boards of which it is a part and is the intelligent element that stores and processes the data.

- **CNA**

Calypso Networks Association.

- **Contactless card**

A contactless medium, e.g. a smart card, a java card, a smartphone, USB stick with a contactless interface, or any other contactless medium available to customers.

- **Data model**

The purpose of the data model is to describe how the information is coded and stored in the card and its management rules. The data model constitutes a common language that allows interoperability between mobility actors sharing the same client medium.

- **DES**

Ciphering algorithm producing 8 bytes of data from 8 input bytes, using a 7 bytes key (as defined in ANSI X3.92-1981). Also called "Simple DES", now obsolete.

- **DESX**

Ciphering algorithm producing 8 bytes of data from 8 input bytes, using a 15 bytes key (as defined in How to Protect DES Against Exhaustive Key Search by Kilian & Rogaway), now deprecated.

- **Eclipse**

The Eclipse Foundation is a non-profit organisation overseeing the development of the Eclipse open source IDE and related projects, and helps cultivate an open source community and an ecosystem of complementary products and services around Eclipse.

- **ECP**

Apple VAS Enhanced Contactless Polling (ECP), is an Apple proprietary extension of EMV level 1 and ISO/IEC 14443.

- **EMVCo**

EMVCo is a global technical body that facilitates the interoperability and acceptance of secure payment transactions worldwide by managing and evolving EMV specifications and EMV specifications and associated testing processes. EMVCo is collectively owned by American Express, Discover, JCB, Mastercard, UnionPay and Visa.

- **HCE**

Host Card Emulation. By the end of 2013, Google released Android version 4.4, called “KitKat”, introducing several capabilities for Android applications, among which the Host Card Emulation API (or “HCE”), dedicated to ease and foster usage of NFC phones as “contactless cards”.

- **HOPLINK**

Hoplink is the interoperable ticketing application developed by CNA. Some data and file/ field names may use the Triangle 2 acronym, the former name of Hoplink.

- **Interoperability**

Interoperability is the ability of a system or product to work with other systems or products without requiring additional actions by the traveller.

- **ISO/IEC**

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO and IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

- **NFC**

NFC (Near Field Communication) is a wireless communication technology whose main advantage is, in this case, its short range (up to 10 cm).

- **Open Source Software**

Open Source software is software whose source code is freely accessible, usable and modifiable, distributed under a licence approved by the Open Source Initiative and which guarantees compliance with its rules.

- **PKI**

Public Key Infrastructure: system ensuring information security based on asymmetric cryptography, which allows protecting data by sharing only public keys.

- **SE**

Secure Element: secure microprocessor able to store and operate software, especially ISO/IEC 7816-4 applications.

- **Security Access Module (SAM)**

The security module authenticates the card, the terminal and all data exchanged between them. It is normally a smart card, but as services are nowadays often provided by remote servers, it can also be a hardware component integrated into a server (HSM).

- **TDES**

Symmetric cryptographic algorithm is made of three successive DES operations (as defined in ISO/IEC 18033-3), also called "Triple-DES", or "3DES".

Calypso
Networks Association

🌐 www.calypsonet.org

✉ contact@calypsonet.org

in @calypso-networks-association

▶ @calypso-networks-association

Subscribe to the CNA newsletter via the contact form

Headquarters:
Calypso Networks Association,
Rue Royale 76,
1000 Bruxelles, Belgium

Paris:
Calypso Networks Association,
2 rue de la Roquette, Escalier Avril,
75011 Paris France