Calypso
Networks Association

keyple

Test Kit

USER MANUAL

The information contained in this document is not public.

The authors of this Specification make no other representation or warranty regarding whether any particular physical implementation of any part of this specification does or does not violate, infringe, or otherwise use other patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property of third parties, and thus any person who implements any part of this Specification should consult an intellectual property attorney before any such implementation.

Any party seeking to implement this Specification is solely responsible for determining whether their activities require another license to any technology. Calypso Networks Association shall not be liable for infringements of any third party's intellectual property right.

Author & Editor

Calypso
Networks Association

Links and Contacts

Calypso related Internet sites:

Calypso Networks Association	https://www.calypsonet.org
Calypso Technical Support	https://www.calypsostandard.net

Calypso related email contacts:

Calypso Networks Association	contact@calypsonet.org
Calypso Technical Support	support@calypsonet.org

Revision List

Version	Date	Modifications
2	15/12/2021	Added 3.2 (Extended) profiles for Calypso Prime. Updated other profiles. Modified the web site address of CNA (now calypsonet.org)..
1.7	09-02-2021	Modified the link to the website that lists the Calypso certified product: the information is now on the CNA-Paycert website.
1.6	03-12-2020	Update the test kit content Update the list of Card provider
1.5	10-1-2020	Updated the test kit content and the list of POs Added reference to Calypso Prime rev3.3 Updated the list of card providers Improved the Figure 1: KEYPLE Architecture Introduced the brands Calypso Prime and Calypso Light Changed the references of documents Modified the link of the Keyple project (now keyple.org)
1.4	25-7-2019	Updated the Application Type for Keyple test profile 1 – Application 1
1.3	2-7-2019	Added a Java card. Modified some logos.
1.2	11-3-2019	Changed Test Kit content in §3.1 and sponsors list in §3.4 after the addition of 2 cards in the Test Kit.
1.1	21-2-2019	Editorial improvements
1.7	10-04-2020	Update of the CNA logo Update of the Calypso logo Added a Foreword example Added example of annex with the following sections: • Calypso References • Normatives References • Links and Contacts • Glossary and Acronyms Minor improvements
1.6	09-04-2020	Modified the logo of the Author, Calypso replaced by CNA
1.5	03-03-2020	Added an example of a table for referenced documents Added Warning, Example and remarks paragraph Enhanced recommendation/requirement template
1.4	08-04-2019	Used properties for: date, reference and version Added recommendation/requirement template Added “glossary and acronyms” chapter
1.3	28-03-2019	Removed the reference to Innovatron
1.2	13-09-2017	Corrected some errors on margins Decreased bottom margin.
1.1	12-09-2017	Modified colors Slightly expanded margins

Table of Contents

1 CONTEXT 5

1.1 CALYPSO AND CNA 5

1.2 CALYPSO SPECIFICATION AND CERTIFICATION POLICY 5

1.3 ECLIPSE KEYPLE, AN OPEN-SOURCE SDK 6

1.4 REFERENCES 6

2 TEST KIT FOR KEYPLE 7

2.1 OBJECTIVE OF THE DOCUMENT 7

2.2 KEYPLE ARCHITECTURE 7

3 TEST KIT CONTENT 8

3.1 WHAT IS INSIDE? 8

3.2 SAM 9

3.3 CARDS 9

3.4 CARD MANUFACTURERS 10

4 FILE STRUCTURES 11

4.1 CALYPSO PRIME REGULAR MODE 11

4.2 CALYPSO PRIME EXTENDED MODE - 18

4.3 CALYPSO LIGHT APPLICATION 25

5 GLOSSARY AND ACRONYMS 27

1 CONTEXT

1.1 Calypso and CNA

Calypso is the open standard for secure, fast and flexible public transport ticketing systems deployed all over the world.

Initially fostered by a worldwide group of transport operators, the development program which ensued succeeded in creating the smart card contactless standard adapted to many applications, including public transportation and city services uses. The standard is accessible freely to all authorities, operators and industrial companies, to ensure:

- The birth of this new standard suited to the public transport needs.
- A good products compatibility.
- A fair market concurrence.

Following the large success of the Calypso standard and its widespread use in many parts of the world, **Calypso Networks Association** (CNA) was created in 2003. This non-profit association, based in Belgium, gathers all ticketing actors to let them manage the evolution of the standard.

The main objectives of CNA are:

- To define and direct Calypso reference specifications, while contributing to the international standardization process.
- To deliver services which facilitate interoperability and Calypso implementation.
- To provide support to its members and to facilitate and harmonize the shared members' needs and experiences.
- To implement a certification policy and deliver a label issued by independent organizations to guarantee the compatibility of all Calypso products.

More information may be found on the CNA web site: http://calypsonet.org

1.2 Calypso specification and certification policy

The main Calypso specification is the *Calypso Revision 3 Specification – Portable Object Application* **[PrimeSpec]** that describes the behaviour of a Calypso medium to access public transport and other services. This Portable Object (PO) may be a contactless smartcard, an NFC mobile phone with a Java Applet, a Java Card, a wristwatch with an embedded contactless component…

CNA also published the specification of a Calypso Light Application, *Calypso Light Application for Portable Objects* **[LightSpec]** : this specification aims at enlarging the target of the customers using a Calypso card by offering a middle-end portable object at an intermediary cost, based on Calypso Light, for the users of books of tickets or touristic pass.

The CNA certification policy has led to the award of the Calypso label to more than 20 products coming from several manufacturers.

See the list of Calypso PO on the Calypso-Paycert certification website:

https://www.cna-paycert-certification.eu/cpoc/

1.3 ECLIPSE KEYPLE, an open-source SDK

Terminal applications operating ticketing data contained in the Calypso PO, have to be implemented in many types of devices coming from various providers and with different architectures such as vending machines, control terminals, validators…

For a service provider, to actually manage and control the life cycle of its ticketing system (maintenance, fare policy, new media…) the only way is to have the full property and control of the ticketing software and APIs embedded in its terminals, which is complicated by the multiplicity of environments.

CNA developed and maintains ECLIPSE KEYPLE, the open source SDK for contactless ticketing.

KEYPLE speeds up integration and application development by allowing multimodal transport, public transport, events and activity services to quickly connect with a common ticketing system.

As an open-source technology, KEYPLE offers the consistency of building to the Calypso ticketing standard, but does not lock its user into a specific ticketing system. KEYPLE turns complex ticketing, transport, and event access systems into a simple integration that can be managed by terminal readers and gates that use smart cards and mobile apps to gain entry and exit. Plugins are being created, or can be created by other developers, to ensure ticket processing works with all hardware and is compatible with all transport and event management architectures. Calypso's high standards of security, data privacy and interoperability are, nonetheless, always maintained...

Access to open-source ECLIPSE KEYPLE: https://keyple.org

1.4 References

Reference	*Document Title*	*Version*
[PrimeSpec]	*060708-CalypsoAppli* Calypso Revision 3 Specification – Portable Object Application	3.3
[SAMTestF5]	*110619SDI - Test SAM Description - F5 Configuration* Calypso SAM-TEST-F5 User Manual	6.0
[LightSpec]	*170101-CalypsoLightApplication* Calypso Light Application for Portable Objects "CLAP"	1.1
[FSRegistry]	*060709-CalypsoFiles* File Structure Registry	1.9
[HoplinkApp]	*101101-HoplinkApplication* Hoplink Specifications	2.9

Table 1: **References**

The version numbers identified in the references below are valid at the time of release of this document. The latest version available from CNA should apply.

All these referenced documents are available on the Calypso Technical Support web site (http://www.calypsostandard.net). Most of them required a nominative registration on the site

2 TEST KIT FOR KEYPLE

2.1 Objective of the document

The Test Kit for KEYPLE aims at helping terminal application developers to fully experience KEYPLE with a set of Calypso SAM and Calypso certified portable objects from several manufacturers in various configurations.

This document is the manual user of the KEYPLE Test Kit: it describes the Kit's content and provides all the information necessary for its use. While it does not include the elements contained in the Calypso specifications, it does provide references and links to useful documents.

Even if KEYPLE may hide a lot of complexity of Calypso cryptography, the use of these cards and their file structure requires a minimum understanding of Calypso technology.

2.2 KEYPLE architecture

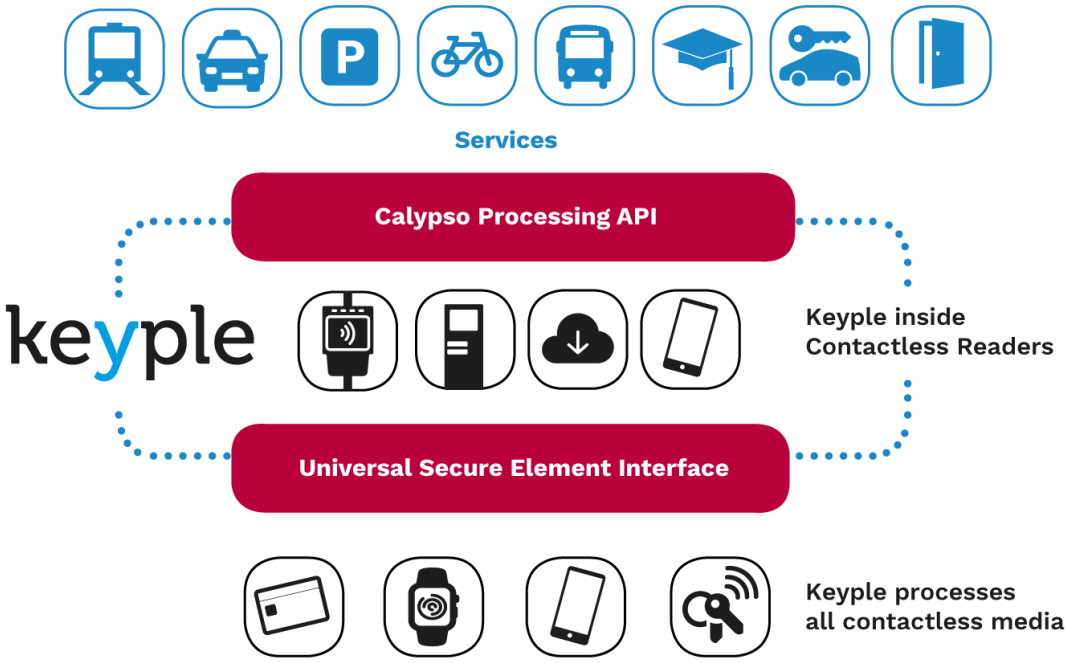

Figure 1: **KEYPLE Architecture**

KEYPLE is an open-source library available in Java and soon in C++. It is compatible with all terminal architectures: mobile, embedded or server and interoperable with any card reader solution: standard or proprietary, local or remote.

Its goal is to allow a simple development of applications communicating with Calypso portable objects, without having to master and develop the entire specific Calypso layer beforehand.

KEYPLE is an abstraction layer that implements two main functions:

- A generic interface to exchange data with secure contactless elements (such as smart card, SIM card, embedded secure element...) via all types of contactless readers (local, remote, standard, proprietary...)
- A library implementing all Calypso processing between a secure contactless element and a secure module in a terminal.

KEYPLE also allows, via its generic interface, to process other contactless card solutions than Calypso (Contactless Memory Tickets, Mifare, …) to allow an easy cohabitation of different media on the same system, especially to manage migrations in an optimal way.

KEYPLE thus allows all types of actors (integrators, start-ups, operators) to have simple and cost-effective access to the entire Calypso technology.

3 TEST KIT CONTENT

3.1 What is inside?

The test kit contains 2 SAMs and 10 cards representative of the Calypso offer among those presented in the table below.

Type	*Product Name*	*Configuration*	*Interface*	*Provider*
SAM	SAM C1	TEST-F5 version 6	ISO7816 T=0	CNA
Multi application Java Card	Cosmo Fly v6.0 + CNA Calypso Applet version 1.3	Prime Regular	ISO14443 B	Idemia
Multi-application smart card	TanGO+ Flash	Prime Regular	ISO14443 B	Paragon ID
	Celego G1 v1	Prime Regular	Dual ISO14443B	Thales
	CD21 – rev3.2	Prime Regular	Dual ISO14443B	STMicroelectronics
	TimeCOS DI Calypso v3.1	Prime Regular	Dual ISO14443B	Watchdata
	SOMA Atlas v2	Prime Extended	ISO14443 B	HID Global
	SOMA Atlas v2	Prime Extended	ISO14443 A	HID Global
	SOMA Atlas CLAP v1	Light Reference	ISO14443 B	HID Global
	SOMA Atlas CLAP v1	Light Classic	ISO14443 B	HID Global

Mono-application smart card	ELIPSE Calypso v1	Light Reference	ISO14443 A	SELP
	ELIPSE Calypso v1	Light Classic	ISO14443 A	SELP
	Calypso G-CLAP1	Light Reference	ISO14443 B	Thales
	Calypso G-CLAP1	Light Classic	ISO14443 B	Thales
	TimeCOS CLAP	Light Reference	ISO14443 B	Watchdata
	TimeCOS CLAP	Light Classic	ISO14443 B	Watchdata
	Tango CLAP v1	Light Reference	ISO14443 B	Paragon ID
	Tango CLAP v1	Light Classic	ISO14443 B	Paragon ID

Table 2: **Test Kit Content**

3.2 SAM

The SAM is a secure module of a Calypso system that contains the master keys of the service provider. It is a smart card permanently connected with the equipment interacting with the portable objects (present inside the equipment or remotely connected to it).

CNA provides 2 SAMs in a test configuration: the **[SAMTestF5]** document describes the contents and the Calypso generic test security module configuration, called “SAM-TEST-F5 v6”; they include the Hoplink test keys.

KEYPLE manages the cryptographic exchanges between the card and the SAM; it is then not necessary to have a detailed understanding of the SAM specification.

3.3 Cards

The generic Calypso Card Application is described in the document **[PrimeSpec]**.

It specifies an exact set of commands, forbidding any proprietary options. This allows for a better compatibility between products and allows the terminal to abstract its operations from specific products.

There are three options of the **Calypso Prime** revision 3 cards:

- **Regular** mode: previously known as rev 3.1, this mode includes the minimum functions of Calypso Prime with TDES and DESX cryptographic algorithms.
- **Extended** mode: previously known as rev 3.2, allows to enhance the security using longer signatures and optionally AES keys and allows optional encryption of the data and authentications during the Calypso Secure Session. Extended mode is additional options to Regular mode
- **PKI** mode: previously known as rev3.3, adds the functionnality of authentication of the Calypso card application, and possibly of its data, using only a public key (no SAM necessary for this authentication). PKI mode includes Extended mode. Calypso Prime PKI mode are not yet available in the test kit.

Multi-application cards provided in the test kit are either Regular or Extended. PKI mode cards are expected soon.

To extend the success of the Calypso standard, CNA has decided to issue the specifications of the **Calypso Light** application – see document **[LightSpec]**.

Without aiming at replacing every low cost contactless tickets, CNA considers that, due to the evolution of the market for microprocessor components, there is an actual opportunity to enlarge the target of the customers using a Calypso card by offering a middle-end portable object at an intermediary cost, based on Calypso Light, for the users of books of tickets or touristic pass.

Such a medium will also give small networks the opportunity to move towards teleticketing at a lower cost.

Mono-application smart cards provided in the test kit are products based on Calypso Light. The document **[LightSpec]** identifies two possible files structure for a Calypso Light card which are available in the test kit.

- The **Reference** file structure allows management of data according to a subset of the Hoplink specification (see **[HoplinkApp]**).
- The **Classic** file structure aims at limiting differences with systems used to files structures of Calypso Revision 1.

The contactless ISO protocol, ISO 14443 is available in two types, A & B. They are both available in the test kit. Some samples have a dual interface, i.e. contact and contactless.

3.4 Card manufacturers

All cards included in the Test kit are contributions from the following partners.

The Java Card uses the Calypso CNA applet version 1.3 which complies with the Calypso Prime rev3.1 specification.

4 FILE STRUCTURES

4.1 Calypso Prime Regular Mode

A Calypso card may contain more than one Calypso application: the Calypso Prime cards of the test kit contains up to 5 Calypso applications.

The Calypso Prime Specification does not mandate a specific file structure, it however defines in the Calypso File Structure Registry **[FSRegistry]** several file structures that may be used directly, or that may be customized. It is also possible to define a completely new file structure.

Each Calypso application owner (transit networks, regional authorities, etc.) may choose the best file structure for its needs among the registry or may define a new file structure. The file structure, as well as the model of the data stored in a Calypso application, is an essential part of the interoperability of a Calypso system and should be specified by the service providers within the area of interoperability.

The file structure of a Calypso application is defined before activation of the Calypso application (during initialization of the card or of the Calypso application).

Multi-application cards of the test kit may support up to 5 Calypso applications, if allowed by the platform; at least application 1; 2 & 3 must be present, 4 and 5 are optional.

For the Calypso Prime Regular Profile, referenced as **Test Profile 1**:

- Application 1 (AID 304554502E494341h): Calypso stored value application with reference structure 20h (TDES keyset TEST F5v6 MK_SVx_T KVC 79h)
- Application 2 (AID 315449432E49434131h): Calypso ticketing application with reference structure 02h (TDES keyset TEST F5v6 MK_RTx_T KVC 79h): Revision 2 Minimum with MF files.
- Application 3 (AID A000000291A00000019102h): Calypso ticketing application with reference structure 0Ch or 0Dh (TDES keyset TEST F5v6 MK_RTx_T5 KVC 0Ch): Hoplink application with 8 or 16 contracts, allowing EF sharing with application 4
- Application 4 (AID 315449432E49434132h): Calypso ticketing application with reference structure 13h (keyset TEST F5v6 MK_RTx_T2 KVC 78h): Intercode 2.2 with Hoplink access.
- Application 5 (AID D2760000850101h): Calypso ticketing application with proprietary structure F4h (keyset TEST F5v6 MK_MPPx_T KVC 79h): NFC Forum NDEF Tag Type 4.

4.1.1 Calypso Prime Regular Profile – Application 1

This is the Calypso **Stored Value** application.

The management of a Calypso Stored Value application is optional for a Calypso Prime card.

The Calypso stored value application manages a stored value, with a specific security access.

When available, the stored value commands may be used directly from another Calypso application, without an explicit selection of the stored value application. It may be used within a secure session, or independently.

The stored value may range from -8,388,608 to 8,388,607. If expressed in euro cents, the value may therefore range from approximately -83,886 euros to +83,886 euros.

The possible stored value transactions are:

- Loading the stored value.
- Debiting the stored value.
- "Undebiting" the stored value (for a partial or total refund of the last debit).

Every transaction increases the Stored Value Transaction Number (SV TNum), which allows a maximum of 65,535 operations. The last stored value transactions are recorded in the stored value log files (Load Log and Purchase Log).

More details about the Store Value commands are available in **[PrimeSpec]**. The file structure is known in **[FSRegistry]** under the reference **20h.**

Calypso Prime Regular Profile - Application 1

Type:	Calypso Stored Value		AID:	**304554502E494341**h		ASCII: "0ETP.ICA"
Startup:	Session Modifications:	highest referenced value supported by the product				
	Application Type:	coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}				
	Application SubType:	20h	referenced Calypso file structure '20h': **Stored Value**			

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	01h	79h	90h	MK_SV1_T			
#2 Load	07h	79h	90h	MK_SV2_T	shared Calypso PIN:	30303030h	"0000"
#3 Debit	10h	79h	90h	MK_SV3_T			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	1000h	-	-	-	Session 1	Session 3	-	-	-
Load Log	Cyclic	1014h	14h	1	29	Always	Never	Never	Never	-
Purchase Log	Cyclic	1015h	15h	3	29	Always	Never	Never	Never	-

Table 3 **: Calypso Prime Regular Profile – Application 1 File Structure**

4.1.2 Calypso Prime Regular Profile – Application 2

This is the Calypso **Rev2 Minimum with MF files** application. This structure emulates a common ticketing Calypso application present on the public transport networks that moved early to contactless ticketing and is referenced as number **02h** in **[FSRegistry]**.

Calypso Prime Regular Profile - Application 2

Type: Calypso Ticketing — AID: **315449432E49434131**h — ASCII: "1TIC.ICA1"

Startup: Session Modifications: highest referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: 02h referenced Calypso file structure '02h': **Revision 2 Minimum with MF files**

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	79h	90h	MK_RT1_T			
#2 Load	27h	79h	90h	MK_RT2_T	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	79h	90h	MK_RT3_T			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2000h	-	-	-	Session 1	Session 3	-	-	-
ICC	Linear	0002h	02h	1	29	Always	Never	Session 1	-	-
ID	Linear	0003h	03h	1	29	PIN	Session 2	Never	-	-
Environment	Linear	2001h	07h	1	29	Always	Session 1	Never	-	-
Events Log	Cyclic	2010h	08h	3	29	Always	Session 3	Session 3	Session 3	-
Special Events	Linear	2040h	1Dh	1	29	Always	Session 3	Never	-	-
Contract List	Linear	2050h	1Eh	1	29	Always	Session 3	Never	-	-
Contracts	Linear	2020h	09h	4	29	Always	Session 2	Session 3	-	-
Counters	Counters	2069h	19h	1	29	Always	Session 2	Session 3	Session 2	-

Initial data:

File	Rec. Num	Size	Pre-personalized data
Contracts (2020h / 09h)	1	29	00000**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**h
	2		
	3		
	4		

Table 4 **: Calypso Prime Regular Profile – Application 2 File Structure**

4.1.3 Calypso Prime Regular Profile – Application 3

This is the Calypso **Hoplink** application

Hoplink is a multimodal, interoperable and multi-e-ticketing application in a Calypso Portable Object, compliant with standards (Calypso, EN1545, etc.)

Hoplink is the result of a European Project launched by Calypso Networks Associations (CNA) and supported by the European Union. It offers a solution for transregional and cross-border interoperability.

Hoplink is a dedicated application that coexists with the usual local application and may cooperate with it.

The application 3 may be present with 2 different file structures, according to the memory size of the Calypso card.

The nominal Hoplink file structure requires a large memory and contains a Picture ID file to store the scan of the passport photo of the card holder and is referenced as **0Dh** in **[FSRegistry]**.

The alternative configuration is used in PO with limited memory and is known as **0Ch** in **[FSRegistry]**.

4.1.3.1 *Hoplink Nominal Configuration*

Calypso Prime Regular Profile - Application 3 'Nominal configuration'

Type: Calypso Ticketing AID: **A000000291A00000019102**h

Startup: Session Modifications: highest Calypso referenced value supported by the product

Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}

Application SubType: 0Dh referenced Calypso file structure '0Dh': **Hoplink** configuration '0Dh' **with** picture files

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	0Ch	90h	MK_RT1_T5			
#2 Load	27h	0Ch	90h	MK_RT2_T5	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	0Ch	90h	MK_RT3_T5			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2100h	-	-	-	Session 1	Session 3	-	-	-
T2 Environment	Linear	2111h	14h	1	32	Always	Session 1	Never	-	2111h
T2 Contracts	Linear	2112h	15h	16	64	Always	Session 2	Session 3		2112h
T2 Usage	Linear	2113h	1Ah	16	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2114h	1Bh	1	48	Always	Session 2	Always	Session 2	2114h
T2 Counters B	Counters	2115h	1Ch	1	48	Always	Session 2	Session 3	Session 2	2115h
T2 Names	Linear	2116h	18h	16	64	Always	Session 3	Never	-	2116h
T2 Picture Data	Binary	2117h	12h	4096		Always	Session 2	Never	-	2117h
T2 Picture Attributes	Linear	2118h	13h	1	64	Always	Session 2	Never	-	2118h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 3 has **external** EF sharing: the application 3 **grants** limited access of its files to the application 4.

The Hoplink application could share its EF to other ticketing application with **restricted** access: the access indicated in red are defined differently

Initial data:

File	Rec. Num	Size	Pre-personalized data
T2 Contracts (2112h / 15h)	1	64	
	2		
	3		
	4		
	5		
(the eleventh byte at FFh)	6		
	7		00000000000000000000**FF**0000000000
	8		00000000000000000000000000000000
	9		00000000000000000000000000000000
	10		00000000000000000000000000000000h
	11		
	12		
	13		
	14		
	15		
	16		

Table 5 **: Calypso Prime Regular profile – Application 3 nominal configuration File Structure**

4.1.3.2 *Hoplink Alternative Configuration*

Calypso Prime Regular Profile - Application 3 'Alternative configuration' (limited memory)

Type: Calypso Ticketing AID: **A000000291A00000019102**h

Startup: Session Modifications: highest Calypso referenced value supported by the product

Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}

Application SubType: 0Ch referenced Calypso file structure '0Ch': **Hoplink** configuration '0Ch' **without** picture files

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	21h	0Ch	90h	MK_RT1_T5	
#2 Load	27h	0Ch	90h	MK_RT2_T5	shared Calypso PIN: 30303030h "0000"
#3 Debit	30h	0Ch	90h	MK_RT3_T5	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2100h	-	-	-	Session 1	Session 3	-	-	-
T2 Environment	Linear	2111h	14h	1	32	Always	Session 1	Never	-	2111h
T2 Contracts	Linear	2112h	15h	8	64	Always	Session 2	Session 3		2112h
T2 Usage	Linear	2113h	1Ah	8	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2114h	1Bh	1	24	Always	Session 2	Always	Session 2	2114h
T2 Counters B	Counters	2115h	1Ch	1	24	Always	Session 2	Session 3	Session 2	2115h
T2 Names	Linear	2116h	18h	8	64	Always	Session 3	Never	-	2116h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 3 has **external** EF sharing: the application 3 **grants** limited access of its files to the application 4.

The Hoplink application could share its EF to other ticketing application with **restricted** access: the access indicated in red are defined differently in the other ticketing application.

Initial data:

File	Rec. Num	Size	Pre-personalized data
T2 Contracts (2112h / 15h)	1	64	
	2		
	3		00000000000000000000**FF**0000000000
	4		00000000000000000000000000000000
	5		00000000000000000000000000000000
(the eleventh byte at FFh)	6		00000000000000000000000000000000h
	7		
	8		

Table 6 **: Calypso Prime Regular profile – Application 3 alternative configuration File Structure**

4.1.4 Calypso Prime Regular Profile – Application 4

The Calypso **Intercode 2.2** application which refers to the **13h** file structure registered in **[FSRegistry]**. This Calypso application is the most common for ticketing on Calypso French networks. It allows shared files with Hoplink (see §2.3.4 of **[PrimeSpecs]**) for more on Shared Files in Calypso.

Calypso Prime Regular Profile - Application 4

Type: Calypso Ticketing — AID: **315449432E49434132**h — ASCII: "1TIC.ICA2"

Startup: Session Modifications: highest Calypso referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: 13h — referenced Calypso file structure '13h': **intercode 2.2** with shared Hoplink files

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	78h	90h	MK_RT1_T2			
#2 Load	27h	78h	90h	MK_RT2_T2	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	78h	90h	MK_RT3_T2			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2200h	-	-	-	Session 1	Session 3	-	-	-
Environment & Holder	Linear	2201h	01h	1	80	Always	Session 1	Never	-	-
Identification (ID)	Linear	2202h	02h	1	48	PIN	Session 2	Never	-	-
Contracts	Linear	2203h	03h	8	64	Always	Session 2	Session 3	-	-
Profiles	Linear	2204h	04h	8	56	Always	Session 2	Session 3	-	-
Counters	Counters	2205h	05h	1	48	Always	Session 2	Session 3	Session 2	-
Free Counters	Counters	2206h	06h	1	24	Always	Session 2	Always	Session 2	-
Lists	Linear	2207h	07h	1	80	Always	Session 3	Never	-	-
Global Events	Linear	2208h	08h	3	48	Always	Session 3	Never	-	-
Contract Events	Linear	2209h	09h	3	48	Always	Session 3	Never	-	-
Cyclic Events	Cyclic	220Ah	0Ah	3	48	Always	Session 3	Session 3	Session 3	-
Free Data	Linear	220Bh	0Bh	1	64	Always	Always	Always	-	-
T2 Environment	Linear	2211h	14h	1	32	Always	Never	Never	-	2111h
T2 Contracts	Linear	2212h	15h	16	64	Always	Never	Session 3		2112h
T2 Usage	Linear	2213h	1Ah	16	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2214h	1Bh	1	48	Always	Never	Always	Never	2114h
T2 Counters B	Counters	2215h	1Ch	1	48	Always	Never	Session 3	Never	2115h
T2 Names	Linear	2216h	18h	16	64	Always	Session 3	Never	-	2116h
T2 Picture Data	Binary	2217h	12h	4096		Always	Never	Never	-	2117h
T2 Picture Attributes	Linear	2218h	13h	1	64	Always	Never	Never	-	2118h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 4 has **external** EF sharing: the application 4 **has** limited access on the files of the application 3.

The ticketing application has a **restricted** access on the files of the Hoplink application: the access indicated in red are defined differently in the Hoplink application.

Table 7 **: Calypso Prime Regular profile – Application 4 File Structure**

4.1.5 Calypso Prime Regular Profile – Application 5

This is the Calypso **NFC NDEF Tag Type 4** application which refers to the **F4h** file structure registered in **[FSRegistry]**. This is a proprietary ticketing file structure.

It's a Calypso ticketing instance personalized with a profile compliant to the "NFC Forum Tag Type 4" specification: a dedicated AID and file structure able to host NFC Data Exchange Format (NDEF) that supports standard ISO read command in free access. The update of the data is managed through a Calypso secure session.

Calypso Prime Regular Profile - Application 5

Type: Calypso Ticketing — AID: **D2760000850101**h

Startup:
- Session Modifications: highest Calypso referenced value supported by the product
- Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **not** supported (Rev3.2)} / {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
- Application SubType: F4h — proprietary file structure 'F4h': **NFC NDEF Tag Type 4**

TDES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	41h	79h	90h	MK_MPP1_T	
#2 Load	47h	79h	90h	MK_MPP2_T	shared Calypso PIN: 30303030h "0000"
#3 Debit	50h	79h	90h	MK_MPP3_T	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	E100h	-	-	-	Session 1	Session 3	-	-	-
Capability File	Binary	E103h	01h	15		Always	Session 1	Never	-	-
NDEF Data File	Binary	E104h	02h	2048*		Always	Always	Always	-	-

* (The size of the EF 'NDEF Data File' is a multiple of 128)

Table 8 **: Calypso Prime Regular profile – Application 5 File Structure**

4.2 Calypso Prime Extended Mode -

A Calypso card may contain more than one Calypso application: the Calypso Prime cards of the test kit contains up to 5 Calypso applications.

The Calypso Prime Specification does not mandate a specific file structure, it however defines in the Calypso File Structure Registry **[FSRegistry]** several file structures that may be used directly, or that may be customized. It is also possible to define a completely new file structure.

Each Calypso application owner (transit networks, regional authorities, etc.) may choose the best file structure for its needs among the registry or may define a new file structure. The file structure, as well as the model of the data stored in a Calypso application, is an essential part of the interoperability of a Calypso system and should be specified by the service providers within the area of interoperability.

The file structure of a Calypso application is defined before activation of the Calypso application (during initialization of the card or of the Calypso application).

Multi-application cards of the test kit may support up to 5 Calypso applications, if allowed by the platform; at least application 1; 2 & 3 must be present, 4 and 5 are optional.

For the Calypso Prime Extended Profile:

- Application 1 (AID 304554502E494341h): Calypso stored value application with reference structure 20h (AES keyset TEST F5v6 MK_SVx_A1 KVC 74h)
- Application 2 (AID 315449432E49434131h): Calypso ticketing application with reference structure 05h (AES keyset TEST F5v6 MK_RTx_A1 KVC 74h): CD Light/GTML Compatibility
- Application 3 (AID A000000291A00000019102h): Calypso ticketing application with reference structure 0Ch or 0Dh (AES keyset TEST F5v6 MK_RTx_A3 KVC 09h): Hoplink application with 8 or 16 contracts, allowing EF sharing with application 4
- Application 4 (AID 315449432E49434132h): Calypso ticketing application with reference structure F3h (AES keyset TEST F5v6 MK_RTx_B1 KVC 75h): Intercode 2.2 with Hoplink access.
- Application 5 (AID D2760000850101h): Calypso ticketing application with proprietary structure F4h (AES keyset TEST F5v6 MK_RTx_B1 KVC 75h): NFC Forum NDEF Tag Type 4.

Extended mode and AES Keyset are supported by all applications.

Pin feature is supported and shared by all applications and Stored value is only supported by applications 1,2 and 4.

4.2.1 Calypso Prime Extended Profile – Application 1

This is the Calypso **Stored Value** application.

The management of a Calypso Stored Value application is optional for a Calypso Prime card.

The Calypso stored value application manages a stored value, with a specific security access.

When available, the stored value commands may be used directly from another Calypso application, without an explicit selection of the stored value application. It may be used within a secure session, or independently.

The stored value may range from -8,388,608 to 8,388,607. If expressed in euro cents, the value may therefore range from approximately -83,886 euros to +83,886 euros.

The possible stored value transactions are:

- Loading the stored value.
- Debiting the stored value.
- "Undebiting" the stored value (for a partial or total refund of the last debit).

Every transaction increases the Stored Value Transaction Number (SV TNum), which allows a maximum of 65,535 operations. The last stored value transactions are recorded in the stored value log files (Load Log and Purchase Log).

More details about the Store Value commands are available in **[PrimeSpec]**. The file structure is known in **[FSRegistry]** under the reference **20h.**

Calypso Prime Extended Profile - Application 1

Type: Calypso Stored Value — AID: **304554502E494341**h — ASCII: "0ETP.ICA"

Startup: Session Modifications: highest referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: 20h referenced Calypso file structure '20h': **Stored Value**

AES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	01h	74h	A0h	MK_SV1_A1	
#2 Load	07h	74h	A0h	MK_SV2_A1	shared Calypso PIN: 30303030h "0000"
#3 Debit	10h	74h	A0h	MK_SV3_A1	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	1000h	-	-	-	Session 1	Session 3	-	-	-
Load Log	Cyclic	1014h	14h	1	29	Always	Never	Never	Never	-
Purchase Log	Cyclic	1015h	15h	3	29	Always	Never	Never	Never	-

Table 9 **: Calypso Prime Extended Profile – Application 1 File Structure**

4.2.1 Calypso Prime Extended Profile – Application 2

This is the Calypso Revision 2 emulation with MF files application. This structure emulates a common ticketing Calypso application present on the public transport networks that moved early to contactless ticketing and is referenced as number **02h** in **[FSRegistry]**.

Calypso Prime Extended Profile - Application 2

Type: Calypso Ticketing — AID: **315449432E49434131**h — ASCII: "1TIC.ICA1"

Startup: Session Modifications: highest referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: 02h referenced Calypso file structure '02h': **Revision 2 Minimum with MF files**

AES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	21h	74h	A0h	MK_RT1_A1	
#2 Load	27h	74h	A0h	MK_RT2_A1	shared Calypso PIN: 30303030h "0000"
#3 Debit	30h	74h	A0h	MK_RT3_A1	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2000h	-	-	-	Session 1	Session 3	-	-	-
ICC	Linear	0002h	02h	1	29	Always	Never	Session 1	-	-
ID	Linear	0003h	03h	1	29	PIN	Session 2	Never	-	-
Environment	Linear	2001h	07h	1	29	Always	Session 1	Never	-	-
Events Log	Cyclic	2010h	08h	3	29	Always	Session 3	Session 3	Session 3	-
Special Events	Linear	2040h	1Dh	1	29	Always	Session 3	Never	-	-
Contract List	Linear	2050h	1Eh	1	29	Always	Session 3	Never	-	-
Contracts	Linear	2020h	09h	4	29	Always	Session 2	Session 3	-	-
Counters	Counters	2069h	19h	1	29	Always	Session 2	Session 3	Session 2	-

Initial data:

File	Rec. Num	Size	Pre-personalized data
Contracts (2020h / 09h)	1	29	00000**FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF**h
	2		
	3		
	4		

Table 10 **: Calypso Prime Extended Profile – Application 2 File Structure**

4.2.1 Calypso Prime Extended Profile – Application 3

This is the Calypso **Hoplink** application

Hoplink is a multimodal, interoperable and multi-e-ticketing application in a Calypso Portable Object, compliant with standards (Calypso, EN1545, etc.)

Hoplink is the result of a European Project launched by Calypso Networks Associations (CNA) and supported by the European Union. It offers a solution for transregional and cross-border interoperability.

Hoplink is a dedicated application that coexists with the usual local application and may cooperate with it.

The application 3 may be present with 2 different file structures, according to the memory size of the Calypso card.

The nominal Hoplink file structure requires a large memory and contains a Picture ID file to store the scan of the passport photo of the card holder and is referenced as **0Dh** in **[FSRegistry]**.

The alternative configuration is used in PO with limited memory and is known as **0Ch** in **[FSRegistry]**.

4.2.1.1 *Hoplink Nominal Configuration*

Calypso Prime Extended Profile - Application 3 'Nominal configuration'

Type: Calypso Ticketing AID: **A000000291A00000019102**h

Startup:
Session Modifications: highest Calypso referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)} / {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: 0Dh referenced Calypso file structure '0Dh': **Hoplink** configuration '0Dh' **with** picture files

AES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	09h	A0h	MK_RT1_A3			
#2 Load	27h	09h	A0h	MK_RT2_A3	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	09h	A0h	MK_RT3_A3			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2100h	-	-	-	Session 1	Session 3	-	-	-
T2 Environment	Linear	2111h	14h	1	32	Always	Session 1	Never	-	2111h
T2 Contracts	Linear	2112h	15h	16	64	Always	Session 2	Session 3		2112h
T2 Usage	Linear	2113h	1Ah	16	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2114h	1Bh	1	48	Always	Session 2	Always	Session 2	2114h
T2 Counters B	Counters	2115h	1Ch	1	48	Always	Session 2	Session 3	Session 2	2115h
T2 Names	Linear	2116h	18h	16	64	Always	Session 3	Never	-	2116h
T2 Picture Data	Binary	2117h	12h	4096		Always	Session 2	Never	-	2117h
T2 Picture Attributes	Linear	2118h	13h	1	64	Always	Session 2	Never	-	2118h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 3 has **external** EF sharing: the application 3 **grants** limited access of its files to the application 4.

The Hoplink application could share its EF to other ticketing application with **restricted** access: the access indicated in red are defined differently in the other ticketing application.

Initial data:

File	Rec. Num	Size	Pre-personalized data
T2 Contracts (2112h / 15h)	1	64	
	2		
	3		
	4		
	5		
(the eleventh byte at FFh)	6		
	7		00000000000000000000**FF**0000000000
	8		00000000000000000000000000000000
	9		00000000000000000000000000000000
	10		00000000000000000000000000000000h
	11		
	12		
	13		
	14		
	15		
	16		

Table 11 **: Calypso Prime Extended profile – Application 3 nominal configuration File Structure**

4.2.1.1 *Hoplink Alternative Configuration*

Calypso Prime Extended Profile - Application 3 'Alternative configuration' (limited memory)

Type: Calypso Ticketing AID: **A000000291A00000019102**h

Startup: Session Modifications: highest Calypso referenced value supported by the product

Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)} / {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}

Application SubType: 0Ch referenced Calypso file structure '0Ch': **Hoplink** configuration '0Ch' **without** picture files

AES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	09h	A0h	MK_RT1_A3			
#2 Load	27h	09h	A0h	MK_RT2_A3	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	09h	A0h	MK_RT3_A3			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2100h	-	-	-	Session 1	Session 3	-	-	-
T2 Environment	Linear	2111h	14h	1	32	Always	Session 1	Never	-	2111h
T2 Contracts	Linear	2112h	15h	8	64	Always	Session 2	Session 3		2112h
T2 Usage	Linear	2113h	1Ah	8	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2114h	1Bh	1	24	Always	Session 2	Always	Session 2	2114h
T2 Counters B	Counters	2115h	1Ch	1	24	Always	Session 2	Session 3	Session 2	2115h
T2 Names	Linear	2116h	18h	8	64	Always	Session 3	Never	-	2116h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 3 has **external** EF sharing: the application 3 **grants** limited access of its files to the application 4.

The Hoplink application could share its EF to other ticketing application with **restricted** access: the access indicated in red are defined differently in the other ticketing application.

Initial data:

File	Rec. Num	Size	Pre-personalized data
T2 Contracts (2112h / 15h)	1	64	
	2		
	3		00000000000000000000**FF**0000000000
	4		00000000000000000000000000000000
	5		00000000000000000000000000000000
(the eleventh byte at FFh)	6		00000000000000000000000000000000h
	7		
	8		

Table 12 **: Calypso Prime Extended profile – Application 3 alternative configuration File Structure**

4.2.1 Calypso Prime Extended Profile – Application 4

This structure is based on the Calypso **Intercode 2.2** application which refers to the **13h** file structure registered in **[FSRegistry]** the most common for ticketing on Calypso French networks. It also contains additional ID2, ID3 Secured Counters and Secured Events files, with Extended mode specific access rights.

It is a proprietary file structure **F3h**. It allows shared files with Hoplink (see §2.3.4 of **[PrimeSpecs]**) for more on Shared Files in Calypso.

Calypso Prime Extended Profile - Application 4

Type: Calypso Ticketing — AID: **315449432E49434132h** — ASCII: "1TIC.ICA2"

Based on file structure '13h' (intercode 2.2) **with** additional ID2, ID3, Secured Counters & Secured Events files, with Extended mode specific access rights

Startup:
- Session Modifications: highest Calypso referenced value supported by the product
- Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)} / {**with** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
- Application SubType: F3h — proprietary file structure 'F3h': **intercode 2.2** — **with** shared Hoplink files — **with** additional ID2, ID3, Secured Counters & Secured Events files

AES Calypso keyset:

	KIF	KVC	ALG	diversified from
#1 Issuer	21h	75h	B0h	MK_RT1_B1
#2 Load	27h	75h	B0h	MK_RT2_B1
#3 Debit	30h	75h	B0h	MK_RT3_B1

issued from the 'Calypso SAM-TEST-F5v6'

shared Calypso PIN: 30303030h "0000"

File structure:

						Group 0	Group 1	Group 2	Group 3	EF Sharing
File	Type	LID	SFI	Rec. Num.	Rec. Size	Read Rehabilitate	Update Invalidate	Write Decrease	Append Increase	Data Ref.
DF	DF	2200h	-	-	-	Session 1	Session 3	-	-	-
Environment & Holder	Linear	2201h	01h	1	80	Always	Session 1	Never	-	-
Identification (ID)	Linear	2202h	02h	1	48	PIN	Session 2	Never	-	-
Contracts	Linear	2203h	03h	8	64	Always	Session 2	Session 3	-	-
Profiles	Linear	2204h	04h	8	56	Always	Session 2	Session 3	-	-
Counters	Counters	2205h	05h	1	48	Always	Session 2	Session 3	Session 2	-
Free Counters	Counters	2206h	06h	1	24	Always	Session 2	Always	Session 2	-
Lists	Linear	2207h	07h	1	80	Always	Session 3	Never	-	-
Global Events	Linear	2208h	08h	3	48	Always	Session 3	Never	-	-
Contract Events	Linear	2209h	09h	3	48	Always	Session 3	Never	-	-
Cyclic Events	Cyclic	220Ah	0Ah	3	48	Always	Session 3	Session 3	Session 3	-
Free Data	Linear	220Bh	0Bh	1	64	Always	Always	Always	-	-
Identification (ID2)	Linear	220Ch	0Ch	1	48	confidential 3	confidential 1	Never	-	-
Identification (ID3)	Linear	220Dh	0Dh	1	48	PIN & confidential 3	confidential 2	Never	-	-
Secured Counters	Counters	220Eh	0Eh	1	24	confidential 3	confidential 2	confidential 3	confidential 2	-
Secured Events	Cyclic	220Fh	0Fh	3	48	confidential 3	confidential 3	confidential 3	confidential 3	-
T2 Environment	Linear	2211h	14h	1	32	Always	Never	Never	-	2111h
T2 Contracts	Linear	2212h	15h	16	64	Always	Never	Session 3		2112h
T2 Usage	Linear	2213h	1Ah	16	48	Always	Always	Never	-	2113h
T2 Counters A	Counters	2214h	1Bh	1	48	Always	Never	Always	Never	2114h
T2 Counters B	Counters	2215h	1Ch	1	48	Always	Never	Session 3	Never	2115h
T2 Names	Linear	2216h	18h	16	64	Always	Session 3	Never	-	2116h
T2 Picture Data	Binary	2217h	12h	4096		Always	Never	Never	-	2117h
T2 Picture Attributes	Linear	2218h	13h	1	64	Always	Never	Never	-	2118h

Data sharing: The two bytes data references for sharing are provided as example (different EF sharing the same memory must have identical DataRef values). The application 4 has **external** EF sharing: the application 4 **has** limited access on the files of the application 3.

The ticketing application has a **restricted** access on the files of the Hoplink application: the access indicated in red are defined differently in the Hoplink application.

Table 13 **: Calypso Prime Extended profile – Application 4 File Structure**

4.2.1 Calypso Prime Extended Profile – Application 5

This is the Calypso **NFC NDEF Tag Type 4** application which refers to the **F4h** file structure registered in **[FSRegistry]**. This is a proprietary ticketing file structure.

It's a Calypso ticketing instance personalized with a profile compliant to the "NFC Forum Tag Type 4" specification: a dedicated AID and file structure able to host NFC Data Exchange Format (NDEF) that supports standard ISO read command in free access. The update of the data is managed through a Calypso secure session.

Calypso Prime Extended Profile - Application 5

Type: Calypso Ticketing AID: **D2760000850101**h

Startup: Session Modifications: highest Calypso referenced value supported by the product
Application Type: coding {PKI mode **not** supported (Rev3.3)} / {Extended mode **supported** (Rev3.2)}
/ {**without** Calypso stored value} / {**with** Calypso PIN} / {ratification mode: **as** supported by the product}
Application SubType: F4h proprietary file structure 'F4h': **NFC NDEF Tag Type 4**

AES Calypso keyset:	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'		
#1 Issuer	21h	75h	B0h	MK_RT1_B1			
#2 Load	27h	75h	B0h	MK_RT2_B1	shared Calypso PIN:	30303030h	"0000"
#3 Debit	30h	75h	B0h	MK_RT3_B1			

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	E100h	-	-	-	Session 1	Session 3	-	-	-
Capability File	Binary	E103h	01h	15		Always	Session 1	Never	-	-
NDEF Data File	Binary	E104h	02h	2048*		Always	Always	Always	-	-

* (The size of the EF 'NDEF Data File' is a multiple of 128)

Table 14 **: Calypso Prime Extended profile – Application 5 File Structure**

4.3 Calypso Light Application

The first characteristic of Calypso Light is to be a simplified Calypso OS. It uses a subset of the Calypso Prime commands with several limitations but with the same cryptography and the same security than a full Calypso card. For the hardware, an EAL4+ component or equivalent is required.

Only 2 files structures exist for Calypso Light which are both limited to the management of 2 contracts:

- **Reference** is near to the Hoplink structure
- **Classic** is similar to CD Light, to facilitate the introduction of Calypso Light on existing network

The test kit proposes one of each Calypso Light structures.

4.3.1 Calypso Light Classic

This **Calypso Light Classic File Structure** corresponds to the file structure **32h** of **[FSRegistry]**. Find below the technical details.

Calypso Light Classic profile - Application 1

Type:	Calypso Ticketing		AID:	**315449432E49434133**h	ASCII: "1TIC.ICA3"
Startup:	Session Modifications:	06h	(215 bytes modifications buffer)		
	Application Type:	90h	(Calypso Light identifier)		
	Application SubType:	32h	referenced Calypso file structure '32h': **Calypso Light Classic** File Structure		

TDES Calypso keyset :	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	21h	79h	90h	MK_RT1_T	
#2 Load	27h	79h	90h	MK_RT2_T	
#3 Debit	30h	79h	90h	MK_RT3_T	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2000h	-	-	-	Session 1	Session 3	-	-	-
Environment	Linear	2001h	07h	1	29	Always	Session 1	Never	-	-
Events Log	Cyclic	2010h	08h	3	29	Always	Session 3	Session 3	Session 3	-
Special Events	Linear	2040h	1Dh	1	29	Always	Session 3	Never	-	-
Contract List	Linear	2050h	1Eh	1	29	Always	Session 3	Never	-	-
Contracts	Linear	2020h	09h	2	29	Always	Session 2	Session 3	-	-
Counters	Counters	2069h	19h	1	29	Always	Session 2	Session 3	Session 2	-

Table 15 **: Calypso Light Classic File Structure -**

4.3.2 Calypso Light Reference

This **Calypso Light Reference File Structure** corresponds to the file structure **31h** of **[FSRegistry]**. Find below the technical details.

Calypso Light Reference profile - Application 1

Type: Calypso Ticketing AID: **315449432E49434134**h ASCII: "1TIC.ICA4"

Startup:
Session Modifications: 06h (215 bytes modifications buffer)
Application Type: 90h (Calypso Light identifier)
Application SubType: 31h referenced Calypso file structure '31h': **Calypso Light Reference** File Structure

TDES Calypso keyset :	KIF	KVC	ALG	diversified from	issued from the 'Calypso SAM-TEST-F5v6'
#1 Issuer	21h	79h	90h	MK_RT1_T	
#2 Load	27h	79h	90h	MK_RT2_T	
#3 Debit	30h	79h	90h	MK_RT3_T	

File structure:

File	Type	LID	SFI	Rec. Num.	Rec. Size	Group 0 Read Rehabilitate	Group 1 Update Invalidate	Group 2 Write Decrease	Group 3 Append Increase	EF Sharing Data Ref.
DF	DF	2000h	-	-	-	Session 1	Session 3	-	-	-
Environment	Linear	2014h	14h	1	32	Always	Session 1	Never	-	-
Contracts	Linear	2015h	15h	2	64	Always	Session 2	Session 3	-	-
Usage	Linear	201Ah	1Ah	2	48	Always	Session 3	Never	-	-
Counters A	Counters	201Bh	1Bh	1	6	Always	Session 2	Session 3	Session 2	-
Counters B	Counters	201Ch	1Ch	1	6	Always	Session 2	Session 3	Session 2	-
Auxiliary Contracts	Linear	2009h	09h	2	64	Always	Session 2	Never	-	-
Common Log	Cyclic	2008h	08h	2	64	Always	Session 3	Never	Session 3	-
Park Log	Cyclic	201Eh	1Eh	2	64	Always	Session 3	Never	Session 3	-

Table 16 **: Calypso Light Reference File Structure**

5 GLOSSARY AND ACRONYMS

AES	*Advanced Encryption Standard* (as defined in ISO/IEC 18033-3): symmetrical cryptographic algorithm using 128-bit data and key.
AID	Symbol for *Application Identifier*. Value unique in a portable object, allowing to unambiguously identify an application, as defined in ISO/IEC 7816-4 and ISO/IEC 7816-5.
CLAP	Abbreviation previously used for *Calypso Light Application*
CNA	Abbreviation for *Calypso Networks Association*.
DES	Ciphering algorithm producing 8 bytes of data from 8 input bytes, using a 7 bytes key (as defined in *ANSI X3.92-1981*)
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).
Hoplink	Hoplink is the interoperable ticketing application developed by CNA. Some figures and names of files and fields may use this acronym of Triangle 2, the former denomination of Hoplink KIF Symbol for *Key Identifier*. Value identifying the type of key.
KIF	Symbol for *Key Identifier.* Value on one byte, used to identify the type of the key (transport issuer key, stored value debit key, etc.)
KVC	Symbol for *Key Version and Category*. Arbitrary value identifying a key among several of the same type.
PO	Abbreviation for *Portable Object*. A Portable Object may be any portable device with an ISO/IEC 14443 interface. Progressively replaced by *Card*, in a generic meaning, in the Calypso technical documentations.
SAM	Abbreviation for *Secure Application Module*. A SAM is a smart card permanently connected with the equipment interacting with the portable objects (present inside the equipment or remotely connected to it)
TDES	TDES (also called Triple-DES, or 3DES) is made of three successive DES operations, and uses a double DES key. It is a stronger algorithm than DES, and of equivalent strength to DESX.