CALYPSO FUNCTIONAL SPECIFICATION

‘CNA Calypso rev 3.1 Applet’ Presentation

VERSION 1.1

©2014 Calypso Networks Association. All rights reserved.
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.
First release, the version number is related to the corresponding CNA Applet version and User Guide
# TABLE OF CONTENTS

INTRODUCTION......................................................................................................................................4  
   1.1 Scope .........................................................................................................................................4  
   1.2 Notations ....................................................................................................................................4  

2 REV3.1 FUNCTIONALITIES AND OPTIONS ...................................................................................5  
   2.1 Supported Specifications ............................................................................................................5  
   2.2 Compatibility ...............................................................................................................................6  
   2.3 Options .......................................................................................................................................6  

3 CNA APPLET IMPLEMENTATION SPECIFICITIES .........................................................................9  
   3.1 Applet versions, platform dependencies, & targeted secure elements ........................................9  
   3.2 Applet Memory Use ..................................................................................................................10  

4 ANNEX ...........................................................................................................................................11  
   4.1 References ...............................................................................................................................11  
   4.2 Acronyms..................................................................................................................................12  
   4.3 Links and Contacts ...................................................................................................................13
INTRODUCTION

1.1 Scope

This document describes the functionalities of the CNA Calypso REV3.1 applet running in Portable Objects that embed a Secure Element compliant with the Java Card and the GlobalPlatform specifications. It presents the features and options supported by the CNA implementation of the Calypso Revision 3.1 specifications as a Java Card™ applet.

This document is an extract of the version 1.1 of the “Calypso Specification ‘CNA Calypso REV3.1 Applet’ User Guide” which defines in detail the technical settings of the applet, complementarily to the Calypso Revision 3.1 Portable Object Application and the Calypso Application Downloading specifications.

1.2 Notations

In the following,
- the term “application” used alone refers to the product provided by the Calypso Networks Association: the ‘CNA Calypso Revision 3.1 Java Card™ applet’;
- the term “Calypso REV3 application” indicate a Calypso ticketing instance installed from the applet.

All hexadecimal values are quoted or suffixed with the letter ‘h’. For instance, ‘10’ or 10h (hexadecimal) represents 16 (decimal).

Within this document, the keywords shall, should and may are to be interpreted as follows, when used in the italic form:
- The word shall is used to indicate mandatory requirements strictly to be followed in order to avoid common error situations and to avoid situations where the security or the operation of an application may be compromised. No deviation to such indications should be permitted (shall equals is required to).
- The word should is used to indicate that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is not recommended but not strictly prohibited (should equals is recommended that).

The word may is used to indicate a course of action permissible within the limits of the platform (may equals is permitted to).
2 REV3.1 FUNCTIONALITIES AND OPTIONS

The purpose of this chapter is to present the features and options supported by the CNA implementation of the Calypso Revision 3.1 specifications as a Java Card™ applet.

2.1 Supported Specifications

The application supports the following specifications:

- **CALYPSO SPECIFICATION REV.3**
  Portable Object Application
  Version 3.1 (dated 10 March 2009)
  Ref: 060708-CalypsoAppli
  Calypso Networks Association

- **CALYPSO SPECIFICATION REV.3**
  Calypso Generic Example File Structures
  Version 1.4 (dated 9 May 2013)
  Ref: 060709-CalypsoFiles
  Calypso Networks Association

- **CALYPSO SPECIFICATION**
  Application Downloading
  Version 1.1 (dated 26 May 2011)
  Ref: 090128-ApplicationDownload
  Calypso Networks Association

- **CALYPSO SPECIFICATION**
  Calypso Activation SAM – User Manual
  Version 1.1 (dated 6 August 2008)
  Ref: 080118-UM-ActivationSAM
  Calypso Networks Association

- **CALYPSO SPECIFICATION**
  Portable Object Application – Activation Cryptographic Algorithms – Revision 3
  Version 1.3 (dated 29 November 2010)
  Ref: 080610-SSAActivation
  Calypso Networks Association

- **CALYPSO TECHNICAL NOTE #001**
  Calypso Startup Information: Specification and Management
  Version dated 20 May 2013
  Ref: CalypsoTN001
  Calypso Networks Association

- **CALYPSO SPECIFICATION**
  Portable Application - Stored Value Algorithms
  Version 2.1
  Ref: 080520-NT-R3SVAlg
  Calypso Networks Association
2.2 Compatibility

Starting from the revision 3.1, the Calypso Portable Object specification is designed to support Java Card environment, indeed all non-optional features of the revision 3.1 are fully compliant with Java Card.

Except the extended version of binary EF, the application supports all features of the revision 3.1 which are compliant with Java Card. The application is an implementation of the revision 3.1, but it could also emulate a revision 2.4 product restricted to features compliant with Java Card (no Select Application with class byte 94h, no ratification on deselect signal, ...).

2.3 Options

This section details the implementation decisions that were made during the implementation of the application regarding the options defined in the Calypso Revision 3.1 specification. All of those decisions are within the boundaries defined in this specification.

Details:

- R3: After entering Phase 2, an instance of the application complies with the requirements of Calypso Revision 3.1. It has no data field, command or parameter other than those explicitly authorized in Calypso Revision 3.1.
- R4: The AID is defined during Phase 1.
- R7: Fetching the EF-DIR data with a Get Data command prior to the selection of an instance of the application is not supported.
- R8: When multiple instances of the application from the same package are installed in a Java Card, the Calypso Serial Number is shared between instances of the application.
- R9: The possible value for the number of Session Modifications is between 6 and 9 (both inclusive).
- R13-R17: The value of the Platform, Application Type, Application Subtype, Software Issuer and Software Version and Revision bytes of the Startup Information is defined by the entity in charge of the GlobalPlatform personalisation of an instance of the application using DGI 2100 as defined in CALYPSO SPECIFICATION, Application Downloading 1.1.
- R18: The Calypso PIN mechanism is supported by Calypso Instances. Stored Value instances do not support PIN mechanism.
- R23: Each instance of the application has its own Calypso PIN.
- R24: The Calypso Stored Value application is available: a dedicated Calypso Stored Value instance could be installed, or the support of the Stored Value feature could be added to a Calypso REV3 instance during its personalization.
- R27: The Java Card API does not trigger an applicative event when the underlying card receives a Disconnect frame, so the entity in charge of the personalisation of an instance of the application shall indicate "No ratification on disconnect" in the Application Type assigned to the instance.
- R28: The application does not support a MF.
- R29: The Shared EF mechanism is supported.
- R29:
  - o The application supports up to 255 records per file.
  - o The application supports up to 250 bytes per record.
- R41: DES, DESX and TDES are supported.
- R60: The ratification state is local for each instance of the application.
- R65: The session state is set to "ratified" when an instance of the application receives any applicative command (including Select Application).
- R68: The Default initial value of the Transaction Counter is 200.000. This value can be personalised using the DGI 2200.
• R70: The Transaction Counter is only decremented by the commands listed in R69. It is not decremented if an error is detected in the format of the command or if the command is incompatible with the current state of the instance of the application.

• R74: The Transaction Counter is global to the package.

• R81: The PO challenge is also reset when the instance of the application is deselected or when the PO is powered off.

• R81.1:
  o The application accepts CLA=94h for all commands except select application command if the hosting platform allows it.
  o The application supports CLA=FAh for the SV commands.

• R82:
  o 6E00h is returned when the Class is incorrect.
  o 6D00h is returned when the Instruction is incorrect.

• R84: The maximum size of the Data Field is limited by the capabilities of the Java Card™ hosting the application. All JC2.2 products and later versions allow the applet to support 250 bytes as maximum size of the Data field.

• R88: The application supports the transmission protocol managed by the hosting platform, T=0 if the contact mode is available.

• R93: The application supports the modes of operation of Select Application supported by the Java Card™ hosting the application.

• R94:
  o Only CLA=00h is supported for the Select Application command (Java Card platforms do not supports Select Application with CLA=94h).
  o P2=0Ch and P2=0Eh are supported.
  o For the GP2.2.1 version dedicated for NFC mobile, if the applet is selected on the contact interface with T=0 or T=1 and P2=00h or P2=02h:
    ▪ the applet doesn’t return SW=6283h if the application is invalided (this hack allows a better support with mobile environment);
    ▪ the applet returns SW=6200h in case of exception during the self-activation process (see §Erreur ! Source du renvoi introuvable.).

• R98.1: The application supports the parameters combinations described in 98.1.

• R99:
  o The selected file or DF shall be in the current selected DF.
  o The application supports the selection mode with P1= 08h and P2 = 00h

<table>
<thead>
<tr>
<th>Action</th>
<th>P1</th>
<th>P2</th>
<th>Lc</th>
<th>Data In</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a given file</td>
<td>08</td>
<td>00</td>
<td>02</td>
<td>File LID</td>
<td>‘Current DF’ or ‘Local EF’</td>
</tr>
</tbody>
</table>

• R102: CLA=94h is supported.

• R105: CLA=94h is supported.

• R107: CLA=94h is supported.

• R108: The application supports the Get Data command with the following optional tags:
  o 0062h    current FCP
  o 006Fh    current FCI
  o 0185h : Traceability Information (defined in chapter §Erreur ! Source du renvoi introuvable.)

• R111/R112: Put Data is not supported.

• R116: CLA=94h is supported.

• R118: CLA=94h is supported.

• R120: CLA=94h is supported.

• R122: CLA=94h is supported.

• R124: CLA=94h is supported.

• R125: The extended version of Read Binary is not supported.

• R135: The extended version of Update Binary is not supported.

• R140: The extended version of Write Binary is not supported.
• R144: CLA=94h is supported.
• R145: CLA=94h is supported.
• R147: CLA=94h is supported.
• R149: CLA=94h is supported.
• R151: CLA=94h is supported.
• R152: Change PIN is supported.
• R153: CLA=94h is supported.
• R154: Verify PIN is supported.
• R155: CLA=94h is supported.
• R157: The Stored Value application is supported.
• R158: DF LID defined at 1000h (cf. §Erreur ! Source du renvoi introuvable.).
• R159: Load Log LID defined at 1014h.
• R160: Purchase Log defined at 1015h.
• R164: CLA=94h & FAh are supported.
• R170: CLA=94h & FAh are supported.
• R176: CLA=94h & FAh are supported.
• R182: CLA=94h & FAh are supported.
3 CNA APPLET IMPLEMENTATION SPECIFICITIES

3.1 Applet versions, platform dependencies, & targeted secure elements

CNA provides the application in three main versions:
- ‘GlobalPlatform 2.1.1 for Java Card™ 2.1.x’,
- ‘GlobalPlatform 2.1.1 for Java Card™ 2.2.x’,
- ‘GlobalPlatform 2.2.1 for Java Card™ 2.2.x’.

The GP2.1.1 application could address most of contactless Java Card Secure Element; versions optimized for JC2.1.x & JC2.2.x are available. These versions support only the personalization process with a selection of the application.

The GP2.2.1 application is dedicated for NFC mobile:
- This version manages in addition the personalization process through the associated Security Domain (required OTA channel usage).
- The ‘Select Application’ command in contact mode could return only response status at 9000h or 61XYh in order to assure a good interoperability with mobile environments.
- In contact mode, in case the contactless interface is disabled, the application calls the self-activation privilege on the processing of the Select Application command. The usage of the self-activation privilege has to be firstly declared at the installation of the instance.

The GP2.2 application is dependent upon the Java Card™ 2.2.1 API.

CNA proposes also:
- an experimental version ‘GlobalPlatform with OTA push’, this application extends the ‘GP2.2 regular’ version with the support of the Calypso APDU commands through an OTA channel (see §Erreur ! Source du renvoi introuvable.).
- Reserved for Calypso licensees, a special version ‘VOP2.0.1/GP2.1.1 for Factory Personalization’ is available too. This version shall be used for indoor personalization only; it allows the support of Java Card platforms not managing RSA in 1536 bits (see [CSFP]).

API & dependencies:
- For all versions:
  o The application is not multi-selectable. In other words, it does not implement the "javacard.framework.MultiSelectable" Interface.
  o The application does not rely on proprietary extensions of the underlying Portable Object.
  o The application does not implement the "org.globalplatform.Application" Interface.
  o The application implements the "javacard.framework.Shareable" Interface.
- For the NFC mobile version:
  o The application does not use the SIM Toolkit API.
  o For the OTA personalization, the application implements the extended
    processData(...) method of the "org.globalplatform.Personalization"
    Interface (amendment A 1.0 of GlobalPlatform 2.2, cf. [CCCM]).
  o To manage the self-activation privilege, the application uses the
    "org.globalplatform.contactless.GPCLSystem" Interface (amendment C 1.0.0
    of GlobalPlatform 2.2.1, [CCS]).

By default, the CNA provides the applet in versions only dependent on the Java Card & GlobalPlatform
API. The applet could also be packaged to support a cryptographic patch API in order to increase the
performance (cf. [CCAPG]).

### 3.2 Applet Memory Use

The following table gives an estimation of the memory allocated by the applet in persistent memory
(EEPROM) and in RAM (Transient memory allocated in Clear on Reset for the GP2.2 with OTA push
applet, in Clear on Deselect for the other versions).

<table>
<thead>
<tr>
<th></th>
<th>GP2.1.1 (Bytes)</th>
<th>GP2.2.1 (Bytes)</th>
<th>GP2.2 with OTA push (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EEPROM</td>
<td>RAM</td>
<td>EEPROM</td>
</tr>
<tr>
<td>Package</td>
<td>23 kB</td>
<td>26,5 kB</td>
<td>28 kB</td>
</tr>
<tr>
<td>Setup instance</td>
<td>778</td>
<td>800</td>
<td>780</td>
</tr>
<tr>
<td>Rev3 instance</td>
<td>2604</td>
<td>210</td>
<td>2656</td>
</tr>
<tr>
<td>Total for 1 instance</td>
<td>26,3 kB</td>
<td>1010</td>
<td>29,8 kB</td>
</tr>
<tr>
<td>Total for 2 instances</td>
<td>28,8 kB</td>
<td>1010</td>
<td>32,4 kB</td>
</tr>
</tbody>
</table>

In this example, the static RAM allocation (shared by all Rev3 instances) is defined for a modification
session buffer of 215 bytes and a signature accumulation buffer of 512 bytes. The configuration is based
on the reference file structure 01h.
(For GP2.2 version with OTA push, the RAM memory is not released when the application is not used;
the RAM amounts add up if several packages are loaded.)
# 4 ANNEX

## 4.1 References

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Title</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Calypso Networks Association (<a href="http://www.calypsostandard.net">www.calypsostandard.net</a>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calypso Networks Association (<a href="http://www.calypsostandard.net">www.calypsostandard.net</a>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calypso Networks Association (ask <a href="mailto:applet@calypsonet-asso.org">applet@calypsonet-asso.org</a>)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calypso Networks Association (reserved for licensees / ask <a href="mailto:applet@calypsonet-asso.org">applet@calypsonet-asso.org</a>)</td>
<td></td>
</tr>
<tr>
<td>[CPOPD]</td>
<td>Calypso Specification – Portable Object Profile Declaration</td>
<td>Version 0.96 – March 14, 2014</td>
<td>Ref: 130920-CalypsoPOProfileDeclaration_V0.96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Calypso Networks Association (<a href="http://www.calypsostandard.net">www.calypsostandard.net</a>)</td>
<td></td>
</tr>
<tr>
<td>[CCAPG]</td>
<td>CNA Calypso Applet Specification – Java Card Applet Patch Guide</td>
<td>Version 1.0.2 – April 30, 2009</td>
<td>Calypso Networks Association (ask <a href="mailto:applet@calypsonet-asso.org">applet@calypsonet-asso.org</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version 1.0.1 – January 2011</td>
<td>GlobalPlatform (<a href="http://www.globalplatform.org">www.globalplatform.org</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version 1.1 – April 2013</td>
<td>GlobalPlatform (<a href="http://www.globalplatform.org">www.globalplatform.org</a>)</td>
</tr>
<tr>
<td>[24014]</td>
<td>ISO 24014-1 – Public transport – Interoperable fare management system</td>
<td>Final Draft</td>
<td>ISO (<a href="http://www.iso.org">www.iso.org</a>)</td>
</tr>
<tr>
<td>[102225]</td>
<td>ETSI TS 102 225</td>
<td>Smart Cards: Secured packet structure for UICC based applications (Release 7)</td>
<td>ETSI (<a href="http://www.etsi.org">www.etsi.org</a>)</td>
</tr>
<tr>
<td>[102226]</td>
<td>ETSI TS 102 226</td>
<td>Smart Cards: Remote APDU structure for UICC based applications (Release 7)</td>
<td>ETSI (<a href="http://www.etsi.org">www.etsi.org</a>)</td>
</tr>
</tbody>
</table>
### 4.2 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>APSD</td>
<td>Application Provider Security Domain</td>
</tr>
<tr>
<td>C-MAC</td>
<td>Command MAC</td>
</tr>
<tr>
<td>CA</td>
<td>Controlling Authority</td>
</tr>
<tr>
<td>CMS</td>
<td>Card Management System</td>
</tr>
<tr>
<td>DF</td>
<td>Dedicated File</td>
</tr>
<tr>
<td>DGI</td>
<td>Data Grouping Identifier</td>
</tr>
<tr>
<td>EF</td>
<td>Elementary File</td>
</tr>
<tr>
<td>EMV</td>
<td>Eurocard MasterCard Visa</td>
</tr>
<tr>
<td>FCI</td>
<td>File Control Information</td>
</tr>
<tr>
<td>GP</td>
<td>GlobalPlatform</td>
</tr>
<tr>
<td>GP-CMS</td>
<td>GlobalPlatform Card Management System</td>
</tr>
<tr>
<td>ICV</td>
<td>Initial Chaining Vector</td>
</tr>
<tr>
<td>ISD</td>
<td>Issuer Security Domain</td>
</tr>
<tr>
<td>ISO/IEC</td>
<td>International Organization for Standardization / International Electrotechnical Commission</td>
</tr>
<tr>
<td>LSB</td>
<td>Least Significant Byte</td>
</tr>
<tr>
<td>M/O</td>
<td>Mandatory/Optional</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MIDP</td>
<td>Mobile Information Device Profile</td>
</tr>
<tr>
<td>MSB</td>
<td>Most Significant Byte</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-the-Air</td>
</tr>
<tr>
<td>OTI</td>
<td>Over-the-Internet</td>
</tr>
<tr>
<td>RAM</td>
<td>Remote Application Management</td>
</tr>
<tr>
<td>RFU</td>
<td>Reserved for Future Use</td>
</tr>
<tr>
<td>R-MAC</td>
<td>Response MAC</td>
</tr>
<tr>
<td>ROM</td>
<td>Read-Only Memory</td>
</tr>
<tr>
<td>SAM</td>
<td>Secure Application Module</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Channel Protocol</td>
</tr>
<tr>
<td>SD</td>
<td>Security Domain</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SFI</td>
<td>Short File Identifier</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SSD</td>
<td>Supplementary Security Domain</td>
</tr>
<tr>
<td>SW</td>
<td>Status Word</td>
</tr>
<tr>
<td>SWP</td>
<td>Single-Wire Protocol</td>
</tr>
<tr>
<td>TLV</td>
<td>Tag Length Value</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third-Party</td>
</tr>
</tbody>
</table>
4.3 Links and Contacts

Calypso related Internet sites:

<table>
<thead>
<tr>
<th>Calypso Documentation</th>
<th><a href="http://www.calypsostandard.net">http://www.calypsostandard.net</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Calypso Networks Association</td>
<td><a href="http://www.calypsonet-asso.org">http://www.calypsonet-asso.org</a></td>
</tr>
<tr>
<td>Innovatron</td>
<td><a href="http://www.innovatron.com">http://www.innovatron.com</a></td>
</tr>
</tbody>
</table>

Calypso related email contacts:

<table>
<thead>
<tr>
<th>CNA Calypso Applet Support</th>
<th><a href="mailto:applet@calypsonet-asso.org">applet@calypsonet-asso.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Calypso Networks Association</td>
<td><a href="mailto:contact@calypsonet-asso.org">contact@calypsonet-asso.org</a></td>
</tr>
<tr>
<td>Innovatron</td>
<td><a href="mailto:calypso@innovatron.fr">calypso@innovatron.fr</a></td>
</tr>
</tbody>
</table>