**Implementation** **Conformance Statement**

For



on Java Card platform with 

**REVISION LIST**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Chapter** | **Comment** |
| V1.0.0 | 23/10/2019 | - | Release |
| V1.1.0 | 24/11/2020 | 4. | Add new applet v1.3.9 |
| V1.2.0 | 11/12/2020 | 4. | Add new configuration for applet v1.3.9 |
| V1.3.0 | 18/03/2021 | 4. | Update list of type of products and Calypso platform table |
| V1.4.0 | 23/09/2021 | 4. | Update Size capacity for package 1 |
| V1.5.0 | 27/01/2022 | 4. | Renaming and packages update |
| V1.6.0 | 14/03/2022 | 2 | Update references |
| V1.7.0 | 27/06/2022 | 2 | Update references |
| V1.8.0 | 06/10/2022 | 2/4 | Update references |
| V1.9.0 | 05/10/2023 | 4 | Update packages with RN applet v1.3.10 v3 |

Content

[1. Scope of the documents 4](#_Toc115709604)

[2. References 4](#_Toc115709605)

[3. Applicant 4](#_Toc115709606)

[4. Card description 5](#_Toc115709607)

[5. Additional comments 9](#_Toc115709608)

[6. Laboratory Information 9](#_Toc115709609)

[7. Certification Body 11](#_Toc115709610)

# Scope of the documents

The purpose of the present Implementation Conformance Statement (ICS) is to describe the characteristics and capabilities of the Calypso card submitted for testing. This template shall be completed by the vendor, with the assistance of the Evaluation Laboratory, if necessary, before starting the evaluation process.

The ICS will be part of the Certificate to be issued and provide information about the product implementation to the end users of the certificate. The evaluation and certification process are described in the Calypso Card Functional Certification Process document (ref.: 191104-GU-CalypsoCardFunctionalCertificationProcess).

For details on the Calypso card profiles, please refer to the Calypso Card Functional Certification Process document (ref.: 191104-GU-CalypsoCardFunctionalCertificationProcess) and the Calypso Prime Profiles Definition document (ref.: 191214-TL-CalypsoPrime-ProfileDefinition).

# References

* Calypso Specification – Calypso Prime

 *060708-SP-CalypsoPrime (3.3 Edition 2 – July 2022)*

* Release Note – Calypso Card Applet – Version 1.3.10

 *211227-RN-CalypsoCardApplet-1.3.10-ReleaseNote v3 (September 2023)*

* Technical Note #001 – Calypso Startup Information – Specification and Management

 *000907-TN-001-StartupInfo*

# Applicant

|  |
| --- |
| **Vendor Identification** |
| Company Name: | Click here to enter your text. |
| Company Location: |  Click here to enter your text. |
| **Main Contact** |
| Contact Name: | Click here to enter your text. |
| Telephone: | Click here to enter your text. |
| Email Address: | Click here to enter your text. |
| **Backup Contact** |
| Contact Name: | Click here to enter your text. |
| Telephone: | Click here to enter your text. |
| Email Address: | Click here to enter your text. |
| **Certification Request** |
| Date: | Click here to enter the date. |
| Request Type \*: |  |
| Previous ICS registration Number:*(If renewal)* | Click here to enter your text. |
| Summary of changes*(If applicable)* | Click here to enter your text. |

\* Renewal: request for an already approved product without change

 Product change: request for a minor change of an already approved product. Vendor to explain the change and impact from his point of view

# Card description

|  |
| --- |
| **Product Identification** |
| Commercial Name and version : | Click here to enter your text. |
| Technical Name and version : | Click here to enter your text. |
| OS Name and version: | Click here to enter your text. |
| OS Owner | Click here to enter your text. |
| Type of product : | Select one type of product[ ]  Other, if applicable: Click here to enter your text. |
| RF Protocol Type  | [ ]  Type A [ ]  Type B[ ]  Other: Click here to enter your text. |
| Mode *If PKI Mode selected, extended mode included too*. | **X** Regular mode[ ]  Extended mode[ ]  PKI mode |
| Main features  | ☒ PIN ☒ Stored Value☒ Shared files |
| **Calypso Applet Reference**  | Select one reference. |
| .cap File Name | Select one. |
| .cap HMAC-SHA-1 | Select one. |
| Load File DataBlock Hash without DescriptorHMAC-SHA-1 for DAP Signature | Select one. |
| **Platform Dependencies** |
| JavaCard Version | Click here to enter your text. |
| Global Platform Version  | Click here to enter your text. |
| Persistent Memory Capacity | Click here to enter your text. |
| Transient Memory Capacity*Available for the Calypso applet* | Click here to enter your text. |

|  |
| --- |
| **Hardware Component** |
| Calypso Platform reference 2 | Select your platformOther : $ Enter the value Platform Enter the value |
| Hardware identification and Revision 3 | Click here to enter your text. |
| Hardware Manufacturer | Select oneOther : $ Enter the value Platform Enter the value |
| CC certification | Issuing AuthorityCertificate IDLevel | Click here to enter your text.Click here to enter your text.Click here to enter your text. |

 The reference will be used on public documents and available on the website.

2 For Calypso Platform reference, see Platform Table (T3) in Technical Note #001 document (ref.: 000907-TN-001-StartupInfo) and complete with value and platform (i.e. 06).

3 Define the complete identification with memory size.

**Vendor declaration**

Please complete the main options implemented by the product.

|  |  |  |
| --- | --- | --- |
|  | Is the card sample self powered? | Click here |
| INTERFACE | Does the card support Contact interface? | Click here |
| Number of logical channel available for the contactless interface*(T=1: ISO 14443 or NFC SWP)* | [ ] 1 or [ ] 4 or [ ] 20 |
| Number of logical channel available for the contact interface*(ISO 7816-3: T=0, SPI: T=0/1,* *HCI APDU GATE: T=0/1)* | [ ] 0 [ ] 1 or [ ] 4 or [ ] 20 |
| Is Manage Channel supported ?  |  [ ]  Yes [ ]  No |
| SIZE/CAPACITY | What is the maximum value of the Session Modifications byte of the Startup Information supported?*The value of the Session Modification field of a Calypso Prime application shall be between 7 and 55 (decimal). Depending on the Calypso Applet personalization, this value is between 7 and 12 (decimal).**For NFC secure element, CNA recommends processing the tests with* ***12 (0Ch).****For contactless card, CNA recommends processing the tests with* ***8 (08h).*** | Select a size.Define a value if different (num/hexa) |
| What is the maximum number of records in a file? | 250 |
| What is the maximum record size supported? | 250 |
| What is the maximum Lc supported? | 250 |
| What is the maximum Le supported? | 250 |
| What is the maximum size of binary file supported by the product?*Maximum value is 32,768bytes (8000h) for the Calypso Applet if the available persistent memory capacity of the product allow it.* | 32,768 |
| What is the maximum number of data bytes entering a given Session MAC / Session Signature? | 49,152 |

**Applicability declaration for compatibility with legacy terminal**

The following applicabilities are present only for compatibility with legacy terminals that follow previous versions of the Calypso Prime specification. These compatibilities feature could be removed from future versions of the Calypso Prime specification.

Please specify the functions supported by the provided sample. Tests which require functions not supported by the provided Calypso Prime card will be skipped during the tests.

|  |  |  |  |
| --- | --- | --- | --- |
| **Object** | **Constraint linked** | **Applicability supported****CONTACT** | **Applicability supported****CONTACTLESS** |
| CLA byte ‘94’ supported for the other Calypso command4 | CLA\_94 | [ ]  Yes [ ]  No | [ ]  Yes [ ]  No |
| CLA byte ‘FA’ supported5 | CLA\_FA | [ ]  Yes [ ]  No | [ ]  Yes [ ]  No |

4 This option could not be supported or be restricted, for some specific logical channel numbers, in case the tested physical interface manages more than 4 logical channels (e.g. 20).

5 This option may not be supported or restricted, for some specific logical channel numbers, in case the tested physical interface manages more than 1 logical channel (e.g. 4 or 20).

These other applicabilities are fixed for the Calypso Applet.

|  |  |  |
| --- | --- | --- |
| **Object** | **Constraint linked** | **Applicability supported** |
| CLA byte ‘94’ supported for the Select Application Command | CLA\_94\_SEL | [ ]  Yes [x]  No |
| DES key supported | DES | [x]  Yes [ ]  No |
| DESX key supported | DESX | [x]  Yes [ ]  No |
| Historical bytes of ATR readable using GET DATA | GET\_ATR | [ ]  Yes [x]  No |
| Ratification on contactless deselection | RAT\_ON\_DESELECT | [ ]  Yes [x]  No |

**Applicability declaration for product**

These applicabilities are fixed for the Calypso Applet.

Tests which require functions not supported by the provided Calypso Prime card will be skipped during the tests.

|  |  |  |
| --- | --- | --- |
| Object | Constraint linked | Applicability supported. |
| AES key supported | AES | [ ]  Yes [x]  No |
| List of Application available through ISO APDU Command(cf Calypso Prime specification version 3.3 edition 2 §4.3) | APP\_AV | [ ]  Yes [x]  No |
| Default application selected at reset | DEF\_APP | [ ]  Yes [x]  No |
| DF contains another DF | DF\_IN\_DF | [ ]  Yes [x]  No |
| Get response for a partial read of available bytes on the card supported6 | GETRESP\_PARTIAL | [x]  Yes [ ]  No |
| Master File supported | MF | [ ]  Yes [x]  No |
| Select Command without request for FCI supported | NO\_FCI | [x]  Yes [ ]  No |
| PUT DATA (for AID) supported | PUT\_AID | [ ]  Yes [x]  No |
| PUT DATA (for SV link) supported | PUT\_SV\_LINK | [ ]  Yes [x]  No |

6 This option is only available on contact interface

# Additional comments

Comments and addition explanations:

Click here to enter your text.

# Laboratory Information

|  |
| --- |
| **Laboratory Identification** |
| Laboratory Name: | Click here to enter your text |
| Laboratory Location: | Click here to enter your text |
| **Main Contact** |
| Contact Name: | Click here to enter your text |
| Telephone: | Click here to enter your text |
| Email Address: | Click here to enter your text |
| **Backup Contact** |
| Contact Name: | Click here to enter your text |
| Telephone: | Click here to enter your text |
| Email Address: | Click here to enter your text |

|  |
| --- |
| **Report Confidentiality** |
| The report must be ciphered (using PGP) when sent by email: | [ ]  YES [ ]  NO |

# Certification Body

|  |
| --- |
| **Certification Body Identification** |
| Company Name: | Click here to enter your text |
| Company Location: | Click here to enter your text |
| **Main Contact** |
| Contact Name: | Click here to enter your text |
| Telephone: | Click here to enter your text |
| Email Address: | Click here to enter your text |
| **Backup Contact** |
| Contact Name: | Click here to enter your text |
| Telephone: | Click here to enter your text |
| Email Address: | Click here to enter your text |

|  |
| --- |
| **ICS Status** |
| Status: | To be Validated |
| ICS Registration Number: | Cliquez ici pour entrer du texte. |
| Date of validation by the Certification Body: | Cliquez ici pour entrer une date. |

Signature of the Certification Body’s representative:

