**Implementation** **Conformance Statement**

For Calypso Card Certification



*Prime*

(Applet)

**REVISION LIST**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Chapter/Section** | **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 |

Content

[1. Scope of the documents 4](#_Toc485225355)

[2. References 4](#_Toc485225356)

[3. Applicant 5](#_Toc485225357)

[4. Product 6](#_Toc485225358)

[5. Additional comments 8](#_Toc485225359)

[6. Laboratory Information 9](#_Toc485225360)

[7. Certification Body 10](#_Toc485225361)

# Scope of the documents

The purpose of the present Implementation Conformance Statement (ICS) is to describe the characteristics and capabilities of the 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 a dedicated procedure (ref. *CER\_PRO\_2017-001*).

# References

* Calypso Startup Information: Specification and Management

*CalypsoTN001-StartupInfo* Calypso Technical Note #001

* Calypso Revision 3 Specification Card Application

*060708-CalypsoAppli-33 (10th September 2019)*

# 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. |
| 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 Data  Block Hash without Descriptor  HMAC-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 \* | Select your platform  Other : $ Enter the value Platform Enter the value | |
| Hardware identification and Revision 2 | Click here to enter your text. | |
| Hardware Manufacturer | Select one  Other : $ Enter the value Platform Enter the value | |
| CC certification | Issuing Authority  Certificate ID  Level | 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 Define the complete identification including memory size.

\*For Calypso Platform reference, see CalypsoTN001 Platform Table

**Vendor declaration**

Please complete the main options implemented by the Calypso card.

|  |  |  |
| --- | --- | --- |
|  | 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 |
| SIZE/CAPACITY | What is the maximum number of records in a file? | 250 |
| What is the maximum record size supported? | 250 |
| What is the Session buffer size?  *Depending on the applet personalization, the session buffet size is between 215 and 4096 bytes.*  *For UICC & eSE, CNA recommends to process the tests for modifications buffer set a* ***608*** *bytes.*  *Startup information defined at 0Ch* | Select a size.  Define a value if different |
| What is the maximum Lc supported? | 250 |
| What is the maximum Le supported? | 250 |
| RATIFICATION | When is the ratification managed? | ☒ APDU only  ☐ Deselect + APDU |

**Applicability declaration**

Please confirm both functions supported by the samples. For details on the Calypso Card profiles, please refer to the CPOC-Guidelines.

|  |  |  |
| --- | --- | --- |
| Object | Applicability supported CONTACT | Applicability supported  CONTACTLESS |
| **CLA byte ‘94’** supported for the other Calypso command 1 (CLA\_94) | Yes  No | Yes  No |
| **CLA byte ‘FA’** supported 2 (CLA\_FA) | Yes  No | Yes  No |

The other functions are currently fixed for the applet:

|  |  |  |
| --- | --- | --- |
| Object | Constraint linked | Applicability supported. |
| AES cryptographic algorithm supported | AES | ☐ Yes ☒ No |
| Command Rev 3.2 supported | Rev3.2 | ☐ Yes ☒ No |
| List of Application available through ISO APDU Command (cf Calypso Specification Rev 3 §5.3) | APP\_AV | ☐ Yes ☒ No |
| Challenge invalidated at reset | CHAL\_INV | ☒ Yes  No |
| CLA byte ‘94’ supported for the Select Application Command | CLA\_94\_SEL | Yes  No |
| Default application selected at reset. | DEF\_APP | Yes  No |
| Default EF selected through Select application | DEF\_EF\_SEL | Yes  No |
| DES key supported | DES | Yes  No |
| DF Context Invalidation supported | DF\_INV | Yes  No |
| DF contains another DF | DF\_IN\_DF | Yes  No |
| Extended mode for binary commands supported | EXT\_MODE | Yes  No |
| List of AID of the applications linked readable using GET DATA 3 | GET\_APP\_LINKED | Yes  No |
| Get response for a partial read of available bytes on the PO supported 4 | GETRESP\_PARTIAL | Yes  No |
| Historical bytes of ATR readable using GET DATA | GET\_ATR | Yes  No |
| FCI readable using GET DATA 3 | GET\_FCI | Yes  No |
| FCP readable using GET DATA 3 | GET\_FCP | Yes  No |
| Traceability information readable using GET DATA 3 | GET\_TRACE | Yes  No |
| Master File supported | MF | Yes  No |
| Select Command without request for FCI supported | NO\_FCI | Yes  No |
| PIN supported 3 | PIN | Yes  No |
| PUT DATA (for AID) supported | PUT\_AID | Yes  No |
| PUT DATA (for SV link) supported | PUT\_SV\_LINK | Yes  No |
| Ratification is worked through Frame Command | RAT\_ON\_FRAME | Yes  No |
| Ratification is worked through Select Command | RAT\_ON\_SEL | Yes  No |
| No constraint between group 0 and other group | RIGHT\_FREE | Yes  No |
| Shared files supported | SHA\_EF | Yes  No |
| PIN is shared between applications | SHA\_PIN | Yes  No |
| Ratification is shared between applications 3 | SHA\_RAT | Yes  No |
| Stored Value Application Supported | SV | Yes  No |

1 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).

2 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).

3 This option couldn’t be disabled without updating the package.

4 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:

