©2018 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.

The following Specification includes contactless and applicative technologies which are patented in several countries. Permission to copy and implement the material contained herein is subject to a Calypso license. You may contact Innovatron (calypso@innovatron.fr) for further information.

Any party seeking to implement this Specification is solely responsible for determining whether their activities require another license to any technology. Calypso Networks Association, Innovatron, RATP, SNCF and Spirtech shall not be liable for infringements of any third party’s intellectual property right.
FOREWORD
This document was developed through Calypso Networks Association workgroup 1 (specifications and technical development).
The association wishes to thank its active contributors to this document. A special thank you is addressed to Spirtech for its leading role on the subject and for writing the successive versions of this document.

REVISION LIST

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>18/04/2018</td>
<td>First version released.</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1  **OVERVIEW** ........................................................................................................................................... 4  
   1.1 Introduction to HCE .......................................................................................................................... 4  
   1.2 Document Scope and Purpose ........................................................................................................... 4  
   1.3 Definitions ......................................................................................................................................... 5  
   1.4 Interfaces ........................................................................................................................................... 5  
   1.5 References ......................................................................................................................................... 6  

2  **DATA ORGANIZATION** ...................................................................................................................... 7  
   2.1 HCE Persistent Data .......................................................................................................................... 7  

3  **CALYPSO FUNCTIONALITY** ............................................................................................................. 9  
   3.1 Calypso HCE Security ...................................................................................................................... 9  
      3.1.1 Risk Mitigation .......................................................................................................................... 9  
      3.1.2 Functional Requirements ......................................................................................................... 9  
      3.1.3 Android Security Features ....................................................................................................... 9  
      3.1.4 Android Key Store (AKS) and Hardware Credential Storage (HCS) ........................................ 9  
      3.1.5 Calypso HCE Security Overview ............................................................................................ 10  
      3.1.6 Recommendations for Personalization and Loading ............................................................... 11  
   3.2 Summary of the Calypso Commands ................................................................................................. 12  

4  **CALYPSO APPLICATION LIFE CYCLE OVERVIEW** ........................................................................ 13  
   4.1 Life Cycle ........................................................................................................................................... 13  
   4.2 Application Identifier (AID) ............................................................................................................. 16  
   4.3 Calypso PIN ....................................................................................................................................... 16  
   4.4 Calypso Stored Value ....................................................................................................................... 16  

5  **SECURITY MECHANISMS OVERVIEW** .......................................................................................... 17  
   5.1 Overview ........................................................................................................................................... 17  
   5.2 Application Activation ....................................................................................................................... 17  
   5.3 Cryptographic Keys ........................................................................................................................... 18  

6  **ANNEX** ............................................................................................................................................... 19
1 OVERVIEW

1.1 Introduction to HCE

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

Important Notice

The current version of this document applies only to Android, since at present (June 2018) it is the only HCE API widely available on NFC phones. It will be updated when other HCE APIs will become widely available.

Previously, using an NFC phone as a contactless card (i.e. receiving contactless commands and providing responses) required in practice a dedicated application hosted and operated in a secure element of the phone, such as its SIM.

With HCE, an Android application in the phone can directly receive, process and respond to contactless commands, without the need for support from any secure element.

However, HCE is much less secure that a contactless smart card or a SIM. Therefore, specific security requirements are necessary to implement a secure application (such as a Calypso application) to achieve an acceptable level of security.

Note that even with the security requirements of the present specification, the level of security for HCE applications remains much lower than for smart cards. The risks and benefits of using an HCE application must therefore be weighted for each specific implementation.

1.2 Document Scope and Purpose

The present document is a technical general overview of a Calypso HCE application. The full specifications are available from the Calypso Networks Association:

- 141113-CalypsoHCEApplication Calypso Application applied to Host Card Emulation
- 150422-CalypsoHCEGuidelines HCE Guidelines

A Calypso HCE application is a software application containing data organized as a Calypso file structure, and implementing the Calypso features with a good level of compatibility with existing Calypso applications, as defined in the Calypso Portable Object Application Specification (Revision 3), and using the NFC HCE interface provided by the Android operating system since its version 4.4 (“KitKat”).

Since HCE applications do not offer the same level of security to store information as do secure elements such as smartcards, cloning, reversal of data to an earlier state, and modification of data stored in a portable object should be considered possible in an HCE application.

However, contrary to cards, mobile phones are connected objects. It is possible to lower the risk by regular connections of the mobile phone to the remote system responsible for overseeing the security of the applications deployed.
Therefore, in order achieve a good compatibility with Calypso Revision 3 systems with an acceptable level of security to prevent fraud, the scope and purpose of this document is:

- to specify the specific cryptographic data and mechanisms that shall be implemented in Calypso HCE applications, and

- based on the *Calypso Portable Object Application Specification* (Revision 3.2), which is assumed to be known, to specify the differences for Calypso HCE applications.

**Calypso HCE Applications Interoperability**

Compliance with the present document ensures interoperability at contactless interface (i.e. with contactless terminals, including Calypso SAM), and for all processes involving cryptograms and related data for secure procurement of activation data (certified public key, Calypso serial number, Debit Key).

But the relative level of security of an HCE application requires a more comprehensive approach of security. Unlike a secure element built to protect data for a long period, a mobile device can only ensure their protection for a very limited period of time depending on the security techniques adopted to delay the attacks on the software and the countermeasures implemented to detect a fraud at the level of the central system, based on a constant back-end monitoring.

A Calypso HCE project shall rely both on the Calypso HCE application specification (141113-CalypsoHCEApplication) and on the Calypso HCE Guidelines (150422-CalypsoHCEGuidelines).

### 1.3 Definitions

In the present document, the following definitions apply:

- **“Calypso card application”** refers to any Calypso application stored and operated in a secure element, complying with the Calypso Revision 3 specifications (060708-CalypsoApp).

- **“Phone”** refers to any kind of NFC device implementing HCE.

- A **“Calypso HCE application”** is a set of software elements within a phone, behaving as a single Calypso card application as seen from the contactless interface, and complying with the present specification.

- A single **“Android application”** may implement one to many Calypso HCE applications, and usually implements a user interface.

- **“Command”** is synonym to an ISO/IEC 7816-4 command APDU, unless indicated otherwise.

- **“Authorization Module”** refers to the physically secure device ensuring the security specific to the Calypso HCE system.

- **“HCE activation system”** refers to any part of the remote information system used to manage the Calypso HCE application.

### 1.4 Interfaces

A Calypso HCE application exchanges data with external equipments or components through the following specific interfaces:

- **Contactless**: only Calypso Revision 3 APDUs are exchanged on the contactless (NFC) link of the phone. Some of the Calypso APDUs are not supported for a Calypso HCE Application, and a few APDUs are modified.

- **Server**: specific cryptograms and related data exchanged with a server (and its Authorization Module) are defined in the present specification for secure procurement of activation data (certified public key, Calypso serial number), pre-personalization data
(Debit Key) or personalization data. In the Calypso HCE system several kinds of servers may be defined depending on their functions, for example an Activation Server for registration and identification, and a Security Server for pre-personalization and personalization.

- **Android application**: the host Android application may exchange information with its Calypso HCE applications, for example to read some files, to manage the user interface, for administration (instantiation, deletion, etc.), or as a proxy with an HCE activation system. These exchanges are not in the scope of the present specification.

- **Other**: any other exchanges (e.g. procurement of the CA Public Key, error management) are not in the scope of the present specification.

### 1.5 References

Portable Object Application – Calypso Specification Rev.3 – Version 3.2 060708-CalypsoApplication

Calypso Specification for a Portable Object Application, here called “Calypso card application”.

Calypso Application applied to Host Card Emulation 141113-CalypsoHCEApplication

Specifications of the Calypso HCE applications.

Calypso Specification – HCE Guidelines 150422-CalypsoHCEGuidelines

Best practices for an efficient and secure implementation of a Calypso HCE systems.

Calypso Technical Note #001 CalypsoTN001-StartupInfo

Definition and registry for Platform and Manufacturer ID bytes of Startup Information field.

android.nfc.cardemulation


Android Host Card Emulation (HCE) API specification.

Android Keystore System https://developer.android.com/training/articles/keystore.html

Android Key Store (AKS) description.

Hardware Credential Storage

https://developer.android.com/about/versions/android-4.3#HardwareKeyChain

Description of the introduction of Hardware Credential Storage (HCS) in Android.

PKCS #1 v2.2: RSA Cryptography Standard


Specification of RSA algorithms.
2 DATA ORGANIZATION

Calypso HCE applications manage file structures exactly as Calypso card applications. An Android application may contain several Calypso HCE applications (e.g. a Calypso application for public transport and a Calypso Stored Value application).

2.1 HCE Persistent Data

The persistent data used by Calypso HCE applications are presented below in two tables, for data also used by Calypso card applications and for data specific to Calypso HCE applications.

Calypso HCE applications persistent data also used by Calypso card applications:

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AID</td>
<td>Application identifier, as defined in Calypso card application specifications.</td>
</tr>
<tr>
<td>Calypso serial number</td>
<td>Calypso serial number, as returned by the Select Application command.</td>
</tr>
<tr>
<td></td>
<td>For Calypso HCE applications, the Calypso serial number is made of two parts:</td>
</tr>
<tr>
<td></td>
<td>SN Header: 2 first bytes (leftmost, most significant).</td>
</tr>
<tr>
<td></td>
<td>SN Value: 6 last bytes (rightmost, least significant).</td>
</tr>
<tr>
<td></td>
<td>Only SN Value is significant to identify the application. The full Calypso serial number is used only for cryptographic operations. Calypso serial numbers are provided by an HCE Authorization Modules.</td>
</tr>
<tr>
<td>Debit Key</td>
<td>Triple-DES key used to secure Calypso validations. Optionally, it may also be an AES key. A Debit Key value is provided by an HCE Authorization Module.</td>
</tr>
<tr>
<td>File structure</td>
<td>Dedicated file (DF) of the application(^1), and its files (EF).</td>
</tr>
<tr>
<td></td>
<td>Each Calypso HCE application has a file structure, as defined in Calypso Revision 3.</td>
</tr>
</tbody>
</table>

Persistent data specific to Calypso HCE applications, related to public keys management:

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Public Key</td>
<td>RSA public key of the certification authority trusted to authenticate other public keys. This key is implicitly trusted (i.e. not provided in a public key certificate).</td>
</tr>
</tbody>
</table>

\(^1\) The Application Subtype byte of the Startup Information returned by the Select Application command is also data of the file structure.
PO Key Pair  Asymmetric key pair generated, stored and used by the Android device (initially from the Android Key Store). Authenticates a Calypso HCE application.

AM Key Certificates  Certificate containing the RSA public key of the Authorization Module. Its signature is verified with the CA Public Key.

PO Key Certificate  Certificate containing the PO Public Key of the Calypso HCE application. Its signature is verified with the RSA public key embedded in the RAM Key Certificate.

ISN Certificate  Cryptogram containing the SN Value and the RSA public key of the Calypso HCE application. Its signature is verified with the RSA public key embedded in the AM Key Certificate.

The diagram below shows the authenticity verification chain, for all kinds of certificate and authenticator:
3 CALYPSO FUNCTIONALITY

3.1 Calypso HCE Security

3.1.1 Risk Mitigation
As any Android application, Calypso HCE applications themselves are not physical secure containers. Therefore, it is not possible to ensure the security of information stored in a Calypso HCE application as well as in microprocessor smart card components.

However, Calypso defines mechanisms allowing to build a system significantly mitigating the risk of fraud while preserving as much as possible compatibility with existing Calypso terminals.

3.1.2 Functional Requirements
Calypso HCE applications are intended to be used as normal Calypso card applications through the contactless NFC interface for validation and control operations.

For example, the following operations are possible using the NFC interface of the phone, with performances as good as possible:

- validation on entrance,
- control during the travel.

Personalization and Loading
For security reasons, personalization and load transactions are not possible through the NFC interface, and must be done with a secure connection to a server, using a dedicated public key infrastructure.

This applies for example to the loading of transportation rights, which cannot be performed with contactless transactions and must therefore be performed on-line with a server.

3.1.3 Android Security Features
Android applications are cryptographically signed by their provider so that only applications with a correct signature may be installed on a phone.

Android executes applications in sandboxed environments, so that data of each application are isolated from others (unless an application explicitly chooses to share some of its data).

Android also provides tools to manage secure communication (e.g. TLS and HTTPS protocols) and to manage cryptography. Among these tools, the present specification relies on the Android Key Store (AKS) and on the Hardware Credential Storage (HCS).

3.1.4 Android Key Store (AKS) and Hardware Credential Storage (HCS)
The Android Key Store (AKS) is a cryptographic storage and computation toolbox, currently supporting only RSA keys.

For Calypso HCE applications, it is used to:

- generate and store RSA key pairs,
- produce signatures using an RSA private key,
- decrypt using the RSA private key.

The AKS is implemented in Android with some software protection mechanisms, making it somewhat difficult for defrauders to retrieve private keys.

---

2 Not by Google or any other trusted third party.
3 Unless the phone user has disabled this verification.
To improve this protection, most NFC Android phones implement the AKS in a secure element called the Hardware Credential Storage (HCS). When HCS is available, it is always used by the AKS.

### 3.1.5 Calypso HCE Security Overview

For contactless transactions, Calypso HCE applications contain only the Debit Key of a Calypso card application. It must be a Triple-DES key, or optionally an AES key. The value of this key results from the derivation (diversification) of a master key with the Calypso serial number of the application.

As for any Calypso application, a Calypso HCE application has a unique serial number. For security reasons, the serial numbers of Calypso HCE application are specifically identified by having their 4th byte equal to or above 80h (e.g. 0000009876543210h).

Furthermore, to allow changing the value of a diversified Debit Key without changing the master key, only the last 6 bytes of the serial number (SN Value part) are significant for identification of the phone application. The full Calypso serial number (including the SN Header part) is used only for cryptographic operations (e.g. diversification with a SAM or Authorization Module).

To manage the security of other operations (e.g. installation, activation, remote loading of personalization data or of rights), a Calypso HCE application uses an RSA key pair (the PO Key Pair), provided by the AKS.

This PO Key Pair is certified by a certification authority, which provides a certificate of the application’s public key, the *PO Key Certificate* (which procurement process is out of scope).

---

4 Six last (rightmost, least significant) bytes.
5 Two first (leftmost, most significant) bytes.
This certificate is authenticated with the public key of a certification authority, the *CA Public Key*, provided previously to the application (procurement process also out of scope).

Calypso HCE applications cannot be used through the NFC interface until their activation is successfully completed.

**Calypso Secure Session Management by Terminals**

Since all operations on the NFC interface are secured with a standard Calypso TDES key, Calypso HCE applications are usable without modification of terminals which:

- support Calypso sessions with TDES keys (i.e. each *Digest Update* command of the SAM contains only one card APDU),
- have a SAM containing TDES master debit keys,
- can manage Calypso portable objects in ISO/IEC 14443 Type B and Type A.

When supported by the Calypso HCE application and by the Calypso SAM, a Calypso AES key may also be used.

A real test with mobile phones and the specific terminals involved should be performed to confirm such compatibility.

### 3.1.6 Recommendations for Personalization and Loading

**Security Mechanism**

To load initial data or to load rights (e.g. transportation rights) in Calypso HCE applications, it is recommended to use a dedicated PKI mechanism and to rely not only on SSL/TLS and derived protocols like HTTPS.

Such dedicated mechanism may for example use the CA Public Keys and PO Key Pair defined in the Calypso HCE application specification.

**Rights Renewal**

It is recommended to load in Calypso HCE application only data having a short lifespan (e.g. a few days or even less), and, if no fraud is detected, to renew them as often as possible using a server and attaching cryptographic authenticators to the data.

The end of life conditions should be included in the data and taken into account in the authentication process, ensuring that the data are not out of date.

For example, the rights (contracts) may be authenticated with a MAC verified by the contactless terminals (e.g. validation, control), the value of this MAC depending on the full Calypso serial number (SN Header included), so that the contract data are not valid anymore if not renewed at the same time as the Debit Key.

Note that the SN Header allows up to two renewals of the Debit Key each day, if the remote loading infrastructure allows it.
3.2 Summary of the Calypso Commands

Below is the list of the Calypso card application commands which are managed by Calypso HCE applications.

File level commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>Selects the indicated application or file</td>
</tr>
<tr>
<td>Invalidate</td>
<td>Invalidates the application</td>
</tr>
</tbody>
</table>

Data object handling commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Data</td>
<td>Reads a data object (AID, EF list)</td>
</tr>
</tbody>
</table>

Data access commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Binary</td>
<td>Reads data from a Binary file</td>
</tr>
<tr>
<td>Read Records</td>
<td>Reads one or more records of a file</td>
</tr>
<tr>
<td>Read Record Multiple</td>
<td>Reads parts of one or more records of a file</td>
</tr>
<tr>
<td>Search Record Multiple</td>
<td>Searches in one or more records of a file</td>
</tr>
<tr>
<td>Append Record</td>
<td>Appends a new record to a Cyclic file, erasing the oldest record of the file</td>
</tr>
<tr>
<td>Update Binary</td>
<td>Writes data in a Binary file, replacing the existing one</td>
</tr>
<tr>
<td>Update Record</td>
<td>Writes data in a file record, replacing the existing one</td>
</tr>
<tr>
<td>Write Binary</td>
<td>Writes data over a Binary file (OR operation with the existing data)</td>
</tr>
<tr>
<td>Write Record</td>
<td>Writes data over a file record (OR operation with the existing data)</td>
</tr>
<tr>
<td>Decrease</td>
<td>Decreases the value of a file counter</td>
</tr>
<tr>
<td>Decrease Multiple</td>
<td>Decreases the value of one to many counters</td>
</tr>
<tr>
<td>Increase</td>
<td>Increases the value of a file counter</td>
</tr>
<tr>
<td>Increase Multiple</td>
<td>Increases the value of one to many counters</td>
</tr>
</tbody>
</table>

Security related commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Secure Session</td>
<td>Opens a secure session (contactless link only)</td>
</tr>
<tr>
<td>Close Secure Session</td>
<td>Closes a secure session (contactless link only)</td>
</tr>
<tr>
<td>Get Challenge</td>
<td>Read the Transaction Counter</td>
</tr>
</tbody>
</table>

Stored Value commands (optional):

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SV Debit</td>
<td>Debits the stored value</td>
</tr>
<tr>
<td>SV Get</td>
<td>Initializes a stored value operation (reload, debit, un-debit)</td>
</tr>
<tr>
<td>SV Undebit</td>
<td>Reloads the stored value by the amount of the last debit</td>
</tr>
<tr>
<td>SV Reload</td>
<td>Reloads the stored value by any amount (server link only)</td>
</tr>
</tbody>
</table>

The following commands are not supported by Calypso HCE Applications: Get Response, Put Data, Manage Secure Session, Change Key, Change PIN and Verify PIN.
## 4.1 Life Cycle

A possible life cycle of a Calypso HCE application is described below:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Operations</th>
</tr>
</thead>
</table>
| 1 Installation | **1.1 Load**  
Android application loading in the phone  
CA Public Key procurement |
|            | **1.2 Registration**  
PO Key Pair generation  
PO Key Certificate procurement (PO Key Pair authentication) |
| 2 Activation | **2.1 Instantiation**  
Calypso HCE application AID assignment  
Calypso HCE application configuration (file structure, Startup Information, etc.) |
|            | **2.2 Identification**  
Calypso serial number procurement (if not already available in the Android application) |
|            | **2.3 Pre-Personalization**  
Debit Key procurement (initial or renewal) |
| 3 Personalization | Initial data writing  
Usage rights writing |
| 4 Normal use | Daily use with contactless terminals (validation and control) |
| 5 End of life | Invalidation, deletion |
The following diagram describes a possible life cycle for an Android application which contains only one Calypso HCE application, of predefined configuration (AID, Startup Information and file structure) so that Phase 2.1 is implicit, where Phase 2.2 and Phase 2.3 occur simultaneously:
The following diagram describes a possible life cycle for an Android application behaving as a container of several Calypso HCE applications, where Phase 2.2 occurs before Phase 2.1:
4.2 Application Identifier (AID)

A Calypso HCE application is selected using its AID in a Select Application command, as for any Calypso application. However, unlike smart card applications, several HCE applications in the same phone may have the same AID (the choice being made for example by the user).

With an Android NFC phone in card emulation mode, if several NFC applications share the same AID (e.g. two HCE applications, or an HCE application and an application of the UICC), when the phone receives on the NFC interface a Select Application command with such conflicting AID if notifies automatically the user, who may choose the application to select.

To avoid such situation, it is strongly recommended to ensure that several Calypso applications are not selectable on the contactless interface with the same AID at the same time.

4.3 Calypso PIN

Calypso HCE applications do not support the Calypso PIN.

4.4 Calypso Stored Value

Stored Value support is optional for Calypso HCE applications, as for Calypso card applications (its availability being indicated by Application Type).
5 SECURITY MECHANISMS OVERVIEW

5.1 Overview

The goals of the Calypso HCE specification are:

- allow the largest possible compatibility with existing terminals (for debit, validation and control),
- preserve intact the security of existing Calypso applications (non HCE),
- reach the best possible security level for HCE, considering the limitation of the Android platform.

To achieve these goals, Calypso HCE applications use only the TDES (or AES, if supported) algorithm for contactless operations, with **only the debit key** of Calypso card applications. There is no change required to existing SAMs and to the software management of the fare offer and back office applications\(^8\).

**Android Security for Cryptographic Operations**

The Android operating system provides a secure environment for RSA key pairs, the **Android Key Store** (AKS).

Android ensures that it is difficult to extract private keys from the AKS. For additional security, it is recommended to use phones supporting the **Hardware Credential Storage** (HCS).

A secure environment (software, and possibly hardware when HCS is available) is provided by Android for AES symmetric keys only since Android 6.0, but not for TDES symmetric keys, and also not for Calypso files data protected with these keys (either AES or TDES).

The purpose of asymmetric cryptography for Calypso HCE applications is to compensate as much as possible for the lack of physical security for symmetric keys and for Calypso files data.

**Public Key Infrastructure (PKI)**

Public key infrastructures (PKI) are based on a series of certificates successively entrusting public keys, from an initial public key implicitly trusted, and until the public key used to protect sensitive information.

A certificate is the association of some data and a signature authenticating them. The signature is verified with a trusted public key.

When the data include a public key, the trust put in the authenticating key is transferred to the authenticated key\(^9\).

Such PKI is used to protect the transmission of a Calypso symmetric key (Debit Key) and a Calypso serial number from a physically secure device (Authorization Module) to a Calypso HCE application. This process is the application activation, described in the following sections.

5.2 Application Activation

Calypso HCE application activation takes place when the application is in Phase 2 of its life cycle. During Phase 1, the AKS provided access to a PO Key Pair which was signed by a certification authority. This PO Key Pair may be shared by several Calypso HCE applications of the same phone.

---

\(^8\) Assuming that the SAM contains TDES or AES keys and that the terminal already supports Calypso sessions with these keys, the only change required is to manage the validity end date in the serial number.

\(^9\) Providing that the data also contain an indication that the trust is allowed to be transferred.
Processing Phase 2 and entering Phase 3 is the Calypso HCE application activation: getting a Calypso serial number and a Debit Key, provided by an Authorization Module.

Once entering Phase 3, Calypso HCE applications may operate on the NFC interface.

Afterward, it is possible to repeat pre-personalization (Phase 2.3) to renew the Debit Key.

The exchanges between the Authorization Module and the Android application hosting the Calypso HCE application are secured end-to-end (e.g. HTTPS protocol for exchanges between Android application and HCE activation system, and Authorization Module in the same physically secured location as the HCE activation system).

5.3 **Cryptographic Keys**

In the PKI for Calypso HCE applications:

- **The CA Public Key** is used to authenticate AM Public Keys. It is implicitly trusted. All Calypso HCE applications and Authorization Modules use this public key.
- **AM Public Keys** are used to verify all signatures generated by Authorization Modules. Each Authorization Module contains its own AM Public Key.
- **PO Public Keys** are used to verify all signatures generated by Calypso HCE applications. Each Calypso HCE application uses one PO Public Key, contained in the host Android application, and possibly shared with other Calypso HCE applications within the same Android application.

The certification authority provides its CA Public Key to Calypso HCE applications by a trusted mechanism.

Each Calypso HCE application also contains one TDES key (or AES if supported), the Debit Key, to manage contactless transactions with the Calypso secure session mechanism (as defined in the Calypso card application specification). It is provided to the application under control of the PKI keys.
6 ANNEX

Glossary

AKS  Android Key Store. Custom Java Security Provider in the KeyStore facility which allows generating and saving private keys that may be seen and used only by a specific app.

Authorization Module  Physically secure device providing PO Key Certificates, Calypso serial numbers and Debit Keys to Calypso HCE applications.

HCE  Host Card Emulation.

HCS  Hardware Credential Storage. Android feature providing more security by making cryptographic private keys unavailable for extraction, also called hardware-backed key store (HBK).

RSA  Prevalent asymmetric cryptographic algorithm, based on factorization of large prime numbers. Also known as “PKCS #1” (IETF RFC 3447 v2.2).

SHA-256  Standard hash algorithm (FIPS PUB 180-4) providing a 256-byte hash.