Calypso Networks Association

# Official bulletin

12 March 2018

## HCE security principles in a Calypso environment


As the guarantor of the security and integrity of systems that use Calypso technology, CNA published the final version of the specification of a Calypso HCE application based on several pre-requisites:

1. **being compatible with the Calypso 3.1 command set,**
2. **being compatible with existing ticketing systems without requiring major evolutions of legacy equipment,**
3. **guaranteeing a security level on par with the current Calypso systems,**
4. **guaranteeing a reasonable level of security when compared with state-of-the-art Calypso security.**

To complement these specifications, CNA published an implementation guide, Calypso HCE guidelines, that describes the Calypso HCE ecosystem and prescribes security countermeasures that should be implemented. This guide is derived from recommendations from a security audit commissioned by AFIMB, the French agency for multimodal information and ticketing, and carried out by an independent expert from the Mines-Télécom Institute.

Unlike hardware secure components such as chip cards, SIM cards and eSEs, which are designed to protect data over a long period of time, a mobile phone HCE application is hosted on a purely software environment and therefore can only offer protection for a limited amount of time. It features intrinsic weaknesses that require security countermeasures to be implemented in a back-office system.

Calypso
Networks Association

**Hence, Calypso HCE guidelines define the following security requirements:**

- Calypso HCE applications must use a specific range of serial numbers on eight bytes: Six bytes are reserved for uniquely identifying the application and two bytes for the validity date, the whole eight bytes being used for cryptographic operations, in particular for diversifying the debit key.
- Once the validity date of the serial number and hence of the debit key have expired, these elements must be renewed through the HCE server. The maximum validity duration of the HCE application serial number is three days.
- Sensitive data such as transport products must be signed by including the eight byte serial number in the signature in order to connect the validity of these data to that of the serial number. So, a long-term contract must be signed as often as is required by the above mechanism in order to remain valid.

To be entitled to the Calypso brand, any rollout of an HCE solution must comply with the sets of prescriptions from these two documents, in particular with the security countermeasures described above.

Besides, the Calypso HCE application processing software of ticketing terminals must, among other things:

- implement version 3.1 of the Calypso specifications,
- recognise an HCE-specific Calypso serial number and be able to interpret its validity date in order to discard HCE applications that use an expired serial number,
- function only with SAMs that implement TDES and the signing function (using the associated signature keys),
- check the validity of the transport contract data signature.

Download the **Calypso HCE functional specifications**

Download the **Calypso HCE guidelines, revision 1.0***

* *for CNA members only*

**Philippe Vappereau**
Chairman, Calypso Networks Association