HCE Security issues

*A “Security” study with Mines Telecom Paris, led jointly by CNA and AFIMB, the French Ticketing Governmental Association.*

As the representative of the security and integrity of Calypso based ticketing systems, CNA has written and published the specification for a Calypso HCE application, based on several prerequisites:

1. Be compatible with the Calypso transaction dynamic
2. Work with existing ticketing infrastructures without occurring major changes on field equipment’s
3. Avoid jeopardizing the security of Calypso systems already in use.

Unlike a smartcard or UICC card, it is possible to clone, reverse data to an earlier state, and modify data stored in a portable object in an HCE application, which involve a lack of security.

However mobile phones are connected objects, allowing risk diminution by regular connections to a remote system, responsible for overseeing the security of deployed applications.

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

Furthermore, in case where the device is rooted, the possibility to modify every data applications will make mandatory the protection of valuable data integrity with a data signature mechanism.

The description of those techniques, which could impact the evolution of existing infrastructures, will be part of a mandatory supplement to the specification and will be defined in another document currently in construction, the Calypso HCE Guidelines, which will also specify the minimum security requirements for the use of the Calypso trademark.

As the Calypso HCE Guidelines are not published yet, the specification Calypso HCE application shall be considered as experimental, and dedicated for pilot projects. The feedback of pilot projects launched by CNA members will provide inputs to the Guidelines in a refining process necessary for a not yet mature environment.

In parallel and with the support of CNA, the AFIMB, the French agency for multimodal information and smart-ticketing, linked with the French Ministry of Ecology, Sustainable Development and Energy, has launched on December 7th 2016 a survey from an academic independent expert, M. Pascal Urien; teacher and researcher from Mines-Telecom Paris Institute, about the security of HCE, with a focus on the Calypso implementation on HCE.

The final report of that study should be available mid-2017 and will be one of the main inputs of the Calypso HCE Guidelines.