Calypso Networks Association

www.calypsonet-asso.org

2014-10-27

« Calypso Secure » argument

Calypso security, to protect operators and customers.

Calypso security principles have been defined in order to protect not only transport operators and authorities, but also the customers.

Other ticketing solutions often only focus on security from the operator's point of view, in order to avoid any counterfeiting of cards. Calypso also targets the protection of the customers by ensuring that no counterfeit terminals can transact with their cards, which makes electronic pickpocketing impossible.

For this, Calypso security principles guarantee, in all ticketing transactions, both authentication of the card (more generally of the customer medium) and authentication of the terminal.

Calypso security, for what goals?

Calypso security is designed to answer to the following main requirements which allow defining the fair level at the fair cost:

- To guarantee the impossibility of counterfeiting transport rights which may represent values of several thousand euros.
- To allow multiservice applications and particularly implementation of electronic purse, with the agreement of financial institutes.
- To allow a "distance reloading" of a card (more generally a customer medium), on Internet, on mobile phones, etc.
- To guarantee the customer the confidentiality of his data, and for retailing on Internet or mobile phones, the authenticity of the transaction.

Calypso security management by CNA

Security is a concern in each moment in the life cycle of a ticketing system, not only at its launching.

Security of a ticketing scheme like Calypso doesn’t require static management, but a dynamic one.

All the hackings of existing ticketing technologies are not the consequence from the initial level of security at their creation, but are due to a lack of a roadmap of security improvements in their life cycle. A security certification (as the EAL classification) is of no interest if it is not linked to a period of time.

Recent successful hacking of a well-known ticketing technology is clearly the result of a total lack, from the manufacturer, of evolution of the mechanisms of security for at least ten years. But the ones facing, on the field, the financial and image consequences are the operators and transport authorities, with no possible influence on the manufacturer policy.

Calypso has implemented a completely different paradigm, in order to not depend on the good willingness of manufacturers to improve their security solutions: to put the security policy in the hands of the community of transport operators and authorities which constitutes Calypso. Two main principles, based on the independence of the hardware and software solutions, are leading this policy:

- To use the best existing technological platforms (i.e. hardware components from IC manufacturers) to implement Calypso software. These platforms are those issued by these manufacturers to answer the needs of the bank sector, with the regular evolutions imposed by this sector, which guarantees always benefiting from the best secured hardware.
- To manage software evolutions under the responsibility of the Calypso community, represented by its Board and operationally ensured by a dedicated working group regrouping the best experts in this matter.

Consequently, from its origin in 2000, there have been 4 major evolutions in the Calypso software security and no hacking of Calypso has been reported.

Remark: the migration of a security step of Calypso remains under the responsibility of the operator or transport authority which has issued the ticketing system (new software version and/or new hardware platform), but Calypso always ensures the availability of solutions at the best level of security.

Calypso security technical implementation

The main technical issues of Calypso security are:

- Exclusive use of microprocessor components as hardware platform for cards and all portable objects.

- Exchanges of secure data exclusively between microprocessor components, customer media from one side, secure modules in the terminal from the other side.
- Use of standardized cryptography for the exchanges of data and the calculation ensured by the microprocessor components, 3DES and AES today, DES at the origin of Calypso, intermediate step with DESX,.
- Specific keys used by the cryptography mechanisms (3DES, AES …) for each function of a ticketing scheme: personalization, loading, validation), for each application area.
- Diversification of the keys for each card or customer medium, so that the hacking of a key in one card does not compromise the security of the system.

All these security mechanisms are completely integrated in the transaction scheme in coherence with the **session/ratification** protocol invented by Calypso in order to ensure the stable state of the card, even if the customer removes his card from the electromagnetic field before the completion of the transaction.