

ABSTRACT

Method for generating cryptographic half-keys, and associated system

The present invention relates to a method for generating cryptographic half-keys. The method makes it possible to generate n pairs (K_1^i, K_2^i) , $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs making it possible to reconstruct an access key K_{PL} specific to a secure apparatus, said method comprising at least the following steps:

- generating (202) and storing, with the help of a management center distinct from said apparatus, a first series (217) of n half-keys K_1^i on a recording medium (213);
- 10 - supplying (203) the apparatus with said recording medium (213) so as to generate, with the help of said local key K_{PL} and of the n half-keys K_1^i stored on said medium, a second series of n half-keys K_2^i making it possible to form said n pairs (K_1^i, K_2^i) .

The invention applies notably to the creation of several keys for access to a secure apparatus.

Figure 2 to be published.



162162



G00002