

ABSTRACT

The objective of the present invention is to propose a method that guarantees the encryption of the exchanged data a security module and a user unit by a pairing key specific to the couple user unit/security module, and at the same time leaving
5 the possibility for the security module to be paired with other user units.

According to the invention, this objective is achieved by a method consisting in:

- detecting by the user unit if the connected security module is paired with it,
- if it is so, using a unique pairing key specific to the couple user unit/security module to encrypt the exchanged data,
- 10 - if it is not so, requesting the operating centre the authorisation to pair with this security module, a request accompanied by the identifications of the user unit and the security module,
- verifying by the operating centre the conformity of this pairing request and transmitting the result to the user unit,
- 15 - if the authorisation is given, establishing a paring key unique to the couple user unit/security module to encrypt the exchanged data.



G00002



I62162