

ABSTRACT**Method for verifying the password of a dongle, associated computer program, dongle and user terminal**

A method for verifying the password of a dongle (30) storing the encrypted confidentially only CHIFF_CST_dongle_i of a first constant CST_dongle_i using a first symmetric key Ksym_i cryptographically derived from the password of the dongle, the memory (32) of the dongle (30) further storing the symmetric key obtaining function DERIVE_Ksym(;): comprising:

- determining a second symmetric key Ksym_i' by applying the said function DERIVE_Ksym(;) for obtaining a symmetric key to a password to be validated received;
- obtaining a second constant CST_dongle_i' by decrypting CHIFF_CST_dongle_i using the determined second symmetric key; and
- delivery by the dongle of a datum determined according to the second constant CST_dongle_i' to the user terminal, in order for the latter to validate the password entered according to the said data and the first constant.

Figure for the abstract: figure 1