

VALIDATING AN AUTHENTICATION CHIP USING A SECRET KEY

ABSTRACT

A method for validating the existence of an untrusted authentication chip, the method includes the steps of: generating a secret random number and calculating a signature for the random number using a signature function, in a trusted authentication chip; encrypting the random number and the signature using a symmetric encryption function using a first secret key, in the trusted authentication chip; passing the encrypted random number and signature from the trusted authentication chip to an untrusted authentication chip; decrypting the encrypted random number and signature with a symmetric decryption function using the first secret key, in the untrusted authentication chip; calculating a signature for the decrypted random number using the signature function in the untrusted authentication chip; comparing the signature calculated in the untrusted authentication chip with the signature decrypted; in the event that the two signatures match, encrypting the decrypted random number together with a data message read from the untrusted chip by the symmetric encryption function using a second secret key and returning it together with the data message to the trusted authentication chip; encrypting the random number together with the data message by the symmetric encryption function using the second secret key, in the trusted authentication chip; comparing the two versions of the random number encrypted together with the data message using the second key, in the trusted authentication chip; in the event that the two versions match, considering the untrusted authentication chip and the data message to be valid; otherwise, considering the untrusted authentication chip and the data message to be invalid.

Fig. 18