12 AUG 2004

ABSTRACT

This invention concerns a consumable authentication protocol for validating the existence of an untrusted authentication chip, as well as ensuring that the authentication chip lasts only as long as the consumable. In a further aspect it concerns a consumable authentication system for the protocol. A trusted authentication chip has a test function; and the untrusted authentication chip has a read function to test data from the trusted chip, including a random number and its signature, encrypted using a first key, by comparing the decrypted signature with a signature calculated from the decrypted random number. In the event that the two signatures match, it returns a data message and an encrypted version of the data message in combination with the random number, encrypted using the second key. The test function operates to encrypt the random number together with the data message using a second secret key, compare the two versions of the random number encrypted together with the data message using the second key. Iin the event that the two versions match, the untrusted authentication chip and the data message are considered to be valid; otherwise, they are considered to be invalid.

Fig. 8



162162



G00001