AUTH06

12 AUG 2004

ABSTRACT

This invention is a validation protocol for determining whether an untrusted authentication chip is valid, or not. In another aspect it concerns a validation system for the protocol. The protocol may be used to determine the physical presence of a valid authentication chip. In this case a system may call the trusted chip to generate a random number and a digital signature for it, encrypt them with a first key and then call a prove function in the untrusted chip. The prove function decrypts the random number and signature, and calculates another signature from the decrypted random number, for comparison with the decrypted one. If the comparison is successful the random number is encrypted with another key and sent back. Finally, a test function is called in the trusted chip to generate its own encrypted version of the random number using the second key and then compare it with the received version to validate the untrusted chip. The untrusted chip may be associated with a consumable so that validation of the untrusted chip authenticates the consumable.

Fig. 5



162162



G00001