

13 AUG 2004

ABSTRACT

The invention is a method and system in which an authentication chip having secret information stored within it, including secret data stored in multi-level flash memory, is protected from unauthorised
5 modification of values stored in the flash memory. The secret information is stored using an internal command and can only be accessed by one or more further commands. Secret data in the information is stored in intermediate states of the multi-level flash memory between the minimum and maximum voltage level states. A validity check is performed on secret data items before allowing them to be read out by a command accessing them. The validity check involves calculation of a checksum and comparison of the result with a
10 checksum stored using the internal command as part of the secret information.

Fig. 18



162162



G00001