Abstract

Memory cards are cheap and contain memory means, but can be forged and duplicated easily. Smart-cards contain also a microprocessor and can be used for cryptographic purposes, but are much more expensive.
The plastic support (14) of the card contains randomly distributed ferrite particles (11) (eg. small steel marbles, introduced into the plastic paste during the melting process). This random distribution of the particles is assumed to be impossible to control or influence during the process of fabrication. For personalizing a card, the issuing authority scans the plastic support of the card with a magnetic inductance detector, thereby reading the emplacement of the ferrite particles as a number p. Then the authority computes s = SIG(ID,p), where "SIG" denotes any secure public-key digital signature algorithm and ID the identification details of the card's owner. Finally, s and ID are recorded in the memory means (13) of the card. When such a card is inserted into a reader, the reader scans the plastic part of the card and reads the distribution characteristics as a number p. Then ID and s are retrieved from the card's memory means and the reader checks that s is the valid signature of {ID,p}

Fig. 1

This Sheet Has Been Replaced