

A method for certifying a running total in a reader.

ABSTRACT

5 At the time of the exchange of information
between an electronic purse and a reader, there is
transmitted (22), from the reader to the electronic
purse, the running total contained in the reader, a
certificate associated with this running total and a
10 public encryption key corresponding to a private key,
which is unknown, with which the certificate was
produced from the running total. In the smart card,
the certificate is decrypted (24) from the public key,
and it is verified (25) that the running total is
15 consistent. For a following transaction, there is
calculated (21) a new running total, and then a new
certificate (31), from a private key belonging to the
receiving card. Next there is sent (33), to the
reader, the new running total, the new certificate and
20 the public key corresponding to the card which has just
performed the operation. It is shown that, by acting
thus, there is no longer any need to store, in the
reader, a secure circuit for carrying out
certifications.

25

Figure 2

This Sheet Has Been Replaced

