ABSTRACT

In a service system distributed as, for example, pay-television, the information exchanged between the operating centre and the user modules uses cryptographic means to guarantee the authenticity and confidentiality of the data. The code processing needs of the operating centre are substantial. For this reason a cryptographic system is proposed that has modularity and security for the cryptographic operations by means of monolithic security units in the form of smart cards.

(Figure 2)



162162



G00002