ABSTRACT

MICROPROCESSOR CARD PAYMENT SYSTEM

The present invention is a system for implementing electronic payment with a tamper resistant microprocessor card. The microprocessor card generates joint digital signatures under a joint digital signature scheme which derives its secret signature key from secret values contributes by different parties such as user, bank and service provider of electronic commerce. The joint signature is used to certify the payment among other information. It follows that no one party has complete knowledge of the secret signature keys of the other parties; therefore, the use of joint digital signature in conjunction with a microprocessor card provides unprecedented security. The present invention also defines a protocol including payment, deposit, withdrawal and account opening in providing added protection against potential security attacks. Above all, the protocol also supports off-line payment transactions, thus allowing transaction to be conducted scalably and economically over various forms of electronic networks, including unsecured ones.

Figure 4.