IDENTIFICATION ALGORITHMS FOR PAYMENT CARDS

Boychenko O.V., Znamenskaya Y.A.

From the very beginning of the introduction of EC became apparent that the cardholder identification methods used in conventional transactions, are unsatisfactory for the EC transaction.

In the world of plastic cards with a magnetic strip most reliable way to protect transactions from fraud is to use the PIN-code to identify the card holder's bank-issuer.

Secret information, which has a card holder is PIN-code, appears a sequence consisting of 4-12 digits, known only to the cardholder and the issuing bank.

However, to date, is a problematic solution to the problem of the broadcasting the PIN-code is encrypted using an asymmetric cryptographic algorithm, a PIN-code is encrypted on a symmetric encryption algorithm technology standard Hardware Security Module.

There are other, non-classical decision on the use of PIN-code. For example, it is possible for a computer to encrypt cardholder's PIN-code and some dynamically changing from transaction to transaction data on key known only to the issuer and the cardholder.

Such an approach would require solving the problem of the distribution of secret keys, which is a very difficult task that makes sense for other, more effective, compared with the PIN-code verification, identification methods cardholder.

An alternative method is to check the PIN-code to enhance the security of transactions EC on the cards database (DB) are stored on the host processor STB CARD.

As a result, the technology verification PIN-code, adopted in the STB CARD, in fact, not only provides a dynamic client authentication, but also guarantees a 'through' the integrity of some of the data transaction (transaction amount, card number).

The analysis formed the basic requirements for a transaction schemes EC provides the necessary level of security:

1. Authentication of participants of purchase (the buyer, TA and its servicing bank). By authenticating the buyer (seller) is a procedure that proves (at the level of reliability of the known cryptographic algorithms) the fact that the owner of the card really is a client of a party of the issuer (the service of a member bank) of this payment system. Authentication service bank proves the fact that the Bank is a party to this payment system;

2. Details of the payment card (card number, expiration date, CVC2 / CVV2, and so on. N.), Used in carrying out the transaction EC, must be kept confidential for the TP;

3. The non-repudiation of transactions for all participants in the transaction EC, ie the presence of all participants conclusive evidence of the fact of purchase (or payment order).

Keywords: payment cards, identification, e-commerce, transaction security.