A METHOD AND SYSTEM FOR SECURELY AND AUTOMATICALLY DOWNLOADING A MASTER KEY IN A BANK CARD PAYMENT SYSTEM

Abstract

A method and system for securely and automatically downloading a master key TMK in a bank card payment system is disclosed, wherein the bank card payment system includes a Point Of Sale POS, a Terminal Management system TMS, a PIN PAD and a HSM. A pair of public and private keys are generated by the TMS invoking the HSM. The master key TMK is randomly generated by the POS terminal invoking the PIN PAD. The TMK is encrypted with the public key of the TMS, and the encrypted TMK is uploaded to the TMS. The TMK is decrypted with the private key by the TMS invoking the HSM, and the decrypted TMK is stored. According to the present invention, the TMK is randomly generated, and the process of transmission is not exposed, and thus the TMK plaintext will not be exposed outside the secure storage devices. The TMK remains encrypted with the public key during the entire process of transmission. The TMK cipher text will not be decrypted until it reaches the HSM of the TMS. Thus, the present invention is of high security level.

(Fig. 3)