METHOD AND DEVICE FOR SECURELY DISPLAYING DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a SG national application of PCT application No. PCT/CN2018/095186 filed on July 10, 2018, which claims priority to Chinese Patent Application No. 201710753841.3, filed on August 28, 2017 by Tendyron Corporation, titled "Method and Device for Securely Displaying Data".

TECHNICAL FIELD

The present disclosure relates to a field of security payment, and more particularly, to a method and device for securely displaying data.

BACKGROUND

With the rapid development of information technologies, online payment is popularized. However, there are many security risks in the online payment. For example, in a process of the payment using a mobile terminal, user transaction data is displayed on the screen to be confirmed by the user to implement the transaction. However, hackers may hijack a main processor (for example, CPU). When transaction data to be displayed is processed, tampered transaction data is sent to a security module of a mobile terminal for signature, and the user's original transaction data is sent to a display module for display. The user confirms the transaction data displayed by the display module, but the tampered data is signed by the security module. Therefore, the mobile terminal does not process the original transaction data, but the tampered transaction data. The data signed by the mobile terminal is not the data displayed on the screen (i.e., "what you see is not what you sign for"). That is, it is difficult to guarantee that the signed data is the transaction data displayed by the display module during the payment by the mobile terminal, which makes the online payment unsafe.

In the related art, in order to ensure the security of the online payment, a display screen of a KEY (USBKEY or audio KEY) connected to a terminal can be used to display the user's transaction data, and physical keys provided on the KEY can be used to confirm the transaction information. Since the attacker cannot hijack the CPU of the KEY and cannot tamper with the transaction data, the transaction data displayed on the KEY is the real transaction data, which guarantees "what you see is what you signed for". Although this method guarantees "what you