Title (en)

Method and device for enhancing manipulation-proof of critical data

Title (de)

Verfahren und Anordnung zur Erhöhung der Manipulationssicherheit von kritischen Daten

Title (fr)

Procédé et dispositif pour augmenter la protection contre la manipulation de données critiques

Publication

EP 0762337 A2 19970312 (DE)

Application

EP 96250191 A 19960906

Priority

- DE 19534527 A 19950908
- DE 19534529 A 19950908

Abstract (en)

The control unit (6) has a microprocessor or an OTP (one-time programmable) processor that has, in addition to CPU (6a), other units in common housing, forming the OTP ROM (6b), and OTP ROM (6c) and acting as a security unit against unauthorised manipulation. The first non-volatile memory (NVM 20) is an EEPROM, serving as a second line of defence against manipulation. There is also an external non-volatile memory (NUM 25) acting in the same way connected to the processor (6) through an input/output control module (4), particularly against taking information out.

Abstract (de)

Ein Verfahren zur Erhöhung der Manipulationssicherheit von kritischen Registerdaten umfaßt die Schritte: Laden eines Codewortes, eines Zeigers oder MAC's, welcher einem Codewortes zugeordnet ist, in einen ersten nichtflüchtigen Speicher (20 bzw. 25), der gegen Herausnahme und Manipulation abgesichert ist, Laden eines Codewortes oder eines mittels des Codewortes gebildeten MAC's in zweite die Postregisterdaten enthaltende zu schützende nichtflüchtige Speicher (NVM 5a, 5b), wobei das Codewort dem letzten Betriebszustand der Frankiermaschine zugeordnet ist, Gültigkeitsprüfung des Codewortes oder des mittels des Codewortes gebildeten MAC's mindestens zum Zeitpunkt des Einschaltens der Frankiermaschine und nachfolgend mindestens aufgrund einer Pseudozufallsfolge in Abständen, Ersetzen des alten Codewortes durch ein vorbestimmtes neues Codewort, wenn der Prozessor, nach Gültigkeitsprüfung die Gültigkeit des alten Codewortes oder oder die Gültigkeit des mittels des Codewortes gebildeten MAC's anerkennt oder, Blockierung der Frankiermaschine nach dem Zeitpunkt des Einschaltens der Frankiermaschine, wenn der Prozessor nach Gültigkeitsprüfung die Gültigkeit des alten Codewortes oder die Gültigkeit des mittels des Codewortes gebildeten MAC's aberkennt. <IMAGE>

IPC 1-7

G07B 17/04

IPC 8 full level

G07B 17/00 (2006.01)

CPC (source: EP US)

G07B 17/00362 (2013.01 - EP US); G07B 2017/00395 (2013.01 - EP US); G07B 2017/00403 (2013.01 - EP US); G07B 2017/00411 (2013.01 - EP US); G07B 2017/00427 (2013.01 - EP US)

Cited by

EP1811460A1; FR2758033A1; DE19755796B4

Designated contracting state (EPC)

CH DE FR GB IT LI

DOCDB simple family (publication)

EP 0762337 A2 19970312; **EP 0762337 A3 20000119**; US 5771348 A 19980623

DOCDB simple family (application)

EP 96250191 A 19960906; US 71109196 A 19960909