

Title (en)

Method for the secure distribution of security modules

Title (de)

Verfahren zur sicheren Distribution von Sicherheitsmodulen

Title (fr)

Procédé pour la distribution sécurisée de modules de sécurité

Publication

EP 1150256 A1 20011031 (DE)

Application

EP 01104610 A 20010223

Priority

DE 10020904 A 20000428

Abstract (en)

An initial marking is assigned to the packaged (8) security equipment, e.g. a franking machine (7). This is in the form of a label (9). A second marking is added at a handling point (2) and this is registered and identified before data can be loaded into the franking machine.

Abstract (de)

Die Erfindung betrifft ein Verfahren und ein Distributionssystem zur sicheren Distribution von Sicherheitsmodulen, insbesondere für Frankiermaschinen. Zum Schutz vor Manipulationen von Sicherheitsmodulen wird durch die Erfindung ein Verfahren und ein Distributionssystem geschaffen, bei dem unter allen Umständen, d. h. selbst bei umfassender Unterwanderung der kryptographischen Initialisierung am Produktionsort, gewährleistet wird, dass nur Geräte mit solchen Sicherheitsmodulen vom Kunden in Betrieb genommen werden können, deren Schlüssel nicht kompromittiert sind. Dazu ist erfindungsgemäß die Erzeugung und Überprüfung von Markierungen ggf. in Kombination mit Zertifikaten vorgesehen. Eine erste Markierung (9) der versandfertigen Verpackung (8) des Sicherheitsmoduls (7) erfolgt am Herstellerort (1) nach einer ersten kryptographischen Initialisierung, wobei die erste Markierung (9) vorzugsweise ein auf ein erstes Label gedruckter öffentlicher Schlüssel ist. Eine zweite Markierung (13) erfolgt in entfernt vom Herstellerort am Einfuhrpunkt (2) beim Registrieren der Verpackung (8) und ermöglicht eine Identifikation beim späteren Registrieren des Gerätes, ausgelöst von dem am Einsatzort befindlichen Benutzer (3) vor dem Laden von angeforderten Daten in die Frankiermaschine. <IMAGE>

IPC 1-7

G07B 17/00

IPC 8 full level

G07B 17/00 (2006.01)

CPC (source: EP US)

G07B 17/00733 (2013.01 - EP US); **G07B 2017/0087** (2013.01 - EP US); **G07B 2017/00967** (2013.01 - EP US)

Citation (search report)

- [A] EP 0948158 A2 19991006 - FRANCOTYP POSTALIA GMBH [DE]
- [A] EP 0735722 A2 19961002 - PITNEY BOWES INC [US]
- [A] WO 9857302 A1 19981217 - PITNEY BOWES INC [US], et al
- [A] "INFORMATION-BASED INDICIA PROGRAM (IBIP) PERFORMANCE CRITERIA FOR INFORMATION-BASED INDICIA AND SECURITY ARCHITECTURE FOR CLOSED IBI POSTAGE METERING SYSTEMS", INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION,XX,XX, 12 January 1999 (1999-01-12), pages COMPLETE, XP002138350

Cited by

CN104229243A; DE102007011309B4; DE102007011309A1; EP1967976A2

Designated contracting state (EPC)

CH DE FR GB IT LI

DOCDB simple family (publication)

EP 1150256 A1 20011031; **EP 1150256 B1 20070502**; DE 10020904 A1 20011108; DE 10020904 B4 20041209; DE 50112418 D1 20070614; US 2002046175 A1 20020418; US 6850912 B2 20050201

DOCDB simple family (application)

EP 01104610 A 20010223; DE 10020904 A 20000428; DE 50112418 T 20010223; US 84133501 A 20010424