9804440-7
IPOS COPY

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10	A1	(11) International Publication Number: WO 97/37331
		(43) International Publication Date: 9 October 1997 (09.10.97)

(21) International Application Number: PCT/EP97/01553

(22) International Filing Date: 25 March 1997 (25.03.97)

(30) Priority Data:
96200867.8 29 March 1996 (29.03.96) EP
(34) Countries for which the regional or international application was filed: NL et al.

(71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventor: DRUPSTEEN, Michel, Marco, Paul; Aert de Gelderlaan 36, NL-1816 NA Alkmaar (NL).

(74) Agent: BEITSMA, Gerhard, Romano; Koninklijke PTT Nederland N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

(81) Designated States: AU, BG, BR, CA, CN, CZ, EE, HU, IL, JP, KR, LT, LV, MX, NO, NZ, PL, RO, SG, SI, SK, TR, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD OF SECURELY LOADING COMMANDS IN A SMART CARD

(57) Abstract

The invention relates to a method of securely loading and validating commands (COM) in a smart card (SC). Especially in the case where application-specific commands are loaded by an application provider (AP), that is off-line with respect to the card issuer (CI), it must be ensured that the commands are valid. The invention provides a method involving the protection of the commands (COM) by means of authentication codes, these codes (MAC1, MAC2) being produced using two different keys: one key (K1) is stored by the card issuer (CI), the other (K2) by a trusted third party (TTP). A further authentication code (MAC3), produced using a key from a set of keys (K3*), may be utilized to selectively validate commands for individual applications (e.g. AP1, AP2).

