(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 138 320**
A3

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **84305480.0**

(22) Date of filing: **10.08.84**

(51) Int. Cl.⁴: **H 04 L 9/02**
G 06 F 15/30, G 07 F 7/10

(30) Priority: **02.09.83 US 529161**

(43) Date of publication of application:
24.04.85 Bulletin 85/17

(88) Date of deferred publication of search report: **19.02.86**

(84) Designated Contracting States:
DE FR GB SE

(71) Applicant: **VISA U.S.A. Inc.**
101 California Street
San Francisco California 94111(US)

(72) Inventor: **Campbell, Carl Merritt**
809 Malin Road
Newtown Square Pennsylvania 19073(US)

(74) Representative: **Jackson, David Spence et al,**
REDDIE & GROSE 16, Theobalds Road
London, WC1X 8PL(GB)

(54) **Cryptographic key management system.**

(57) A central host computer (20) is connected to a plurality of transaction card issuing institutions (e.g.banks) 24 and to a plurality of transaction terminals (22). The host (20) generates a master key which is distributed to all terminals (22), and generates a plurality of secondary keys, one for each issuer (24), each secondary key being generated by encryption of data identifying the respective issuer (24). The issuer (24) places the data identifying itself (BIN) on each card it issues. Also authorization information is encrypted under the respective secondary key and placed on the card. The authorization information can include anticounterfeiting digits or a personal identification number (PIN). When the card is applied to a transaction terminal (22), the encrypted information is read by the terminal, and also the respective secondary key is derived by the terminal (22) by encryption of the issuer identifying data (BIN) under the master key. The secondary Key thus derived is used by the terminal (22) to permit off-line analysis of the encrypted authorization information on the card by comparison with data entered manually at the terminal (22) by the card owner, and/or with non-encrypted data on the card.

EP 0 138 320 A3

J...

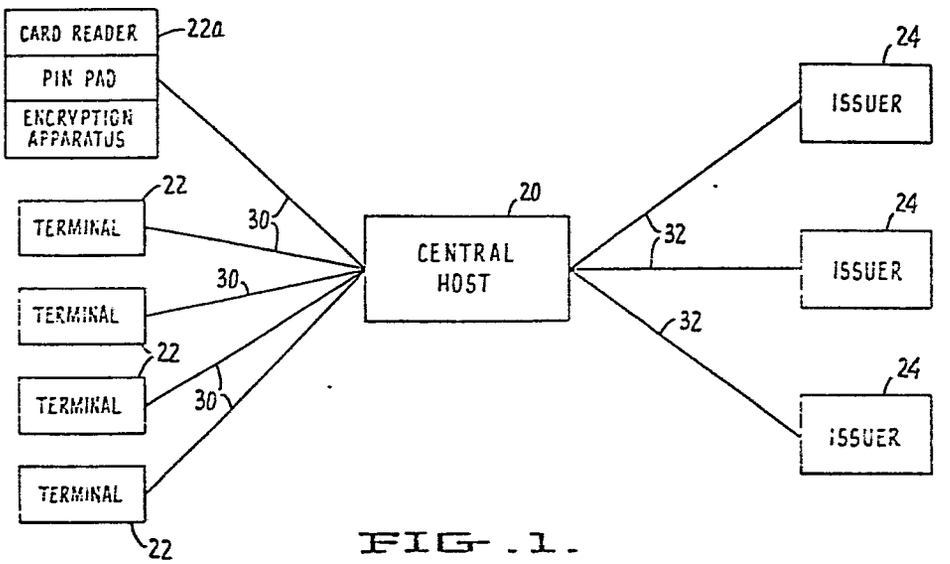
CARD READER
PIN PAD
ENCRYPTION APPARATUS
22a
TERMINAL
TERMINAL
TERMINAL
TERMINAL
22
22
22
30
30
30
CENTRAL HOST
20
32
32
ISSUER
ISSUER
ISSUER
24
24
24

FIG. 1.

European Patent Office

EUROPEAN SEARCH REPORT

0138320
Application number

DOCUMENTS CONSIDERED TO BE RELEVANT

EP 84305480.0

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int Cl 4)
	EP - A2 - 0 003 756 (INTERNATIONAL BUSINESS MACHINES) * Abstract; page 1, line 16 - page 5, line 31; page 7, line 19 - page 9, line 11; fig. 1 *	1,2,5,8	H 04 L 9/02 G 06 F 15/30 G 07 F 7/10
Y	WO - A1 - 81/02 655 (SENDROW) * Page 1, line 5 - page 7, line 29; page 8, line 18 - page 12, line 27; fig. 1,2 *	1,2,5,8	
A	EP - A1 - 0 068 805 (VISA) * Page 1, line 5 - page 7, line 2; page 11, line 32 - page 16, line 13; fig. 1 *	1,2,5,8	
			TECHNICAL FIELDS SEARCHED (Int Cl 4) H 04 L G 06 F G 07 F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	29-11-1985	HAJOS

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503 03 82