

Title (en)  
Cryptographic key management system.

Title (de)  
System zum Verteilen von kryptografischen Schlüsseln.

Title (fr)  
Système pour la répartition de clés cryptographiques.

Publication  
**EP 0138320 A2 19850424 (EN)**

Application  
**EP 84305480 A 19840810**

Priority  
US 52916183 A 19830902

Abstract (en)  
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.

IPC 1-7  
**H04L 9/02**; **G07F 7/10**

IPC 8 full level  
**G06Q 40/00** (2006.01); **G07D 1/00** (2006.01); **G07D 9/00** (2006.01); **G07F 7/10** (2006.01)

CPC (source: EP)  
**G07F 7/1016** (2013.01); **G07F 19/206** (2013.01)

Cited by  
US5796835A; EP2558997A4; EP0237815A3; EP0281057A3; EP0588339A3; FR2829332A1; CN1327361C; EP1443440A4; EP0595720A1; FR2697361A1; US2014279559A1; JP2016514328A; AU2014237800B2; US9947001B2; US7110986B1; FR2719925A1; US5729609A; AU692876B2; FR2600190A1; US6831982B1; WO0137478A3; WO9530976A1; US8019084B1; US8090663B1; US7328337B2; US8181018B2; US8683198B2; WO9859327A1; WO9410660A1

Designated contracting state (EPC)  
DE FR GB SE

DOCDB simple family (publication)  
**EP 0138320 A2 19850424**; **EP 0138320 A3 19860219**; **EP 0138320 B1 19890315**; DE 3477331 D1 19890420; JP S6061863 A 19850409

DOCDB simple family (application)  
**EP 84305480 A 19840810**; DE 3477331 T 19840810; JP 16873484 A 19840810