Title (en)

DATA VERIFICATION SYSTEM AND METHOD

Title (de)

DATENPRÜFSYSTEM UND -VERFAHREN

Title (fr)

SYSTEME ET PROCEDE DE VERIFICATION DE DONNEES

Publication

EP 0731941 A4 19990317 (EN)

Application

EP 95904152 A 19941129

Priority

- IL 10778993 A 19931129
- US 9413645 W 19941129

Abstract (en)

[origin: WO9514968A1] A system and method of verifying data (D) sent by a card having a private key (S) and identification number (ID). The method is independent of a challenge received from the interrogating terminal and the challenge input to the system public transformation (H) is replaced by data input. The input (ID) is transformed by system private transformation (T), by the verifying terminal, yielding a private key (S). The system public transformation (H) is executed on the data (D) and the private key (S) to result in a verification value (G). The verifying terminal then executes a reference transformation (TH) using the data (D) and the identification number (ID) which results in a reference value (G'). The value (G') obtained by the verifying terminal equals the value (G) if (ID) and (D) were genuinely submitted by the card that possesses (S) associated with (ID).

IPC 1-7

G06F 7/04; H04L 9/32

IPC 8 full level

G07F 7/10 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

G06Q 20/341 (2013.01); **G06Q 20/40975** (2013.01); **G07F 7/1008** (2013.01); **H04L 9/3247** (2013.01); **H04L 9/3271** (2013.01)

Citation (search report)

- [Y] EP 0292247 A2 19881123 - GEN ELECTRIC CO PLC [GB]
- [YA] EP 0427465 A2 19910515 - AMERICAN TELEPHONE & TELEGRAPH [US]
- [A] DE 4138861 A1 19921001 - SIEMENS NIXDORF INF SYST [DE]
- [A] US 5016274 A 19910514 - MICALI SILVIO [US], et al
- [A] EP 0077238 A1 19830420 - CII HONEYWELL BULL [FR]
- [A] EP 0037762 A1 19811014 - CII HONEYWELL BULL [FR]
- See references of WO 9514968A1

Designated contracting state (EPC)

AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)

WO 9514968 A1 19950601; EP 0731941 A1 19960918; EP 0731941 A4 19990317; IL 107789 A0 19950315

DOCDB simple family (application)

US 9413645 W 19941129; EP 95904152 A 19941129; IL 10778993 A 19931129