

Title (en)
A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

Title (de)
VERSCHLÜSSELUNGSVERFAHREN UND VORRICHTUNG DAFÜR

Title (fr)
PROCEDE DE CRYPTAGE ET APPAREIL ASSOCIE

Publication
EP 1129436 A1 20010905 (EN)

Application
EP 98954915 A 19981110

Priority
SG 9800088 W 19981110

Abstract (en)
[origin: WO0028493A1] A method of encryption for creating token bound output data from user data using a symmetric key capable token is disclosed, said method comprising the steps of providing the user data or a representation thereof as an input to a symmetric key operation supported by the token, retrieving the output of the symmetric key operation as the token signature; and combining the token signature with the user data to generate the token bound output data. Preferably the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

IPC 1-7
G07F 7/10; **G07C 9/00**

IPC 8 full level
G07F 7/10 (2006.01); **G07F 7/12** (2006.01)

CPC (source: EP)
G06Q 20/341 (2013.01); **G06Q 20/40145** (2013.01); **G06Q 20/40975** (2013.01); **G07F 7/08** (2013.01); **G07F 7/1008** (2013.01)

Citation (search report)
See references of WO 0028493A1

Designated contracting state (EPC)
DE FR GB

DOCDB simple family (publication)
WO 0028493 A1 20000518; **WO 0028493 A8 20010201**; AU 1184499 A 20000529; EP 1129436 A1 20010905

DOCDB simple family (application)
SG 9800088 W 19981110; AU 1184499 A 19981110; EP 98954915 A 19981110