

Title (en)
OPTIMISTIC AUTHENTICATOR SYSTEMS

Title (de)
OTIMISTISCHE AUTHENTIFIZIERUNGSSYSTEME

Title (fr)
SYSTEMES D'AUTHENTIFICATEURS OPTIMISTES

Publication
EP 1163752 A1 20011219 (EN)

Application
EP 00926087 A 20000417

Priority
• US 0010398 W 20000417
• US 12938099 P 19990415

Abstract (en)
[origin: WO0064088A1] A digital authentication system that can be used in place of signature schemes is disclosed. Instead of allowing the provider of the message to become convinced upon receipt that an authenticator is valid (2.4), as with signature schemes, it is optimistically assumed that the authenticating party does not cheat. Parties may wait until periodic audit during which the validity of all authenticators asserted to be valid, at showing and even at issuing, can be established with high probability. Nevertheless conventional digital signature techniques can be used to sign the authenticators at issuing, at least in batches, to provide a kind of proof for use if an authenticating party does cheat. One example application is for electronic cash protocols, for which additional techniques are disclosed. Another example application is for untraceable credentials systems, and again further techniques are also disclosed in the context of such credential applications.

IPC 1-7
H04K 1/00

IPC 8 full level
G06Q 20/00 (2006.01); **G07F 7/10** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)
G06Q 20/06 (2013.01); **G06Q 20/341** (2013.01); **G06Q 20/403** (2013.01); **G06Q 20/40975** (2013.01); **G07F 7/1008** (2013.01); **G07F 7/1016** (2013.01); **H04L 9/3218** (2013.01); **H04L 9/3257** (2013.01); **H04L 2209/56** (2013.01)

Citation (search report)
See references of WO 0064088A1

Designated contracting state (EPC)
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)
WO 0064088 A1 20001026; AU 4467200 A 20001102; EP 1163752 A1 20011219

DOCDB simple family (application)
US 0010398 W 20000417; AU 4467200 A 20000417; EP 00926087 A 20000417