Title (en)

METHODS AND APPARATUS FOR THE SECURE IDENTIFICATION AND VALIDATION OF THINGS AND EVENTS

Title (de)

VERFAHREN UND VORRICHTUNG ZUR SICHEREN IDENTIFIKATION UND ECHTHEITSPRÜFUNG VON GEGENSTÄNDEN UND EREIGNISSEN

Title (fr)

METHODES ET DISPOSITIFS PERMETTANT UNE IDENTIFICATION PROTEGEE D'ELEMENTS ET D'EVENEMENTS

Publication

**EP 1031260 A2 20000830 (EN)**

Application

**EP 98951640 A 19981104**

Priority

- IB 9801834 W 19981104
- IL 12210697 A 19971104

Abstract (en)

[origin: WO9927676A2] Methods for non-repudiable, non-trackable, possibly one-way identification and validation of remote entities to identification devices, wherein the identification devices do not require access to databases of remote entity information. An arbitrator entity preferably characterizes and distributes a specific algorithm to each remote entity. An identification device (or system operating an identification device) preferably distributes one reversible algorithm to each remote entity. Each time a remote entity identifies itself to an identification device, it applies its arbitrator provided algorithm to either a time-based variable (one-way identification) or to a challenge provided by the identification device, computing a first result. The remote entity then applies the reversible algorithm to the challenge/time-based variable, to its identification data and to the first computed result, computing a second result which is transmitted to an identification device. The identification device then may apply the reverse algorithm to the second result, computing a presumed challenge/time-based variable, presumed identification data and presumed first result. The identification device then may compare the challenge/time-based variable to the presumed challenge/time-based variable. If they match (within some tolerance for a time-based variable), the identification device transmits the presumed first result, the presumed identification data and the challenge to the arbitrator. The arbitrator then may apply the particular algorithm distributed to that remote entity and apply it to the challenge/time-based variable, thereby computing a valid first result. The arbitrator then may compare the valid first result to the presumed first result. If they match (within a tolerance for time-based variables), the arbitrator may corroborate the authenticity of the identification to the identification device.

IPC 1-7

**H05K 1/00**

IPC 8 full level

**H04L 9/32** (2006.01)

CPC (source: EP)

**H04L 9/3213** (2013.01); **H04L 9/3271** (2013.01)

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 9927676 A2 19990603**; **WO 9927676 A3 19990902**; AU 9757898 A 19990615; CA 2308474 A1 19990603; EP 1031260 A2 20000830; EP 1031260 A4 20010328; IL 122106 A0 19981206; IL 122106 A 20101130

DOCDB simple family (application)

**IB 9801834 W 19981104**; AU 9757898 A 19981104; CA 2308474 A 19981104; EP 98951640 A 19981104; IL 12210697 A 19971104