Title (en)

METHOD AND SYSTEM FOR SECURE DATA TRANSFER IN A TACHOGRAPH SYSTEM

Title (de)

VORRICHTUNG UND VERFAHREN ZUR SICHEREN DATENÜBERTRAGUNG IN EINEM TACHOGRAPHENSYSTEM

Title (fr)

MÉTHODE ET SYSTÈME DE TRANSMISSION SÉCURISÉE DE DONNÉES DANS UN TACHYGRAPHE

Publication

EP 2238733 A2 20101013 (DE)

Application

EP 09706804 A 20090107

Priority

- EP 2009050112 W 20090107
- DE 102008006840 A 20080130

Abstract (en)

[origin: WO2009095286A2] In a data transmission method for a tachograph system, digital messages are transmitted between a speed transmitter (MS) and a recording unit (RU). Said digital messages contain a pair of keys comprising a public key (KMP, KRP) and a private key (KMS, KRS), as well as a certificate (ZM, ZR) derived from the respective pair of keys. The public keys (KMP, KRP) and the certificates (ZM, ZR) are mutually verified between the recording unit (RU) and the speed transmitter (MS). If the verification is positive, the speed transmitter (MS) detects sensor data, and a digital message is generated therefrom. In addition, the speed transmitter (MS) generates authentication data for the message in accordance with the pair of keys (KMP, KMS) thereof. The message and the authentication data are transmitted to the recording unit and are processed there in accordance with a validity of the authentication data verified by the recording unit (RU).

IPC 8 full level

H04L 29/06 (2006.01); **G01P 1/12** (2006.01)

CPC (source: EP US)

G01P 1/122 (2013.01 - EP US); **H04L 9/3263** (2013.01 - EP US); **H04L 9/3271** (2013.01 - EP US); **H04L 63/0823** (2013.01 - EP US); **H04L 63/12** (2013.01 - EP US); H04L 2209/805 (2013.01 - EP US); H04L 2209/84 (2013.01 - EP US)

Citation (search report)

See references of WO 2009095286A2

Citation (examination)

MILLER V S: "USE OF ELLIPTIC CURVES IN CRYPTOGRAPHY", SECURITY IN COMMUNICATION NETWORKS : THIRD INTERNATIONAL CONFERENCE ; REVISED PAPERS / SCN 2002, AMALFI, ITALY, SEPTEMBER 11 - 13, 2002; [LECTURE NOTES IN COMPUTER SCIENCE , ISSN 0302-9743], SPRINGER VERLAG, DE, 1 January 1985 (1985-01-01), pages 417 - 426, XP000775808, ISBN: 978-3-540-24128-7

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA RS

DOCDB simple family (publication)

WO 2009095286 A2 20090806; **WO 2009095286 A3 20091112**; DE 102008006840 A1 20090813; EP 2238733 A2 20101013; RU 2010136270 A 20120310; RU 2462827 C2 20120927; US 2010322423 A1 20101223; US 8484475 B2 20130709

DOCDB simple family (application)

EP 2009050112 W 20090107; DE 102008006840 A 20080130; EP 09706804 A 20090107; RU 2010136270 A 20090107; US 86555609 A 20090107