Title (en)

METHOD AND DEVICE FOR TRANSMITTING MESSAGES IN REAL TIME

Title (de)

VERFAHREN UND VORRICHTUNG ZUR ÜBERTRAGUNG VON NACHRICHTEN IN ECHTZEIT

Title (fr)

PROCÉDÉ ET DISPOSITIF POUR LA TRANSMISSION DE MESSAGES EN TEMPS RÉEL

Publication

EP 2260609 A1 20101215 (DE)

Application

EP 09729803 A 20090220

Priority

• EP 2009052017 W 20090220
• DE 102008018001 A 20080409

Abstract (en)

[origin: WO2009124803A1] A method and a system for transmitting a message in real time between subscribers in a closed network of a vehicle (1), in particular a rail-bound vehicle, is provided. To this end, an encryption (S1) of security-relevant real-time data (D) of a message (N), including a transmitter ID of a transmitter (3) inside the closed network, is performed using a private key (KprivA) of the transmitter (3) to generate an encrypted message (N'); a transmission (S2) of the encrypted message (N') together with the unencrypted transmitter ID of the transmitter (3) from the transmitter (3) is performed via a vehicle bus (2) to a receiver (4) within the closed network, and a decryption of the encrypted message (N') is performed by the receiver (4) using a public key (KpublicA) of the transmitter (3), which is identified by the received unencrypted transmitter ID, to reacquire the unencrypted message (N). The received transmitter ID is compared to the transmitter ID, which is contained in the required message (N), in order to establish whether the transmission of the message (N) has been performed correctly.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/3236 (2013.01 - EP US); H04L 2209/84 (2013.01 - EP US)

Citation (search report)

See references of WO 2009124803A1

Citation (examination)

• MENEZES ET AL: "Handbook of Applied Cryptography", USA, 1 January 1997 (1997-01-01), USA, XP055103228, Retrieved from the Internet <URL:http://www.cacr.math.uwaterloo.ca/hac/> [retrieved on 20170927]
• "Chapter 1: Overview of Cryptography ED - Menezes A J; Van Oorschot P C; Vanstone S A", 1 October 1996 (1996-10-01), XP001525001, ISBN: 978-0-8493-8523-0, Retrieved from the Internet <URL:http://www.cacr.math.uwaterloo.ca/hac/> [retrieved on 20170927]

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 2009124803 A1 20091015; CN 101990748 A 20110323; DE 102008018001 A1 20091022; EP 2260609 A1 20101215; RU 2010145270 A 20120520; RU 2459369 C2 20120820; TW 200952432 A 20091216; TW I439102 B 20140521; US 2011055564 A1 20110303; US 8577036 B2 20131105

DOCDB simple family (application)

EP 2009052017 W 20090220; CN 200980112604 A 20090220; DE 102008018001 A 20080409; EP 09729803 A 20090220; RU 2010145270 A 20090220; TW 98108904 A 20090319; US 93739809 A 20090220