Title (en)

METHOD AND DEVICE FOR ESTABLISHING PASSWORD BASED SECURE CHANNEL

Title (de)

VERFAHREN UND VORRICHTUNG ZUR HERSTELLUNG EINES PASSWORTBASIERTEN SICHEREN KANALS

Title (fr)

PROCÉDÉ ET DISPOSITIF POUR ÉTABLIR UN CANAL SÉCURISÉ SUR LA BASE D'UN MOT DE PASSE

Publication

EP 4264875 A1 20231025 (EN)

Application

EP 21783477 A 20210924

Priority

EP 2021076391 W 20210924

Abstract (en)

[origin: WO2023046294A1] A method of establishing a secure channel between devices. The method includes at each of two devices generating a random variable, calculating a random function based on the random variable, generating a hash for a predetermined password, and generating a message including the hashed password and corresponding function. The method further includes, sending the generated message to the other device, and receiving the message generated by the other device, computing the random function of the other device based on the received message and the hashed password, and computing a transcript based on the ID of both devices, and the generated messages of both devices. The method further includes, generating, using a crypto hash function, session keys, such as an integration key, and an encoding key to establish a secure channel between devices. The method provides the secure channel between two devices with enhanced security and reduced communication and computational complexity.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP)

H04L 9/0844 (2013.01); **H04L 9/3066** (2013.01)

Citation (search report)

See references of WO 2023046294A1

Designated contracting state (EPC)

AL 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 RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

WO 2023046294 A1 20230330; EP 4264875 A1 20231025

DOCDB simple family (application)

EP 2021076391 W 20210924; EP 21783477 A 20210924