Title (en)

METHOD FOR OBTAINING A SEQUENCE OF CRYPTOGRAPHIC KEYS

Title (de)

VERFAHREN ZUR ERLANGUNG EINER SEQUENZ VON KRYPTOGRAPHISCHEN SCHLÜSSELN

Title (fr)

PROCEDE D'OBTENTION D'UNE SUCCESSION DE CLES CRYPTOGRAPHIQUES

Publication

EP 3818659 A1 20210512 (FR)

Application

EP 19749777 A 20190701

Priority

- FR 1856170 A 20180704
- FR 2019051616 W 20190701

Abstract (en)

[origin: WO2020008131A1] The invention relates to a method for obtaining a sequence of L cryptographic keys k1,m . ki,m, ki+1,m, kL,m in which, before an instant t1,m, a group of receivers establishes (140) a first connection to a key server and receives, during said first connection, the information required to obtain the key k1,m, and, subsequently, for each index i between 2 and L: the group of receivers obtains (150) the subsequent key ki,m by running a key derivation algorithm initialised by means of the previous key ki-1,m and without using any information other than that received during the first connection; and the average run-time TCi,m of the key derivation algorithm by the group of receivers in order to obtain the key ki,m is higher than 0,2Vi-1,m., where V1-i,m is the duration of the validity interval of the previous key ki-1,m.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP)

H04L 9/0819 (2013.01); **H04L 9/0861** (2013.01); **H04L 9/088** (2013.01); **H04L 9/0891** (2013.01); **H04L 9/50** (2022.05)

Citation (search report)

See references of WO 2020008131A1

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

DOCDB simple family (publication)

WO 2020008131 A1 20200109; CN 112602288 A 20210402; EP 3818659 A1 20210512; FR 3083660 A1 20200110; FR 3083660 B1 20201204

DOCDB simple family (application)

FR 2019051616 W 20190701; CN 201980055283 A 20190701; EP 19749777 A 20190701; FR 1856170 A 20180704