Title (en)

TECHNIQUE FOR PROTECTING A CRYPTOGRAPHIC KEY BY MEANS OF A USER PASSWORD

Title (de)

VERFAHREN ZUM SCHUTZ EINES KRYPTOGRAFISCHEN SCHLÜSSELS MITTELS EINES BENUTZERPASSWORTES

Title (fr)

TECHNIQUE DE PROTECTION D'UNE CLÉ CRYPTOGRAPHIQUE AU MOYEN D'UN MOT DE PASSE UTILISATEUR

Publication

EP 3724799 A1 20201021 (FR)

Application

EP 18833097 A 20181212

Priority

- FR 1762283 A 20171215
- FR 2018053233 W 20181212

Abstract (en)

[origin: WO2019115943A1] The invention relates to a technique for protecting a cryptographic key. A user has an identifier and an associated password. Said first cryptographic key is designed to decrypt at least one piece of encrypted data. The user device generates (E00) a second cryptographic key by applying a key derivation algorithm to at least the password, then encrypts (E01) the first cryptographic key by applying an encryption algorithm parameterized by the second cryptographic key. The user device then provides said encryption of the first cryptographic key to a management device for storage. A response associated with a question is obtained from the user. The user device then calculates (E02) the result of the application of a function to at least one response associated with one question, then provides (E03) at least one value dependent on said result to the management device for storage. Said value then enables the user device to determine the password when it has the response to the corresponding question.

IPC 8 full level

G06F 21/45 (2013.01); **H04L 9/08** (2006.01)

CPC (source: EP US)

G06F 21/45 (2013.01 - EP); **H04L 9/0618** (2013.01 - US); **H04L 9/0822** (2013.01 - EP US); **H04L 9/0861** (2013.01 - EP); **H04L 9/0863** (2013.01 - EP US); **H04L 9/0894** (2013.01 - EP US); **H04L 9/30** (2013.01 - US); **H04L 9/3218** (2013.01 - US); **H04L 9/3226** (2013.01 - US); **H04L 9/3271** (2013.01 - US); G06F 2221/2103 (2013.01 - EP US); G06F 2221/2107 (2013.01 - EP); G06F 2221/2131 (2013.01 - EP US)

Citation (search report)

See references of WO 2019115943A1

Cited by

CN116633544A

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 2019115943 A1 20190620; EP 3724799 A1 20201021; FR 3075423 A1 20190621; US 11483146 B2 20221025; US 2020389302 A1 20201210

DOCDB simple family (application)

FR 2018053233 W 20181212; EP 18833097 A 20181212; FR 1762283 A 20171215; US 201816772478 A 20181212