Title (en)

IDENTITY VERIFICATION

Title (de)

IDENTITÄTSPRÜFUNG

Title (fr)

VÉRIFICATION D'IDENTITÉ

Publication

EP 3577849 A1 20191211 (EN)

Application

EP 18705732 A 20180131

Priority

- GB 201701645 A 20170201
- IB 2018050587 W 20180131

Abstract (en)

[origin: WO2018142291A1] A need exists for a user 1 to control their digital identity without reliance on third party service providers 40, 50. A user 1 will use cryptographic keys to verify their identity in the digital world, e.g. over the Internet 25. A method is herein described to permit the user 1 to securely access such cryptographic keys. The method comprises generating, using a physical or virtual authentication tool 10, an intermediate key based on a PIN or similar code provided by the user 1 and a unique code contained in the authentication tool 10. An offset value is applied to the intermediate key to generate a decryption key, thus allowing for multiple authentication tools 10 having different unique codes to be used. The decryption key is used to decrypt an encrypted cryptographic key. The encrypted cryptographic key and the offset(s) are meaningless without the authentication tool 10 and the user code, and so may be freely stored in any location, even on (semi-)public servers 30, without compromising the security of the cryptographic keys of the user 1. Also provided is a method for generating new encrypted cryptographic keys and for generating offsets to permit new authentication tools 10 to access such encrypted cryptographic keys.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

H04L 9/0822 (2013.01); **H04L 9/0861** (2013.01); **H04L 9/0866** (2013.01); **H04L 9/3271** (2013.01); **H04L 63/0428** (2013.01); **H04L 63/0861** (2013.01)

Citation (search report)

See references of WO 2018142291A1

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 2018142291 A1 20180809; EP 3577849 A1 20191211; GB 201701645 D0 20170315

DOCDB simple family (application)

IB 2018050587 W 20180131; EP 18705732 A 20180131; GB 201701645 A 20170201