

Title (en)

METHOD FOR CONFIGURING A SECURITY MODULE WITH AT LEAST ONE DERIVED KEY

Title (de)

VERFAHREN FÜR DAS KONFIGURIEREN EINES SICHERHEITSMODULS MIT MINDESTENS EINEM ABGELEITETEN SCHLÜSSEL

Title (fr)

PROCÉDÉ POUR LA CONFIGURATION D'UN MODULE DE SÉCURITÉ AVEC AU MOINS UNE CLÉ DÉDUITE

Publication

EP 3928463 A1 20211229 (DE)

Application

EP 20714915 A 20200316

Priority

- EP 19167509 A 20190405
- EP 2020057077 W 20200316

Abstract (en)

[origin: WO2020200729A1] The invention claims a method for configuring a security module (SD) with at least one derived key, having the following steps: - providing a key (MK); - deriving (KDF) a further key (K1 to KN) from the provided key or from a key previously derived from the provided key, characterized in that said further key is derived by using an alterable digital fingerprint (FP) as key derivation parameter, which is formed on the basis of a measurable current runtime configuration of a runtime environment (R) communicating with the security module.

IPC 8 full level

G06F 21/57 (2013.01); **G06F 21/60** (2013.01); **H04L 9/08** (2006.01); **H04L 29/06** (2006.01); **H04W 12/04** (2021.01)

CPC (source: EP US)

G06F 21/57 (2013.01 - EP); **G06F 21/72** (2013.01 - EP); **H04L 9/0643** (2013.01 - EP US); **H04L 9/0825** (2013.01 - US); **H04L 9/0866** (2013.01 - EP US); **H04L 9/0877** (2013.01 - EP US); **H04L 63/06** (2013.01 - EP); **H04L 2463/081** (2013.01 - EP)

Citation (search report)

See references of WO 2020200729A1

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)

EP 3720039 A1 20201007; CN 113647053 A 20211112; EP 3928463 A1 20211229; US 2022150056 A1 20220512; WO 2020200729 A1 20201008

DOCDB simple family (application)

EP 19167509 A 20190405; CN 202080027078 A 20200316; EP 2020057077 W 20200316; EP 20714915 A 20200316; US 202017599780 A 20200316