Title (en)

DEVICE, METHOD AND PROGRAM FOR SECURE COMMUNICATION BETWEEN WHITE BOXES

Title (de)

VORRICHTUNG, VERFAHREN UND PROGRAMM ZUR SICHEREN KOMMUNIKATION ZWISCHEN WHITEBOXS

Title (fr)

DISPOSITIF, MÉTHODE ET PROGRAMME POUR UNE COMMUNICATION SÉCURISÉE ENTRE BOÎTES BLANCHES

Publication

EP 4183098 A1 20230524 (FR)

Application

EP 21739226 A 20210708

Priority

- FR 2007425 A 20200715
- EP 2021069068 W 20210708

Abstract (en)

[origin: CA3183198A1] The invention relates to a cryptographic data processing method for implementing a cryptographic function, which method is implemented within an electronic data processing device comprising a processor, a memory and a set of cryptographic processing modules, the method comprising the following steps implemented by a current cryptographic processing module of the set of cryptographic processing modules, the current cryptographic processing module belonging to a chain of at least two cryptographic processing modules executed for the implementation of the cryptographic function: - receiving (10) incoming data (D_A); - determining (20) a decryption key (K_I) to be applied to the incoming data (D_A) according to a master key and a position of the current cryptographic processing module; - decrypting (30) the incoming data (D_A), with the key (K_I), delivering unencrypted incoming data (DI_nc); - implementing (40) at least one cryptographic operation on the unencrypted incoming data (Di_nc), delivering unencrypted outgoing data (DO_nc); - optionally, determining (45) a subsequent cryptographic processing module to be executed on the unencrypted outgoing data; - obtaining (50) an encryption key (K_O) for the unencrypted outgoing data (DO_nc); - encrypting (60) the unencrypted outgoing data (DO_nc) with the previously determined encryption key (K_O) for the outgoing data, delivering the encrypted outgoing data (D_B), which may be intermediate data.

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP US)

H04L 9/0819 (2013.01 - US); **H04L 9/0866** (2013.01 - EP US); H04L 2209/16 (2013.01 - EP US)

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)

FR 3112643 A1 20220121; **FR 3112643 B1 20240503**; CA 3183198 A1 20220120; EP 4183098 A1 20230524; US 2023275745 A1 20230831; WO 2022013072 A1 20220120

DOCDB simple family (application)

FR 2007425 A 20200715; CA 3183198 A 20210708; EP 2021069068 W 20210708; EP 21739226 A 20210708; US 202118016374 A 20210708