(12) International Application Status Report

Received at International Bureau: 10 December 2019 (10.12.2019)
Information valid as of: 19 May 2020 (19.05.2020)
Report generated on: 20 September 2020 (20.09.2020)

(10) Publication number:
WO2020/115265

(43) Publication date:
11 June 2020 (11.06.2020)

(26) Publication language:
English (EN)

(21) Application Number:
PCT/EP2019/083943

(22) Filing Date:
06 December 2019 (06.12.2019)

(25) Filing language:
English (EN)

(31) Priority number(s):
18306629.9 (EP)

(31) Priority date(s):
06 December 2018 (06.12.2018)

(31) Priority status:
Priority document received (in compliance with PCT Rule 17.1)

(51) International Patent Classification:
H04L 9/08 (2006.01); ***H04L 9/30*** (2006.01); **H04L 9/32** (2006.01)

(71) Applicant(s):
SECURE-IC SAS [FR/FR]; 15 rue Claude Chappe ZAC des Champs Blancs 35510 CESSON-SEVIGNE (FR) *(for all designated states)*

(72) Inventor(s):
DUGARDIN, Margaux; 22 rue Louise de Bettignies 35200 RENNES (FR)
FACON, Adrien; 85 rue de Rivoli 75001 PARIS (FR)
GUILLEY, Sylvain; 3, rue Françoise Dolto 75013 PARIS (FR)

(74) Agent(s):
HNICH-GASRI, Naïma; Immeuble "Visium" 22, Avenue Aristide Briand 94117 ARCUEIL (FR)

(54) Title (EN): CERTIFICATELESS PUBLIC KEY ENCRYPTION USING PAIRINGS

(54) Title (FR): CRYPTAGE DE CLÉS PUBLIQUES SANS CERTIFICAT À L'AIDE D'APPARIEMENTS

(57) Abstract:
(EN): A transmitter device (103) for sending an encrypted message to a receiver device (105) in an identity-based cryptosystem (100), the transmitter device (103) being associated with a transmitter identifier. The transmitter device (103) is configured to receive a transmitter partial private key from a trusted center (101), the transmitter device (103) being configured to: - send a request for two public session keys to the receiver device (105); - receive from the receiver device (105) a first ciphertext set, the first ciphertext set being derived from an encryption and authentication of two public session keys; - decrypt and authenticate the two public session keys from the first ciphertext set using a receiver identifier and the transmitter partial private key; - determine a second ciphertext set from the transmitter partial private key, from the receiver identifier, and from the two public session keys, the second ciphertext comprising an encrypted message; - send the second ciphertext set to the receiver device (105).

(FR): La présente invention concerne un dispositif émetteur (103) conçu pour envoyer un message crypté à un dispositif récepteur (105) dans un système cryptographique basé sur l'identité (100). Le dispositif émetteur (103) est associé à un identifiant d'émetteur. Le dispositif émetteur (103) est configuré pour : - recevoir une clé privée partielle de l'émetteur provenant d'un centre de confiance (101) ; - envoyer au dispositif récepteur (105) une demande relative à deux clés de session publiques ; - recevoir du dispositif récepteur (105) un premier ensemble de cryptogrammes, le premier ensemble de cryptogrammes étant dérivé d'un cryptage et d'une authentification des deux clés de session publiques ; - décrypter et authentifier les deux clés de session publiques à partir du premier ensemble de cryptogrammes à l'aide d'un identifiant de récepteur et de la clé privée partielle de l'émetteur ; - déterminer un second ensemble de cryptogrammes à partir de la clé privée partielle de l'émetteur, de l'identifiant de récepteur et des deux clés de session publiques, le second ensemble de cryptogrammes contenant un message crypté ; et - envoyer le second ensemble de cryptogrammes au dispositif récepteur (105).

International search report:
Received at International Bureau: 09 March 2020 (09.03.2020) [EP]

International Report on Patentability (IPRP) Chapter II of the PCT:
Not available

(81) Designated States:
AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW
European Patent Office (EPO) : AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR
African Intellectual Property Organization (OAPI) : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG
African Regional Intellectual Property Organization (ARIPO) : BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW
Eurasian Patent Organization (EAPO) : AM, AZ, BY, KG, KZ, RU, TJ, TM