



(51) International Patent Classification:
H04W 12/04 (2021.01)

(21) International Application Number:
PCT/EP2021/073966

(22) International Filing Date:
31 August 2021 (31.08.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20315412.5 17 September 2020 (17.09.2020) EP

(71) Applicant: **THALES DIS FRANCE SA** [FR/FR]; 6, rue de la verrerie, 92190 MEUDON (FR).

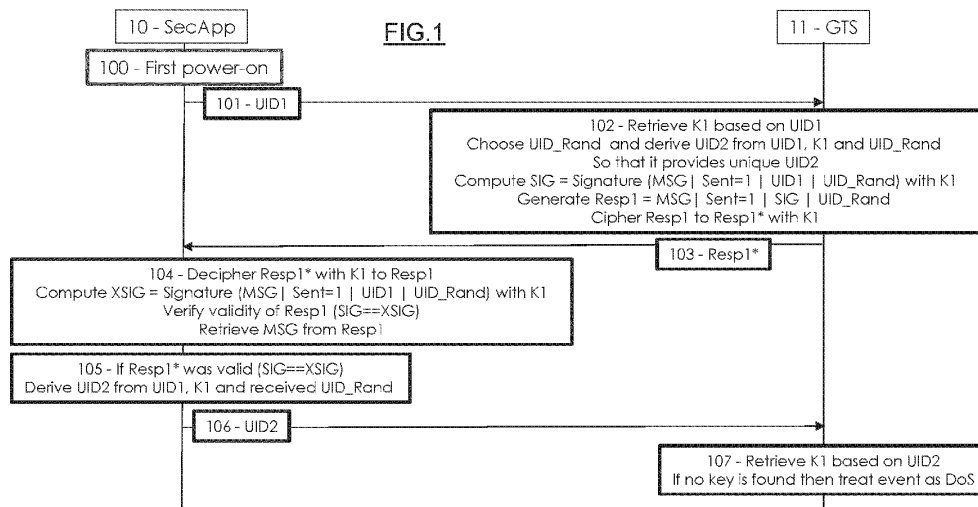
(72) Inventors: **PHAN, Ly Than**; THALES DIS FRANCE SA, Intellectual Property Department, 525, Avenue du

Pic de Bertagne, CS12023, 13881 GEMENOS CEDEX (FR). **GROS, Jean-Francois**; THALES DIS FRANCE SA, Intellectual Property Department, 525, Avenue du pic de Bertagne, CS12023, 13881 GEMENOS CEDEX (FR). **DANY, Vincent**; THALES DIS FRANCE SA, Intellectual Property Department, 525, Avenue du Pic de Bertagne, CS12023, 13881 GEMENOS CEDEX (FR).

(74) Agent: **SCHEER, Luc**; THALES DIS FRANCE SAS, Avenue du Jujubier, ZI Athelia IV, 13705 LA CIOTAT (FR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): 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, IT, 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,

(54) Title: A METHOD FOR SENDING A MESSAGE FROM A REMOTE SERVER TO A TERMINAL



(57) **Abstract:** The present invention relates to a method for sending a message (MSG) from a remote server (11) to a terminal (10), the remote server (11) and the terminal (10) sharing a secret key (K1), the method comprising: i- Sending from the terminal (10) to the remote server (11) a first identity (UID1); ii- Retrieving at the remote server (11) the first identity (UID1) and retrieving the secret key (K1) based on the first identity (UID1); iii- At the remote server (11), choosing a random number (UID_RAND) and generating a second identity (UID2) thanks to the first identity (UID1), the random number (UID_RAND) and the secret key (K1); iv- At the remote server (11), generating a signature (SIG) from the first identity (UID1), the message (MSG), a counter value (Sent), the random number (UID_RAND) and the secret key (K1); v- At the remote server (11), generating a first response (Resp1) for the terminal (10), the first response (Resp1) being a concatenation of the message (MSG), a counter value (Sent), the signature (SIG) and the random number (UID_RAND), and ciphering the first response (Resp1) with the secret key (K1) and sending the first ciphered response (Resp1*) to the terminal (10); vi- At the terminal (10), deciphering the first ciphered response (Resp1*) with the secret key (K1) to obtain the first

[Continued on next page]

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

response (Resp1), retrieving the message (MSG), the counter value (Sent), the signature (SIG) and the random number (UID_RANDOM), deriving the expected signature (XSIG) of the first response (Resp1), verifying that the signature (SIG) is equal to the expected signature (XSIG) and verifying that the counter value (Sent) is correct, and if it is correct, derive the second identity (UID2) from the first identity (UID1), the secret key (K1) and the random number (UID_RANDOM).