

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(10) International Publication Number
WO 2020/065132 A1

(43) International Publication Date
02 April 2020 (02.04.2020)

(51) International Patent Classification:

H04W 12/08 (2009.01) H04W 60/00 (2009.01)
H04L 29/06 (2006.01)

(21) International Application Number:

PCT/FI2019/050685

(22) International Filing Date:

24 September 2019 (24.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/735,732 24 September 2018 (24.09.2018) US

(71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI];
Karakaari 7, 02610 Espoo (FI).

(72) Inventor: LIU, Jennifer; 3104 Oak Springs Dr., Plano,
Texas 75025 (US).

(74) Agent: NOKIA TECHNOLOGIES OY et al.; Ari Aarnio,
IPR Department, Karakaari 7, 02610 Espoo (FI).

(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, 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.

(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).

Published:

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

WO 2020/065132 A1

(54) Title: SYSTEMS AND METHOD FOR SECURITY PROTECTION OF NAS MESSAGES

(57) Abstract: Systems and methods that provide NAS security protection for mobile networks. In one embodiment, a network element of a mobile network performs a NAS procedure in multiple phases to establish a NAS communication session with User Equipment (UE) when no NAS security context exists. For a first phase, the network element receives an initial NAS message from the UE populated with a subset of NAS protocol Information Elements (IEs) designated for security-related handling, selects a NAS security algorithm for the NAS security context, and sends a response to the UE that indicates the NAS security algorithm. For a second phase, the network element receives a subsequent NAS message from the UE having a NAS message container that contains the initial NAS message populated with each of the NAS protocol IEs for the NAS procedure, and decrypts the NAS message container of the subsequent NAS message using the NAS security algorithm.