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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2020 (15.10.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/208996 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04W 12/08* (2009.01)
H04W 12/04 (2009.01) *H04W 88/06* (2009.01)

(21) International Application Number:
PCT/JP2020/010735

(22) International Filing Date:
12 March 2020 (12.03.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201941014041 08 April 2019 (08.04.2019) IN

(71) Applicant: **NEC CORPORATION** [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

(72) Inventors: **TIWARI Kundan**; c/o NEC Technologies India Pvt. Ltd., SP Infocity, Block-A, 9th Floor, Module-2A, 40, MGR Salai, Kandanchavadi, Perungudi, Chennai, Tamil Nadu, 600096 (IN). **TAMURA Toshiyuki**; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). **DE KIEVIT Sander**; c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

(74) Agent: **IEIRI Takeshi**; HIBIKI IP Law Firm, Asahi Bldg. 5th Floor, 3-33-8, Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 2210835 (JP).

(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, 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,

(54) **Title:** PROCEDURE TO PROVIDE INTEGRITY PROTECTION TO A UE PARAMETER DURING UE CONFIGURATION UPDATE PROCEDURE

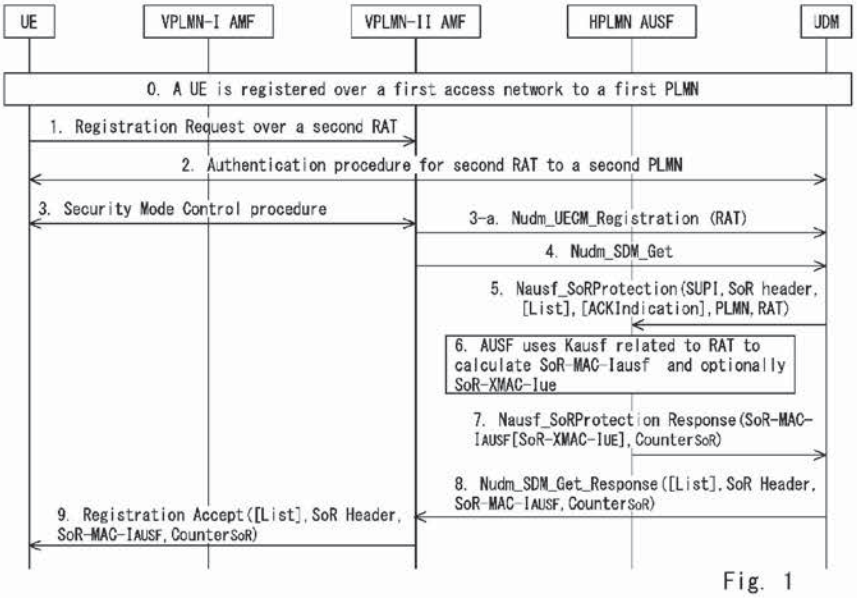

Fig. 1

(57) **Abstract:** A method in a user equipment (UE), the method comprising: storing security keys, wherein each of the security keys corresponds to a RAT(Radio Access Technology); receiving from a communications apparatus, a message including information of a first RAT which the UE communicates with; and determining a first security key in the security keys based on the information of the first RAT, the first security key being used to verify integrity of the message.

WO 2020/208996 A1

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))*

Description

Title of Invention: PROCEDURE TO PROVIDE INTEGRITY PROTECTION TO A UE PARAMETER DURING UE CONFIGURATION UPDATE PROCEDURE

Technical Field

[0001] This disclosure is related to the procedure to provide integrity protection to a UE parameter during the Steering of Roaming and UE parameter update procedure using Control Plane signaling. More specifically the method provides a mechanism to choose a security key to integrity protect a UE parameter when the UE is registered to more than one PLMN (Public land mobile network) and more than one security key existing in the network.

Background Art

[0002] When a UE registers to two different PLMNs which are not equivalent PLMNs via a 3GPP access and a non-3GPP access, then the UE is registered to two different AMFs (Access and Mobility Management Functions) belonging to each PLMN. In this scenario, the UE maintains two independent 5G security contexts (K_{AMF} and keys lower in the key hierarchy), one for each serving PLMN. When a UE is registered to a same PLMN or equivalent PLMN via a 3GPP access and a non-3GPP access, then the UE is registered to the single AMF and maintains one security context.

[0003] When the UDM (Unified Data Management) decides to update the preferred PLMN list or RAT (Radio Access Technology) to the UE when the UE is registered to the visited PLMN, then the UDM initiates Steering of Roaming (SoR) procedure to transfer the steering information (preferred list of PLMN or RAT) for PLMN selection. The steering of roaming information is integrity protected using the security key K_{AUSF} at an AUSF (Authentication Server Function). When the UE receives steering information, the UE uses K_{AUSF} to verify the integrity protection. Similar procedure is applied to update the UE parameters using the UDM control plane procedure.

Citation List

Non Patent Literature

[0004] NPL 1:3GPP TR 21.905: "Vocabulary for 3GPP Specifications". V15.0.0 (2018-03).

NPL 2:3GPP TS 23.501: "System Architecture for the 5G System; Stage 2". V15.4.0 (2019-01).

NPL 3:3GPP TS 23.502: "Procedures for the 5G System; Stage 2" V15.4.0 (2019-01).

NPL 4:3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol Stage 3" V15.2.1

(2019-01).

NPL 5:3GPP TS 33.501: "Security architecture and procedures for 5G system" V15.3.1 (2018-12).

Summary of Invention

Technical Problem

[0005] Problem Statement 1:

When a UE is registered to two different PLMNs which are not equivalent PLMNs via a 3GPP access and non-3GPP access, then the UE has two 5G security contexts (e.g Security Keys) at the various network nodes. In this scenario, the AUSF has one K_{AUSF}, namely the K_{AUSF} resulting from the latest authentication. During the registration procedure over one access network if the UDM decides to send steering information to the UE and sends a message containing steering information and requesting AUSF to provide integrity protection to the steering information, the AUSF calculates the MAC-I for integrity protection of the message using the K_{AUSF} resulting from the latest authentication. Then, if the UE receives the message, it is unclear to the UE which K_{AUSF} the AUSF has used for the calculation of the MAC-I for integrity protection of the steering of roaming message.

[0006] In an another scenarios, when the UEs are registered to two different PLMNs which are not equivalent and the UDM decides to send steering information to the UE, then it is not clear at UDM among two registered PLMNs which PLMN is chosen to send Steering information.

[0007] Problem Statement 2:

When a UE is registered to two different PLMNs which are not equivalent PLMNs via a 3GPP access and non-3GPP access, then the UE has two 5G security contexts (e.g Security Keys) at the various network nodes. In this scenario, when a UDM decides to perform UE parameter update procedure to update the UE configuration (e.g. Routing Identity) using control plane signalling, then it is not clear among two registered PLMNs which PLMN the UDM will choose to send an updated UE configuration.

Solution to Problem

[0008] In a first aspect of the present disclosure, a method in a user equipment (UE), the method comprising: storing security keys, wherein each of the security keys corresponds to a RAT(Radio Access Technology); receiving from a communications apparatus, a message including information of a first RAT which the UE communicates with; and determining a first security key in the security keys based on the information of the first RAT, the first security key being used to verify integrity of the message.

[0009] In a second aspect of the present disclosure, a method in a first communications apparatus comprising, storing security keys, wherein each of the security keys corresponds to a RAT(Radio Access Technology); receiving, from a second communications apparatus, information of a first RAT which a UE communicates with; and determining a first security key in the security keys based on the information of the first RAT.

[0010] In a third aspect of the present disclosure, a user equipment (UE) comprising: a memory configured to store security keys, wherein each of the security keys corresponds to a RAT(Radio Access Technology); a transceiver configured to receive from a communications apparatus, a message including information of a first RAT which the UE communicates with; and a controller configured to determine a first security key in the security keys based on the information of the first RAT, the first security key being used to verify integrity of the message.

[0011] In a fourth aspect of the present disclosure, a first communications apparatus comprising, a memory configured to store security keys, wherein each of the security keys corresponds to a RAT(Radio Access Technology); a transceiver configured to receive, from a second communications apparatus, information of a first RAT which a UE communicates with; and a controller configured to determine a first security key in the security keys based on the information of the first RAT.

Brief Description of Drawings

[0012] [fig.1]Fig. 1 is a diagram showing the procedure according to a first embodiment of the present disclosure.

[fig.2]Fig. 2 is a diagram showing the procedure according to a variant of the first embodiment of the present disclosure.

[fig.3]Fig. 3 is a diagram showing the procedure according to a second embodiment of the present disclosure.

[fig.4]Fig. 4 is a diagram showing the procedure according to a third embodiment of the present disclosure.

[fig.5]Fig. 5 is a diagram showing the procedure according to a variant 1a of the first embodiment of the present disclosure.

[fig.6]Fig. 6 is a diagram showing the procedure according to a fourth embodiment of the present disclosure.

[fig.7]Fig. 7 is a diagram showing the procedure according to a variant of the fourth embodiment of the present disclosure.

[fig.8]Fig. 8 is a block diagram illustrating the main components of the UE.

[fig.9]Fig. 9 is a block diagram illustrating the main components of an exemplary (R)AN node.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.