3GPP; 23.501: SUPI terminology correction; 3GPP draft discloses a "Subscriber Permanent Identifier" so that a globally unique 5G Subscriber Permanent Identifier (SUPI) can be allocated to each subscriber in the 5G system.

3GPP; SA WG3; LS on Security aspects of ECIES for concealing IMSI or SUPI discloses next generation of mobile networks (called the 5G). A new and general term called the SUPI (Subscription Permanent Identifier) is disclosed which is proposed to be used to denote the globally unique 5G subscription permanent identifier. D4 further proposes to conceal IMSI or SUPI over-the-air in 5G by the ECIES (Elliptic Curve Integrated Encryption Scheme).

Summary

In an aspect, the present disclosure refers to a user equipment for a wireless communication system, comprising a processor and memory configured to construct a unified subscription identifier data structure; wherein the unified subscription identifier data structure comprises a plurality of fields that specify a selected one of two or more subscription identifier fields associated with a selected subscription identifier type; and use the selected one of two or more subscription identifier fields in the unified subscription identifier data structure to access one or more networks associated with the wireless communication system based on an authentication scenario corresponding to the selected subscription identifier type.

In another aspect, the present disclosure refers to a method carried out by a user equipment for a wireless communication system and comprising: constructing a unified subscription identifier data structure; wherein the unified subscription identifier data structure comprises a plurality of fields that specify a selected one of two or more subscription identifier fields associated with a selected subscription identifier type; and using the selected one of two or more subscription identifier fields in the unified subscription identifier data structure to access one or more networks associated with the wireless communication system based on an authentication scenario corresponding to the selected subscription identifier type.

In another aspect, the present disclosure refers to a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor of a user equipment in a wireless communication system, causes the processor to:

construct a unified subscription identifier data structure; wherein the unified subscription identifier data structure comprises a plurality of fields that specify a selected one of two or more subscription identifier fields associated with a selected subscription identifier type; and use the selected one of two or more subscription identifier fields in the unified subscription identifier data structure to access one or more networks associated with the wireless communication system based on an authentication scenario corresponding to the selected subscription identifier type.

Illustrative ~~embodiments~~ examples provide improved techniques for managing subscription identifiers in communication systems.

For example, in one illustrative ~~embodiment~~example, a method comprises the following step. At given user equipment in a wireless communication system, a unified subscription identifier data structure is constructed. The unified subscription identifier data structure is stored. The unified subscription identifier data structure comprises a plurality of fields that specify a selected one of two or more subscription identifier fields associated with a selected subscription identifier type. The selected one of two or more subscription identifier fields in the unified subscription identifier data structure is used to access one or more networks associated with the wireless communication system based on an authentication scenario corresponding to the selected subscription identifier type.

Further illustrative ~~embodiments~~ examples are provided in the form of non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the above steps. Still further illustrative ~~embodiments~~ examples comprise apparatus with a processor and a memory configured to perform the above steps.

Advantageously, during different authentication scenarios, the given user equipment utilizes the unified subscription identifier data structure to provide the appropriate subscription identifier (e.g., SUPI, SUCI or IMSI) and associated parameters for the given authentication scenario.

These and other features and advantages of embodiments described herein will become more apparent from the accompanying drawings and the following detailed description.

Brief Description of the Drawings

FIG. 1 illustrates a communication system with which one or more illustrative embodiments may be implemented.

FIG. 2 illustrates user equipment and a network element/function for providing subscriber identifier management during authentication procedures with which one or more illustrative embodiments may be implemented.

FIG. 3A illustrates an IMSI format with which one or more illustrative embodiments may be implemented.

FIG. 3B illustrates a SUPI format with which one or more illustrative embodiments may be implemented.

FIG. 3C illustrates a SUCI format with which one or more illustrative embodiments may be implemented.

FIG. 4 illustrates a unified subscription identifier format, according to an illustrative embodiment.

FIG. 5 illustrates exemplary field lengths of a unified subscription identifier format, according to an illustrative embodiment.

FIG. 6 illustrates a unified subscription identifier format, according to another illustrative embodiment.

Claims

What is claimed is:

1. A user equipment (102, 202) for a wireless communication system (100, 200), comprising a processor (212) and memory (216) configured to ~~perform:~~construct a unified subscription identifier data structure (400, 600);

~~construct, at the user equipment (102, 202) in the wireless communication system (100, 200), a unified subscription identifier data structure;~~

~~store the unified subscription identifier data structure (400, 600),~~ wherein the unified subscription identifier data structure (400, 600) comprises a plurality of fields (402-426, 602-616) that specify a selected one of two or more subscription identifier fields (300, 310, 320) associated with a selected subscription identifier type; and

use the selected one of two or more subscription identifier fields(300, 310, 320) in the unified subscription identifier data structure (400, 600) to access one or more networks associated with the wireless communication system (100, 200) based on an authentication scenario corresponding to the selected subscription identifier type.

2. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426, 602-616) comprises a subscription identifier type field (414, 608).

3. The user equipment (102, 202) of claim 2, wherein a subscription identifier type is selectable from a group comprising a Concealed Subscription Identifier, SUCI, a Subscriber Permanent Identifier, SUPI, and an International Mobile Station Identifier, IMSI.

4. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426, 602-616) comprises a network entity selection parameter field (406, 606).

5. The user equipment (102, 202) of claim 4, wherein a network entity (104, 204) performs one or more of a unified data management, UDM, function and an authentication server function, AUSF.

6. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426) comprises an encryption on/off field (408).

7. The user equipment (102, 202) of claim 6, wherein the plurality of fields (402-426) comprises an encryption algorithm identifier field (426).

8. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426) comprises a key derivation function field (410).

9. The user equipment (102, 202) of claim 8, wherein the plurality of fields (402-426) comprises a key derivation function parameter field (412).

10. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426, 602-616) comprises a mobile country code field (402, 602).

11. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426, 602-616) comprises a mobile network code field (404, 604).

12. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426) comprises a field specifying a selected curve from an elliptic curve integrated encryption scheme (416).

13. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426)comprises an ephemeral public key pair field (418).

14. The user equipment (102, 202) of claim 1, wherein the plurality of fields (402-426, 602-616) comprises a field specifying a length of an encrypted Mobile Station Identification Number, MSIN, field (420, 610).

15. The user equipment (102, 202) of claim 14, wherein the plurality of fields (402-426, 602-616) comprises an encrypted MSIN field (422, 612).

16. The user equipment (102, 202) of claim 14, wherein the plurality of fields (402-426, 602-616) comprises an MSIN message authentication code field (424, 614).

17. The user equipment (102, 202) of claim 1, wherein the wireless communication system (100, 200) comprises a 5G system.

18. The user equipment (102, 202) of claim 1, further comprising sending the unified subscription identifier data structure (400, 600) to at least one network entity (104, 204) in the wireless communication system (100, 200) to gain access to the one or more networks associated with the wireless communication system (100, 200).

19. The user equipment (102, 202) of claim 1, wherein the plurality of fields (602-616) comprises a profile selection field (616).

20. The user equipment (102, 202) of claim 19, wherein the profile selection field (616) enables the user equipment (102, 202) to notify one or more network entities in the one or more networks associated with the wireless communication system (100, 200) to use pre-established values for one or more selectable parameters associated with the selected subscription identifier field (300, 310, 320).

21. The user equipment (102, 202) of claim 20, further comprising sending the unified subscription identifier data structure (600) with the profile selection field (616) and a reduced set of fields to at least one of the one or more network entities in the wireless communication system (100, 200) to gain access to the one or more networks associated with the wireless communication system (100. 200).

22. ~~A method comprising:~~A method carried out by a user equipment (102, 202) for a wireless communication

~~constructing, at a user equipment (102, 202) in a wireless communication~~ system (100, 200~~),~~) and comprising:

constructing a unified subscription identifier data structure (400, 600);

storing the unified subscription identifier data structure (400, 600), wherein the unified subscription identifier data structure (400, 600) comprises a plurality of fields (402-426, 602-616) that specify a selected one of two or more subscription identifier fields (300, 310, 320) associated with a selected subscription identifier type; and

using the selected one of two or more subscription identifier fields (300, 310, 320) in the unified subscription identifier data structure (400, 600) to access one or more networks associated with the wireless communication system (100, 200) based on an authentication scenario corresponding to the selected subscription identifier type.

23. A non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor (212) of a user equipment in a wireless communication system, causes the processor (212) to:

construct, at a user equipment (102, 202) in a wireless communication system (100, 200), a unified subscription identifier data structure (400, 600);

store the unified subscription identifier data structure (400, 600), wherein the unified subscription identifier data structure (400, 600) comprises a plurality of fields (402-426, 602-616) that specify a selected one of two or more subscription identifier fields (300, 310, 320) associated with a selected subscription identifier type; and

use the selected one of two or more subscription identifier fields (300, 310, 320) in the unified subscription identifier data structure (400, 600) to access one or more networks associated with the wireless communication system (100, 200) based on an authentication scenario corresponding to the selected subscription identifier type.