5G Network Identity SUPI/SUCI

Home (http:/
/ 5G Network Identity SUPI/SUCI (http:/
/concealing-of-s

May 15, 2019 (http://5gblogs.com/2019/05/)

5G Network Identity SUPI/SUCI

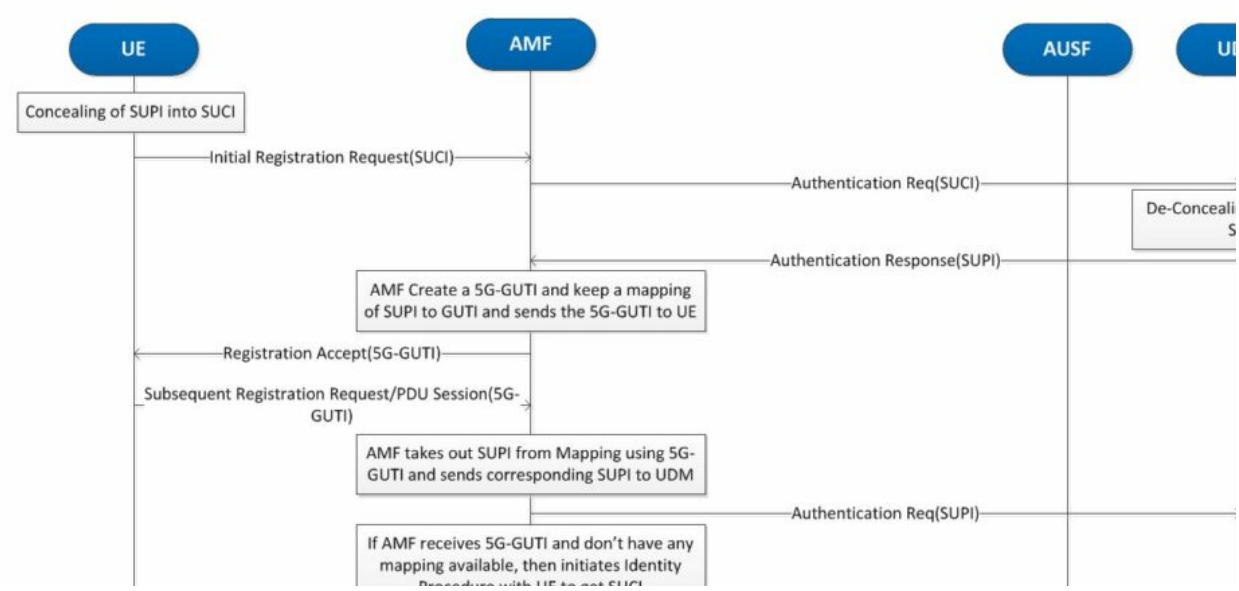
By **prasanna (http://5gblogs.com/author/prasanna/)** in **(http://5gblogs.com/concealing-of-supi-into-s
5G Core (http://5gblogs.com/category/5gcore/), 5GSecurity (http://5gblogs.com/category/5gsecurity/)**

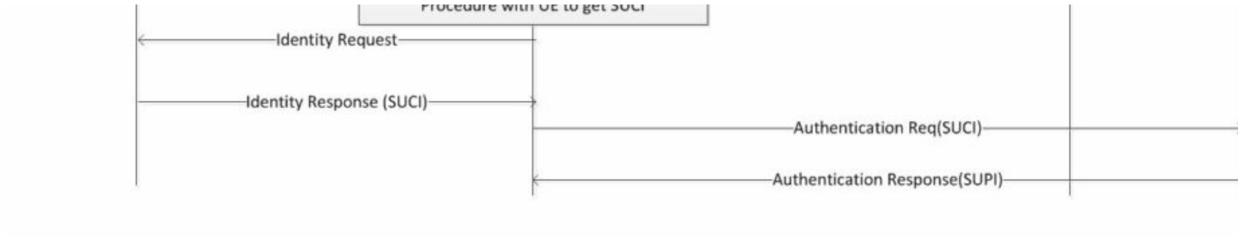
Introduction

In 5G in order to protect UE permanent Identity (SUPI- Subscription Permanent Identifier) UE never t
SUPI as it is. UE conceal(encrypt) SUPI using encryption scheme to create SUCI(Subscription Concealec
Identifier), before sending it to core network.

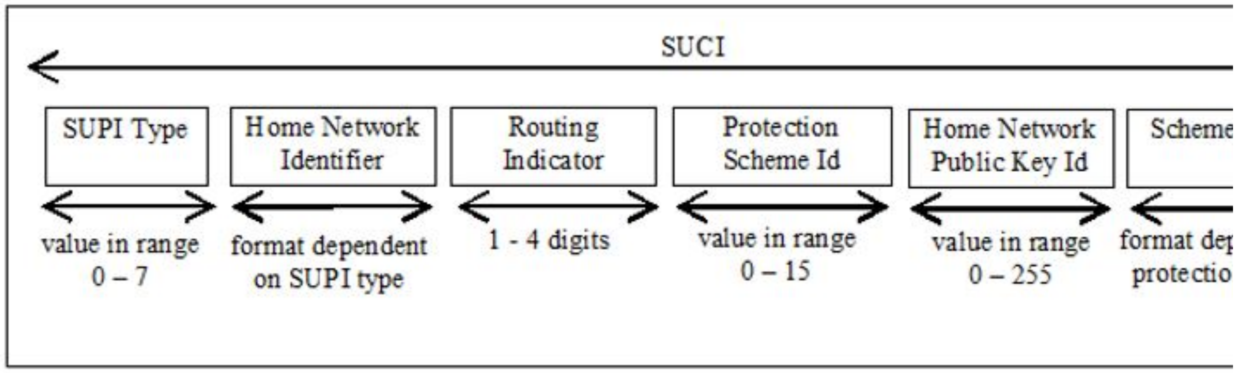
Concealing can be done in USIM or ME(Mobile Equipment) depending on the indication configured in
operator. If no indicator present, ME does the concealing.
In core network only UDM has authority to de-conceal the SUCI.

Identity flow between UE and Network


UE
AMF
AUSF
UI
Concealing of SUPI into SUCI
Initial Registration Request(SUCI)
Authentication Req(SUCI)
De-Conceali
S
Authentication Response(SUPI)
AMF Create a 5G-GUTI and keep a mapping of SUPI to GUTI and sends the 5G-GUTI to UE
Registration Accept(5G-GUTI)
Subsequent Registration Request/PDU Session(5G-GUTI)
AMF takes out SUPI from Mapping using 5G-GUTI and sends corresponding SUPI to UDM
Authentication Req(SUPI)
If AMF receives 5G-GUTI and don't have any mapping available, then initiates Identity
Procedure with UE to get SUCI



Decoding of SUCI



SUPI Type: consisting in a value in the range 0 to 7. It identifies the type of the SUPI concealed in the
following values are defined

- 0: IMSI
- 1: Network Specific Identifier
- 2 to 7: spare values for future use.

Home Network Identifier: identifying the home network of the subscriber.

When the SUPI Type is an IMSI, the Home Network Identifier is composed of two parts:
- Mobile Country Code (MCC), consisting of three decimal digits.
- Mobile Network Code (MNC), consisting of two or three decimal digits.

When the SUPI type is a Network Specific Identifier, the Home Network Identifier consists of a string o characters with a variable length representing a domain name. Ex. abc@xyz.com (mailto:abc@xyz.com

Routing Indicator: consisting of 1 to 4 decimal digits assigned by the home network operator and pr in the USIM.

Routing Indicator: consisting of 1 to 4 decimal digits assigned by the home network operator and pr in the USIM.

Protection Scheme Identifier: consisting in a value in the range of 0 to 15 and represented in 4 bits.

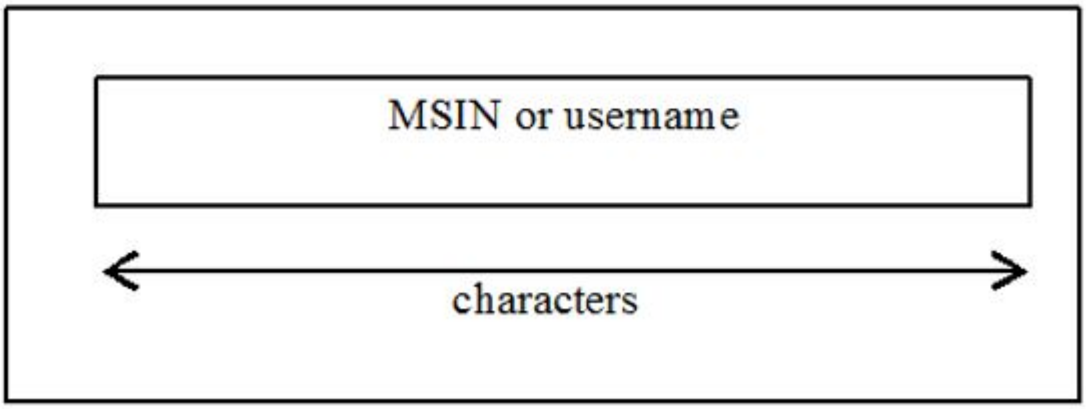
- null-scheme 0x0;
- Profile <A> 0x1;

- Profile <B> 0x2.

Home Network Public Key Identifier: consisting in a value in the range 0 to 255. It represents a pub provisioned by the HPLMN and it is used to identify the key used for SUPI protection. In case of null-sc being used, this data field shall be set to the value 0;

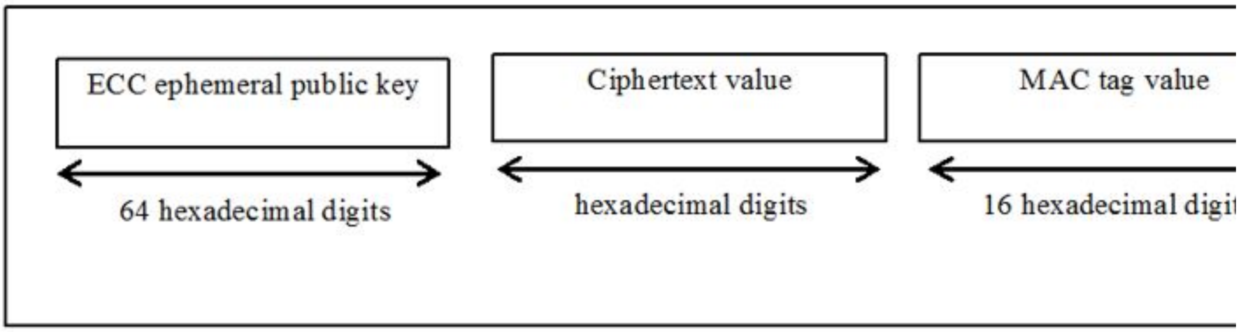
Scheme Output: consisting of a string of characters with a variable length or hexadecimal digits, depe the used protection scheme.

- **Null Scheme** – For null scheme no encryption happens and scheme output field is replaced by MS after taking out MCC and MNC from IMSI) value of IMSI as it is.



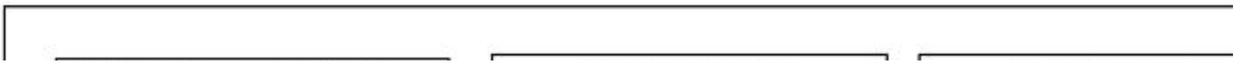
- **Elliptic Curve Integrated Encryption Scheme(ECIES) Profile A** – In this case scheme out put is fu divided in two parts:

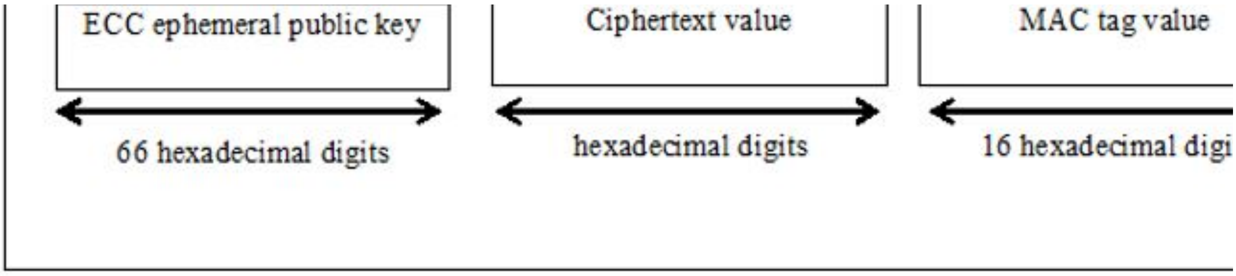
    1. ECC ephemeral public key 64 bits, freshly generated using the provisioned ECIES input parar
    2. Ciphered Text, is of variable length



- **Elliptic Curve Integrated Encryption Scheme(ECIES) Profile B** – In this case scheme out put is fu divided in two parts

    1. ECC ephemeral public key 66 bits, freshly generated using the provisioned ECIES input parar
    2. Ciphered Text, is of variable length





Note: Detailed into **Elliptic Curve Integrated Encryption Scheme(ECIES)** will be discussed in anothe

About Latest Posts

(http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

Prasanna (Http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

I am Prasanna Sahu. I live in Dublin Ireland. I work in 3gpp wireless technology UMTS and LTE and 5G. I love Photography, painting. Know more about me: http://in.linkedin.com/pub/prasanna-sahu/29/257/91a
See my photographs: http://www.flickr.com/photos/24986299@N05/

prasanna (http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

I am Prasanna Sahu. I live in Dublin Ireland. I work in 3gpp wireless technology l and LTE and 5G. I love Photography, painting. Know more about me: http://in.linkedin.com/pub/prasanna-sahu/29/257/91a See my photographs: http://www.flickr.com/photos/24986299@N05/

8 Comments

Alexandre CROGUENNEC Posted on4:03 pm - Oct

(http://in.linkedin.com /pub/prasanna-sahu/29 /257/91a)

Hello Prasanna Sahu,
Thanks for this very clear explanation, which is much more accessible to someone tr understand the difference between SUCI and SUPI than the thousands of pages of tl 5G standard 🙂 !
Unless I miss a point, I believe there is a small typo in the key size mentionned in you the information provided in TS133.501 Rel 16, Annex C.
To my understanding, Profile A, public key size is 256 bits (64 4-bit hexadecimal digits Profile B is 264bits (66 4-bit hexadecimal digits).
I leave it to you to check and eventually correct the text above the 2 images, if you be that makes sense.
Best regards,
Alex

Reply

Joby **Posted on4:35 pm - No**

(http://in.linkedin.com /pub/prasanna-sahu/29 /257/91a)

“Note: Detailed into Elliptic Curve Integrated Encryption Scheme(ECIES) will be discus another Blog”

Did you ever write another blog on this, Prasanna?

Reply

shasha **Posted on8:24 am - Ja**

how ip packet of app will know about UE?

(http://in.linkedin.com /pub/prasanna-sahu/29 /257/91a)

Reply

prasanna **Posted on5:30 pm - Ja**

Hi Sha,
UE IP address is either public Ip or NATed IP. so when UE is registered to the Netw UDM acts as a GW to UE. in case of NATTING it translate the public IP to UE ip bas

(http://in.linkedin.com /pub/prasanna-

sahu/29
/257/91a)

the application port number, in this case always UE need to initiate a request(sam
office network/home router network). in case of public IP UE can communicate w
outside application directly without address translation.

Reply

Raja **Posted on12:21 pm - Jan**

(http://in.linkedin.com
/pub/prasanna-
sahu/29
/257/91a)

How to deconceale SUCI to SUPI in UDM?

Reply

prasanna **Posted on12:32 pm - Feb**

(http://in.linkedin.com
/pub/prasanna-
sahu/29
/257/91a)

Hi Raja,
Concealing/deconcealing are done based on the algorithm and shared key. That r
both UDM and UE SIM has algorithm and shared key provisioned. when you buy
from store, they will provision your sim with appropriate algorithm and shared ke
is provisioned in UDM for that SIM. so now SIM and UDM they can conceal/de-con
SUPI based on the pre-agreed algorithm and keys.

Thanks

Reply

Pinak **Posted on11:58 am - Feb**

(http://in.linkedin.com
/pub/prasanna-
sahu/29
/257/91a)

After a lot of search, got the perfect explaination

Reply

Shri Ganesh **Posted on12:54 pm - Mar**

how the existing 4g sim can be updated thorugh OTA with required files to support 5

(http://in.linkedin.com/pub/prasanna-sahu/29/257/91a)

Reply

Search

Search here

Search

Recent Posts

- ✓ Emergency Services(E911) FallBack procedures in 5G (http://5gblogs.com/emergency-servicese911-fallback-procedures-in-5g/)
- ✓ EPS Fallback Voice in 5G (http://5gblogs.com/eps-fallback-voice-in-5g/)
- ✓ 5G Security (5G AKA Authentication) (http://5gblogs.com/5g-security-5g-aka-authentication/)
- ✓ 5G Quality Of Services (QoS) (http://5gblogs.com/5g-quality-of-services-qos/)
- ✓ 5G Network Identity SUPI/SUCI (http://5gblogs.com/concealing-of-supi-into-suci/)

Archives

- ✓ May 2020 (http://5gblogs.com/2020/05/)
- ✓ April 2020 (http://5gblogs.com/2020/04/)
- ✓ January 2020 (http://5gblogs.com/2020/01/)

- ✓ May 2019 (http://5gblogs.com/2019/05/)
- ✓ April 2019 (http://5gblogs.com/2019/04/)
- ✓ November 2018 (http://5gblogs.com/2018/11/)
- ✓ October 2018 (http://5gblogs.com/2018/10/)