

Exhibit B

Chart Detailing Samsung's Infringement of U.S. Patent No. 11,606,204

Network-1 Techs., Inc. v. Samsung Electronics Co., Ltd., et al., Case No. 2:25-cv-00667-JRG (E.D. Tex.)

Based on the information presently available to it, Network-1 is informed and believes that Samsung directly and indirectly infringes U.S. Patent No. 11,606,204 (“the ’204 Patent”). Samsung directly infringes claims 1, 3-6, 9-11, and 18-20 of the ’204 Patent when it makes, uses, sells, offers to sell, and/or imports the Accused Instrumentalities. Samsung indirectly infringes claims 1, 3-6, 9-11, and 18-20 of the ’204 Patent by actively inducing the direct infringement of its end-user customers, distributors, and re-sellers. For example, Samsung actively induces its end-user customers to use the Accused Instrumentalities, and Samsung actively induces its distributors and re-sellers to sell and/or offer to sell the Accused Instrumentalities to its end-user customers.

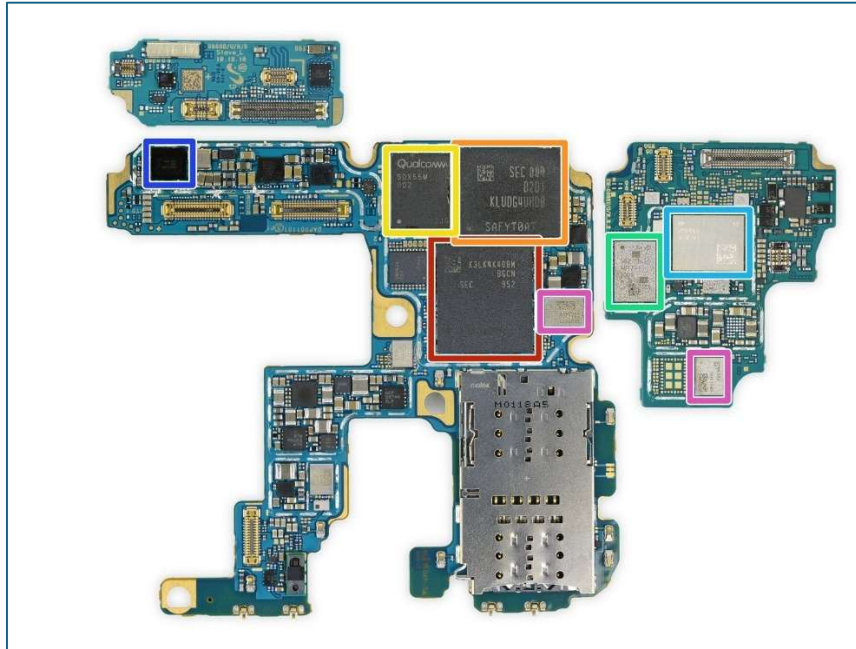
CLAIM 1		'204 PATENT V. SAMSUNG	
1[PRE]. A mobile device comprising:		The Accused Instrumentalities are mobile devices. More specifically, the Accused Instrumentalities include all Samsung mobile devices that support 5G standalone functionality, including (but not limited to) those listed in Network-1's infringement contentions and on the websites listed below. ¹ The ETSI specifications detail 5G standalone functionality for Samsung's mobile devices. Those ETSI 5G specification, which can be found at https://www.etsi.org/standards#Pre-defined%20Collections , include 3GPP TS 33.501 “5G; Security architecture and procedures for 5G System” (“ETSI TS 133 501”) and other standards and documents referenced therein. <i>See</i> ETSI TS 133 501 § 2 (References). This infringement claim chart generally cites the earliest version of the ETSI TS 133 501 specifications (e.g., V15.18.0 Release 15), but later versions are substantively identical.	

¹ <https://www.samsung.com/au/support/mobile-devices/esim-compatibility/>;
<https://www.samsung.com/levant/support/mobile-devices/galaxy-esim-and-supported-network-carriers/>;
<https://www.gsmarena.com/samsung-phones-f-9-15.php>; <https://www.samsung.com/us/mobile/5g/#see-our-latest>;
<https://www.samsung.com/us/mobile/5g/>;
<https://www.globalcertificationforum.org/gcf-certified-products/3gpp-certifications.html?dateCondition=before&certificationDateFrom=&certificationDateTo=&manufacturer=samsung-electronics-co-ltd>.

1(a) at least one processor; and

The Accused Instrumentalities include at least one processor.

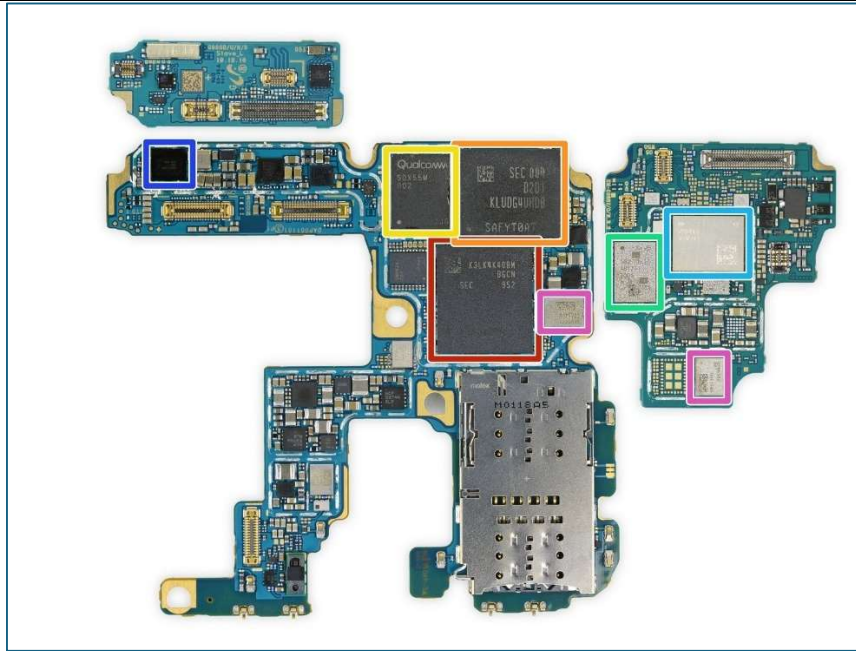
More specifically, the accused Samsung mobile devices have a processor as part of its 5G modem. This figure shows a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes hardware (in yellow, orange, and red) containing at least one processor:



<https://www.ifixit.com/Teardown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141>. This figure shows a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes hardware (in light blue) also containing a processor:

	<i>Id.</i> Each of the other Samsung mobile devices include similar 5G hardware.
1(b) at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least	The Accused Instrumentalities include at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network. More specifically, the accused Samsung mobile devices have data storage connected to the processor on its 5G modem. That memory stores instructions that can be executed by the processor. This figure shows a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes data storage (in orange, yellow, and red) connected to the processor(s):

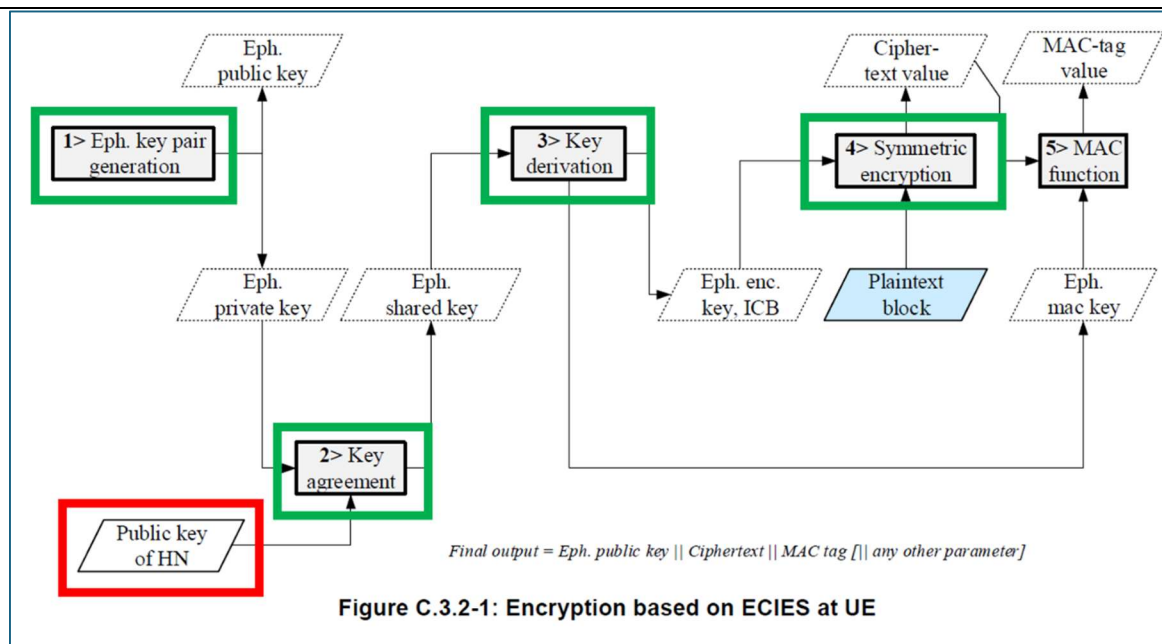
one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:



<https://www.ifixit.com/Teardown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141>. This figure shows a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes hardware (in light blue) also containing data storage connected to the processor:

	<i>Id.</i> Each of the other Samsung mobile devices include similar hardware.
1(b)(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store (1) a server public key, (2) a module identity, (3) cryptographic algorithms, and (4) a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm. More specifically, the data storage of the accused Samsung mobile devices include instructions that when executed cause the processor(s) to store (1) a public key of a home network (e.g., a server public key); (2) a SUPI (e.g., a module identity); (3) algorithms of an Elliptic Curve Integrated Encryption Scheme (ECIES) (e.g., cryptographic algorithms); and (4) a key K (e.g., a pre-shared secret key). The figure below illustrates ECIES encryption described by the ETSI specifications and implemented on the Samsung mobile devices. As that figure illustrates, the mobile device uses the public key of the home network (red) and various algorithms (green) in ECIES, including a symmetric ciphering algorithm (algorithm “4>”):

mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;



ETSI TS 133 501 at § C.3.2 (Processing on UE side) (annotated). In order for the accused Samsung mobile devices to implement ECIES, the cryptographic algorithms are stored on the data storage on the mobile devices. The ETSI specifications further explains that the public key of the home network, IMSI, and key K are stored on the data storage on the accused Samsung mobile devices:

- “5.2.5 Subscriber privacy
The UE shall support 5G-GUTI.
The SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC).
The Home Network Public Key shall be stored in the USIM.
The protection scheme identifier shall be stored in the USIM.
The Home Network Public Key Identifier shall be stored in the USIM.
The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in USIM.”

	ETSI TS 133 501 at §5.2.5 (Subscriber privacy).² • “6.2.2.2 Keys in the UE For every key in a network entity, there is a corresponding key in the UE. Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.
--	--

² All emphasis throughout this claim chart is added by Network1, unless stated otherwise.

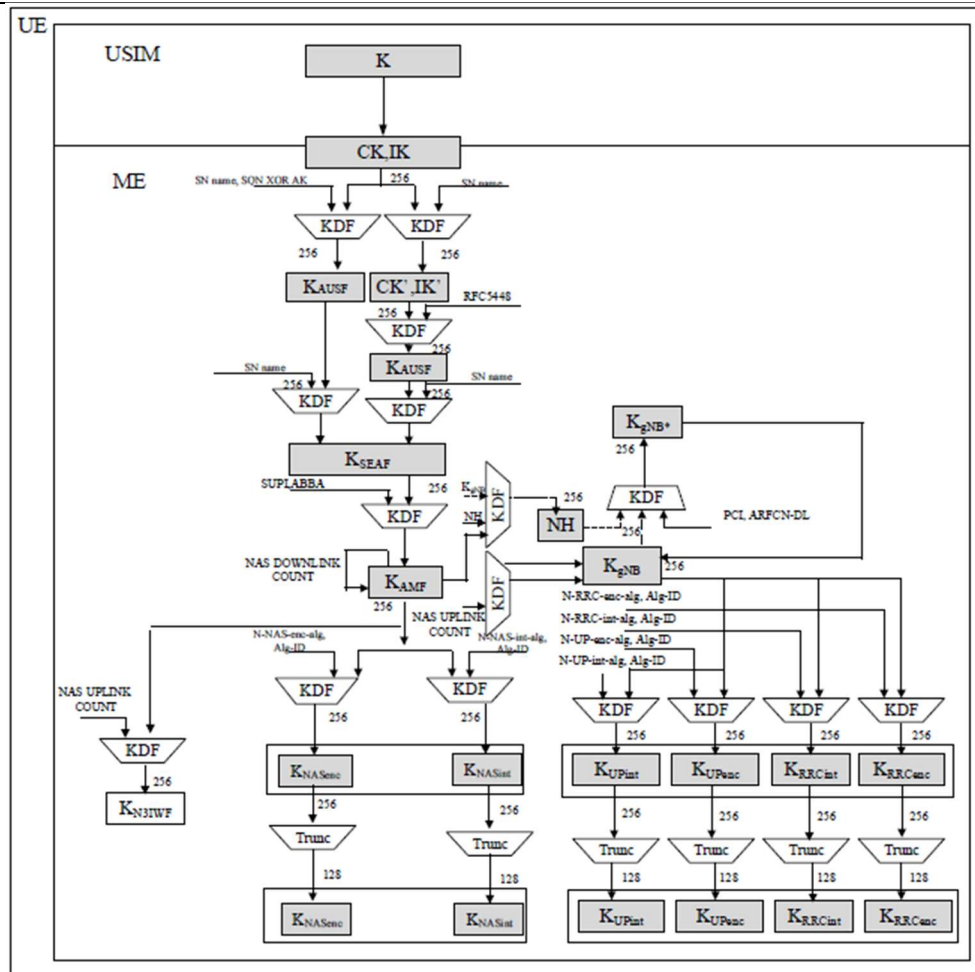


Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE

Keys in the USIM

The USIM shall store the same long-term key K that is stored in the ARPF.

During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME.

	If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI. Keys in the ME The ME shall generate the KAUSF from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3. When 5G AKA is used, the generation of RES* from RES shall be performed by the ME. The UE shall store the KAUSF . If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME.” ETSI TS 133 501 at §6.2.2.2 (Keys in the UE) “subscription credential(s): <u>The set of values in the USIM</u> and in the home operator's network, <u>consisting of at least the long-term key(s) and the subscription identifier SUPI</u>, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network. ETSI TS 133 501 at §3.1 (Definitions) The ETSI specifications explain that the SUPI is a permanent identifier for the mobile device: “6.12 Subscription identifier privacy 6.12.1 Subscription permanent identifier In the 5G system, <u>the globally unique 5G subscription permanent identifier is called SUPI</u> as defined in 3GPP TS 23.501 [2]. The SUCI is a privacy preserving identifier containing the concealed SUPI. The SUPI is privacy protected over-the-air by using the SUCI which is described in clause 6.12.2. Handling of SUPI and privacy provisioning related to concealing the SUPI shall be done according to the requirements specified in clause 5 and details provided in clause 6.12.2. 6.12.2 Subscription concealed identifier The SUBscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI. <u>The UE shall generate a SUCI using a protection scheme</u> with the raw public key, i.e. the Home Network Public Key, that was securely provisioned in control of the home network. <u>The protection schemes shall be the ones specified in Annex C of this document</u> or the ones specified by the HPLMN. The UE shall construct a scheme-input from the subscription identifier part of the SUPI as follows: - For SUPIs containing IMSI, the subscription identifier part of the SUPI includes the MSIN of the IMSI as defined in TS 23.003 [19]. - For SUPIs taking the form of a NAI, the subscription identifier part of the SUPI includes the "username" portion of the NAI as defined in NAI RFC 7542 [57].
--	--

	The UE shall execute the protection scheme with the constructed scheme-input as input and take the output as the Scheme Output.” ETSI TS 133 501 at §6.12 (Subscription identifier privacy).
1(b)(2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to derive a module private key and a corresponding module public key using the cryptographic algorithms. More specifically, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to derive an ephemeral private key and corresponding ephemeral public key using the ephemeral key pair generation algorithm. The figure below illustrates ECIES encryption described by the ETSI specifications and implemented on the Samsung mobile devices. As that figure illustrates, the mobile device derives the ephemeral private key (blue) and the ephemeral public key (orange) using the ephemeral key pair generation algorithm (green): Figure C.3.2-1: Encryption based on ECIES at UE

	ETSI TS 133 501 at § C.3.2 (Processing on UE side) (annotated). This process is further described in SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009 (available at http://www.secg.org/sec1-v2.pdf) (the “ECC specification”) and referenced by the ETSI specifications: • “C.3.2 Processing on UE side The ECIES scheme shall be implemented such that for computing a fresh SUCI, <u>the UE shall use the provisioned public key of the home network and freshly generated ECC (elliptic curve cryptography) ephemeral public/private key pair according to the ECIES parameters provisioned by home network. The processing on UE side shall be done according to the encryption operation defined in [SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009]</u> with the following changes to Section 3.8 and step 5 and 6 of Section 5.1.3. - generate keying data K of length enckeylen + icblen + mackeylen. - Parse the leftmost enckeylen octets of K as an encryption key EK, the middle icblen octets of K as an ICB, and the rightmost mackeylen octets of K as a MAC key MK. The final output shall be the concatenation of the ECC ephemeral public key, the ciphertext value, the MAC tag value, and any other parameters, if applicable.” ETSI TS 133 501 at § C.3.2 (Processing on UE side).
1(b)(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to derive a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function. More specifically, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to derive an ephemeral encryption key using the public key of the home network and the ephemeral private key using the key agreement function and key derivation function. The figure below illustrates ECIES encryption described by the ETSI specifications and implemented on the Samsung mobile devices. As that figure illustrates, the mobile device derives the ephemeral encryption key (pink) using the public key of the home network (red) and the ephemeral private key (blue) using the key agreement function (green) and key derivation function (green).

derivation function;

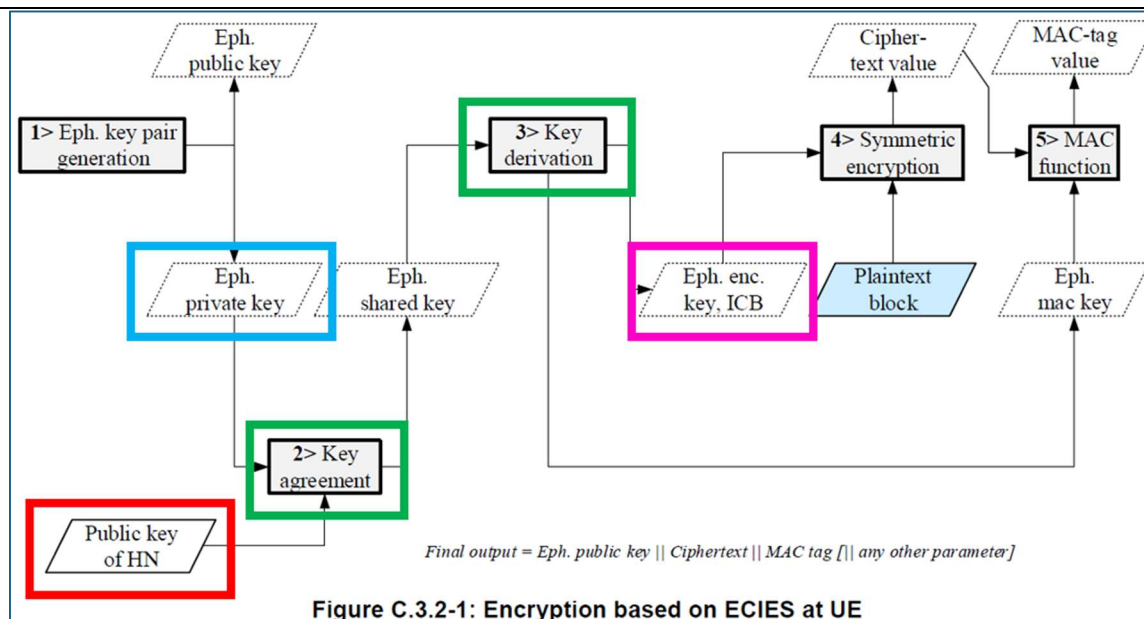


Figure C.3.2-1: Encryption based on ECIES at UE

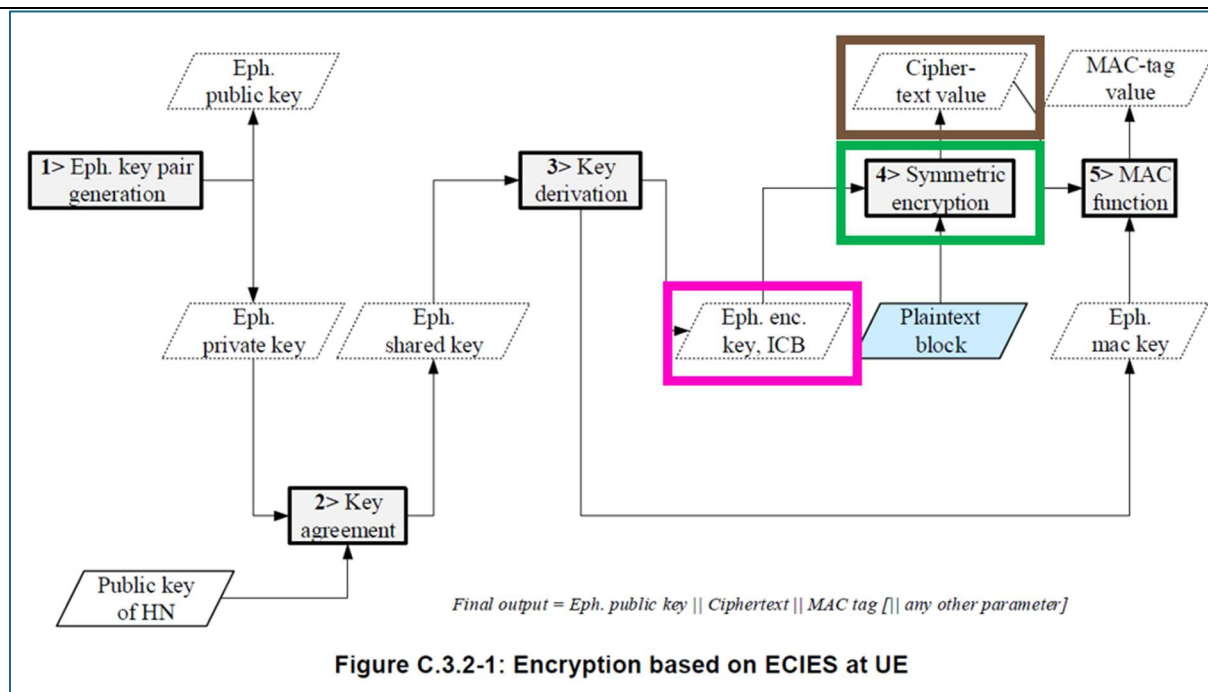
ETSI TS 133 501 at § C.3.2 (Processing on UE side) (annotated). Because ECIES is a symmetric encryption scheme (see “4> symmetric encryption” above), the ephemeral encryption key is a symmetric key.

The ETSI specifications also explain that the key derivation function used in this process is an American National Standards Institute standard X-9.63 key derivation function:

- “C.3.4.1 Profile A
The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:
 - EC domain parameters : Curve25519 [46]
 - EC Diffie-Hellman primitive : X25519 [46]
 - point compression : N/A
 - **KDF : ANSI-X9.63-KDF [29]**
 - Hash : SHA-256
 - SharedInfo1 : □(the ephemeral public key octet string – see [29] section 5.1.3)
 - MAC : HMAC–SHA-256
 - mackeylen : 32 octets (256 bits)
 - maclen : 8 octets (64 bits)
 - SharedInfo2 : the empty string

	- ENC : AES–128 in CTR mode - enckeylen : 16 octets (128 bits) - icblen : 16 octets (128 bits) - backwards compatibility mode : false C.3.4.2 Profile B The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following: - EC domain parameters : secp256r1 [30] - EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive [29] - point compression : true - <u>KDF : ANSI-X9.63-KDF [29]</u> - Hash : SHA-256 - SharedInfo1 : □ (the ephemeral public key octet string – see [29] section 5.1.3) - MAC : HMAC–SHA-256 - mackeylen : 32 octets (256 bits) - maclen : 8 octets (64 bits) - SharedInfo2 : the empty string - ENC : AES–128 in CTR mode - enckeylen : 16 octets (128 bits) - icblen : 16 octets (128 bits) - backwards compatibility mode : false” ETSI TS 133 501 at §C.3.4 (ECIES profiles).
1(b)(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to generate a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity. More specifically, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to generate ciphertext value and scheme output using the ephemeral encryption key and the symmetric encryption algorithm. The figure below illustrates ECIES encryption described by the ETSI specifications and implemented on the Samsung mobile devices. As that figure illustrates, the mobile device generates a ciphertext value (brown) using the ephemeral encryption key and the symmetric encryption algorithm (green):

includes the module identity;



ETSI TS 133 501 at § C.3.2 (Processing on UE side) (annotated). The below example from the ETSI specification further illustrates that the cyphertext value includes and encrypted version of the SUPI and is further included in the scheme output:

C.4.3 ECIES Profile A

The following test data set corresponds to SUCI computation in the UE for **IMSI-based SUPI** and ECIES Profile A.

IMSI consists of MCC|MNC: '274012' and MSIN: '001002086'

ECIES test data

The ECIES Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with the following data

...

Plaintext block:

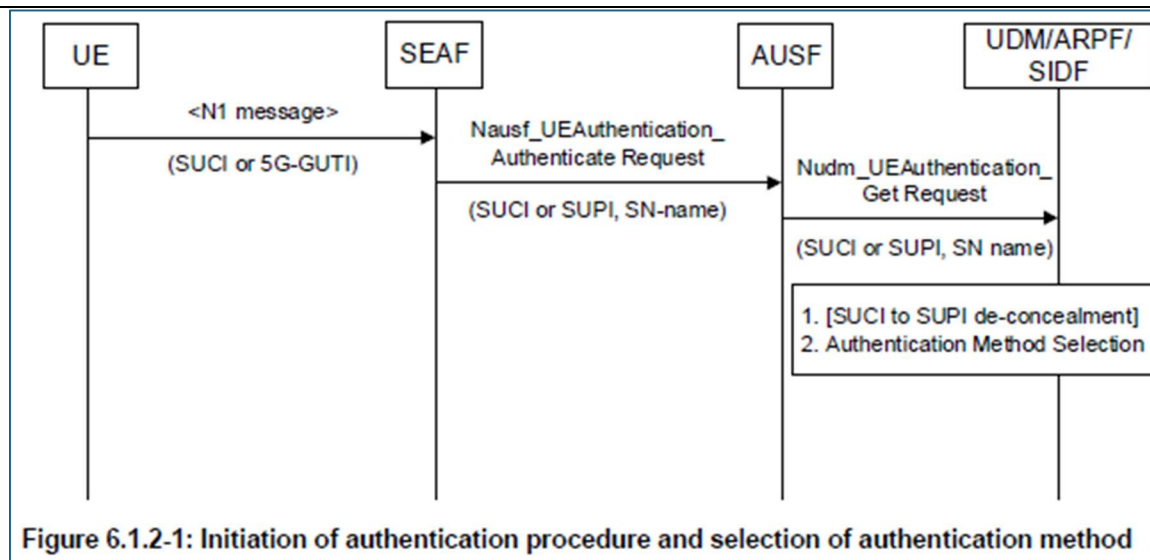
'00012080f6'

Cipher-text value:

'cb02352410'

	... Scheme Output: 'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457d<u>cb02352410</u> cddd9e730ef3fa87' C.4.4 ECIES Profile B The following test data set corresponds to ECIES-based encryption in the UE for <u>IMSI-based SUPI</u> and ECIES Profile B. <u>IMSI consists of MCC MNC: '274012' and MSIN: '001002086'</u> ECIES test data The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data: ... Scheme-input corresponding to the plaintext-block: <u>'00012080F6'</u> Cipher-text value: <u>'46A33FC271'</u> ... Scheme Output: '039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D <u>146A33FC271</u>6AC7DAE96AA30A4D''' ETSI TS 133 501 at § C.4 (Implementers' test data).
1(b)(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to send a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity. More specifically, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to send a N1 message to a server for the wireless network which includes the cypher text and the mobile device's ephemeral public key. The below figure from the ETSI specifications illustrates that initiation of the authentication procedure. As the figure illustrates, the mobile device is capable of transmitting an "N1 message" to the mobile network:

ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and



ETSI TS 133 501 at § 6.1.2 (Initiation of authentication and selection of authentication method). The ETSI specification explains that on initial registration, the N1 message includes the SUCI:

- “The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf_UEAuthentication service by sending a Nausf_UEAuthentication_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

The Nausf_UEAuthentication_Authenticate Request message shall contain either:

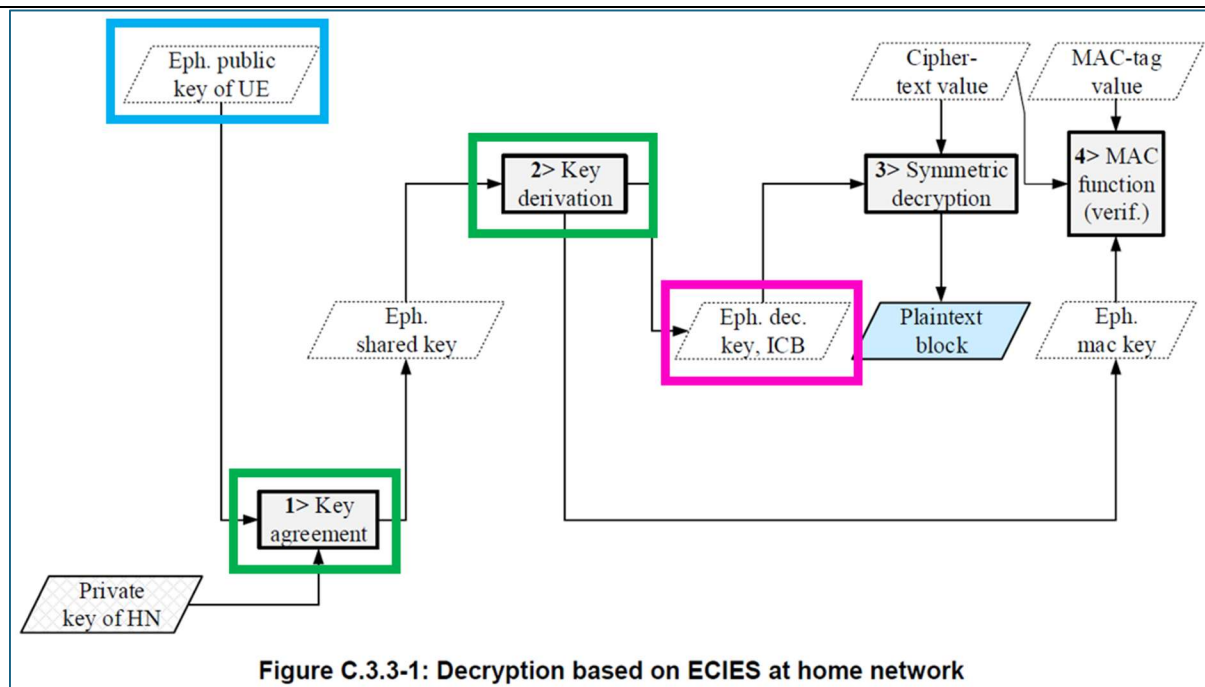
- SUCI, as defined in the current specification, or
- SUPI, as defined in TS 23.501 [2].

The SEAF shall include the SUPI in the Nausf_UEAuthentication Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf_UEAuthentication Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.”

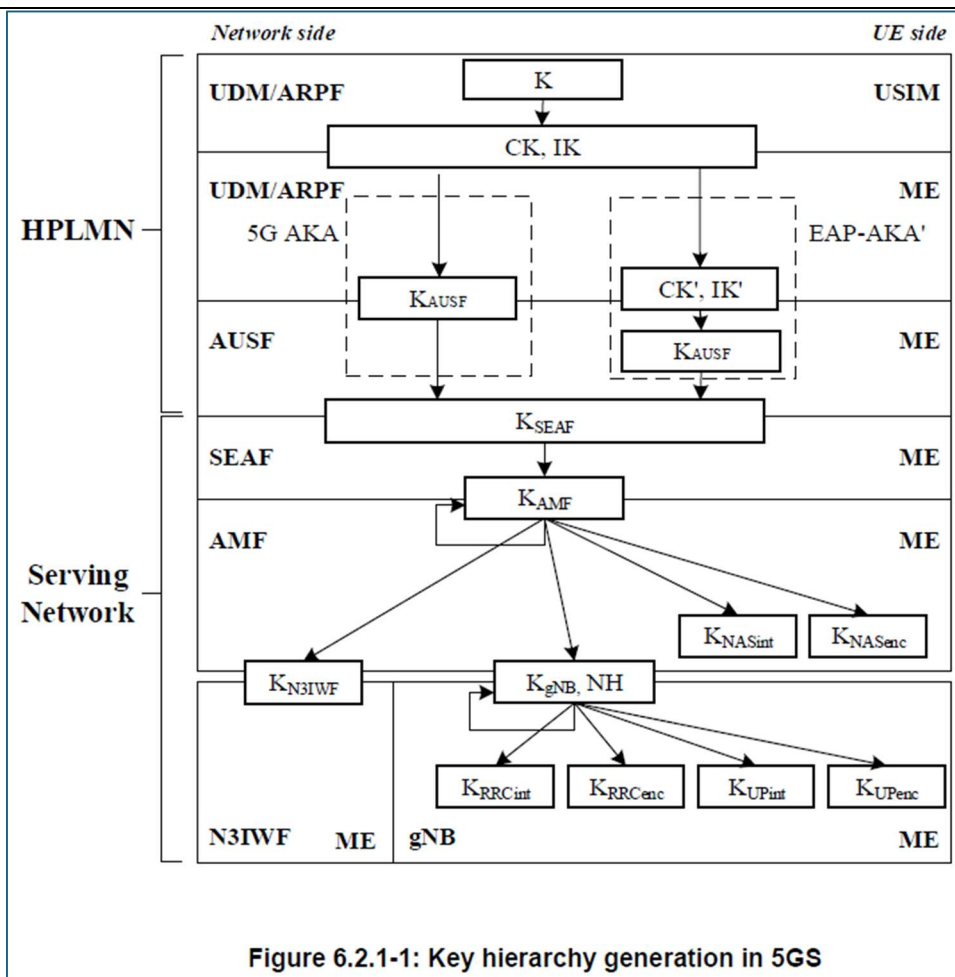
Id. The ETSI specification explains that the SUCI contains the output from the ECIES:

	“subscription concealed identifier: A one-time use subscription identifier, called the Subscription Concealed Identifier (SUCI), which <u>contains the Scheme-Output</u>, and additional non-concealed information needed for home network routing and protection scheme usage.” ETSI TS 133 501 at § 3.1 (Definitions). The below example from the ETSI specification further illustrates that the scheme output includes cyphertext value and the mobile device’s ephemeral public key: C.4.3 ECIES Profile A The following test data set corresponds to SUCI computation in the UE for IMSI-based SUPI and ECIES Profile A. IMSI consists of MCC MNC: '274012' and MSIN: '001002086' ECIES test data The ECIES Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with the following data ... Eph. Public Key: <u>'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457d'</u> ... Plaintext block: '00012080f6' Cipher-text value: <u>'cb02352410'</u> ... Scheme Output: <u>'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457dcb02352410cddd9e730ef3fa87'</u> C.4.4 ECIES Profile B The following test data set corresponds to ECIES-based encryption in the UE for IMSI-based SUPI and ECIES Profile B. IMSI consists of MCC MNC: '274012' and MSIN: '001002086' ECIES test data The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data: ... Eph. Public Key:
--	--

	If compressed: <u>'039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1'</u> ... Scheme-input corresponding to the plaintext-block: '00012080F6' Cipher-text value: <u>'46A33FC271'</u> ... Scheme Output: <u>'039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D</u> <u>146A33FC271</u>16AC7DAE96AA30A4D'" ETSI TS 133 501 at § C.4 (Implementers' test data). The N1 message is capable of causing a server of the network to derive the ephemeral decryption key using the ephemeral public key of the mobile device. The below figure from the ETSI specification illustrates this as the ECIES at the home network, where the server on the home network derives the ephemeral decryption key (pink) using the ephemeral public key of the mobile device (blue) and the key agreement and key derivation algorithms (green):
--	---



ETSI TS 133 501 at § C.3.3 (Processing on home network side) (annotated). Because the encryption algorithm is a symmetric algorithm, the ephemeral decryption key is symmetric and the same as the ephemeral encryption key. The N1 message is also capable of causing the wireless network to select the key K for the mobile device based on the SUPI. The below figure from the ETSI specifications illustrates the key hierarchy of the mobile network and explains that the key K and the corresponding ciphering key (“CK”) and integrity key (“IK”) are held in the Unified Data Management (“UDM”):

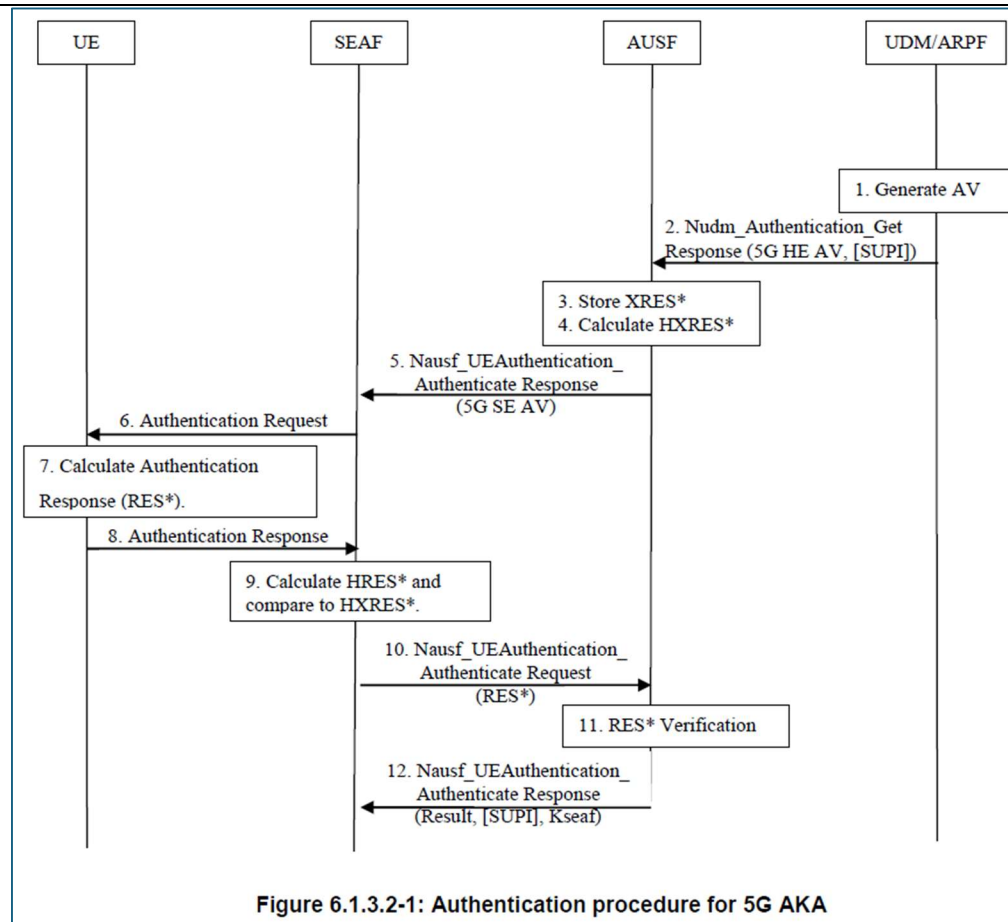


ETSI TS 133 501 at § 6.2.1 (Key hierarchy). The ETSI specification further explains that the UDM controls the security of the keys and decrypts the SUCI to extract the SUPI and use the SUPI to identify the corresponding key:

- “5.8 Requirements on the UDM
5.8.1 Generic requirements

The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected.

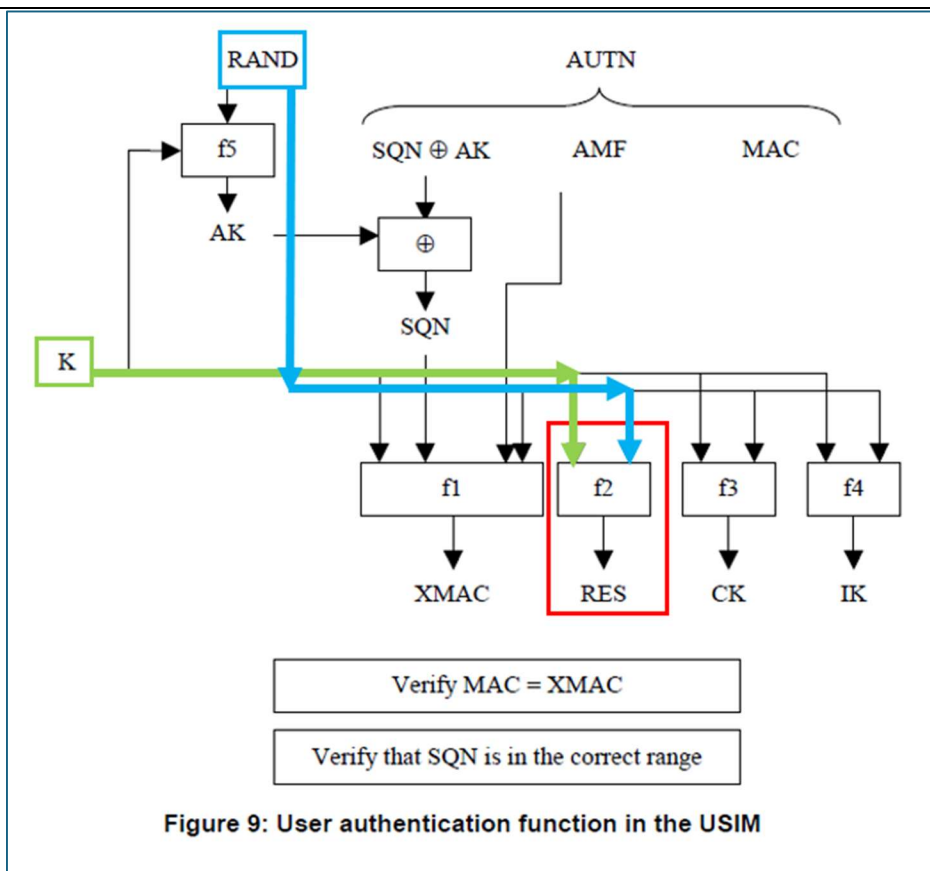
	NOTE 1: Security mechanisms for protection of subscription credentials in ARPF are left to implementation. NOTE 2: Security mechanisms for storage of subscription credentials in the UDR and for the transfer of authentication subscription data (as specified in 3GPP TS 29.505 [70]) between UDR and ARPF are left to implementation. 5.8.2 Subscriber privacy related requirements to UDM and SIDF The SIDF is responsible for de-concealment of the SUCI and shall fulfil the following requirements: - The SIDF shall be a service offered by UDM. - The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI. The Home Network Private Key used for subscriber privacy shall be protected from physical attacks in the UDM. The UDM shall hold the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy. The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.” ETSI TS 133 501 at §5.8 (Requirements on the UDM).
1(b)(6) authenticating with the wireless network using a message digest with the pre-shared secret key.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to authenticate with the wireless network using a message digest with the pre-shared secret key. More specifically, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to authenticate the mobile device with the mobile network by generating a RES and RES* (both of which are message digest) with the key K in response to an authentication request. This step is illustrated as step 7 in the below figure from the ETSI specification describing the 5G AKA authentication process, where the RES* is calculated:



ETSI TS 133 501 at § 6.1.3.2 (Authentication procedure for 5G AKA). In 5G AKA, RES* is generated by the mobile device using the key K (and keys generated from key K: CK and IK) and the RES message digest:

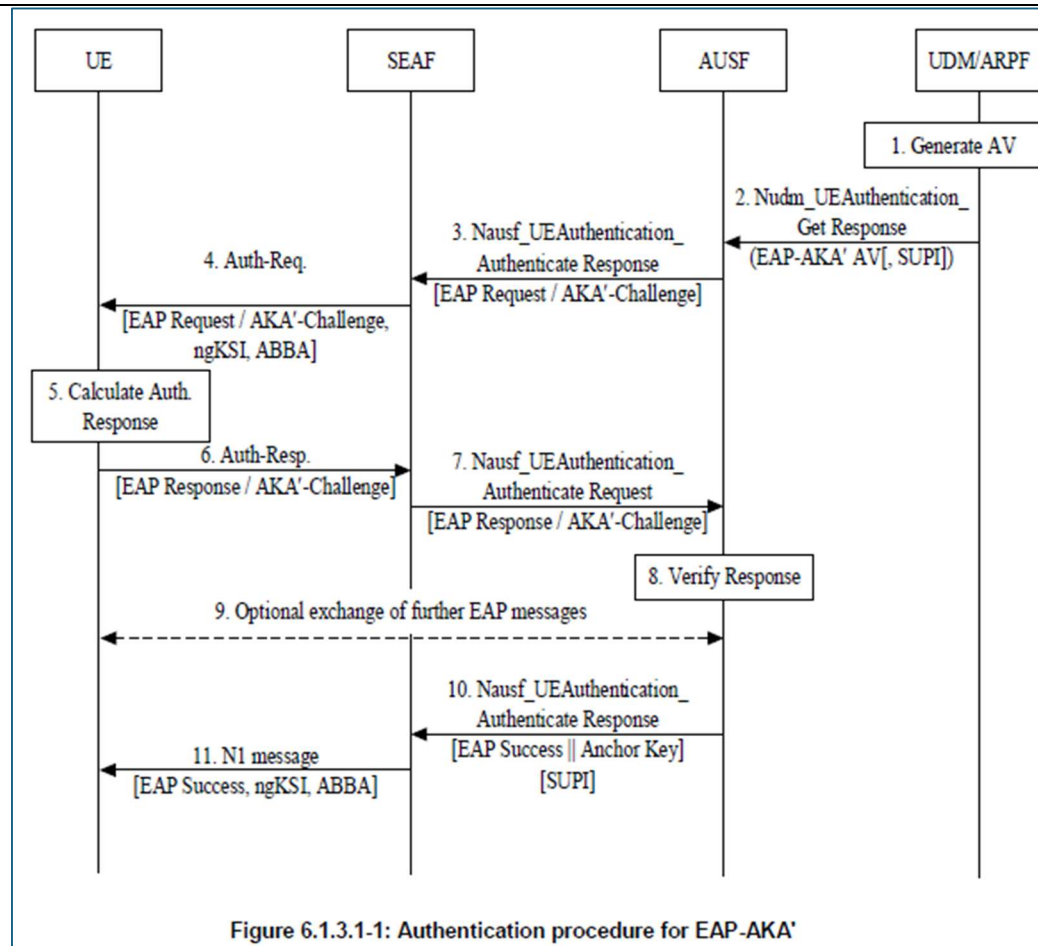
- “7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102[9]. **If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME.** If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. **The ME then shall compute RES* from RES according to Annex A.4. The ME shall calculate KAUSF from CK||IK**

	<u>according to clause A.2.</u> The ME shall calculate KSEAF from KAUSF according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN." ETSI TS 133 501 at § 6.1.3.2 (Authentication procedure for 5G AKA). • "A.4 RES* and XRES* derivation function When deriving RES* from RES, RAND, and serving network name in the UE and when deriving XRES* from XRES, RAND, and the serving network name in the ARPF, <u>the following parameters shall be used to form the input S to the KDF.</u> - FC = 0x6B, - P0 = serving network name, - L0 = length of the serving network name (variable length as specified in 24.501 [35]), - P1 = RAND, - L1 = length of RAND (i.e. 0x00 0x10), - P2 = RES or XRES, - L2 = length RES or XRES (i.e. variable length between 0x00 0x04 and 0x00 0x10). The input key KEY shall be equal to the concatenation CK IK of CK and IK. The serving network name shall be constructed as specified in clause 6.1.1.4. The (X)RES* is identified with the 128 least significant bits of the output of the KDF." ETSI TS 133 501 at Annex A.4. The ETSI TS 133 102 standard illustrates how the mobile device is also capable of calculating RES with Key K (and generate keys CK and IK from key K):
--	--



ETSI TS 133 102 at § 6.3.3 (Authentication and key agreement) (annotated); *see also* ETSI TS 133 501 § 2 (cross referencing ETSI TS 133 102 as “3GPP TS 33.102”).

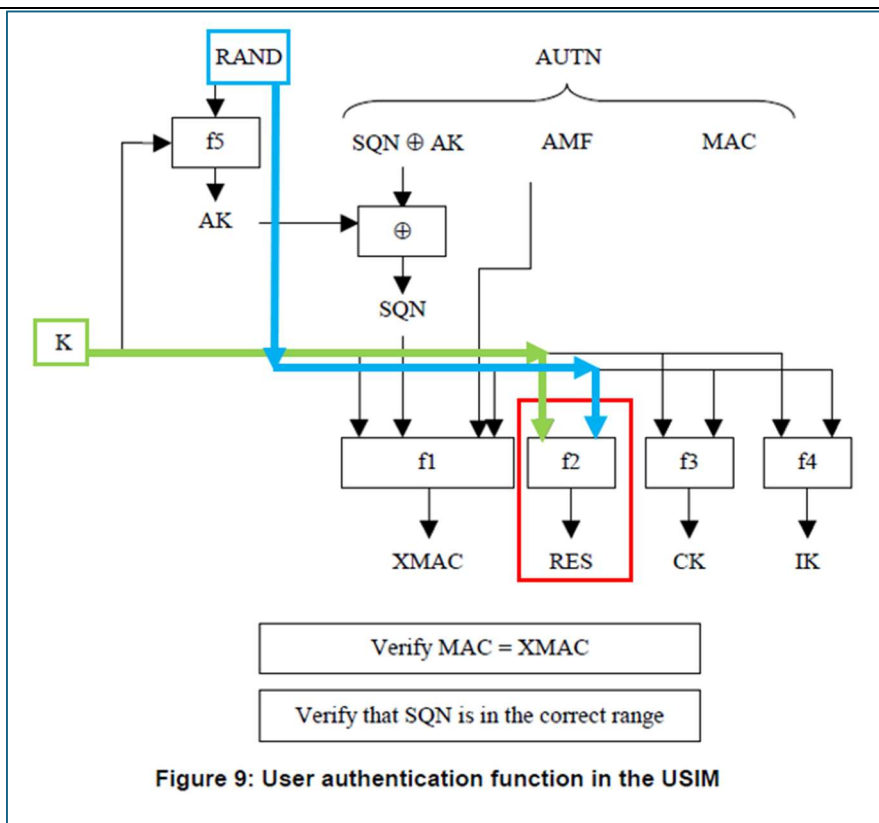
Calculating RES is also illustrated as step 5 in the below figure from the ETSI specification describing the EAP-AKA’ authentication process, where the Authentication Response is calculated:



ETSI TS 133 501 at § 6.1.3.1 (Authentication procedure for EAP-AKA'). In EAP-AKA', a RES is computed and included in an Authentication Response:

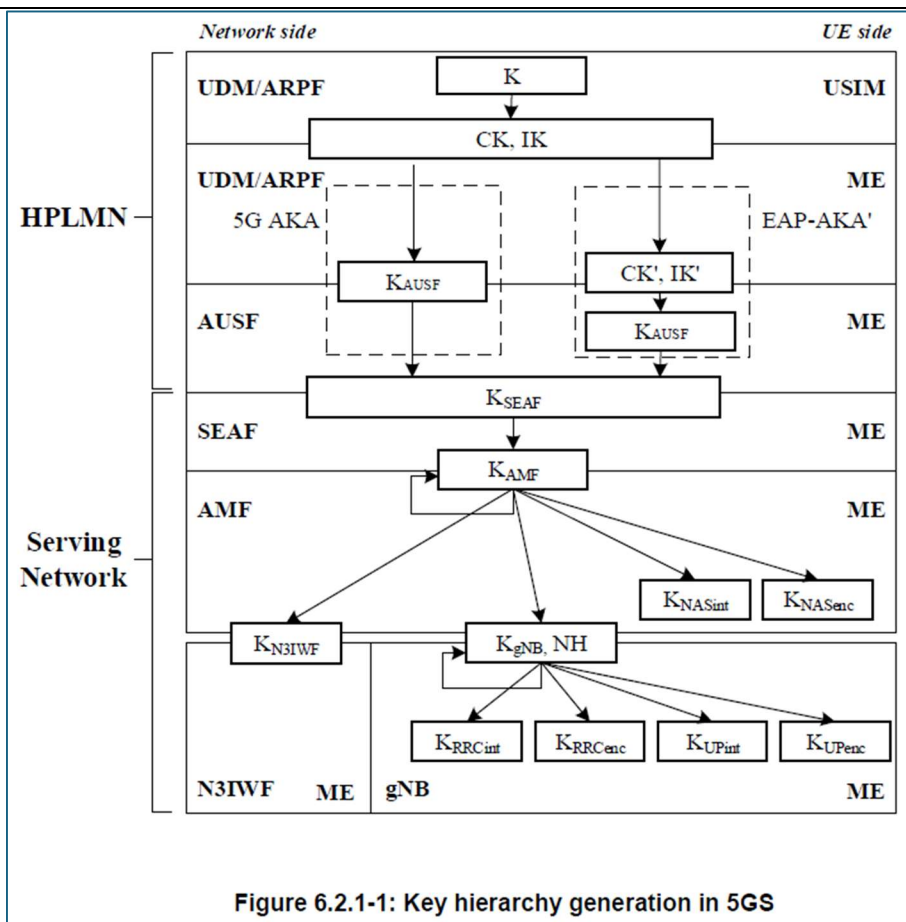
- “5. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [9]. If so, the USIM computes a response RES. The USIM shall return **RES, CK, IK to the ME**. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall

	ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME shall derive CK' and IK' according to Annex A.3. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in subclause 6.1.3. 3. 6. The UE shall send the EAP-Response/AKA'-Challenge message to the SEAF in a NAS message Auth-Resp message.” <i>Id.</i> As noted above, the ETSI TS 133 102 standard explains that mobile device derives RES from (i) RAND and (ii) the key K (“K”):
--	---

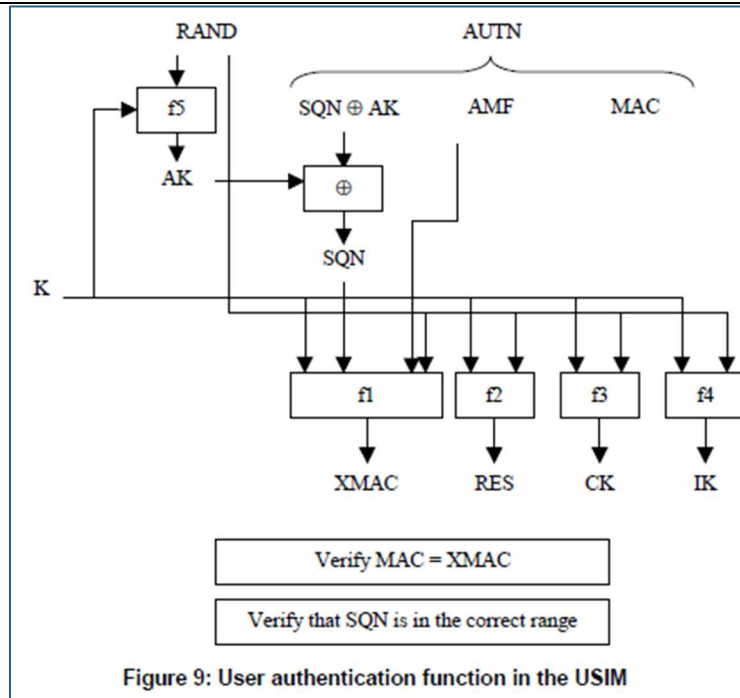


ETSI TS 133 102 at § 6.3.3 (Authentication and key agreement); *see also* ETSI TS 133 501 § 2 (cross referencing ETSI TS 133 102 as “3GPP TS 33.102”).

CLAIM 3	'204 PATENT V. SAMSUNG
3. The mobile device of claim 1, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store a pre-shared secret key, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network. More specifically, as explained above, the pre-shared secret key of the accused Samsung mobile devices comprises a key K. <i>Supra</i> element 1(b)(1). As explained above, the instructions stored on the accused Samsung mobile devices are capable of causing the processor(s) to authenticate the mobile device with the mobile network by generating a response, RES*. <i>Supra</i> element 1(b)(6). The 5G standard explains that the mobile device is capable of generating RES* using a random value and the Key K. Specifically, the mobile device is capable of first deriving IK and CK using key K:

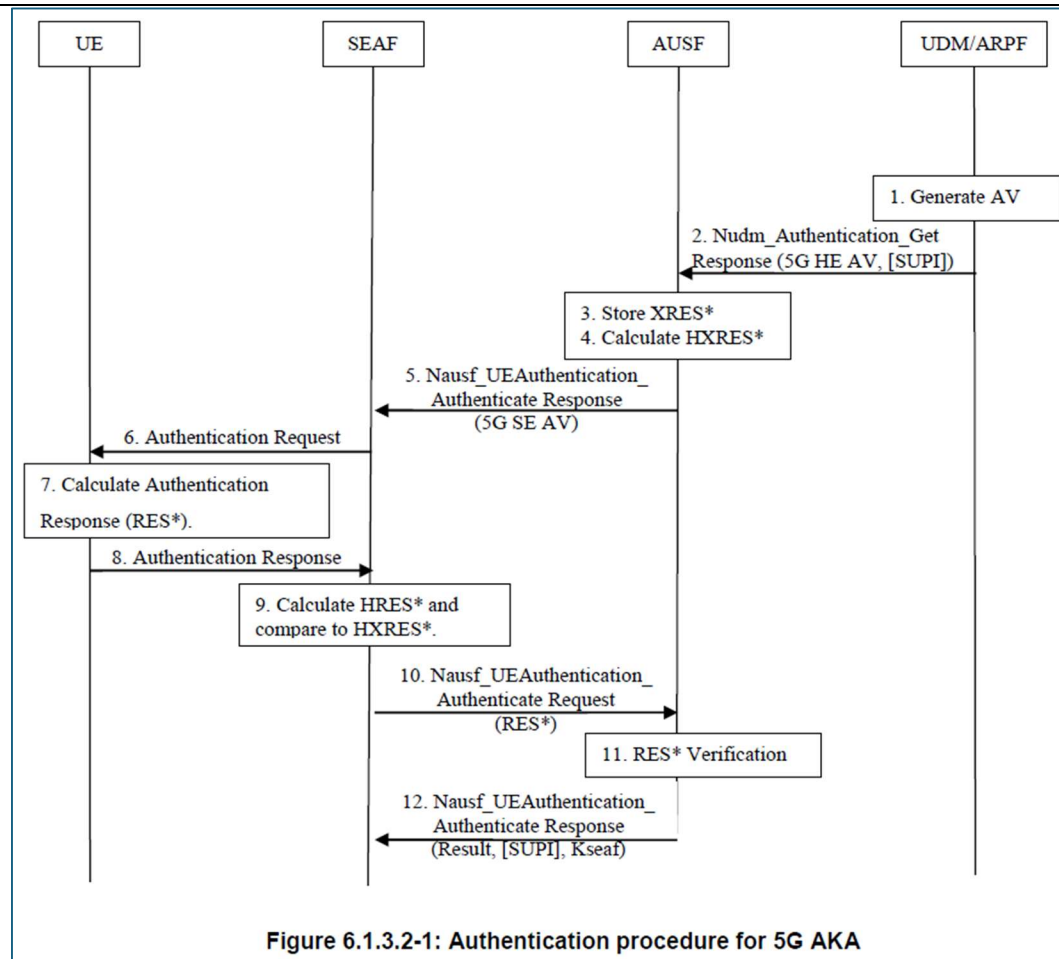


ETSI TS 133 501 at § 6.2.1 (Key hierarchy). The 3GPP TS 33.102 standard illustrates how the mobile device is capable of deriving the CK and IK from Key K:



ETSI TS 133 102 § 6.3.3 (Authentication and key agreement).

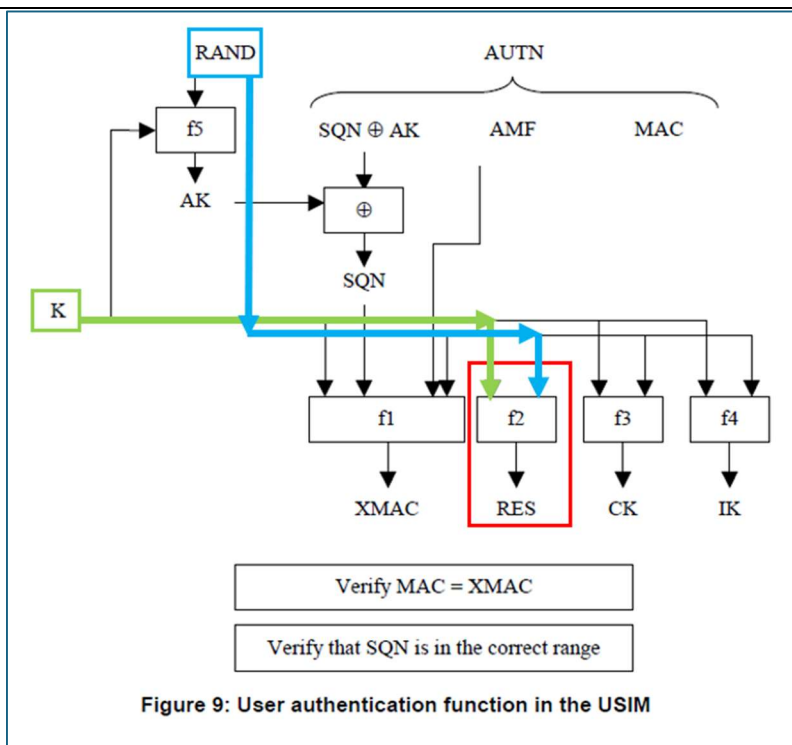
The 5G standard explains that the wireless device is capable of receiving the random value from the wireless network:



ETSI TS 133 501 at § 6.1.3.2 (Authentication procedure for 5G AKA).

- “**6. The SEAF shall send RAND**, AUTN to the UE in a NAS message Authentication Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the KAMF and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM.”

	ETSI TS 133 501 at § 6.1.3.2 (Authentication procedure for 5G AKA). RES* is generated by the mobile device using the key K (and its constituent parts, CK and IK) and RAND: • “7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102[9]. <u>If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME.</u> If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES* from RES according to Annex A.4. The ME shall calculate KAUSF from CK IK according to clause A.2. The ME shall calculate KSEAF from KAUSF according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.” ETSI TS 133 501 at § 6.1.3.2 (Authentication procedure for 5G AKA). • “A.4 RES* and XRES* derivation function When deriving RES* from RES, RAND, and serving network name in the UE and when deriving XRES* from XRES, RAND, and the serving network name in the ARPF, <u>the following parameters shall be used to form the input S to the KDF.</u> - FC = 0x6B, - P0 = serving network name, - L0 = length of the serving network name (variable length as specified in 24.501 [35]), - P1 = RAND, - L1 = length of RAND (i.e. 0x00 0x10), - P2 = RES or XRES, - L2 = length RES or XRES (i.e. variable length between 0x00 0x04 and 0x00 0x10). The input key KEY shall be equal to the concatenation CK IK of CK and IK. The serving network name shall be constructed as specified in clause 6.1.1.4. The (X)RES* is identified with the 128 least significant bits of the output of the KDF.” ETSI TS 133 501 at Annex A.4. The ETSI TS 133 102 standard also explains that mobile device derives RES (an input to RES*, as noted above) from (i) RAND and (ii) the key K (“K”):
--	--



ETSI TS 133 102 at § 6.3.3 (Authentication and key agreement); *see also* ETSI TS 133 501 § 2 (cross referencing ETSI TS 133 102 as “3GPP TS 33.102”).

See also evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 4	'204 PATENT V. SAMSUNG
4. The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store a pre-shared secret key, wherein in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K. More specifically, as explained above, the pre-shared secret key of the accused Samsung mobile devices comprises a key K. <i>Supra</i> element 1(b)(1); claim 3. As explained above, and in more detail below, the key K is stored within a USIM, which comprises a subscriber identity module card. <i>Supra</i> element 1(b)(1): ETSI TS 133 501 at §5.2.5 (Subscriber privacy). • “6.2.2.2 Keys in the UE For every key in a network entity, there is a corresponding key in the UE. Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.

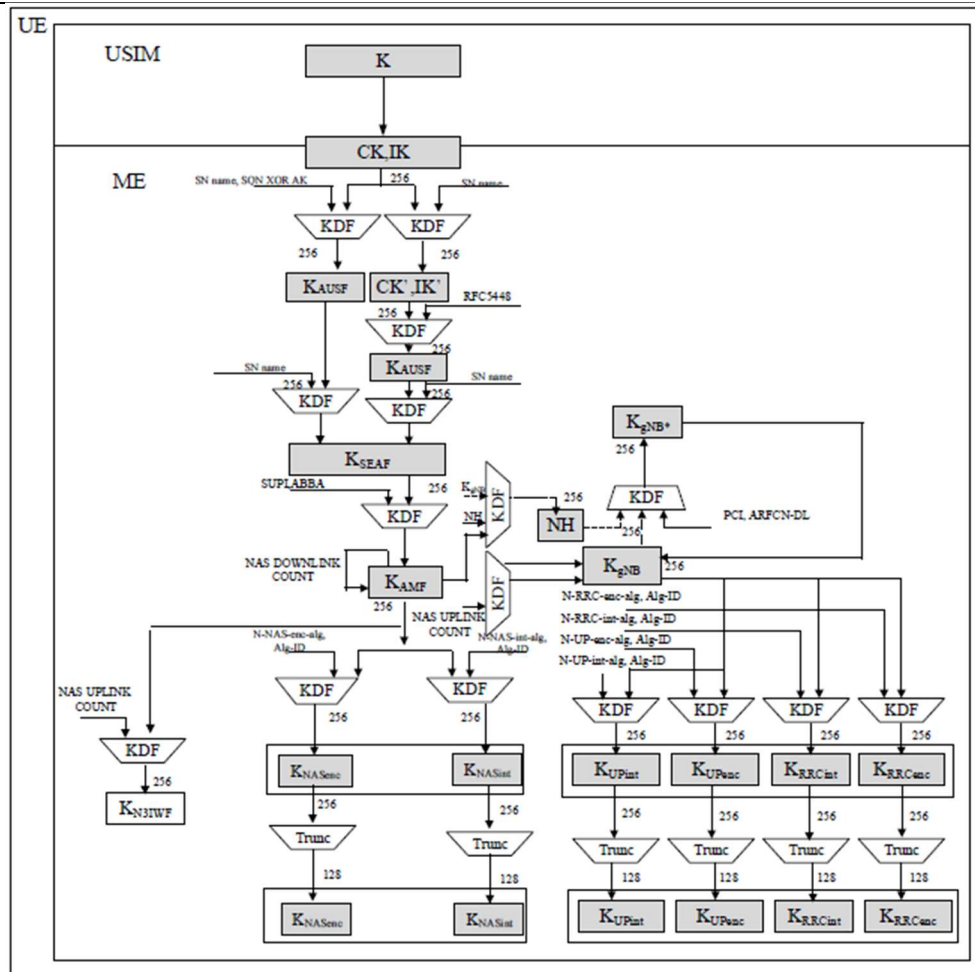


Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE
Keys in the USIM

The USIM shall store the same long-term key K that is stored in the ARPF.

During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME.

	If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI. Keys in the ME The ME shall generate the KAUSF from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3. When 5G AKA is used, the generation of RES* from RES shall be performed by the ME. The UE shall store the KAUSF . If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME.” ETSI TS 133 501 at §6.2.2.2 (Keys in the UE) • “subscription credential(s): <u>The set of values in the USIM</u> and in the home operator's network, <u>consisting of at least the long-term key(s) and the subscription identifier SUPI</u>, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.” ETSI TS 133 501 at §3.1 (Definitions). <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.
--	--

CLAIM 5	'204 PATENT V. SAMSUNG
5. The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store the pre-shared secret key before the the mobile device communicates with the wireless network. More specifically, the accused Samsung mobile devices include code that provide capability for the devices to store the Key K before the mobile device communicates with the wireless network. For example, the 5G standards explain that the key K is stored on the data storage on the accused Samsung mobile devices before authenticating the device on the wireless network and communicating with the wireless network: • “5.2.5 Subscriber privacy The UE shall support 5G-GUTI. The SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC). <u>The Home Network Public Key shall be stored in the USIM.</u> The protection scheme identifier shall be stored in the USIM. The Home Network Public Key Identifier shall be stored in the USIM. The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in USIM.” ETSI TS 133 501 at §5.2.5 (Subscriber privacy). • “6.2.2.2 Keys in the UE For every key in a network entity, there is a corresponding key in the UE. Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.

	If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI. Keys in the ME The ME shall generate the KAUSF from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3. When 5G AKA is used, the generation of RES* from RES shall be performed by the ME. The UE shall store the KAUSF . If the USIM supports 5G parameters storage, KAUSF shall be stored in the USIM. Otherwise, KAUSF shall be stored in the non-volatile memory of the ME.” ETSI TS 133 501 at §6.2.2.2 (Keys in the UE) • “subscription credential(s): <u>The set of values in the USIM</u> and in the home operator's network, <u>consisting of at least the long-term key(s) and the subscription identifier SUPI</u>, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.” ETSI TS 133 501 at §3.1 (Definitions). <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.
--	---

CLAIM 6	'204 PATENT V. SAMSUNG
6. The mobile device of claim 1, further comprising, in step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein, in step (2), the module public key and the module private key are derived using the standard curve.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein the module public key and the module private key are derived using the standard curve. More specifically, the accused Samsung mobile devices include parameters for the cryptographic algorithms are stored in the data storage, and those parameters include Profiles that include a standard curve (including Curve25519 and secp256r1) that are used as parameters when deriving the public key and private key of the mobile device: • “C.3.4.0 General Unless otherwise stated, the ECIES profiles follow the terminology and processing specified in SECG version 2 [29] and [30]. The profiles shall use "named curves" over prime fields.” ETSI TS 133 501 at § C.3.4.0 ([ECIES profiles] General) • “C.3.4.1 Profile A The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following: - EC domain parameters : Curve25519 [46]....” ETSI TS 133 501 at § C.3.4.2 (Profile A) • C.3.4.2 Profile B The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following: - EC domain parameters : secp256r1 [30]....” ETSI TS 133 501 at § C.3.4.2 (Profile B) • “C.3.2 Processing on UE side The ECIES scheme shall be implemented such that for computing a fresh SUCI, the UE shall use the provisioned public key of the home network and freshly generated ECC (elliptic curve cryptography) ephemeral public/private key pair according to the ECIES parameters provisioned by home network”

	ETSI TS 133 501 at § C.3.2 (Processing on UE side). Curve25519 and secp256r1 are examples of standard curves. For example, IETF RFC 7748: “Elliptic Curves for Security” (referenced as [46] in ETSI TS 133 501) describes the Curve25519: • “4.1. Curve25519 For the ~128-bit security level, the prime $2^{255} - 19$ is recommended for performance on a wide range of architectures. Few primes of the form $2^c - s$ with s small exist between 2^{250} and 2^{521}, and other choices of coefficient are not as competitive in performance. This prime is congruent to 1 mod 4, and the derivation procedure in Appendix A results in the following Montgomery curve $v^2 = u^3 + A*u^2 + u$, called "curve25519": $p \ 2^{255} - 19$ $A \ 486662$ order $2^{252} + 0x14def9dea2f79cd65812631a5cf5d3ed$ cofactor 8 $U(P) \ 9$ $V(P) \ 147816194475895447910205935684099868872646061346164752889648818$ 37755586237401 The base point is $u = 9$, $v = 1478161944758954479102059356840998688726$ $4606134616475288964881837755586237401$. This curve is birationally equivalent to a twisted Edwards curve $-x^2 + y^2 = 1 + d*x^2*y^2$, called "edwards25519", where: $p \ 2^{255} - 19$ $d \ 370957059346694393431380835087545651895421138798432190163887855330$ 85940283555 order $2^{252} + 0x14def9dea2f79cd65812631a5cf5d3ed$
--	--

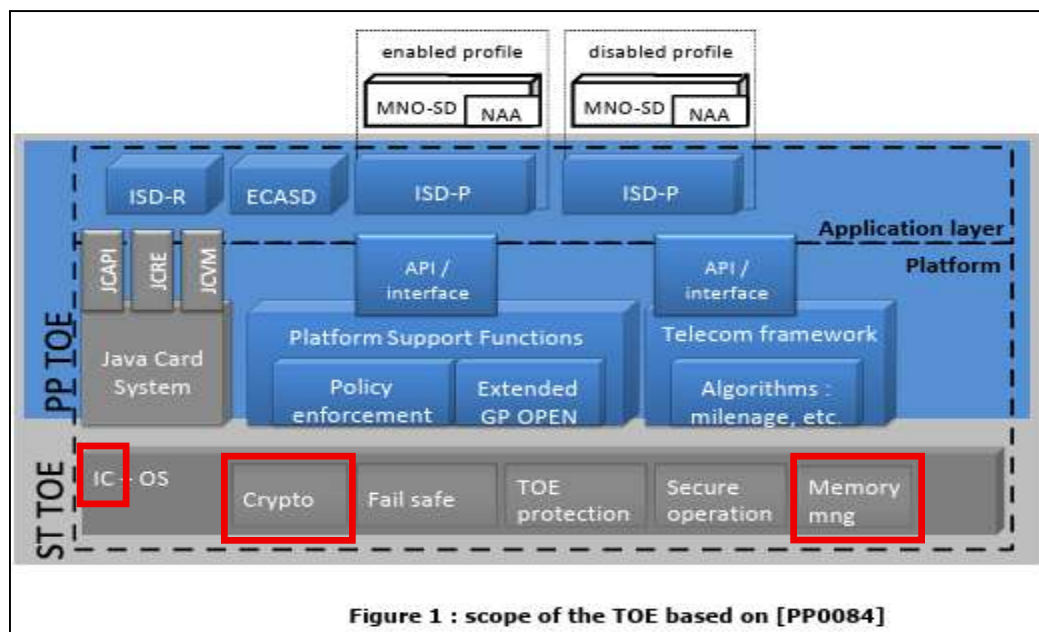
	cofactor 8 X(P) 151122213495354007725011514095885315114540126930418572060461132 83949847762202 Y(P) 463168356949264781694283940034751631413079938662562256157830336 03165251855960 The birational maps are: $(u, v) = ((1+y)/(1-y), \sqrt{-486664} \cdot u/x)$ $(x, y) = (\sqrt{-486664} \cdot u/v, (u-1)/(u+1))$ The Montgomery curve defined here is equal to the one defined in [curve25519], and the equivalent twisted Edwards curve is equal to the one defined in [ed25519].” IETF RFC 7748 § 4.1 Likewise, SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. (referenced as [30] in ETSI TS 133 501) describes the secp256r1 standard curve: “2.4.2 Recommended Parameters secp256r1 The verifiably random elliptic curve domain parameters over F_p secp256r1 are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field F_p is defined by: $p = \text{FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF}$ $= 2^{224}(2^{32} - 1) + 2^{192} + 2^{96} - 1$ The curve $E: y^2 = x^3 + ax + b$ over F_p is defined by: $a = \text{FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFFC}$ $b = \text{5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E}$
--	---

	27D2604B E was chosen verifiably at random as specified in ANSI X9.62 [X9.62] from the seed: $S = \text{C49D3608 86E70493 6A6678E1 139D26B7 819F7E90}$ The base point G in compressed form is: $G = \text{03 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296}$ and in uncompressed form is: $G = \text{04 6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296 4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5}$ Finally the order n of G and the cofactor are: $n = \text{FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551}$ $h = 01$ SECG SEC 2: Recommended Elliptic Curve Domain Parameters § 2.4 (Recommended 256-bit Elliptic Curve Domain Parameters over F_p). SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009 (referenced as [30] in ETSI TS 133 501) explains that these curves provide the parameters for generating the private and public keys for the mobile device: • “3.2 Elliptic Curve Key Pairs All the public-key cryptographic schemes described in this document use key pairs known as elliptic curve key pairs.
--	--

	Given some elliptic curve domain parameters $T = (p, a, b, G, n, h)$ or $(m, f(x), a, b, G, n, h)$, an elliptic curve key pair (d, Q) associated with T consists of an elliptic curve secret key d which is an integer in the interval $[1, n - 1]$, and an elliptic curve public key $Q = (x_Q, y_Q)$ which is the point $Q = dG$. Section 3.2.1 describes how to generate elliptic curve key pairs, Section 3.2.2 describes how to validate elliptic curve public keys, and Section 3.2.3 describes how to partially validate elliptic curve public keys.” SECG SEC 1: Recommended Elliptic Curve Cryptography § 3.2. <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.
--	--

CLAIM 9	'204 PATENT V. SAMSUNG
9. The mobile device of claim 1, further comprising, in step (2), deriving (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to derive (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number. Specifically, the accused Samsung mobile devices include a random number generator connected to a processor and memory that generates a random number for deriving the private key for the mobile device. For example, the GSMA eSIM specification SGP.22 standard requires device to include a random number generator: • “2.6.8 Random Number Generation To protect against attacks, <u>a high quality random number generator is required</u>. Recommendations for appropriate random number generators are given by BSI [78] and NIST [79].” SGP.22-v3.1 at §2.6.8 (Random Number Generation)

The eSIM specifications further show the random number generator (labeled “Crypto”) connected to a processor (labeled “IC”) that is connected to a memory (labeled “Memory mng”):



SGP.05-v4.0 at §1.2.1 (TOE type).

The 5G standards further explain that the private key and public key are derived from a random number generator and a key pair generation algorithm:

- “3.2.1 Elliptic Curve Key Pair Generation Primitive

Elliptic curve key pairs should be generated as follows:

Input: Valid elliptic curve domain parameters $T = (p, a, b, G, n, h)$ or $(m, f(x), a, b, G, n, h)$.

Output: An elliptic curve key pair (d, Q) associated with T .

Actions: Generate an elliptic curve key pair as follows:

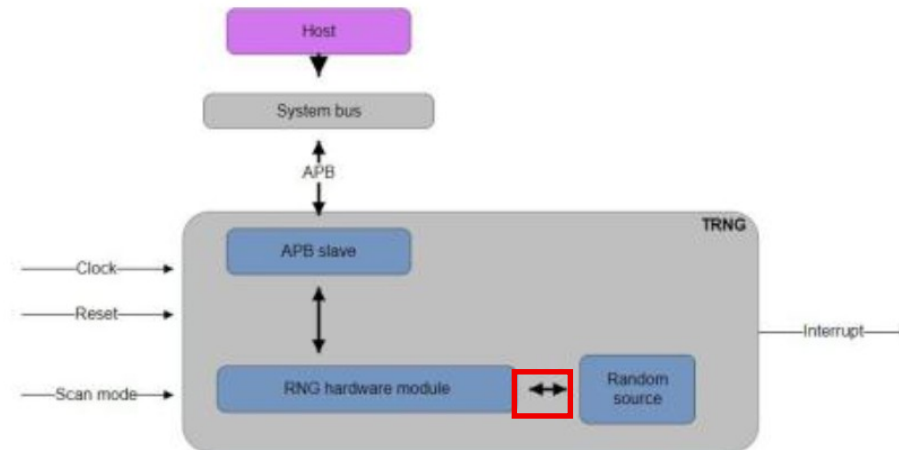
1. **Randomly or pseudorandomly select an integer d in the interval $[1, n - 1]$.**
2. Compute $Q = dG$.
3. Output (d, Q) ”

SECG SEC 1: Recommended Elliptic Curve Cryptography § 3.2 (Elliptic Curve Key Pairs); *see also* ETSI TS 133 501 § 2 (cross SECG SEC 1).

	<i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.
--	--

CLAIM 10	'204 PATENT V. SAMSUNG
10. The mobile device of claim 9, wherein the random number generator is configured to generate the random number from a seed value, and wherein the seed value comprises data from at least one of a sensor and a radio for the mobile device.	The Accused Instrumentalities are mobile devices with a random number generator that is configured to generate the random number from a seed value, wherein the seed value comprises data from at least one of a sensor, the radio, a bus, a clock, a physical interface, the memory, and an operating system. More specifically, the accused Samsung mobile devices include a random number generator that can generate a random number from a seed value that includes data from a sensor and a clock. On information and belief, the random number generator in Samsung’s accused mobile devices is an ARM “True Random Number Generator” or equivalent. The ARM True Random Number Generator includes a block labeled “TRNG” for generating a random number used for key generation: • “True Random Number Generator The Arm True Random Number Generator is a component that generates standards compliant random bit streams. It is designed for simple SoC integration connecting via an AMBA APB2 slave interface to the

SoC system bus. It is used for actions such as **key generation** or seeding approved deterministic random number generators. The only clock is rng_clk and no clock gating mechanism implemented.



Copyright © 1995-2021 Arm Limited (or its affiliates). All rights reserved. „

<https://soclabs.org/technology/true-random-number-generator>.

In the above diagram for a “True Random Number Generator” (TRNG), the TRNG generates a random number in response to an input from a sensor, where the sensor is represented by “< -- >” that senses data from the “Random source” for the “RNG hardware module.” *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 11	'204 PATENT V. SAMSUNG
11. The mobile device of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device.	The Accused Instrumentalities include instructions that, when executed by the at least one processor, cause the mobile device to store the public key in a nonvolatile memory. More specifically, the 5G standards explain that the accused Samsung mobile devices include code to store the home network public key in the data storage on the USIM: • “5.2.5 Subscriber privacy The UE shall support 5G-GUTI. The SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC). <u>The Home Network Public Key shall be stored in the USIM.</u> The protection scheme identifier shall be stored in the USIM. The Home Network Public Key Identifier shall be stored in the USIM. The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in USIM.” ETSI TS 133 501 at §5.2.5 (Subscriber privacy). On information and belief, the data storage in Samsung’s accused mobile devices comprises non-volatile memory that is capable of storing the public key of the server. <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 18	'204 PATENT V. SAMSUNG
18. The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.	The ciphering algorithms stored on Accused Instrumentalities include an Advanced Encryption Standard algorithm and has a length of 128 bits. More specifically, the ECIES profiles of the accused Samsung mobile devices include an ENC parameter that is set to an Advanced Encryption Standard algorithm with a length of 128 bits, as explained by the 5G standard. • “C.3.4.1 Profile A The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following: - EC domain parameters : Curve25519 [46] - EC Diffie-Hellman primitive : X25519 [46] - point compression : N/A - KDF : ANSI-X9.63-KDF [29] - Hash : SHA-256 - SharedInfo1 : □(the ephemeral public key octet string – see [29] section 5.1.3) - MAC : HMAC–SHA-256 - mackeylen : 32 octets (256 bits) - maclen : 8 octets (64 bits) - SharedInfo2 : the empty string - <u>ENC : AES–128 in CTR mode</u> - enckeylen : 16 octets (128 bits) - icblen : 16 octets (128 bits) - backwards compatibility mode : false C.3.4.2 Profile B The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following: - EC domain parameters : secp256r1 [30] - EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive [29] - point compression : true - KDF : ANSI-X9.63-KDF [29] - Hash : SHA-256 - SharedInfo1 : □ (the ephemeral public key octet string – see [29] section 5.1.3) - MAC : HMAC–SHA-256 - mackeylen : 32 octets (256 bits) - maclen : 8 octets (64 bits) - SharedInfo2 : the empty string

	- ENC : AES-128 in CTR mode - enckeylen : 16 octets (128 bits) - icblen : 16 octets (128 bits) - backwards compatibility mode : false" ETSI TS 133 501 at §C.3.4 (ECIES profiles). <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.
--	---

CLAIM 19	'204 PATENT V. SAMSUNG
19. The mobile device of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.	The module identity of Accused Instrumentalities comprises a number for an international mobile subscriber identity number. More specifically, the SUPI of the accused Samsung mobile devices comprises an international mobile subscriber identity (an “IMSI”) • “The UE shall construct a scheme-input from the subscription identifier part of the SUPI as follows: - For SUPIs containing IMSI, the subscription identifier part of the SUPI includes the MSIN of the IMSI as defined in TS 23.003 [19]. ... For SUPIs containing IMSI, the UE shall construct the SUCI with the following data fields: - The SUPI Type as defined in TS 23.003 [19] identifies the type of the SUPI concealed in the SUCI. - The Home Network Identifier is set to the MCC and MNC of the IMSI as specified in 23.003 [19]. - The Routing Indicator as specified in TS 23.003 [19]. - The Protection Scheme Identifier as specified in Annex C of this specification. - The Home Network Public Key Identifier as specified in this document and detailed in TS 23.003 [19]. - The Scheme Output as specified in this document and detailed in TS 23.003 [19].” ETSI TS 133 501 at § 6.12.2 (Subscription concealed identifier). The 5G standards also explain that “In the 5G system, the globally unique 5G subscription permanent identifier is called SUPI as defined in 3GPP TS 23.501 [2].” <i>Id.</i> § 6.12.1 (Subscription permanent identifier). <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 20	'204 PATENT V. SAMSUNG
20. The mobile device of claim 1, wherein the mobile device comprises a smartphone.	The Accused Instrumentalities comprise smart phones. For example, Samsung states that its Galaxy S20 “goes places no mobile phone has gone before.” https://www.samsung.com/us/smartphones/galaxy-s21/. Samsung also describes a number of its Galaxy devices as “smartphones.” https://www.samsung.com/us/mobile/phones/all-phones/ (imploing customers to “Explore Galaxy Smartphones”). <i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.