Exhibit F

Chart Detailing Samsung's Infringement of U.S. Patent No. 12,207,094

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

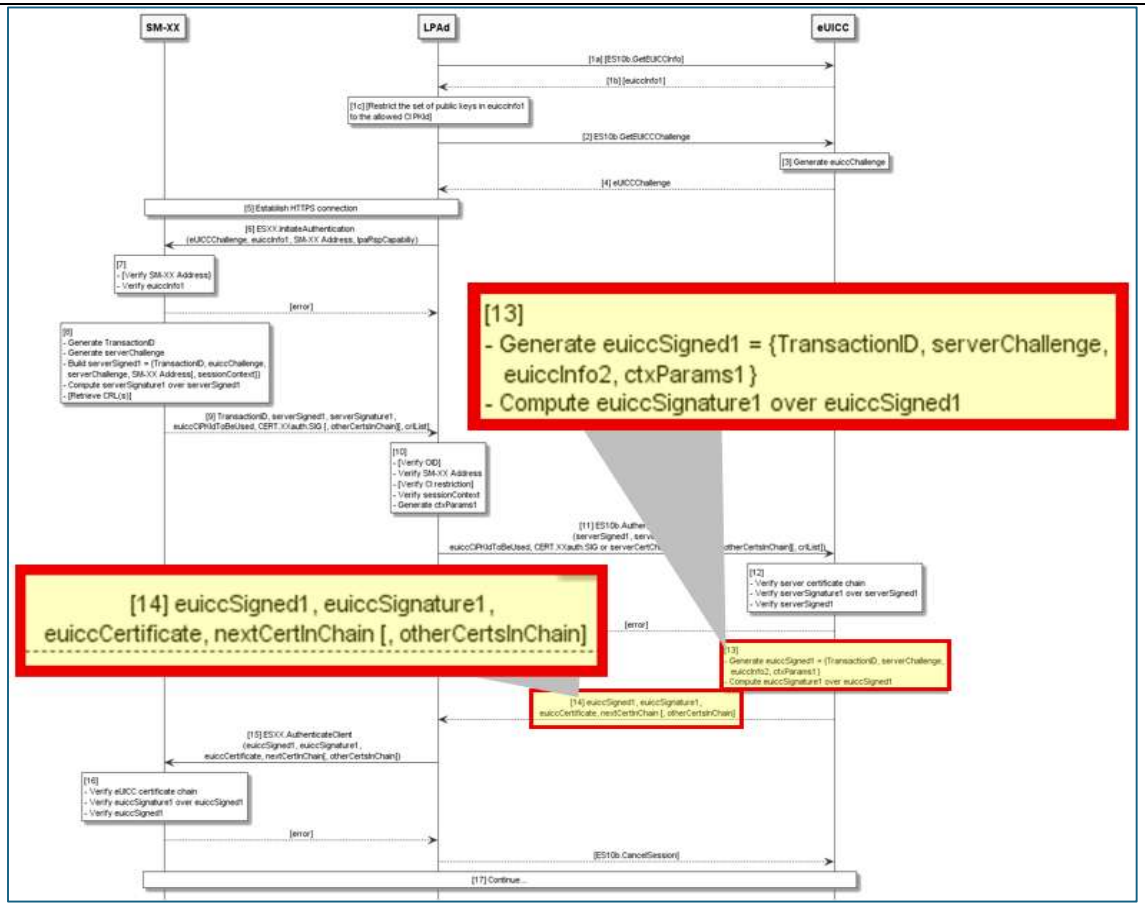
Based on the information presently available to it, Network-1 is informed and believes that Samsung directly and indirectly infringes U.S. Patent No. 12,207,094 ("the '094 Patent"). Samsung directly infringes claims 1, 2, 5-10, 13-15 and 19-21 of the '094 Patent when it uses the Accused Instrumentalities to perform the claimed methods. Samsung indirectly infringes claims 1, 2, 5-10, 13-15 and 19-21 of the '094 Patent by actively inducing the direct infringement of its end-user customers to perform the claimed methods using the Accused Instrumentalities.

CLAIM 1	'094 PATENT V. SAMSUNG
1[PRE]. A method comprising:	The Accused Instrumentalities perform a method. More specifically, the Accused Instrumentalities include a method performed by Samsung devices that support embedded Subscriber Identity Module ("eSIM") functionality, including (but not limited to) those listed in Network-1's infringement contentions and on these websites: 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. The GSMA eSIM specifications detail the eSIM functionality for Samsung's accused devices. Those GSMA eSIM specifications, which can be found at https://www.gsma.com/solutions-and-impact/technologies/esim/esim-specification/, include the Architecture Specifications, Technical Specifications, and Test Specifications. This infringement claim chart generally cites the latest versions of the GSMA eSIM specifications (*e.g.*, SGP.21 v3.1, SGP.22 v3.1, and SGP.23 v3.1), but incorporates the corresponding aspects of prior versions, which are substantively identical. Further evidence that the accused Samsung mobile devices support the GSMA eSIM specifications can be found here: https://research.samsung.com/blog/eSIM-and-the-Latest-eSIM-V3-0-Release; https://news.samsung.com/global/samsung-to-release-gear-s2-classic-3g-with-gsma-compliant-esim; https://semiconductor.samsung.com/security-solution/ese-esim/; https://semiconductor.samsung.com/security-solution/ese-esim/part-number/s3fv9rrp-prime/; https://images.samsung.com/is/content/samsung/sg-gears3-highlight-eSIM_FAQ; https://www.samsung.com/ca/support/mobile-devices/galaxy-esim-and-supported-network-carriers/.

Petitioner Samsung Ex-1029, 0002

1[A] (a) generating a first message comprising: (1) an identity of an embedded universal integrated circuit card (eUICC); (2) a nonce; and (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;	The Accused Instrumentalities include generating a first message comprising: (1) an identity of an embedded universal integrated circuit card (eUICC); (2) a nonce; and (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices generate a first message containing various components, including "euiccSigned1," "euiccSignature1," "euiccCertificate," and "nextCertInChain" components. The euiccCertificate component of the first message contains (1) an eUICC identifier referred to as "EID." The euiccSigned1 component of the first message contains (2) a nonce referred to "serverChallenge." And the euiccSignature1 component of the first message is (3) a first digital signature generated using a first eUICC private key called "SK.EUICC.SIG" that corresponds to a first eUICC public key called "PK.EUICC.SIG." The eSIM specifications include this figure that describes the Common Mutual Authentication Procedure. The box labeled "[14]" illustrates the contents of the first message, while the box labeled "[13]" shows some steps for generating the first message:

Petitioner Samsung Ex-1029, 0003



- Figure 8a: Common Mutual Authentication Procedure

- "13. The eUICC SHALL:
  - **<u>Generate the euiccSigned1 data structure.</u>**
  - **<u>Compute the euiccSignature1 over euiccSigned1 using SK.EUICC.SIG</u>**. When generating the euiccSignature1, the eUICC SHALL use the credentials identified in the previous step.

  14. **<u>The eUICC SHALL return the euiccSigned1, euiccSignature1 and the eUICC certificate chain</u>** related to the credentials used in the previous step."

SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)

Petitioner Samsung Ex-1029, 0004

The eSIM specifications further explain that the eUICC certificate includes a "subject" field with a "serialNumber" attribute that is the "EID":

- "4.5.2.1.0.2 eUICC
  The table below describes the specific fields of a CERT.EUICC.SIG in complement of the description given in section 4.5.2.1.0.0:

Field	Value Description
subject	Distinguished Name of the EUICC. **It SHALL include, at least,** 'organization' and **'serialNumber' attributes**. Others attributes MAY be included for information. The 'organization' attribute SHALL have one of the values allowed in the nameConstraints extension of the EUM Certificate (CERT.EUM.SIG). See note 1. **The 'serialNumber' attribute SHALL be the EID** as a decimal PrintableString (see note 2). The EID SHALL start with one of the EINs allowed in the EUM Certificate (CERT.EUM.SIG). Example of an eUICC DN: o = ACME serialNumber = 89049032123451234512345678901235

Table 11: CERT.EUICC.SIG"

SGP.22-v3.1 at §4.5.2.1.0.2 (eUICC)

The eSIM specifications further explain that the "EID" is an eUICC identifier:

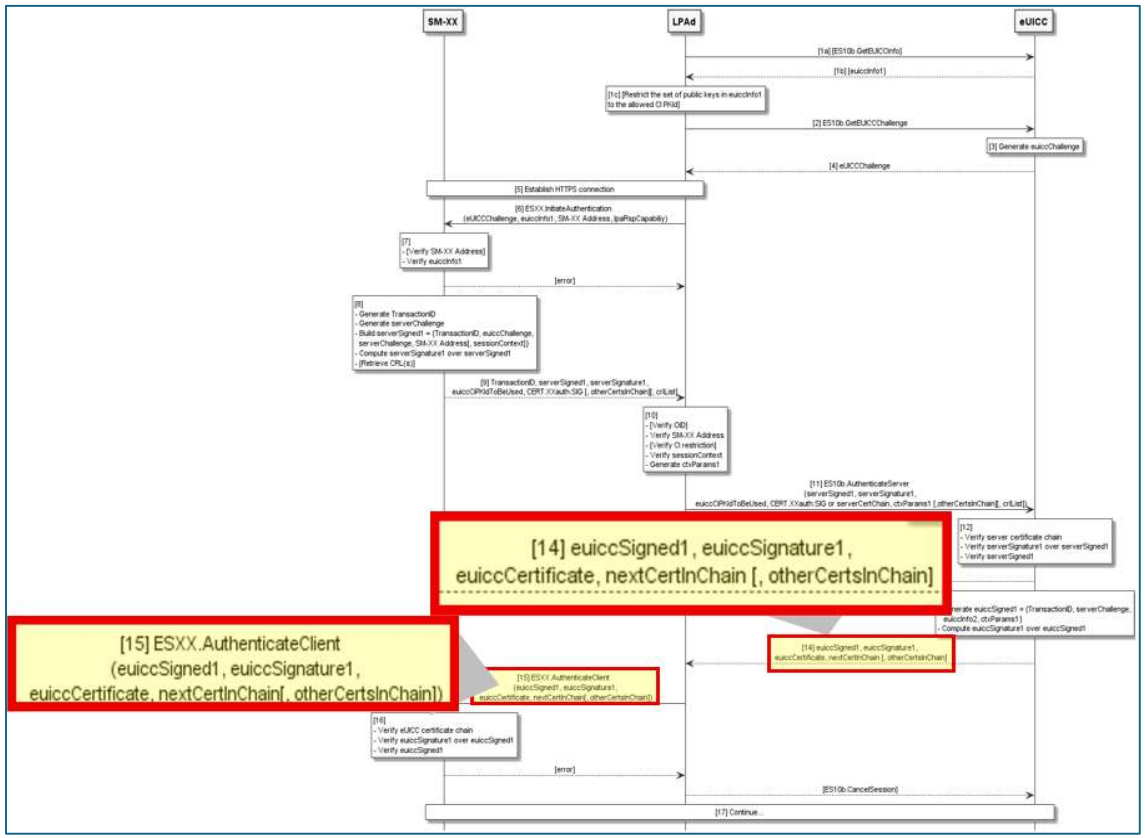
- 1.6 Abbreviations and Notations

Abbreviation	Description
* * * * *	
EID	eUICC identifier

"

SGP.22-v3.1 at §1.6 (Abbreviations and Notations)

	The eSIM specifications further explain that the euiccSigned1 component contains a "serverChallenge" parameter:
	• "Generate **euiccSigned1** = {TransactionID, **serverChallenge**, euiccInfo2, ctxParams1}"
	SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)
	Persons of skill know that a server challenge is a nonce:
	• "Authentication protocols usually employ a **cryptographic nonce as the challenge** to ensure that every challenge-response sequence is unique. This protects against Eavesdropping with a subsequent replay attack." https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication
	• "The server MUST send a set of supported features and a random key to use as part of the challenge. This key is in the form of a 64-bit (8-byte) **nonce value for the ServerChallenge value**. The nonce is a pseudo-random number generated by the server and intended for one-time use." https://learn.microsoft.com/ja-jp/openspecs/windows_protocols/ms-nlmp/b46d85da-050d-4f18-a2e1-14863f587163
	The eSIM specifications further explain that the euiccSignature1 component is a digital signature that is generated using "SK.EUICC.SIG":
	• "13. The eUICC SHALL:
	  • Generate the euiccSigned1 data structure.
	  • **Compute the euiccSignature1** over euiccSigned1 **using SK.EUICC.SIG**. When generating the euiccSignature1, the eUICC SHALL use the credentials identified in the previous step."
	SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)
	The eSIM specifications further explain that "SK.EUICC.SIG" is the eUICC's private key, and that it corresponds to the eUICC's public key, "PK.EUICC.SIG":
	• "The ECASD SHALL contain:
	  • **The eUICC's Private Key(s) (SK.EUICC.SIG)** for creating digital signatures
	  • The eUICC's Certificate(s) for eUICC authentication (CERT.EUICC.SIG) containing the **eUICC's public key(s) (PK.EUICC.SIG)**"
	SGP.22-v3.1 at §2.4.2 (ECASD)

1[B] (b) sending the first message via a network application to a subscription manager system;	The Accused Instrumentalities include sending the first message via a network application to a subscription manager system. More specifically, as part of implementing eSIM functionality, the accused Samsung devices send the first message (containing components including "euiccSigned1," "euiccSignature1," "euiccCertificate," and "nextCertInChain") via a network application called "LPAd" to a subscription manager called "SM-XX" or "SM-DP+." The eSIM specifications include this figure that describes the Common Mutual Authentication Procedure. The boxes labeled "[14]" and "[15]" show that the first message is sent via the LPAd to the SM-XX: •  Figure 8a: Common Mutual Authentication Procedure

Petitioner Samsung Ex-1029, 0007

	• "14. **The eUICC SHALL return the euiccSigned1, euiccSignature1 and the eUICC certificate chain** related to the credentials used in the previous step. 15. **The LPAd SHALL call** the "ESXX.AuthenticateClient" function with input data comprising **euiccSigned1, euiccSignature1 and the eUICC certificate chain**. 16. On **reception** of the "ESXX.AuthenticateClient" function call, the **SM-XX** SHALL:" SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)
1[C] (c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;	The Accused Instrumentalities include deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms. More specifically, as part of implementing eSIM functionality, the accused Samsung devices derive a second eUICC private key called "otSK.EUICC.KA" and a corresponding eUICC public key called "otPK.EUICC.KA." This key generation is performed using a random number generator and a set of cryptographic algorithms. The eSIM specifications specify that, as part of the profile download and installation procedure and the download confirmation sub-procedure, the device containing the eUICC will generate a one-time key pair using an "ECKA" Elliptic Curve cryptography Key Agreement algorithm, and that one-time key pair contains a "otPK.EUICC.KA" public key for the eUICC and a corresponding "otSK.EUICC.KA" private key for the eUICC:

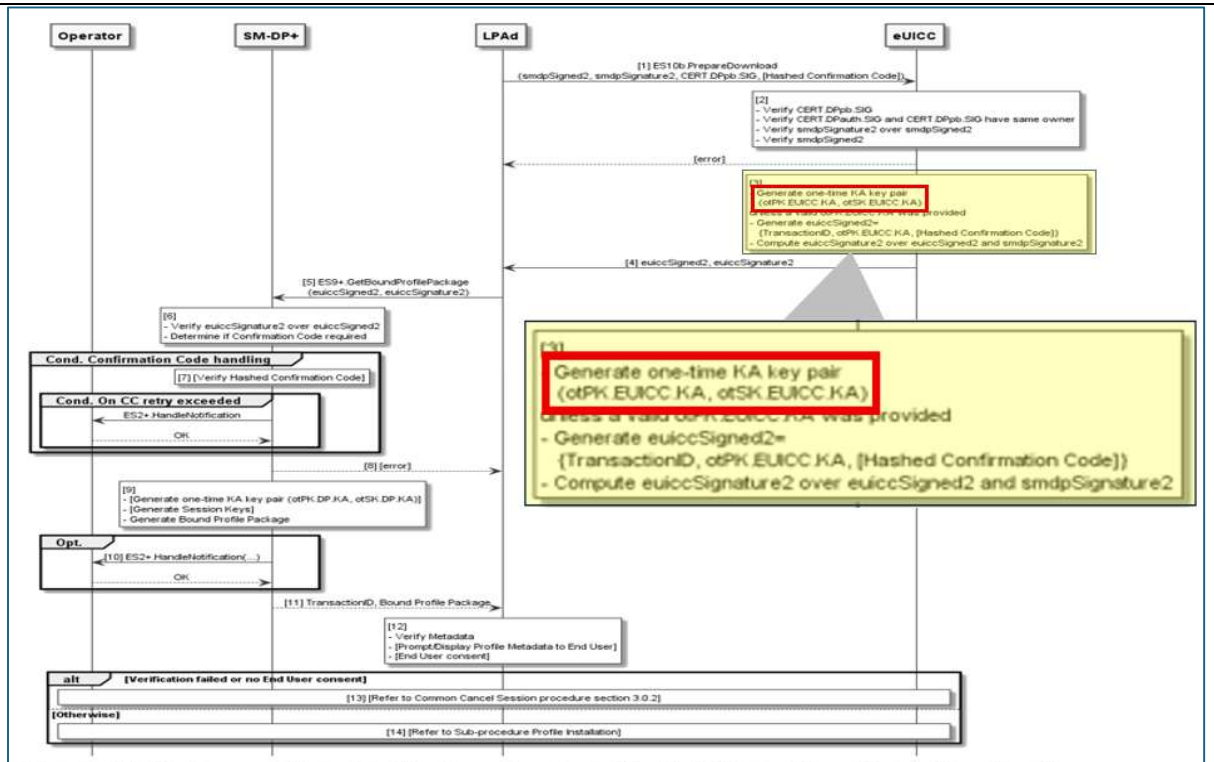


Figure 13: Sub-procedure Profile Download and Installation – Download Confirmation

- SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)
- "3. **<u>The eUICC SHALL</u>**:
  - Use the one-time key pair associated with the bppEuiccOtpk if it is provided by the SM-DP+ and it is still stored in the eUICC, or **<u>generate a new one-time key pair (see section 5.7.5)</u>**.
  - Generate the euiccSigned2 data structure.
  - Compute the euiccSignature2." SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)
- "If these verifications are successful, **<u>the eUICC SHALL</u>**:
  - Extract the public key of the CERT.DPpb.SIG and attach it to the RSP Session.

Petitioner Samsung Ex-1029, 0009

	• If bppEuiccOtpk is provided in smdpSigned2 and it corresponds to a stored one-time KA key pair (otPK.EUICC.KA, otSK.EUICC.KA) for this SM-DP+: use this key pair for the RSP Session. Otherwise: **generate a new one-time KA key pair (otSK.EUICC.KA, otPK.EUICC.KA)** using the parameters indicated by the subjectPublicKeyInfo.algorithmIdentifier.parameters field of the CERT.DPpb.SIG, and attach otSK.EUICC.KA to the RSP Session. • Generate euiccSigned2 data object as defined hereunder which MAY include vendor-specific additional information (e.g., as described in Annex P). • Compute the euiccSignature2 using the SK.EUICC.SIG that was used in the "ES10b.AuthenticateServer" response as described hereunder." SGP.22-v3.1 at §5.7.5 (Function (ES10b): Prepare Download) Persons of skill understand that a random number generator is used to generating a one-time key pair using an ECKA elliptic curve cryptography Key Agreement algorithm: • **Key establishment protocol** [edit] The following example illustrates how a shared key is established. Suppose Alice wants to establish a shared key with Bob, but the only channel available for them may be eavesdropped by a third party. Initially, the domain parameters (that is, (p, a, b, G, n, h) in the prime case or $(m, f(x), a, b, G, n, h)$ in the binary case) must be agreed upon. Also, each party must have a key pair suitable for elliptic curve cryptography, consisting of a private key d (a randomly selected integer in the interval $[1, n-1]$) and a public key represented by a point Q (where $Q = d \cdot G$, that is, the result of adding G to itself d times). Let Alice's key pair be (d_A, Q_A) and Bob's key pair be (d_B, Q_B). Each party must know the other party's public key prior to execution of the protocol. https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman.
1[D] (d) storing a subscription manager public key which corresponds to a subscription manager private key;	The Accused Instrumentalities include storing a subscription manager public key which corresponds to a subscription manager private key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices store a subscription manager public key called "otPK.DP.KA" that corresponds to a subscription manager private key called "otSK.DP.KA." The eSIM specifications explain that, as part of the profile download and installation procedure and the profile installation sub-procedure, the eUICC will receive and store a message containing the "InitialiseSecureChannel" function:

Petitioner Samsung Ex-1029, 0010

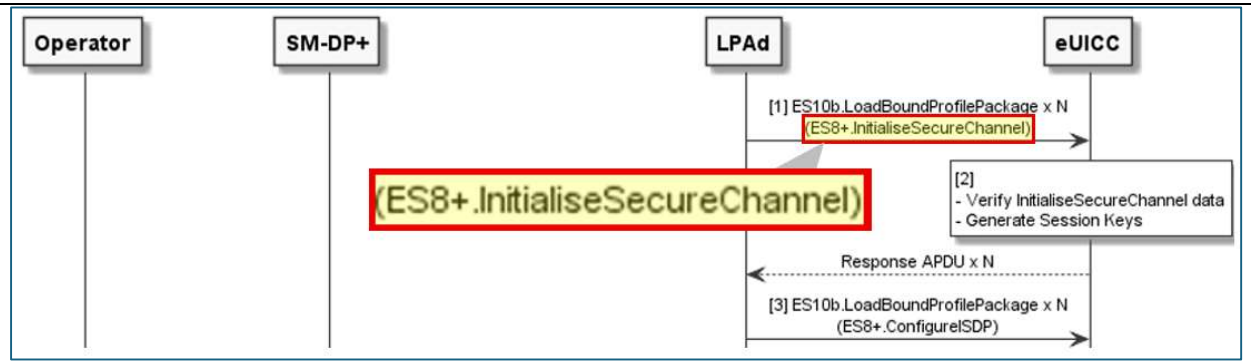


Figure 14: Sub-procedure Profile Installation

- "1. The LPAd SHALL transfer the part of Bound Profile Package containing the "**ES8+.InitialiseSecureChannel**" function to the eUICC by repeatedly calling the "ES10b.LoadBoundProfilePackage" function."

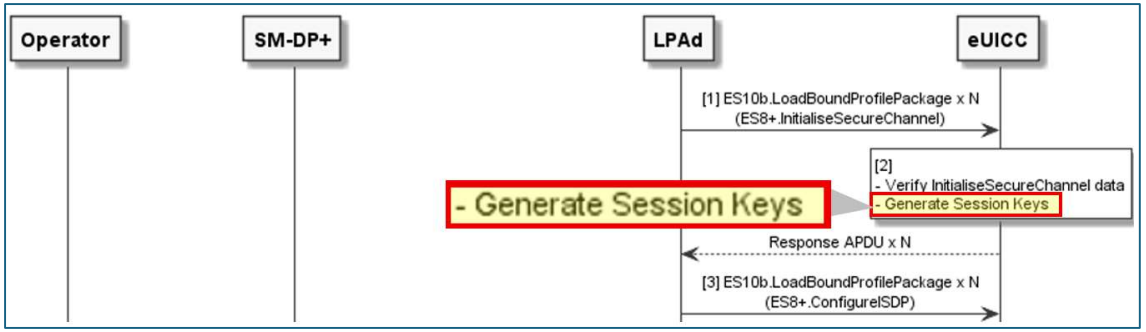
SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation)

The eSIM specifications further explain that the InitialiseSecureChannel function contains the one-time public key generated by the SM-DP+ called "otPK.DP.KA":

- "5.5.1 **Function: InitialiseSecureChannel**
  Related Procedures: Profile Download and Installation
  Function Provider Entity: ISD-R
  Description: This function is used by the SM-DP+ to initialise the secure channel for a Profile Download and Installation with the target eUICC. **The function carries** the identifier of the remote operation type to be performed by the eUICC (e.g., installation of a new Bound Profile Package) and **the necessary material for key agreement** with Perfect Forward Secrecy (PFS), allowing a secure end-to-end communication between the SM-DP+ and the eUICC:
  - Transaction ID
  - Description of the keys to generate
  - **One-time public key for key agreement generated by SM-DP+ (otPK.DP.KA)**
  - Signature upon material (including the previously generated otPK.EUICC.KA, also acting as an eUICC challenge) to ensure its integrity and authenticity."

SGP.22-v3.1 at §5.5.1 (Function: InitialiseSecureChannel)

Petitioner Samsung Ex-1029, 0011

1[E] (e) deriving a profile key using a key exchange algorithm based on at least: (i) the second eUICC private key, and (ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;	The Accused Instrumentalities include deriving a profile key using a key exchange algorithm based on at least: (i) the second eUICC private key, and (ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices derive a profile key called a "session key" using an "ECKA" elliptic curve key agreement algorithm. The session key is based on: (i) the second eUICC private key, "otSK.EUICC.KA;" and (ii) the stored subscription manager public key, "otPK.DP.KA." Further, the session key can be derived at the "SP-DP+" subscription manager based on: the second eUICC public key, "otPK.EUICC.KA;" and the subscription manager private key, "otSK.DP.KA." The eSIM specifications explain that, as part of the profile download and installation procedure and the profile installation sub-procedure, the eUICC will generate a profile key called "Session key" or "S-ENC": •  Figure 14: Sub-procedure Profile Installation • "2. The eUICC SHALL verify the received "ES8+.InitialiseSecureChannel". If the verification succeeds, **the eUICC SHALL generate the Session Keys using the input data received in previous step** and the key agreement algorithm determined according to section 2.6.5. SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation) The eSIM specifications further explain that the "Session key" profile is derived from a shared secret value: • "2.6.4.2 Key derivation **Session keys** and an initial MAC chaining value **are derived from the shared secret value** as follows:

Petitioner Samsung Ex-1029, 0012

- Concatenate the following values as SharedInfo as input for the Key Derivation process (this data is the one given as input data in the function "ES8+.InitialiseSecureChannel"):
  - Key type (1 byte)
  - Key length (1 byte)
  - HostID-LV and EID-LV. HostID-LV comprises the length and the value field of the HostID given in the input data; EID-LV comprises the length and value field of the EID.
- Initial MAC Chaining value, S-ENC and S-MAC are taken from KeyData derived from the shared secret value and the SharedInfo as defined in BSI TR-03111 [41] for the "X9.63 Key Derivation Function". SHA-256 SHALL be used for the key derivation to calculate KeyData of sufficient length. Data is assigned as defined in the following table:

KeyData	Key
1 to L	Initial MAC chaining value
L+1 to 2L	S-ENC
2L+1 to 3L	S-MAC

Table 4c: Key Data"

SGP.22-v3.1 at §2.6.4.2 (Key Derivation)

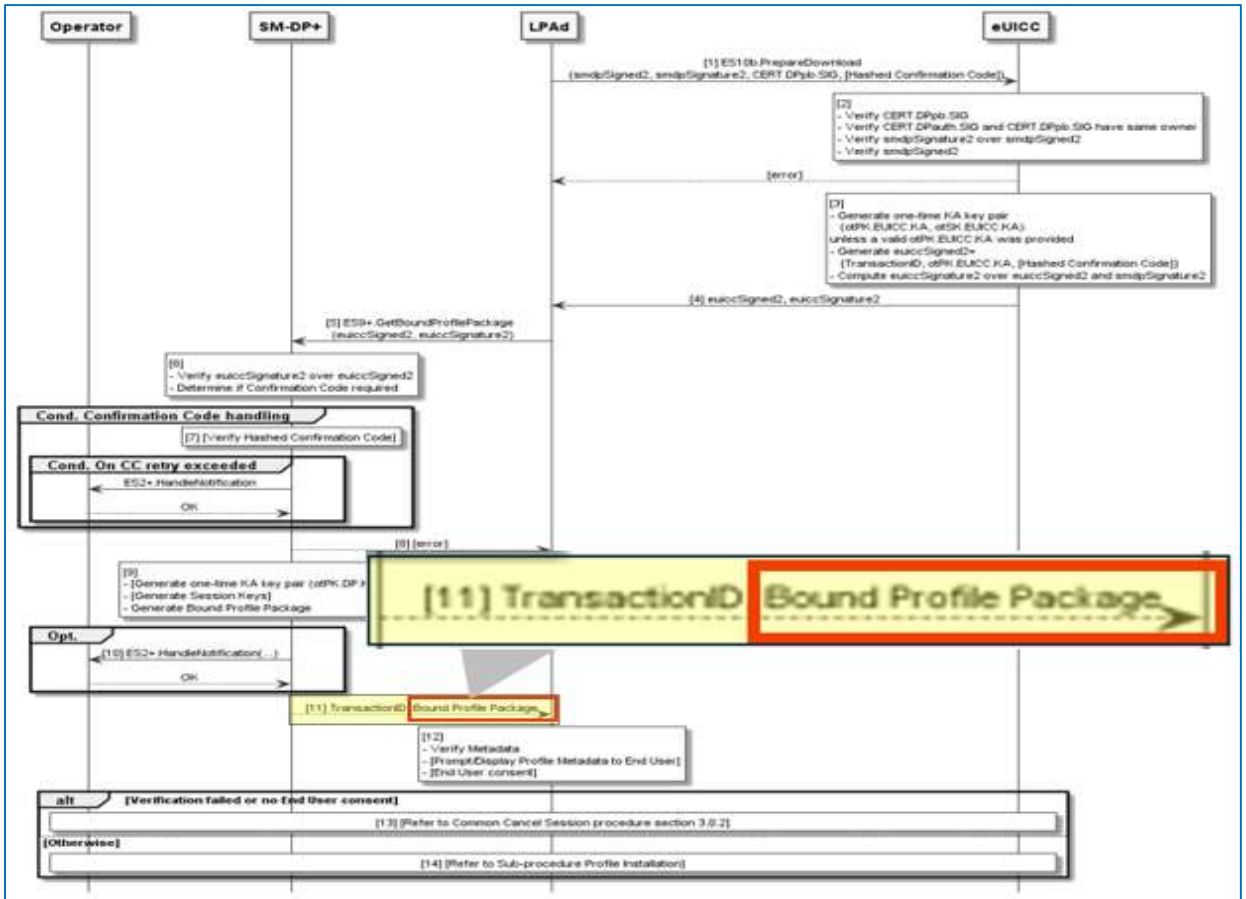
The eSIM specifications further explain that the eUICC calculates the shared secret value using the "otPK.DP.KA" stored subscription manager public key and the "otSK.EUICC.KA" second eUICC private key. Similarly, the SM-DP+ subscription manager also calculates the shared secret value using the "otSK.DP.KA" subscription manager private key and the "otPK.EUICC.KA" second eUICC public key

- "2.6.4.1 Key agreement
  An Elliptic Curve Key Agreement Algorithm (ECKA) is used for the establishment of a shared secret value. It shall follow the definition for the Anonymous Diffie-Hellman Key Agreement in BSI TR-03111 [41]. **The algorithm is executed**
  - **by the SM-DP+ using otPK.EUICC.KA and otSK.DP.KA, and**
  - **by the eUICC using otPK.DP.KA and otSK.EUICC.KA to calculate the shared secret value**."

SGP.22-v3.1 at §2.6.4.1 (Key Agreement)

1[F] (f) receiving from the subscription manager system, an encrypted profile	The Accused Instrumentalities include receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key.

Petitioner Samsung Ex-1029, 0013

comprising a ciphertext including a key K encrypted with a symmetric key;	More specifically, as part of implementing eSIM functionality, the accused Samsung devices receive from the "SM-DP+" subscription manager an encrypted profile called the "Bound Profile Package" that contains a ciphertext including a key K encrypted with a symmetric key called a "Protected Profile Protection Key" or "PPK." The eSIM specifications explain that, as part of the profile download and installation procedure and the profile download and installation – download confirmation sub-procedure, the LPAd within the device receives from the SM-DP+ subscription manager the "Bound Profile Package" encrypted profile: •  **Figure 13: Sub-procedure Profile Download and Installation – Download Confirmation**

Petitioner Samsung Ex-1029, 0014

- "11. **<u>The SM-DP+ returns "ES9+.GetBoundProfilePackage" response</u>** and set the Profile corresponding to the Profile download order in 'Downloaded' state (section 3.1.6)."

SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)

The eSIM specifications further explain that the Bound Profile Package contains various data (including a key K) in the form of a TLV sequence that is part of a traditional SIM profile. In the figure below, this data is within the portion of the Bound Profile Package that is labeled "Segment." This data is encrypted with the "PPK" symmetric key, as indicated by the red hash coloring and the legend:

- "2.5.1 Profile Package Types Overview
  From generation to download, the Profile Package will take different formats. This specification uses the following terms:
  - Unprotected Profile Package (UPP): **<u>Raw eUICC Profile Package TLV sequence</u>**.
  - Protected Profile Package (PPP): Segmented and protected in BSP payload TLVs.
  - **<u>Bound Profile Package (BPP):</u>** Prepended with session key agreement info, key replacement package, ISD-P creation and configuration info.
  - Segmented Bound Profile Package (SBPP): BPP segmented into STORE DATA APDU script for loading into eUICC. This step is performed by the LPD when LPD is in the Device.

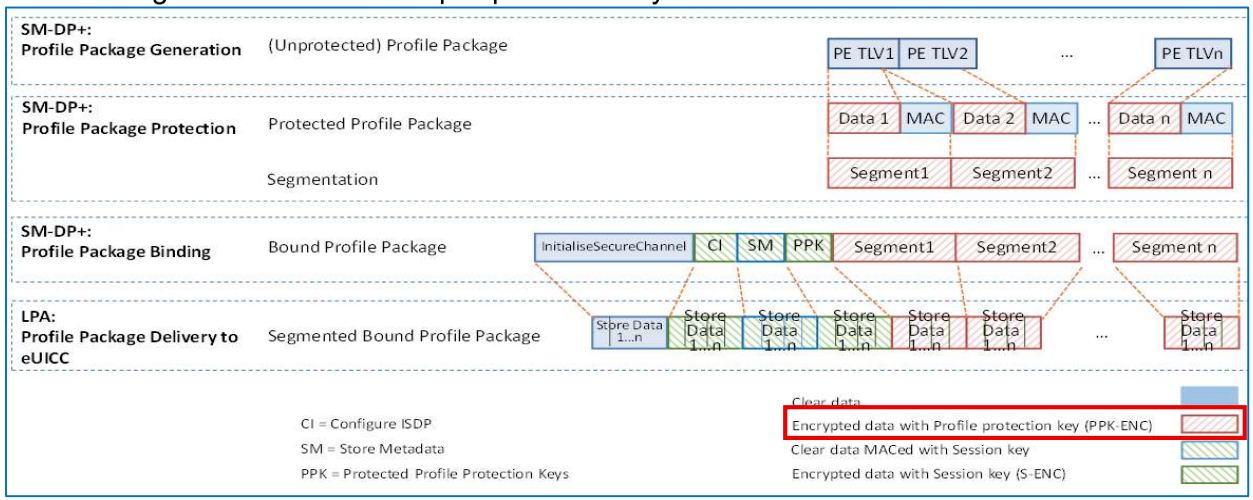


Figure 4: Profile Package stage Description"

SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview)

Petitioner Samsung Ex-1029, 0015

- "**2.5.4 Bound Profile Package**
  The Bound Profile Package (BPP) is generated by the SM-DP+, within the Profile Package Binding function. The purpose of this operation is to link a Protected Profile Package to a particular eUICC. This is done within a key agreement between the eUICC and the SM-DP+. See download and installation procedure (section 3.1.3).
  The BPP comprises a sequence of TLV commands (in this order):
  - TLV command for Key agreement in clear.
  - Set of BSP payload TLVs (tag '87') containing TLV commands for ConfigureISDP
  - Set of BSP payload TLVs (tag '88') containing TLV command for StoreMetadata
  - Set of optional BSP payload TLVs (tag '87') containing TLV command for 'Profile Protection Keys'
  - **Followed by the BSP payload TLVs (tag '86') of the PPP**" SGP.22-v3.1 at §2.5.4 (Bound Profile Package)"

SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview)

Example data within the Bound Profile Package is specified by the GSMA and includes (1) numerous network parameters, including a "Ki" key K:

-

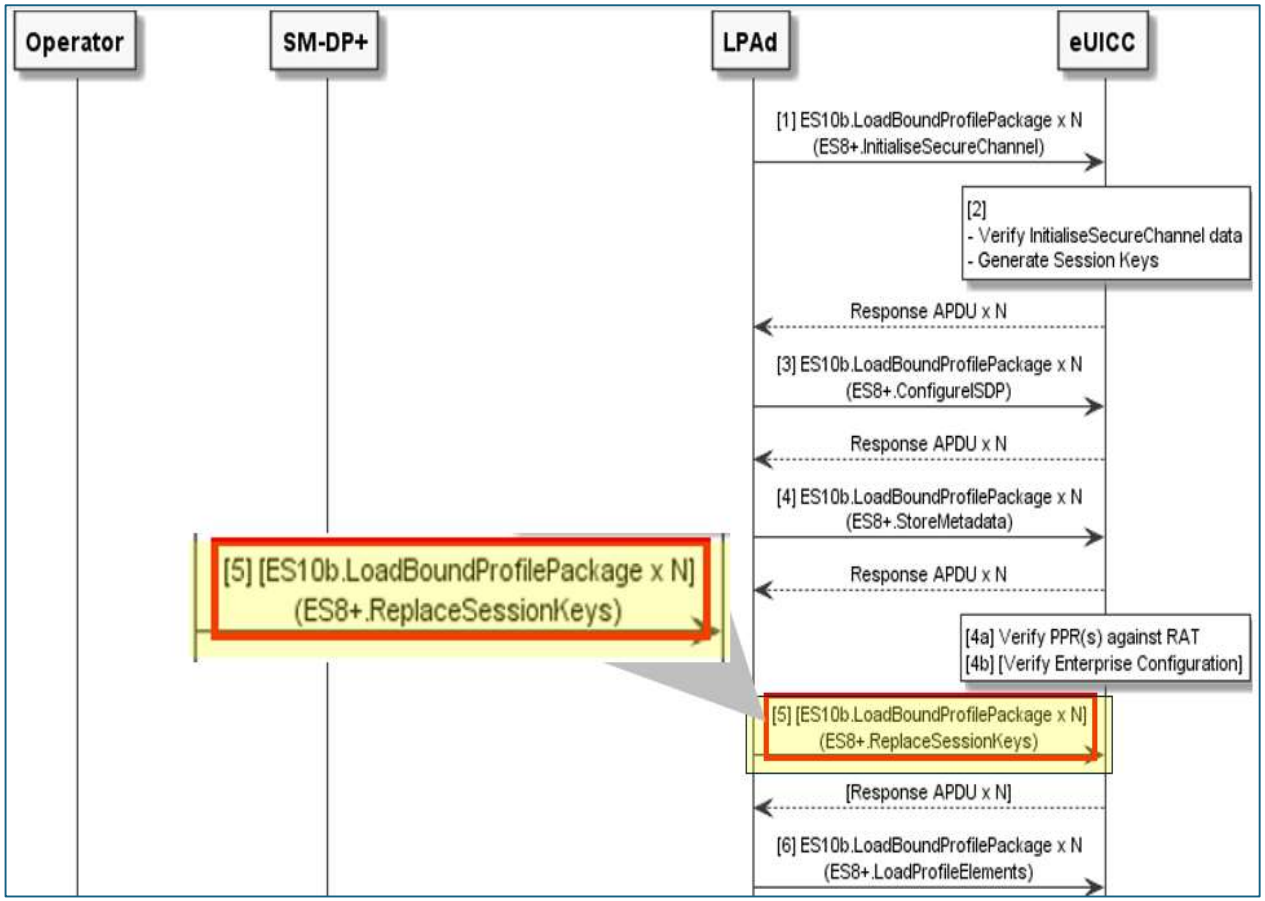
USIM authentication parameters	
Algorithm	XOR 3G
Ki	0x00 0x01 _ 0x0F
Opc	N/A

http://www.gsma.com/newsroom/wp-content/uploads//GSMA_TS48_eSIM_GTP_Profile_Structure-v3.0.xlsx.

The eSIM specifications further explain that the PPK is symmetric because it is used for both encryption and decryption. Indeed, the eSIM specifications explicitly refer to the algorithms used to protect the Protected Profile Package (*i.e.*, the PPK-ENC) as symmetric algorithms:

- "**PPK**-ENC: Optional Profile Protection Key randomly generated by the SM DP+ and **used for encryption/decryption** of a Protected Profile Package." SGP.22-v3.1 at §1.6 (Abbreviations and Notations)
- "**The symmetric algorithms are used in RSP for the protection of the Profile Package (Protected Profile Package)**, see section 2.5." SGP.22-v3.1 at §2.6.5 (Cryptographic Negotiation, Algorithms and Key Length)

Petitioner Samsung Ex-1029, 0016

1[G] (g) receiving the symmetric key;	The Accused Instrumentalities include receiving the symmetric key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices receive a "PPK" symmetric key. The eSIM specifications specify that, as part of the profile download and installation procedure and the profile installation sub-procedure, the mobile device containing the eUICC will receive the "PPK" symmetric key contained in the Bound Profile Package from the "LPAd" network application: •  Figure 14: Sub-procedure Profile Installation

Petitioner Samsung Ex-1029, 0017

- "5. If the Profile Protection Keys (PPK) were included in the Bound Profile Package, **the LPAd SHALL transfer the part of Bound Profile Package containing the "ES8+.ReplaceSessionKeys" function to the eUICC** by repeatedly calling the "ES10b.LoadBoundProfilePackage" function. The eUICC SHALL decrypt the **Profile Protection Keys** and replace the current BSP Session Keys with the decrypted Profile Protection Keys."

SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation)

The eSIM specification further explain that the portion of the Bound Profile Package having TLVs for the ES8+.ReplaceSessionKeys contains the "PPK" symmetric key:

- "The following table describes the various sequences of '86', '87' and '88' TLV

Tag	Length	Value Description			MOC
* * * * *					
'A2'	Var.	secondSequenceOf87 SHALL be absent if no content			C
		'87'	Var.	**BSP segment containing the Profile Protection Keys**, protected with session keys resulting from the key agreement (S-ENC, S-CMAC) (section 2.6.4). **Content: TLV for "ES8+.ReplaceSessionKeys" function (section 5.5.4)**	O
* * * * *					

Table 4: Profile Installation sequences of TLV"

SGP.22-v3.1 at §2.5.4 (Bound Profile Package)

Petitioner Samsung Ex-1029, 0018

The eSIM specifications further explain that the Bound Profile Package contains a Profile Protection Key "PPK" symmetric key, as shown in the figure below:

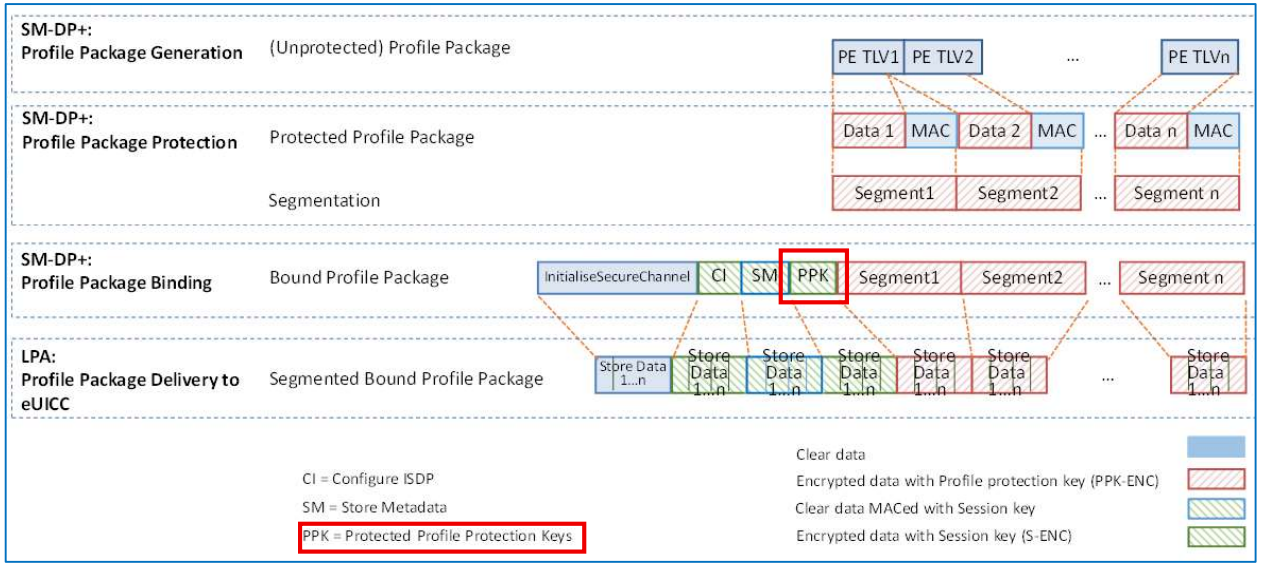


Figure 4: Profile Package stage Description

SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview)

Although use of the PPK is optional in the eSIM specifications, Samsung's accused mobile devices support the use of PPK, and the PPK is used by major American carriers. For example, testing shows the accused Samsung mobile devices receive a Bound Profile Package with a PPK symmetric key. The test environment includes a removable eSIM connected to a USB smart card reader and an AT&T eSIM profile:

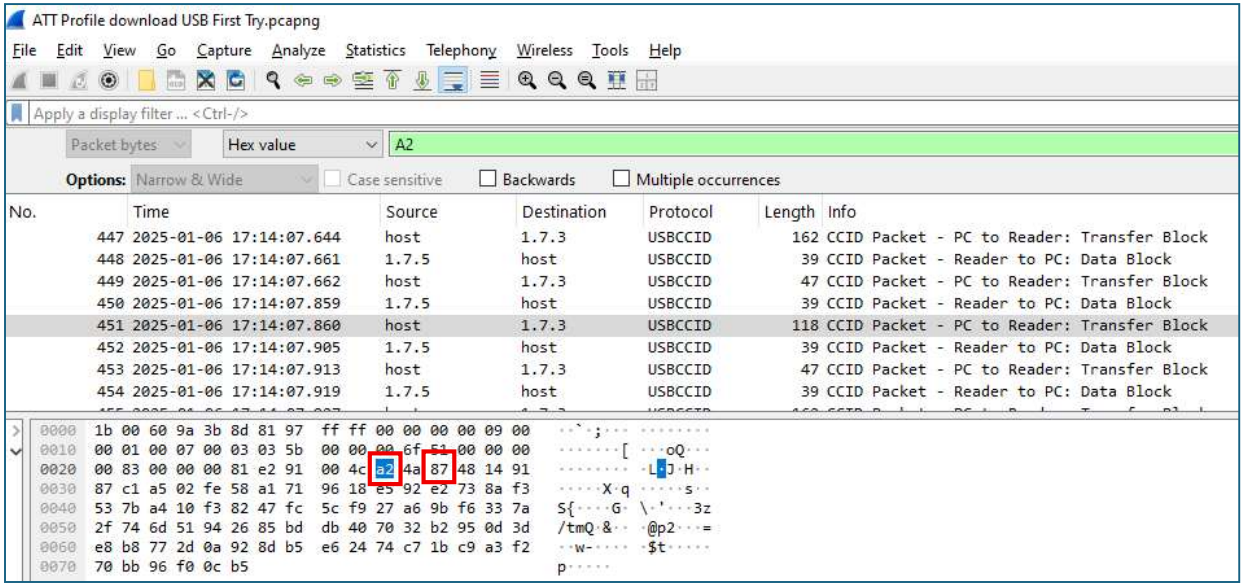
Petitioner Samsung Ex-1029, 0019

AT&T 5G
SKU
UPC
ACTIVATION CODE
ICCID
8 07377 06497 2
89014108334452718892

R301
Smart Card Reader
FEITIAN
Smart Card
FEITIAN
EIOT CLUB
Unlimited eSIM Card
eSIM

•

A wireshark capture shows the Samsung accused devices will receive a bound profile package with tag "A2" and a sequence of "87" TLVs when operating on at least AT&T's network:

- 

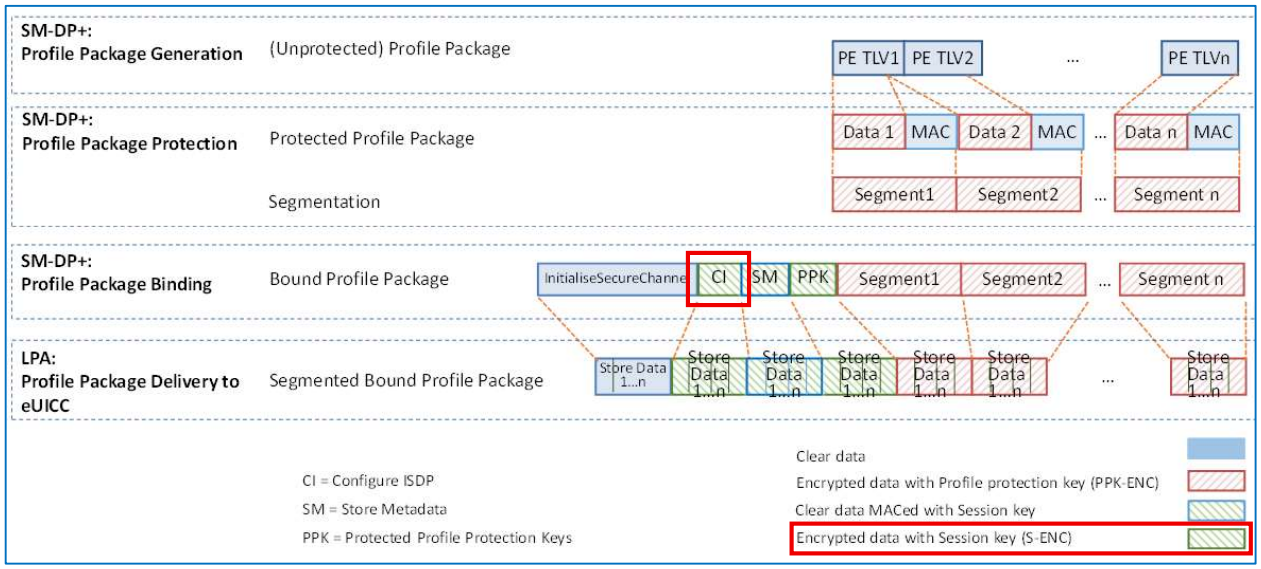
The eSIM specifications show that the "A2" sequence of "87" TLVs from the above wireshark capture contains the PPK Profile Protection Key:

Tag	Length	Value Description			MOC
		* * * * *			
'A2'	Var.	secondSequenceOf87 SHALL be absent if no content			C
		'87'	Var.	BSP segment containing the Profile Protection Keys, protected with session keys resulting from the key agreement (S-ENC, S-CMAC) (section 2.6.4). Content: TLV for "ES8+.ReplaceSessionKeys" function (section 5.5.4)	O

Table 4: Profile Installation sequences of TLV

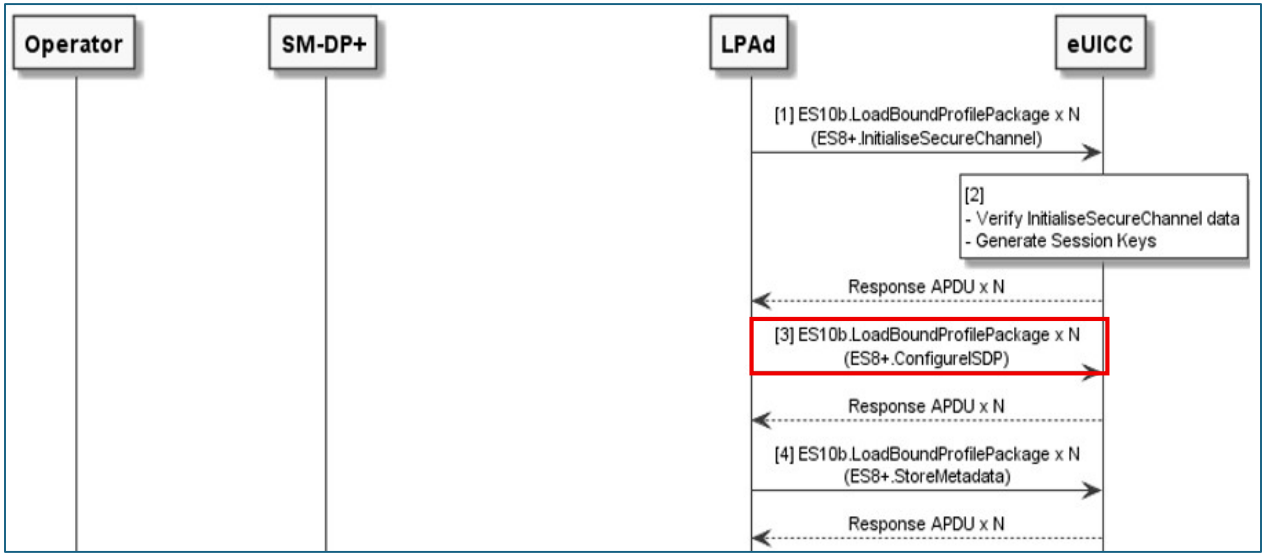
SGP.22-v3.1 at §2.5.4 (Bound Profile Package)

Petitioner Samsung Ex-1029, 0021

1[H] (h) decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key;	The Accused Instrumentalities include decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices have an eUICC that decrypts at least a portion of the "Bound Profile Package" encrypted profile using the "session key" profile key. The eSIM specifications provide the below figure, which shows that the portion of the Bound Profile Package that is colored using green hashes (including at least "CI" or "Configure ISDP") is decrypted using the "Session key (S-ENC)": •  Figure 4: Profile Package stage Description SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview)

Petitioner Samsung Ex-1029, 0022

Other portions of the eSIM specifications similarly explain that the Bound Profile Package contains an "CI" or "Configure ISDP" part that is "protected with" (*i.e.*, decrypted using) a "S-ENC" session key:

- 

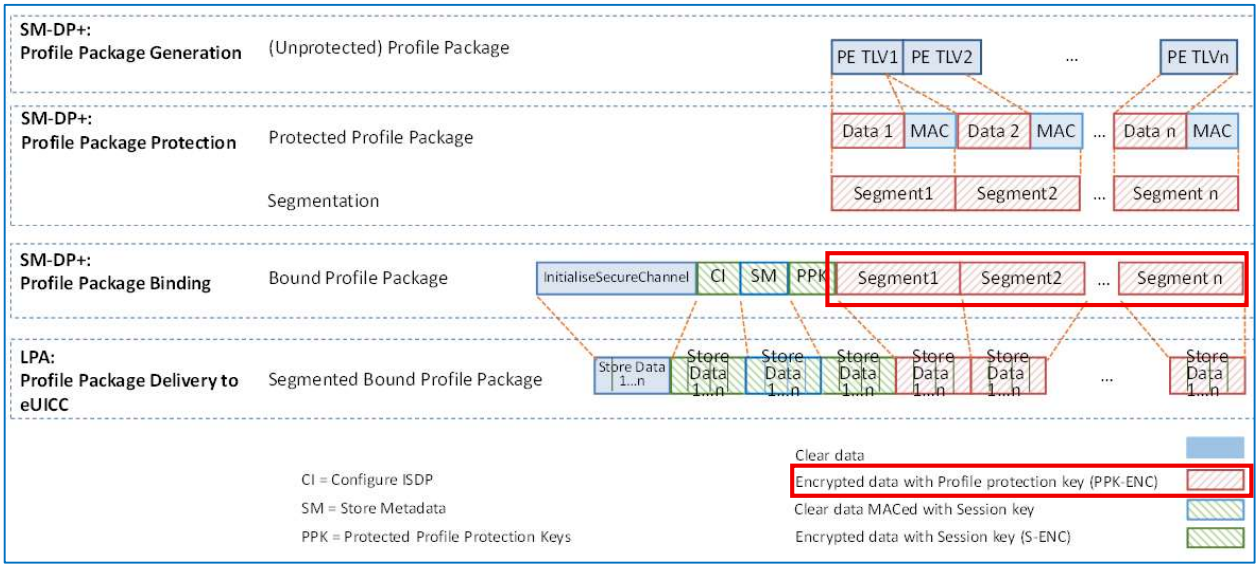
SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation)
- "3. The LPAd SHALL transfer the part of **Bound Profile Package containing the "ES8+.ConfigureISDP" function** to the eUICC by repeatedly calling the "ES10b.LoadBoundProfilePackage" function." SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation)
- "The following table describes the various sequences of '86', '87' and '88' TLV

Tag	Length	Value Description			MOC
'A0'	Var.	firstSequenceOf87			M
		'87'	Var.	BSP segment containing **ConfigureISDP, protected with session keys resulting from the key agreement (S-ENC**, S-CMAC) (section 2.6.4) Content: TLV for "ES8+.ConfigureISDP" function (section 5.5.2)	M

Petitioner Samsung Ex-1029, 0023

	SGP.22-v3.1 at §2.5.4 (Bound Profile Package) • "5.5.2 Function: ConfigureISDP Related Procedures: Profile Download and Installation Function Provider Entity: ISD-R Description: This function is used by the SM-DP+ to provide data to the eUICC for configuring the ISD-P. For this version of the specification, this data element only contains the optional SM-DP+ proprietary data. NOTE: Information like the amount of assigned memory MAY be added in future versions. On reception of this command the eUICC SHALL: • Create the ISD-P for the Profile and assign an AID value from the range reserved for ISD-Ps in SGP.02 [2]. • If the length of the SM-DP+ proprietary data exceeds the maximum size, terminate with error 'incorrectInputValues'. • Store the SM-DP+ proprietary data in the ISD-P." SGP.22-v3.1 at §5.5.2 (Function: Configure ISDP)
1[I] (i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and	The Accused Instrumentalities include decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices have an eUICC that decrypts at least a portion of the ciphertext using the "PPK" symmetric key.

Petitioner Samsung Ex-1029, 0024

	The eSIM specifications provide the below figure, which shows that the portion of the Bound Profile Package that is colored using red hashes (and labeled "Segment") is decrypted using the "Profile Protection Key (PPK-ENC)": •  Figure 4: Profile Package stage Description SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview) As shown above with respect to claim **1[F]**, the eSIM specifications further explain that this portion contains the "Ki" key K.
1[J] (j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.	The Accused Instrumentalities include storing at least the key K in the embedded universal integrated circuit card for use in future communications. More specifically, as part of implementing eSIM functionality, the accused Samsung devices have an eUICC that stores the key K for use in future communications The eSIM specifications further describe storing an eUICC identity containing the key K. For example, the RSP Technical Specification states that operator profiles are stored inside security domains within the eUICC:

Petitioner Samsung Ex-1029, 0025

- "2.4.1 eUICC Overview
  This section describes the internal high-level architecture of the eUICC. It should be noted that the eUICC architecture is very similar to that used in the GSMA Remote SIM Provisioning of Embedded UICC Technical specification [2]. **Operator Profiles are stored inside Security Domains within the eUICC** and are implemented using GlobalPlatform standards. These ensure that it is impossible for any Profile to access the applications or data of any other Profile stored on the eUICC. The same mechanism is currently in use within SIM cards to ensure payment applications are kept secure.

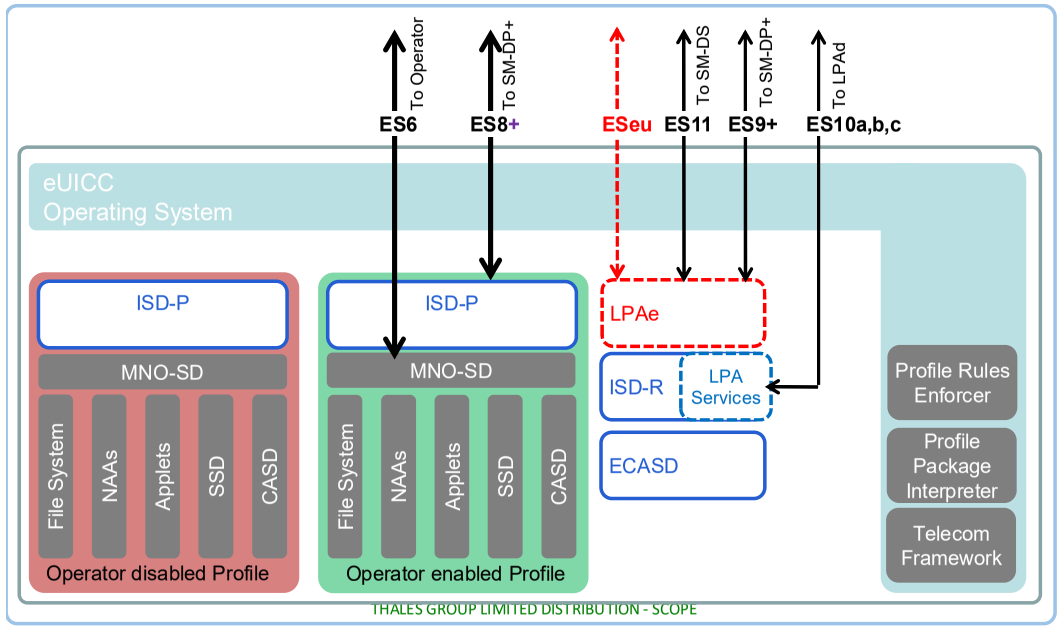


Figure 3: Schematic Representation of the eUICC"

SGP.22-v3.1 at §2.4.1 (eUICC Overview)

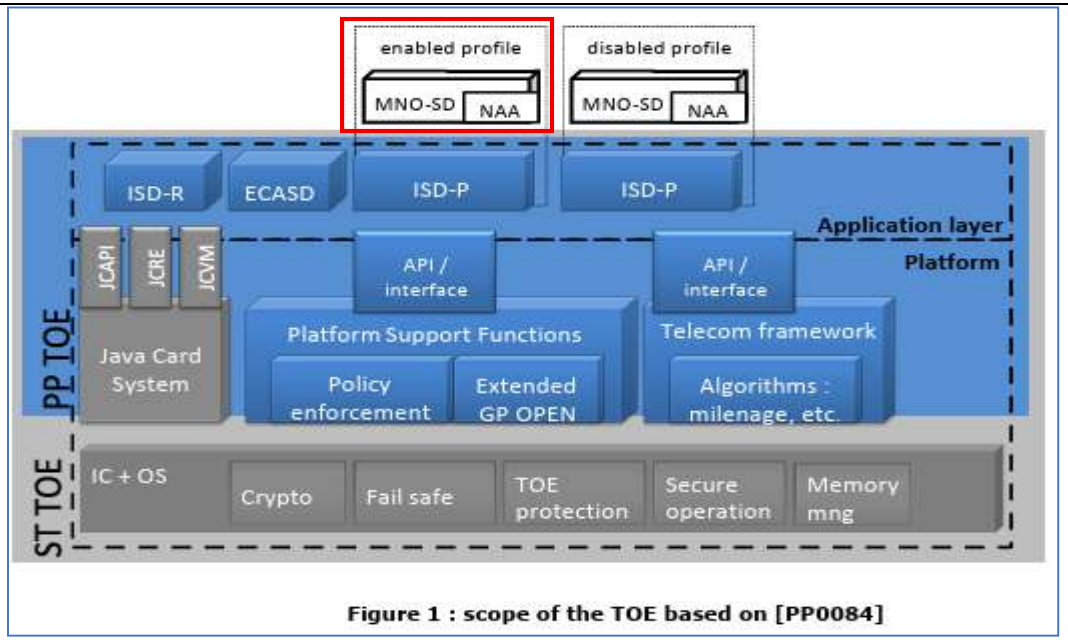


Figure 1 : scope of the TOE based on [PP0084]

- SGP.05-v4.0 at §1.2.1 (TOE type)

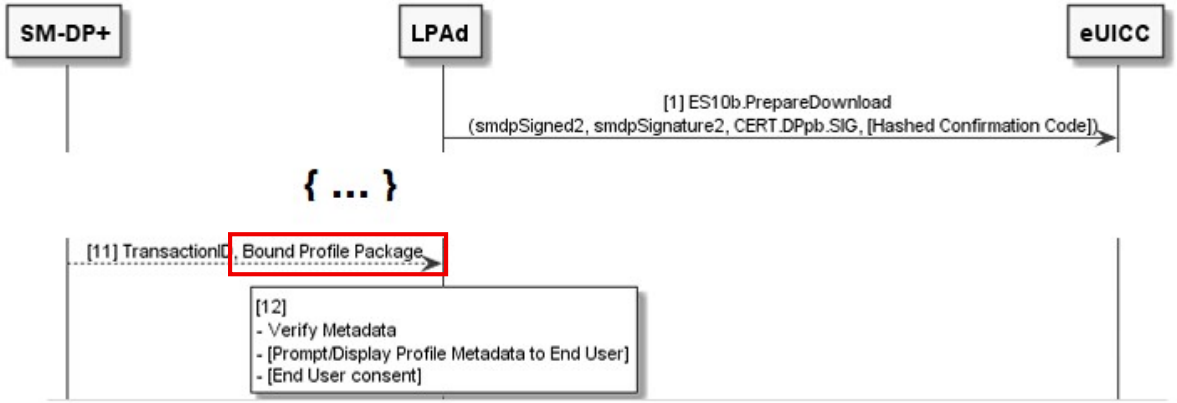
The eSIM specifications provide example profile data that includes a "Ki" key K. The key K is stored for future communications such as authenticating the with mobile operator network:

-

USIM authentication parameters	
Algorithm	XOR 3G
Ki	0x00 0x01 _ 0x0F
Opc	N/A

http://www.gsma.com/newsroom/wp-content/uploads//GSMA_TS48_eSIM_GTP_Profile_Structure-v3.0.xlsx.

Petitioner Samsung Ex-1029, 0027

CLAIM 2	'094 PATENT V. SAMSUNG
2. The method of claim 1, wherein the subscription manager public key is downloaded via the network application.	The Accused Instrumentalities include the subscription manager public key being downloaded via the network application. More specifically, as part of implementing eSIM functionality, the accused Samsung devices download the subscription manager public key (*e.g.*, otPK.DP.KA) via the network application called "LPAd." The eSIM specifications explain the "Bound Profile Package" downloaded by the network application (*e.g.*, LPAd) includes data for "Initialize Secure Channel." The data within "Initialize Secure Chanel" includes the subscription manager public key (*e.g.*, otPK.DP.KA):  • SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)

Petitioner Samsung Ex-1029, 0028

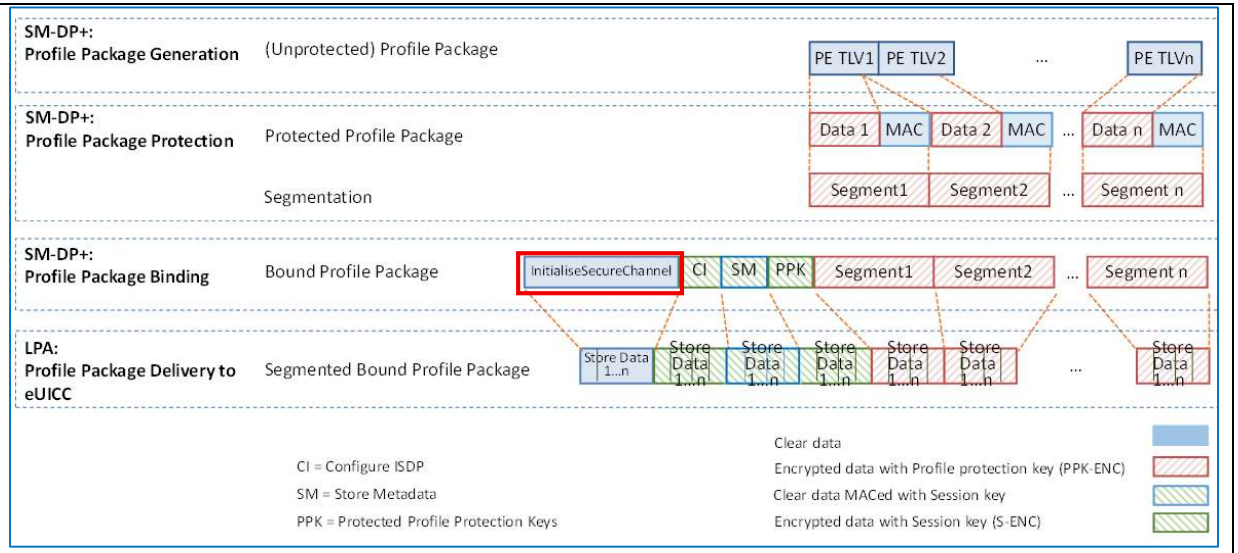


Figure 4: Profile Package stage Description

SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview)

- "5.5.1 **Function: InitialiseSecureChannel**
  Related Procedures: Profile Download and Installation
  Function Provider Entity: ISD-R
  Description: This function is used by the SM-DP+ to initialise the secure channel for a Profile Download and Installation with the target eUICC. **The function carries** the identifier of the remote operation type to be performed by the eUICC (e.g., installation of a new Bound Profile Package) and **the necessary material for key agreement** with Perfect Forward Secrecy (PFS), allowing a secure end-to-end communication between the SM-DP+ and the eUICC:
  - Transaction ID
  - Description of the keys to generate
  - **One-time public key for key agreement generated by SM-DP+ (otPK.DP.KA)**
  - Signature upon material (including the previously generated otPK.EUICC.KA, also acting as an eUICC challenge) to ensure its integrity and authenticity."

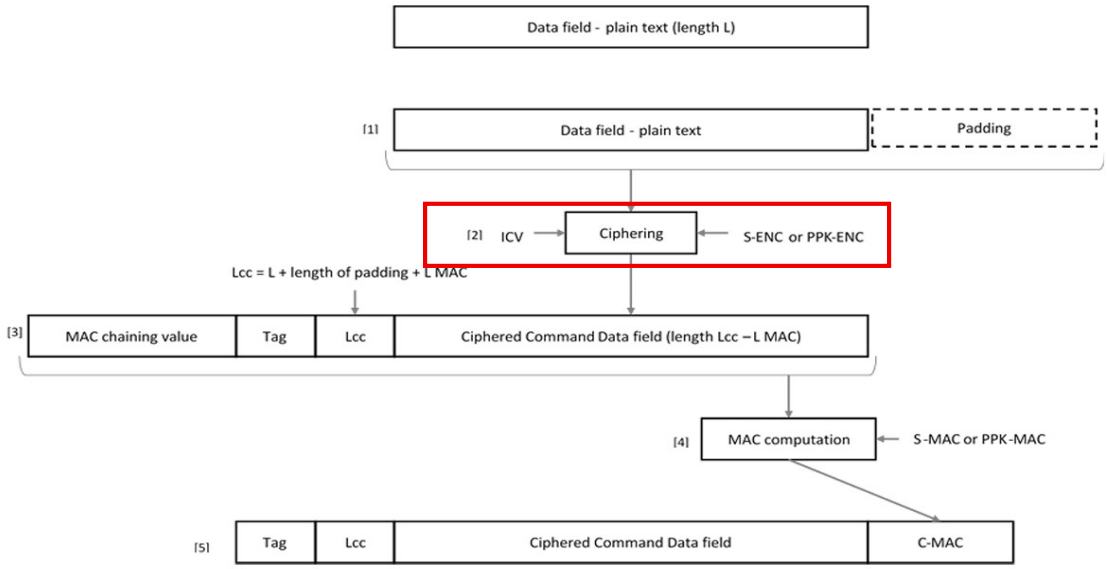
SGP.22-v3.1 at §5.5.1 (Function: InitialiseSecureChannel)

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

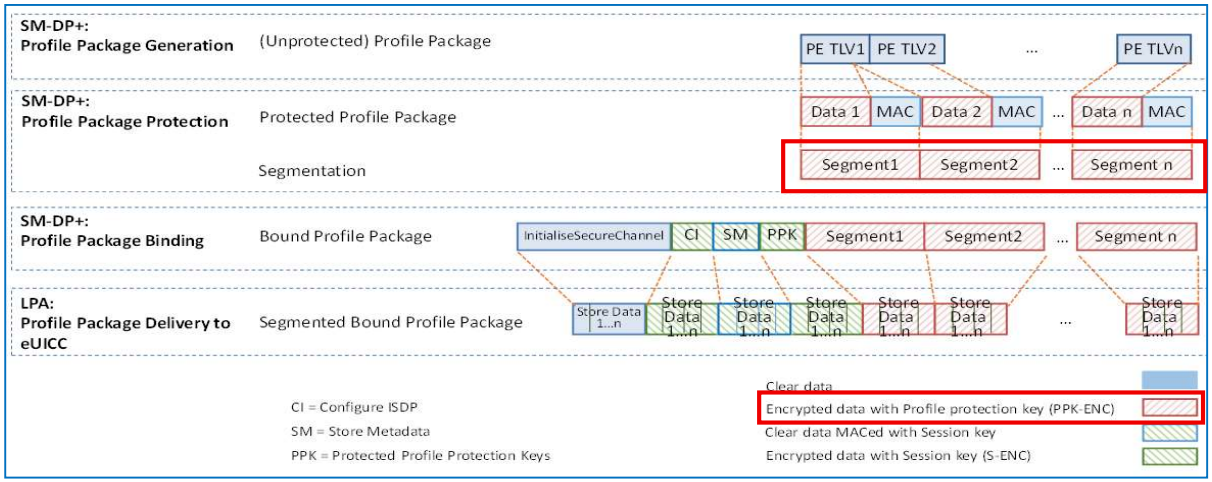
Petitioner Samsung Ex-1029, 0029

CLAIM 5	'094 PATENT V. SAMSUNG
5. The method of claim 1, wherein the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange.	The Accused Instrumentalities include that the key exchange algorithm is an Elliptic Curve Diffie-Hellman key exchange. More specifically, as part of implementing eSIM functionality, the accused Samsung devices include a key exchange algorithm. The key exchange algorithm is an "ECKA" elliptic curve key agreement algorithm. The eSIM specifications further explain the operation of the elliptic curve Diffie-Hellman key exchange: • "2.6.4.1 Key agreement An **Elliptic Curve Key Agreement Algorithm (ECKA) is used** for the establishment of a shared secret value. It shall follow the definition for the Anonymous Diffie-Hellman Key Agreement in BSI TR-03111 [41]. The algorithm is executed • by the SM-DP+ using otPK.EUICC.KA and otSK.DP.KA, and • by the eUICC using otPK.DP.KA and otSK.EUICC.KA to calculate the shared secret value." SGP.22-v3.1 at §2.6.4.1 (Key Agreement) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

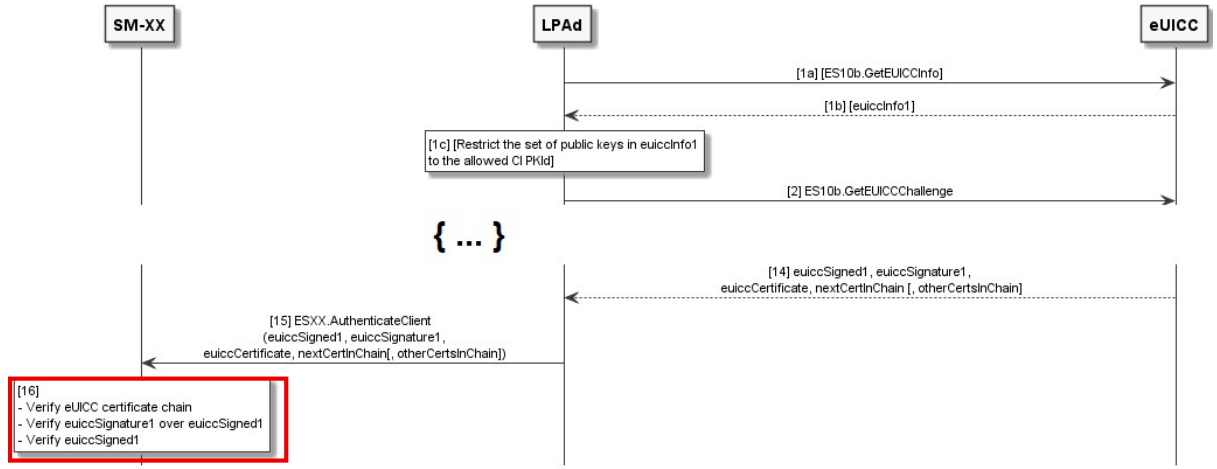
Petitioner Samsung Ex-1029, 0030

CLAIM 6	'094 PATENT V. SAMSUNG
6. The method of claim 1, wherein the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form.	The Accused Instrumentalities include that the encrypted profile is encrypted in a manner so that intermediate nodes on an IP network would not be able to read data within the profile in an unencrypted form. More specifically, as part of implementing eSIM functionality, the accused Samsung devices receive an encrypted profile. The eSIM specifications explain the operation of encrypting the profile, which prevents intermediate nodes from reading the unencrypted form: **2.6.4.4 Command TLV MACing and Encryption** BSP C-MAC and C-ENCRYPTION are done as follows:  • **Figure 4a: TLV Command Data Field Encryption and C-MAC computation** SGP.22-v3.1 at §2.6.4.4 (Comman TLV MACing and Encryption) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0031

CLAIM 7	'094 PATENT V. SAMSUNG
7. The method of claim 1, wherein subscription manager system stores the ciphertext and the symmetric key before step (a).	The Accused Instrumentalities include that subscription manager system stores the ciphertext and the symmetric key before step (a). More specifically, the subscription manager system stores the ciphertext and the symmetric key (*e.g.*, "PPK-ENC") before step (a), when the accused Samsung devices generate a first message in step (a). The eSIM specifications explain the ciphertext, depicted with red hashes, and the symmetric key ("PPK-ENC") can be processed "without having any eUICC knowledge," which would be before receipt of the first message in step (a). •  Figure 4: Profile Package stage Description SGP.22-v3.1 at §2.5.1 (Profile Package Types Overview) • "**<u>The random key mode allows performing Profile Package Protection in advance without having any eUICC knowledge</u>**. It may help to provide a better SM-DP+ scalability." SGP.22-v3.1 at §2.5.3 (Protected Profile Package) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

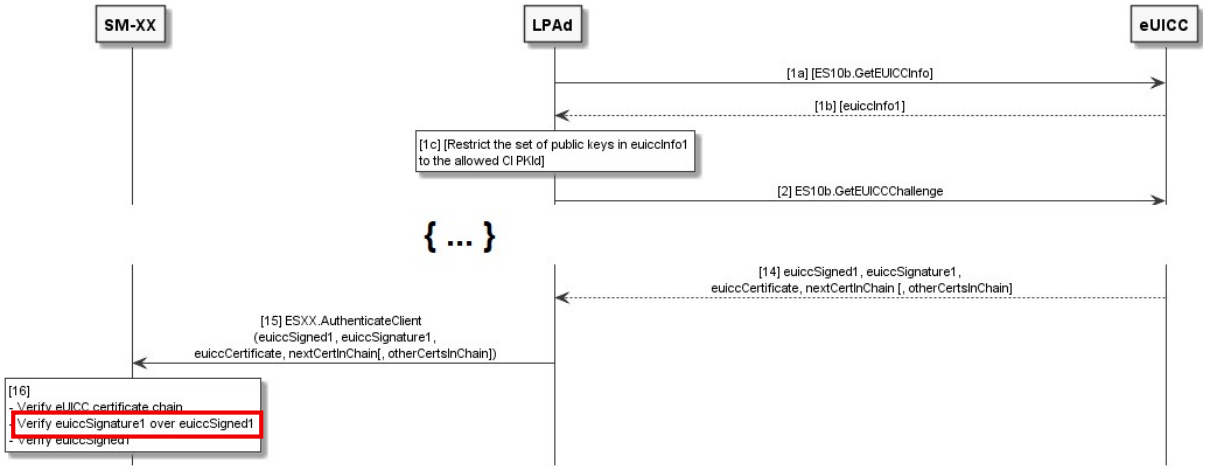
Petitioner Samsung Ex-1029, 0032

CLAIM 8	'094 PATENT V. SAMSUNG
8. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message.	The Accused Instrumentalities include that after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the identity of the embedded universal integrated circuit card included in the first message. More specifically, as part of implementing eSIM functionality, after step 1(b) the accused Samsung devices are authenticated by the subscription manager system (e.g. SM-XX) using at least the identity of the eUICC (e.g. "EID") included in the first message. The eSIM specifications explain the subscription manager system verifies the eUICC certificate information and the digital signature information:  Figure 8a: Common Mutual Authentication Procedure SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure) The eSIM specifications further explain the eUICC is authenticated by the subscription manager system using at least the identity of the eUICC ("EID"). The eUICC certificate with the EID is verified, and then the public key from the eUICC certificate is used to verify euiccSingature1:

Petitioner Samsung Ex-1029, 0033

	• "16. On reception of the "ESXX.AuthenticateClient" function call, the SM-XX SHALL:
	  • Correlate it with the "ESXX.InitiateAuthentication" function processed in steps (7) and (8), by verifying the two TransactionIDs match.
	  • Verify that the Root Certificate of the eUICC certificate chain corresponds to the euiccCiPKIdToBeUsed or euiccCiPKIdToBeUsedV3 that the SM-XX selected when executing the "ESXX.InitiateAuthentication" function.
	  • **Verify that the eUICC Certificate chain is valid as described in section 4.5.2.2.**
	  • **Verify the euiccSignature1 performed over euiccSigned1 using the PK.EUICC.SIG contained in the CERT.EUICC.SIG**.
	  • Verify that serverChallenge contained in euiccSigned1 matches the one generated by the SM-XX during step (7).
	  • Verify that the eUICC and LPA RSP capabilities match those received in ESXX.InitiateAuthentication."
	
	SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)
	
	See also evidence and analysis from claim 1, which is incorporated fully herein by reference.

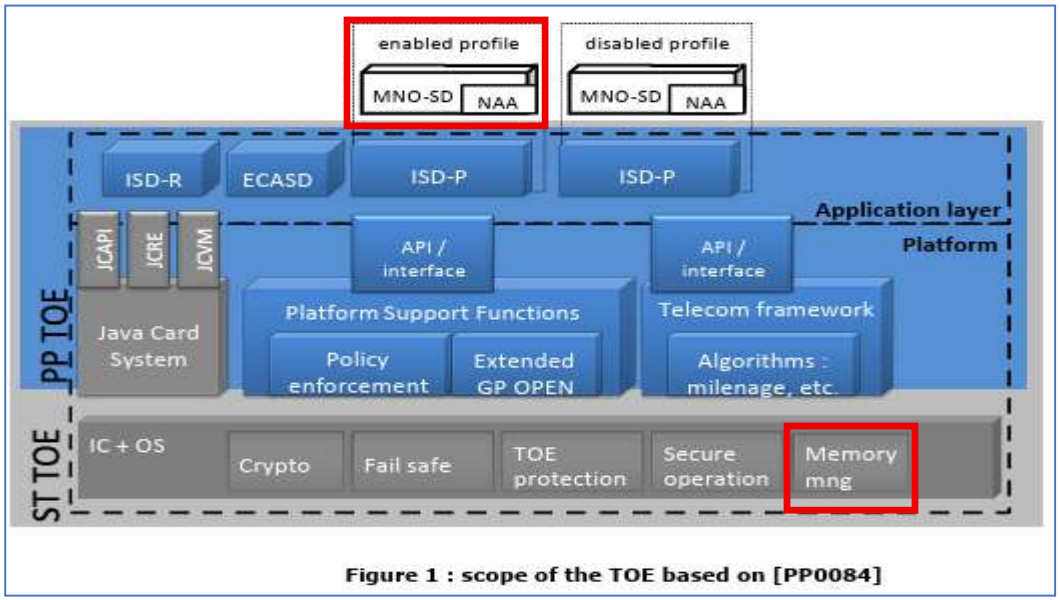
Petitioner Samsung Ex-1029, 0034

CLAIM 9	'094 PATENT V. SAMSUNG
9. The method of claim 1, wherein after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message.	The Accused Instrumentalities include that after the step (b), the embedded universal integrated circuit card is authenticated by the subscription manager system using at least the digital signature included in the first message. More specifically, as part of implementing eSIM functionality, after step 1(b) the accused Samsung devices are authenticated by the subscription manager system (e.g. SM-XX) using at least the digital signature (e.g. euiccSignature1) included in the first message. The eSIM specifications explain the subscription manager system shall "verify euiccSignature1", which is included in the first message:  • Figure 8a: Common Mutual Authentication Procedure SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure) • "16. On reception of the "ESXX.AuthenticateClient" function call, the SM-XX SHALL: • Correlate it with the "ESXX.InitiateAuthentication" function processed in steps (7) and (8), by verifying the two TransactionIDs match.

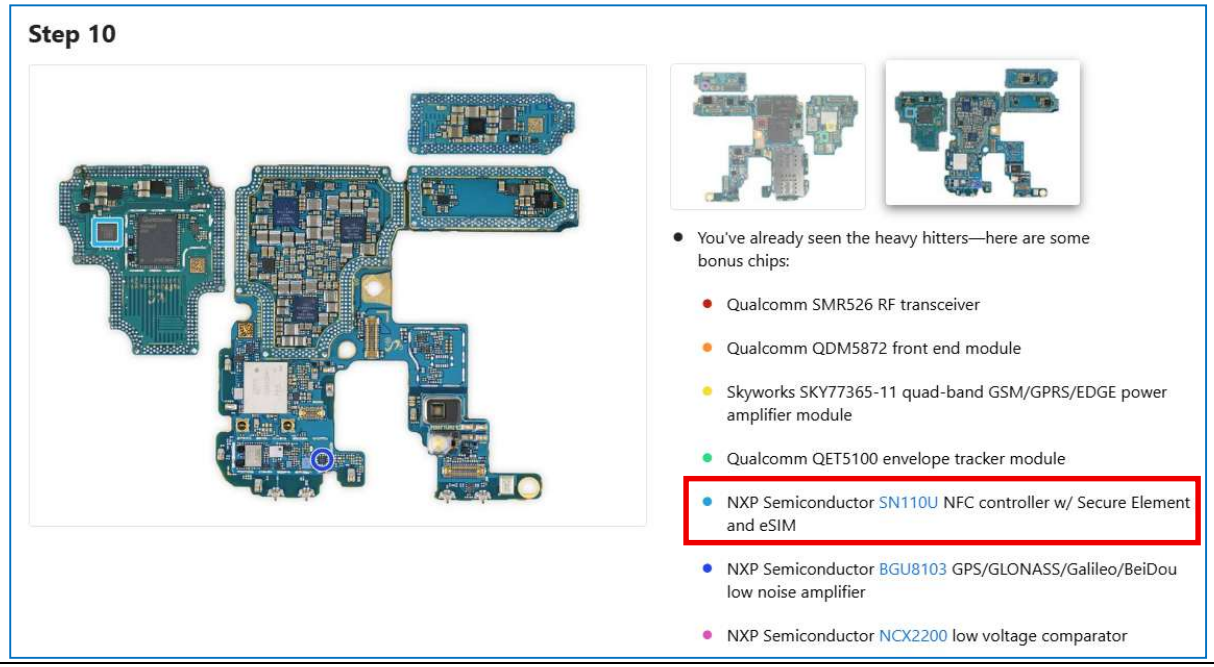
Petitioner Samsung Ex-1029, 0035

	• Verify that the Root Certificate of the eUICC certificate chain corresponds to the euiccCiPKIdToBeUsed or euiccCiPKIdToBeUsedV3 that the SM-XX selected when executing the "ESXX.InitiateAuthentication" function. • Verify that the eUICC Certificate chain is valid as described in section 4.5.2.2. • **Verify the euiccSignature1 performed over euiccSigned1 using the PK.EUICC.SIG contained in the CERT.EUICC.SIG**. • Verify that serverChallenge contained in euiccSigned1 matches the one generated by the SM-XX during step (7). • Verify that the eUICC and LPA RSP capabilities match those received in ESXX.InitiateAuthentication." SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0036

CLAIM 10	'094 PATENT V. SAMSUNG
10. The method of claim 1, wherein the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card.	The Accused Instrumentalities include that the decrypted ciphertext is stored in nonvolatile memory of the embedded universal integrated circuit card. More specifically, as part of implementing eSIM functionality, the accused Samsung devices include an eUICC with nonvolatile memory, such that data in the nonvolatile memory remains stored even if power is removed from the devices. The nonvolatile memory stores the decrypted ciphertext comprising the profile information. The eSIM specifications explain the plaintext profile (*e.g.*, "enabled profile") is stored in a nonvolatile memory for the eUICC (labeled "Memory mng"). The plaintext profile is after decryption of the ciphertext version of the profile: •  **Figure 1 : scope of the TOE based on [PP0084]** SGP.05-v4.0 at §1.2.1 (TOE type) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0037

CLAIM 13	'094 PATENT V. SAMSUNG
13. The method of claim 1, wherein the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module.	The Accused Instrumentalities include that the embedded universal integrated circuit card is operably connected to a module and wherein the module is a wireless module. More specifically, as part of implementing eSIM functionality, the accused Samsung devices include an embedded universal integrated circuit card that is operably connected to a wireless module (e.g. "Galaxy S20"): • 

Petitioner Samsung Ex-1029, 0038

	• https://www.ifixit.com/Teardown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141 *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0039

CLAIM 14	'094 PATENT V. SAMSUNG
14. The method of claim 13, wherein the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology.	The Accused Instrumentalities include that the module is configured to communicate using one or more wireless technologies of types selected from the group consisting of: WiFi, WiMax, General Packet Radio Services, Enhanced Data rates for GSM Evolution and 3rd Generation Partnership Project technology. More specifically, as part of implementing eSIM functionality, the accused Samsung devices are configured to communicate using wireless technologies consisting of at least Wi-Fi, and 3rd Generation Partnership Project (3GPP) technology of 4G LTE and 5G. https://news.samsung.com/global/introducing-the-samsung-galaxy-s20-change-the-way-you-experience-the-world Samsung Newsroom CORPORATE | PRODUCTS | ESG | PRESS RESOURCES Network & Connectivity **5G:** 5G Non-Standalone (NSA), 5G Standalone (SA), Sub6 / mmWave*, Dynamic Spectrum Sharing (DSS) **LTE:** Enhanced 4x4 MIMO, Up to 7CA, LAA, LTE Cat.20 Up to 2.0Gbps Download / Up to 200Mbps Upload **Wi-Fi:** Wi-Fi 802.11 a/b/g/n/ac/ax 2.4G+5GHz, HE80, MIMO, 1024-QAM Up to 1.2Gbps Download / Up to 1.2Gbps Upload **Bluetooth:** Bluetooth® v 5.0 , ANT+, USB type-C, NFC, Location (GPS, Galileo, Glonass, BeiDou) *S20 only supports Sub6 *LTE: LAA is only for US *Actual speed may vary depending on country, carrier, and user environment. *Requires optimal 5G connection. Actual speed may vary depending on country, carrier, and user environment. *Galileo and BeiDou coverage may be limited. BeiDou may not be available for certain countries. https://news.samsung.com/global/introducing-the-samsung-galaxy-s20-change-the-way-you-experience-the-world *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

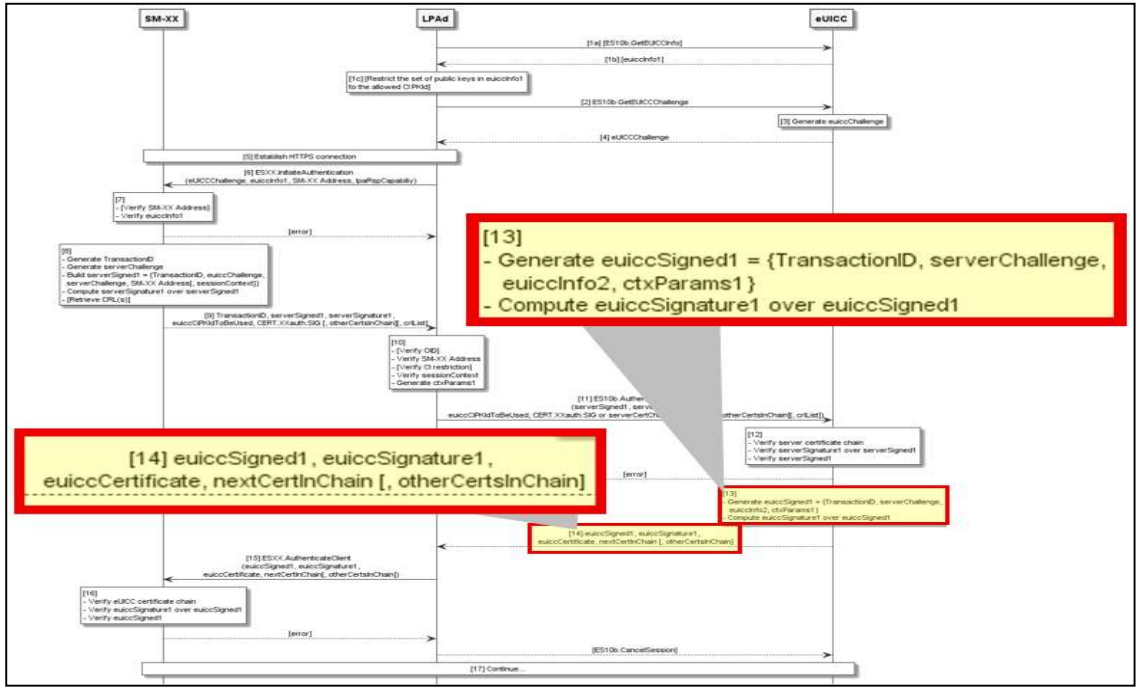
Petitioner Samsung Ex-1029, 0040

CLAIM 15	'094 PATENT V. SAMSUNG
15. The method of claim 13, wherein the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard.	The Accused Instrumentalities include that the module comprises a module of a type selected from the group consisting of the following: wireless handset, cellular phone, smartphone, laptop computer, tracking device, computer with a radio, circuit board with a radio, hand-held device, netbook, portable computer, multiprocessor system, microprocessor based consumer electronic, programmable consumer electronic, network personal computer, minicomputer, mainframe computer and smartcard. More specifically, as part of implementing eSIM functionality, the accused Samsung are examples of a module of a type selected from the group recited: • https://www.ifixit.com/Teardown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141 *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0041

CLAIM 19	'094 PATENT V. SAMSUNG
19. The method of claim 1, wherein the deriving step (c) is performed prior to the generating step (a).	The Accused Instrumentalities include that the deriving step (c) is performed prior to the generating step (a). More specifically, as part of implementing eSIM functionality, in some cases for eSIM profile downloads, the accused Samsung devices perform the deriving step (c) prior to the generating step (a). As one example, the deriving step (c) could be performed during a prior failed attempt to download an eSIM profile, and the subscription manager can specify use of the previously derived keys. The eSIM specifications explain the previously generated keys can be used: • "5. If the eligibility check fails, the SM-DP+ SHALL: • Set the Profile corresponding with the pending Profile download order in 'Error' state (section 3.1.6). • Return an error status to the LPAd and the procedure SHALL stop. Otherwise, the SM-DP+ SHALL: • Determine if a Confirmation Code is required for this pending order. • **Determine whether the Profile is already bound to the EID from a previous unsuccessful download attempt. If so, the SM-DP+ MAY indicate in its response the otPK.EUICC.KA it wants to use.** • Determine if an RPM Package for the eid is also pending. • Generate an smdpSigned2 data structure containing associated data elements. • Compute the smdpSignature2. • Generate the Profile Metadata of the Profile." SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation) *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0042

CLAIM 20	'094 PATENT V. SAMSUNG
20. The method of claim 1, wherein the generating step (a) is performed before the deriving step (c).	The Accused Instrumentalities include that the generating step (a) is performed before the deriving step (c). More specifically, as part of implementing eSIM functionality, for a regular example of eSIM profile download, the accused Samsung devices generate the first message in step (a) before deriving a second eUICC private key and a corresponding second eUICC public key in step (c). The eSIM specifications explain the process for downloading an eSIM profile in the following sequence: (i) the eUICC generates data for the first message, and (ii) the eUICC derives a second eUICC private key and a corresponding second eUICC public key: •  Figure 8a: Common Mutual Authentication Procedure SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)

Petitioner Samsung Ex-1029, 0043

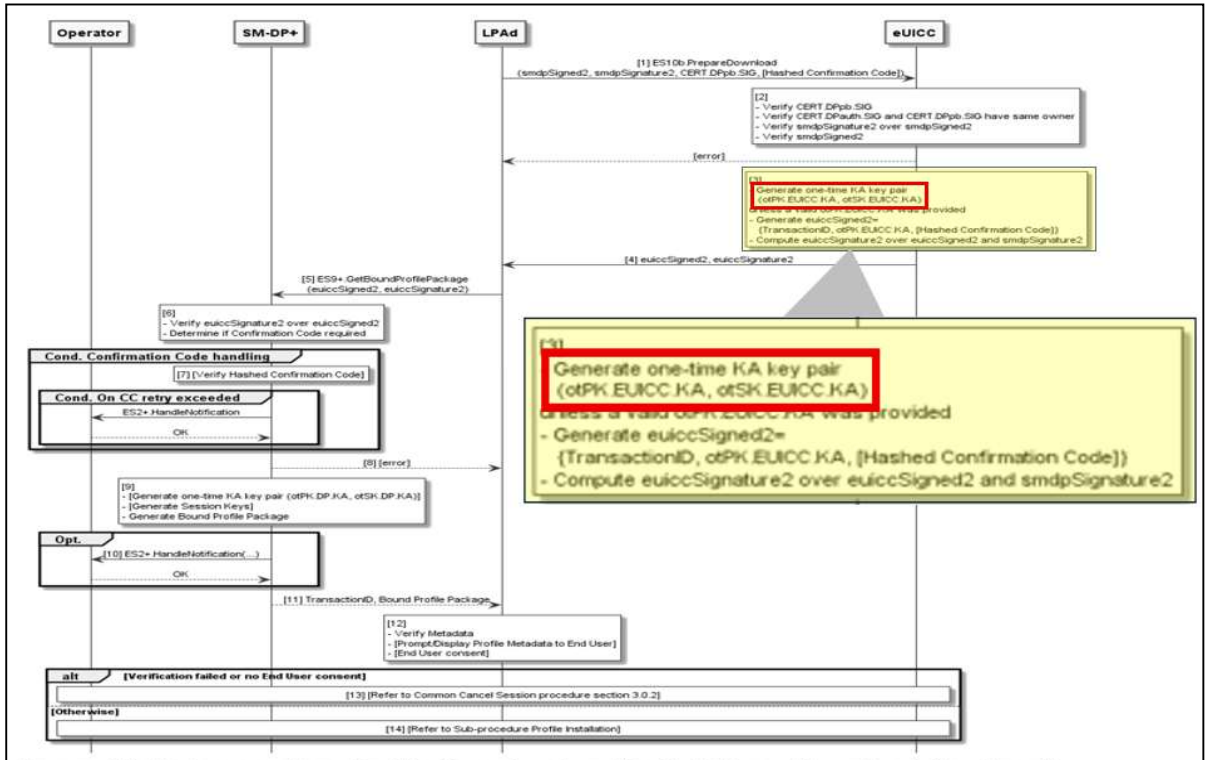
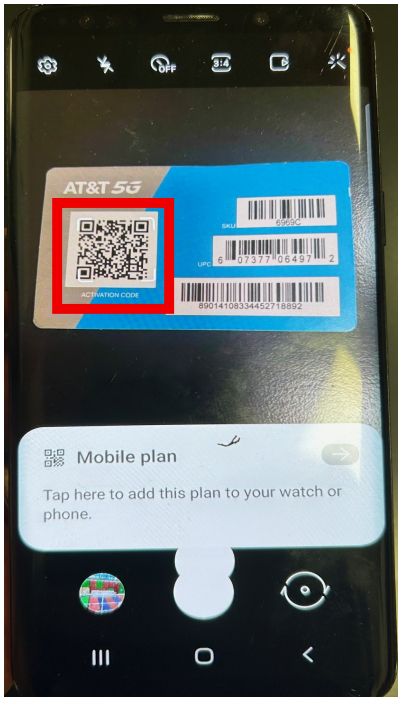


Figure 13: Sub-procedure Profile Download and Installation – Download Confirmation

- SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)

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

Petitioner Samsung Ex-1029, 0044

CLAIM 21	'094 PATENT V. SAMSUNG
21. The method of claim 1, wherein the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key.	The Accused Instrumentalities include that the embedded integrated circuit card is operably connected to a module and a user accesses a user interface of the module to enter authentication information before the module receives the symmetric key. More specifically, as part of implementing eSIM functionality, the accused Samsung devices are examples of modules with eUICCs operably connected. Users access a user interface of the Samsung mobile devices. The users enter authentication information (e.g. an "Activation Code") before the Samsung device receives the symmetric key. For example, the image below shows the user interface when a Samsung mobile device receives a QR code containing the AT&T activation code: •  *See also* evidence and analysis from claim 1, which is incorporated fully herein by reference.

Petitioner Samsung Ex-1029, 0045