

Exhibit C

Chart Detailing Samsung's Infringement of U.S. Patent No. 11,916,893

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. 11,916,893 (“the ‘893 Patent”). Samsung directly infringes claims 1, 2, 4-10, and 12-17 of the ‘893 Patent when it makes, uses, sells, offers to sell, and/or imports the Accused Instrumentalities. Samsung indirectly infringes claims 1, 2, 4-10, and 12-17 of the ‘893 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

1[PRE]. A mobile device for communicating with a wireless network, the mobile device comprising:

'893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices for communicating with a wireless network.

More specifically, the Accused Instrumentalities include all Samsung mobile 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>.

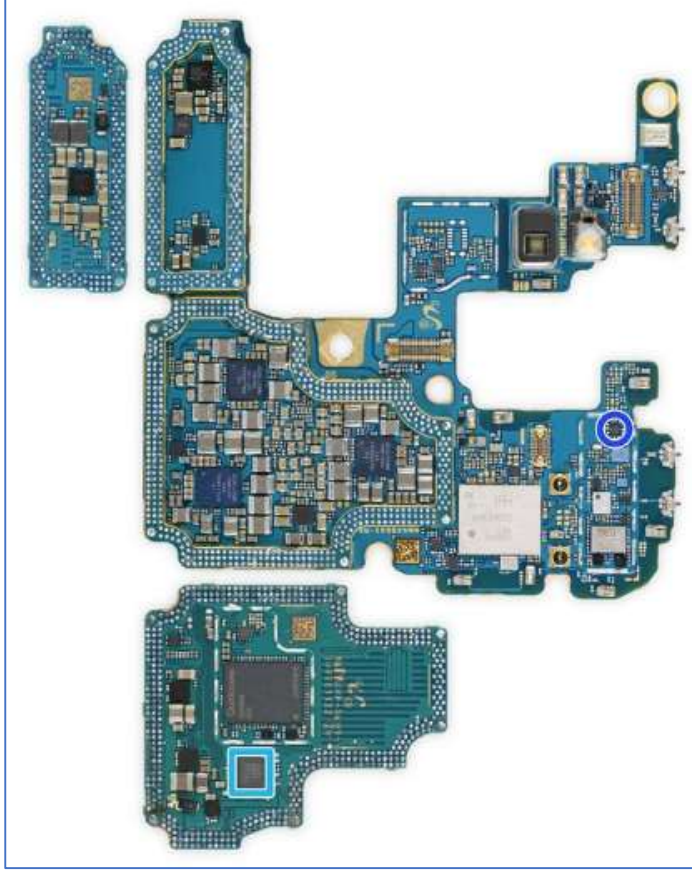
The GSMA eSIM specifications detail the eSIM functionality for Samsung’s mobile devices. Those GSMA eSIM specifications, which can be found at <https://www.gsma.com/solutions-and-impact/technologies/esim/esim-specification/>, include the Architecture Specifications, Technical Specifications, and Test 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://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/>.

1[A] a first memory configured to store an embedded universal integrated circuit card (eUICC) identity;

The Accused Instrumentalities include a first memory configured to store an embedded universal integrated circuit card (eUICC) identity.

More specifically, the accused Samsung mobile devices have a memory that stores an eUICC-ID called an “EID” that identifies the eUICC.

This figure shows a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes eSIM hardware (in light blue) containing a memory for storing an eUICC identity:



<https://www.ifixit.com/TearDown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141>. Each of the other Samsung mobile devices include similar memory hardware.

The eSIM specifications further describe a first memory for storing an eUICC identity. For example, the RSP Technical Specification states that operator profiles are stored inside security domains within the eUICC:

- “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.

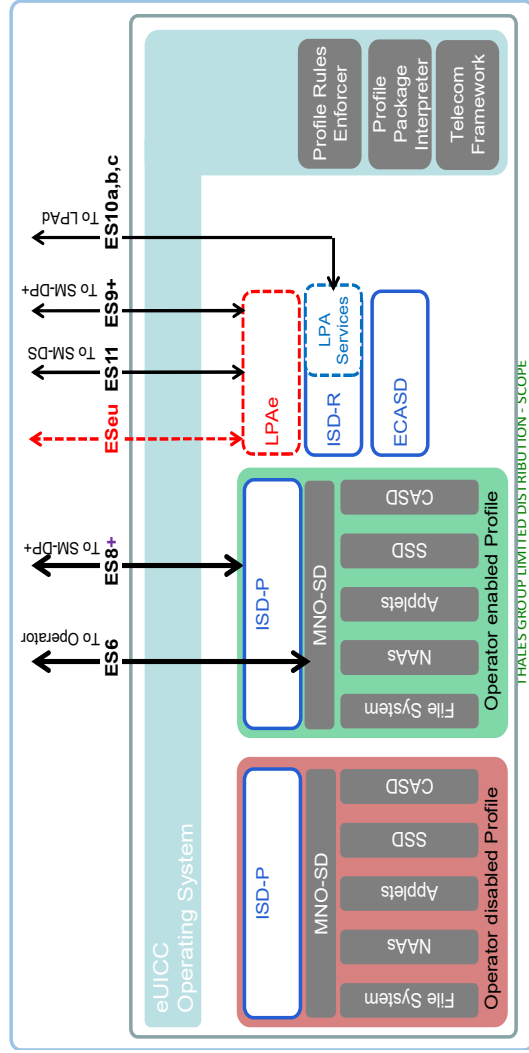


Figure 3: Schematic Representation of the eUICC”

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

The eSIM specifications further explain that the eUICC Controlling Authority Security Domain (ECASD) securely stores the credentials required to support the required security domains on the eUICC. The ECASD contains the eUICC’s certificate for eUICC authentication (CERT.EUICC.SIG):

- “2.4.2 ECASD
The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for secure storage of credentials required to support the required Security Domains on the eUICC.
 These SHALL be only one ECASD on an eUICC....”

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)
- The eSIM Certificate Issuer's (CI) RootCA Public Key(s) (PK.CI.SIG) for verifying off-card entities certificates (e.g., SM-DP+) and Certificate Revocation List (CRL). ECASD MAY contain several public keys belonging to the same eSIM CA or different eSIM CAs. Each PK.CI.SIG SHALL be stored with information coming from the CERT.CI.SIG the key is included in, at least:
 - o eSIM Certificate Issuer OID
 - o Subject Key Identifier: required to verify the Certificate chain of the off-card entity
- The Certificate(s) of the EUM (CERT.EUM.SIG), and, optionally, the Certificate(s) of the EUM SubCA (CERT.EUMSubCA.SIG)"

SGP.22-v3.1 at §2.4.2 (ECASD).

The eSIM specifications further describe the specific fields of the eUICC certificate (CERT.EUICC.SIG), including 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:

¹ All emphasis throughout this claim chart is added by Network1, unless stated otherwise.

Field	Value Description
subject	<p>Distinguished Name of the EUICC. It SHALL include, at least, 'organization' and 'serialNumber' attributes. Others attributes MAY be included for information.</p> <p>The 'organization' attribute SHALL have one of the values allowed in the nameConstraints extension of the EUM Certificate (CERT.EUM.SIG). See note 1.</p> <p>The 'serialNumber' attribute SHALL be the EID as a decimal PrintableString (see note 2). The EID SHALL start with one of the EIDs allowed in the EUM Certificate (CERT.EUM.SIG).</p> <p>Example of an eUICC DN: o = ACME serialNumber = 8904903212345123451234512345678901235</p>

Table 11: CERT.EUICC.SIG”

SGP.22-v3.1 at §4.5.2.1.0.2 (eUICC)

The eSIM specifications further explain 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)

1[B] a random number generator operably connected to a processor connected to a second memory

The Accused Instrumentalities include a random number generator operably connected to a processor connected to a second memory configured to generate a random number for an eUICC private key corresponding to an eUICC public key.

More specifically, the accused Samsung mobile devices have a random number generator connected to a

configured to generate a random number for an eUICC private key corresponding to an eUICC public key;

processor and memory that generates a random number for an eUICC private key called “otSK.EUICC.KA” that corresponds to an eUICC public key called “otPK.EUICC.KA.”

The eSIM specifications require devices to include a random number generator:

- “2.6.8 Random Number Generation
To protect against attacks, **a high quality random number generator is required.** 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”):

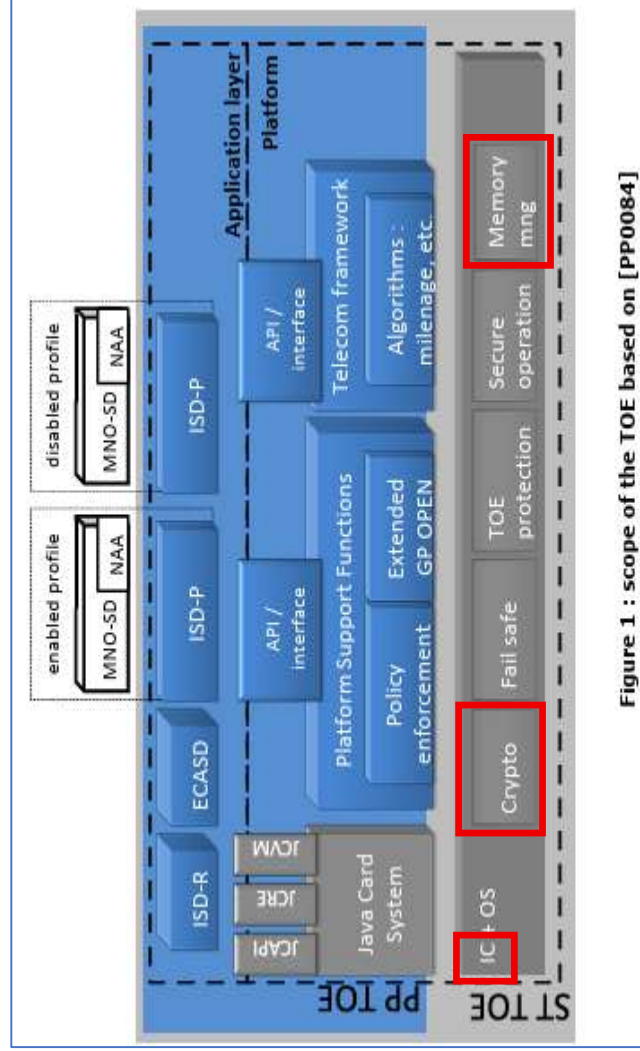


Figure 1 : scope of the TOE based on [PP0084]

SGP.05-v4.0 at §1.2.1 (TOE type)

The eSIM specifications specify that, as part of the profile download and installation procedure and the download confirmation sub-procedure, the mobile device containing the eUICC will generate a one-time key pair using an “ECCA” 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:

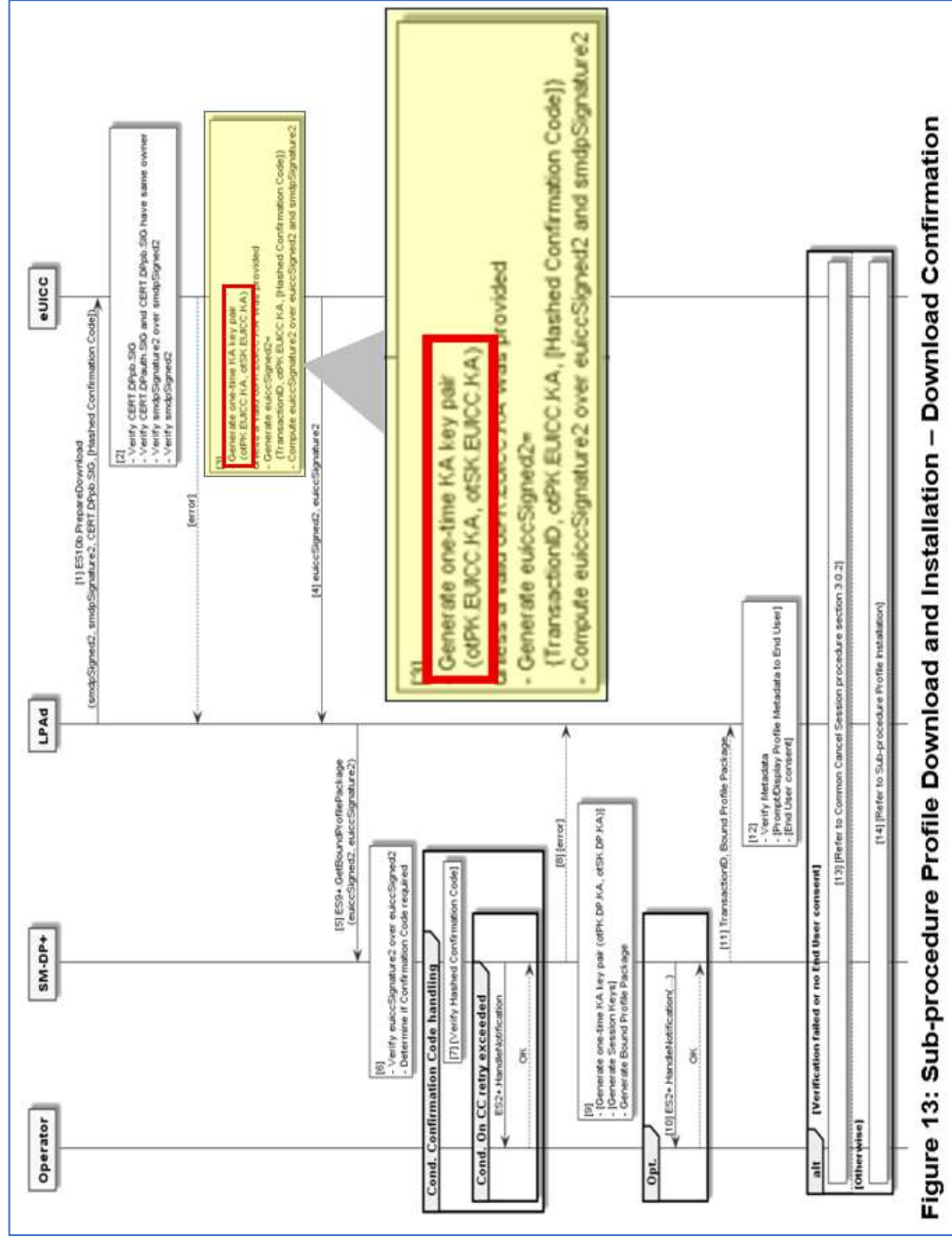


Figure 13: Sub-procedure Profile Download and Installation – Download Confirmation

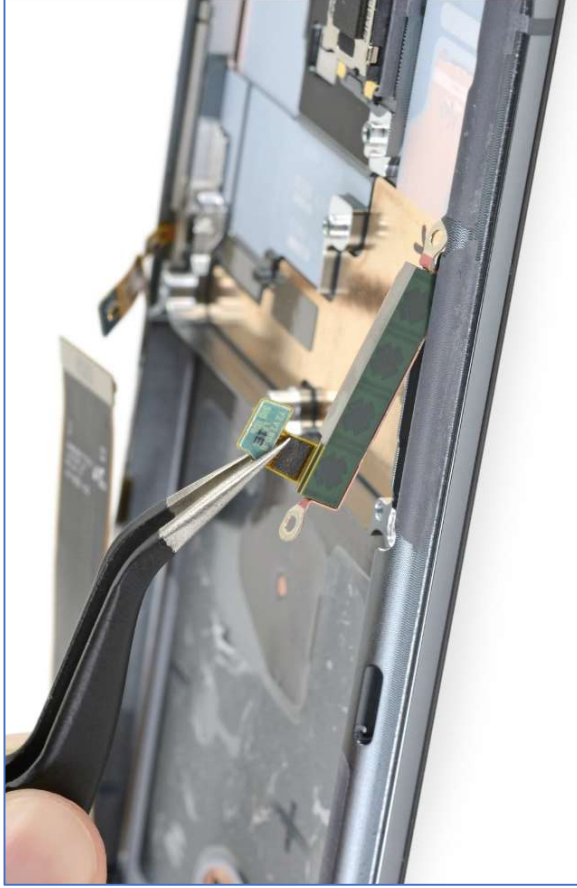
SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)

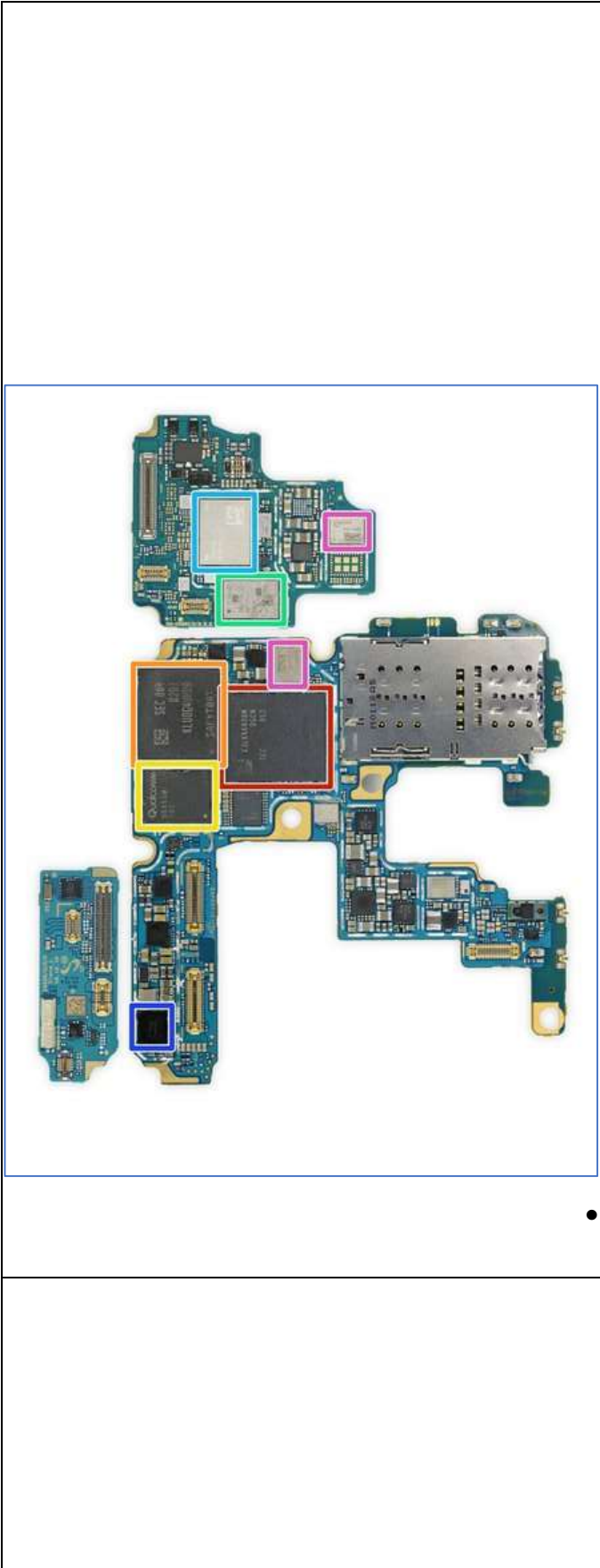
<ul style="list-style-type: none"> • “3. The eUICC SHALL: <ul style="list-style-type: none"> • Use the one-time key pair associated with the bppEuiccOtpk if it is provided by the SM-DP+ and it is still stored in the eUICC, or generate a new one-time key pair (see section 5.7.5). • Generate the euiccSigned2 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, the eUICC SHALL: <ul style="list-style-type: none"> • Extract the public key of the CERT.DPpb.SIG and attach it to the RSP Session. • 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) <p>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:</p>	<div data-bbox="933 241 1177 1470" style="border: 1px solid black; padding: 5px;"> <p>Key establishment protocol [edit]</p> <p>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.</p> </div> <ul style="list-style-type: none"> • https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman.
<p>1[C] a radio including one or more transmit antennas and one or more receiving</p>	<p>The Accused Instrumentalities include a radio including one or more transmit antennas and one or more receiving antennas.</p>

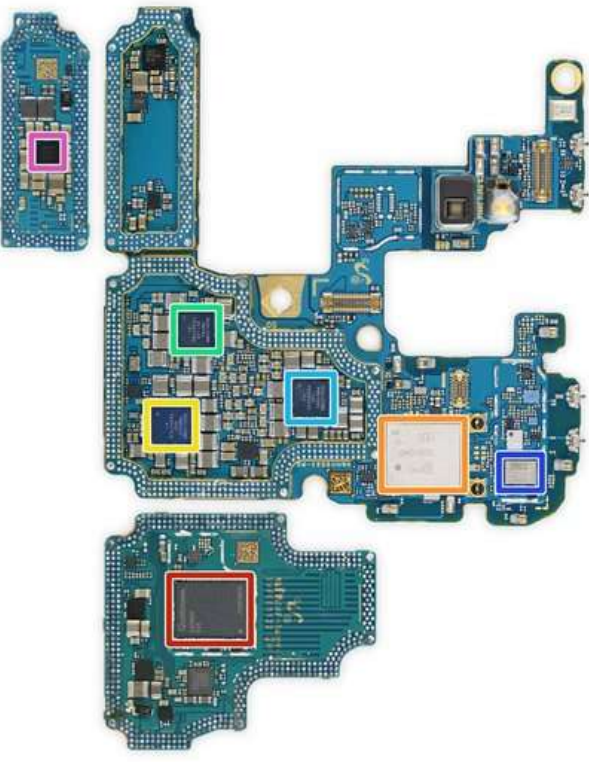
antennas configured
to:

More specifically, the accused Samsung mobile devices have a radio with at least one transmitting/receiving antenna.

These pictures show a tear-down of an exemplary Samsung mobile device (a Galaxy S20) that includes transmit/receive antennae (top) and various radio transceivers, e.g., RF transceivers from Qualcomm and Skyworks (bottom):





	<p>1[C][a] a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and</p>
	<p>• https://www.ifixit.com/Teardown/Samsung+Galaxy+S20+Ultra+Teardown/131607#s283141. Each of the other Samsung mobile devices include similar hardware.</p> <p>The Accused Instrumentalities include a radio that is configured to transmit, to a subscription manager, the eUICC identity and the eUICC public key.</p> <p>More specifically, the accused Samsung mobile devices have a radio that can transmit to a “SM-XX”/“SM-DP+” subscription manager both the “EID” eUICC identity and the “otPK.EUICC.KA” eUICC public key.</p>

The eSIM specifications explain that, as part of the Common Mutual Authentication Procedure, the LPAad within the mobile device transmits the eUICC certificate called “euiccCertificate” to the “SM-XX” subscription manager:

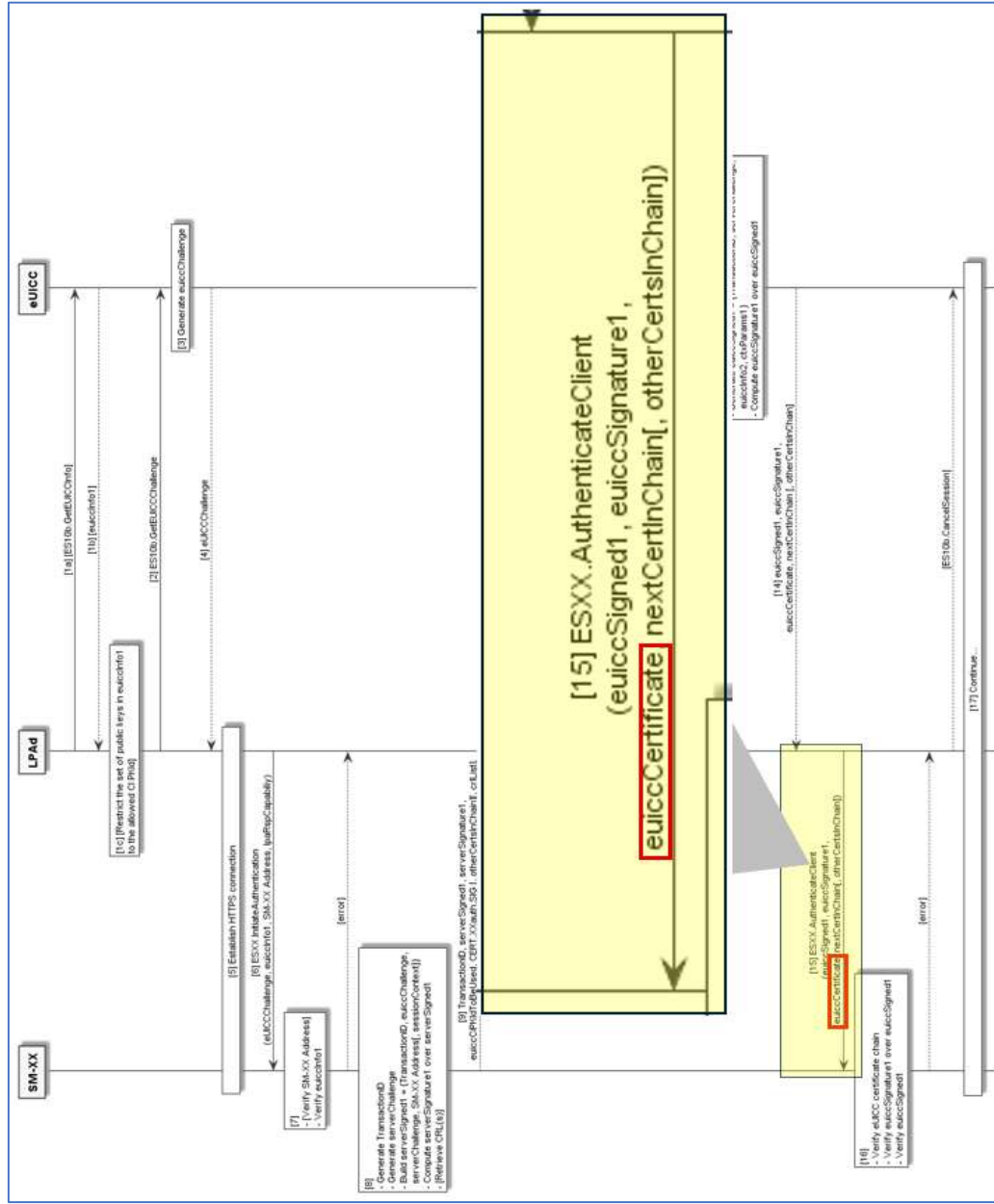


Figure 8a: Common Mutual Authentication Procedure

- 15. The LPAAd 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)

The eSIM specifications 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	<p>Distinguished Name of the EUICC. It SHALL include, at least, 'organization' and 'serialNumber' attributes. Others attributes MAY be included for information.</p> <p>The 'organization' attribute SHALL have one of the values allowed in the nameConstraints extension of the EUM Certificate (CERT.EUM.SIG). See note 1.</p> <p>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).</p> <p>Example of an eUICC DN: o = ACME serialNumber = 89049032123451234512345678901235</p>

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, as part of the profile download and installation procedure and the download confirmation sub-procedure, the LPAd within the mobile device transmits the “eUiccSigned2” data structure to the “SM-DP+” subscription manager, and that eUiccSigned2 data structure contains the “otPK.EUICC.KA” eUICC public key:

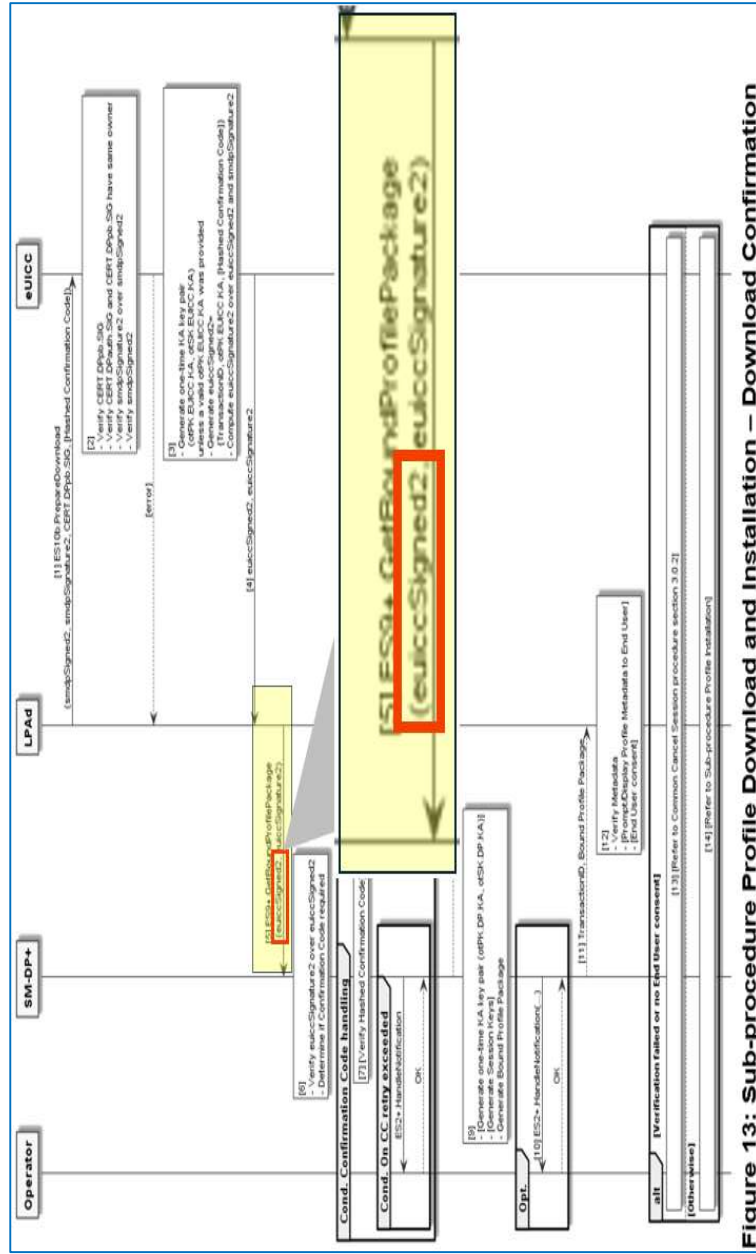


Figure 13: Sub-procedure Profile Download and Installation – Download Confirmation

	<ul style="list-style-type: none"> • “- Generate euiccSigned2 = {TransactionID, otPK.EUICC.KA, [Hashed Confirmation Code]}” SGP.22-v3.1 at §3.1.3.2 (Sub-procedure Profile Download and Installation – Download Confirmation)
<p>1[C][b] b. receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key;</p>	<p>The Accused Instrumentalities include a radio that is configured to receive, from the subscription manager, i) an eUICC profile comprising network parameters, a key K, and a subscriber identity and ii) a symmetric key. More specifically, the accused Samsung mobile devices have a radio that can receive from a “SM-XX”/“SM-DP+” subscription manager a “Bound Profile Package” eUICC profile containing: various network parameters (like the “HPPLMN” Home Public Land Mobile Network and the “UST” Service Table); the “Ki” key K; the “IMSI” subscriber identity; and the “PPK” symmetric key.</p>

The eSIM specifications further explain that the Bound Profile Package contains various data (including network parameters, a key K, and a subscriber identity) 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”:

- “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): Raw eUICC Profile Package TLV sequence.**
 - **Protected Profile Package (PPP):** Segmented and protected in BSP payload TLVs.
 - **Bound Profile Package (BPP):** 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.

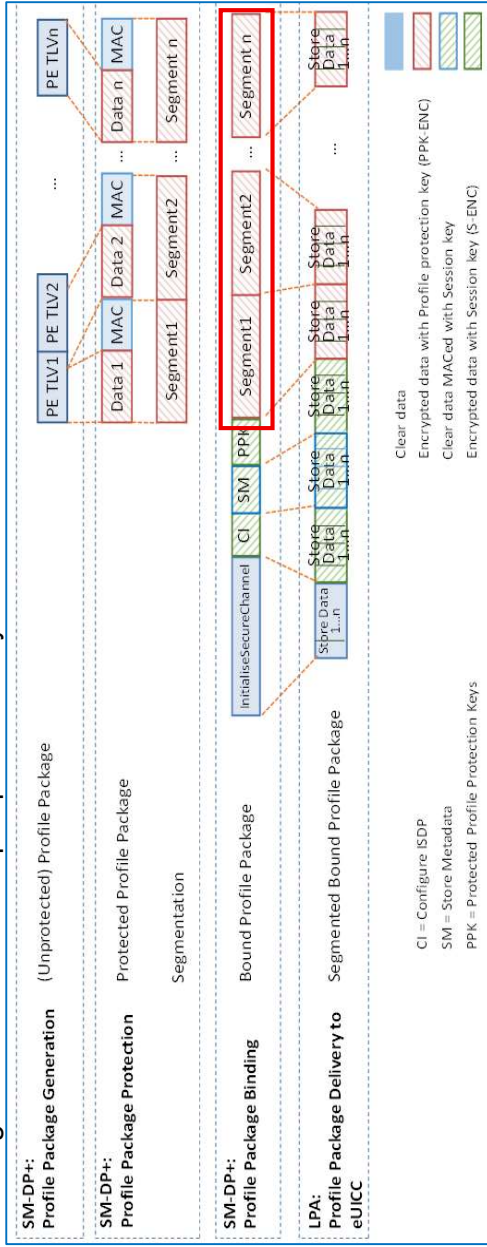


Figure 4: Profile Package stage Description”

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

- “**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 ConfigureSDP
- 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, e.g., (a) the "HPPLMN" Home Public Land Mobile Network parameter that has settings that define the preferred home network, and (b) the "UST" USIM Service Table parameter that defines which services can be activated or deactivated; (2) a "KI" key K; and the "IMSI" subscriber identity:

A		B
1	Default Test SIM Profile	
2		
3	File Id	File Name
4		
111	6F07	IMSI
111	6F08	Keys
112	6F09	KeysPS
113	6F2C	DCK
114	6F31	HPPLMN
115	6F32	CML
116	6F37	ACMMAX
117	6F38	UST
118	6F39	ACM
119	6F3B	FDN
USIM authentication parameters		
Algorithm		XOR_3G
Ki		0x00 0x01 _ 0x0F
Upc		N/A

http://www.gsma.com/newsroom/wp-content/uploads/GSMA_TS48_eSIM_GTP_Profile_Structure-v3.0.xlsx; see also <https://www.dialogic.com/glossary/home-public-land-mobile-network-hplmn> (explaining

that the “Home Public Land Mobile Network (HPLMN) identifies the PLMN (Public Land Mobile Network) in which the subscribers profile is held.”); <https://blog.wirelessmoves.com/2021/07/5g-the-sim-card-and-the-suci.html> (explaining that the UST “contains a bitmap, and each bit represents a service that can be activated or deactivated”)

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

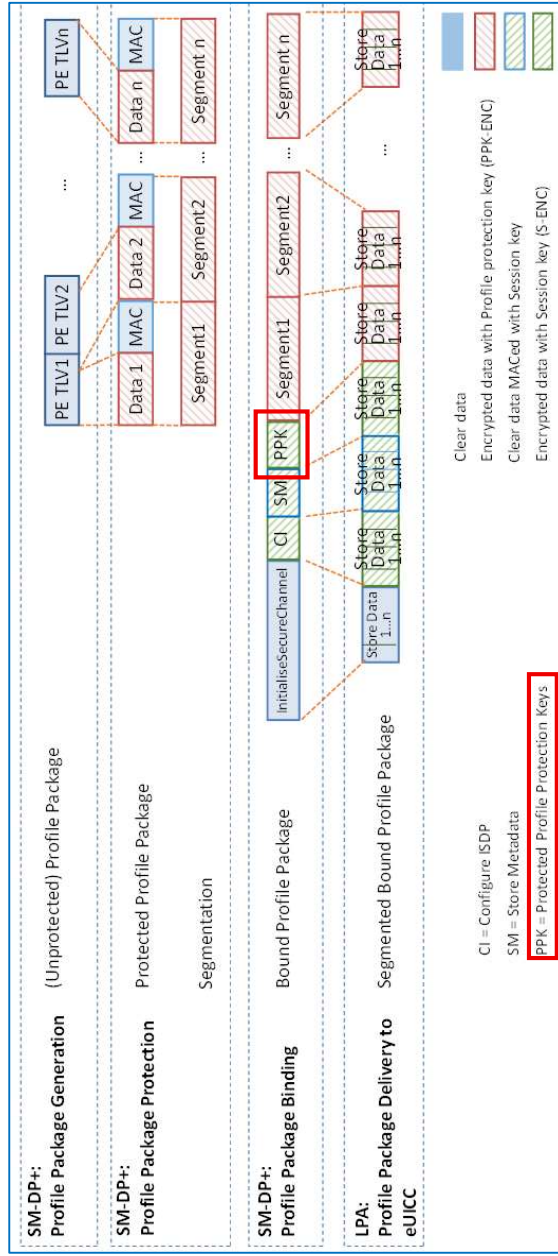


Figure 4: Profile Package stage Description

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

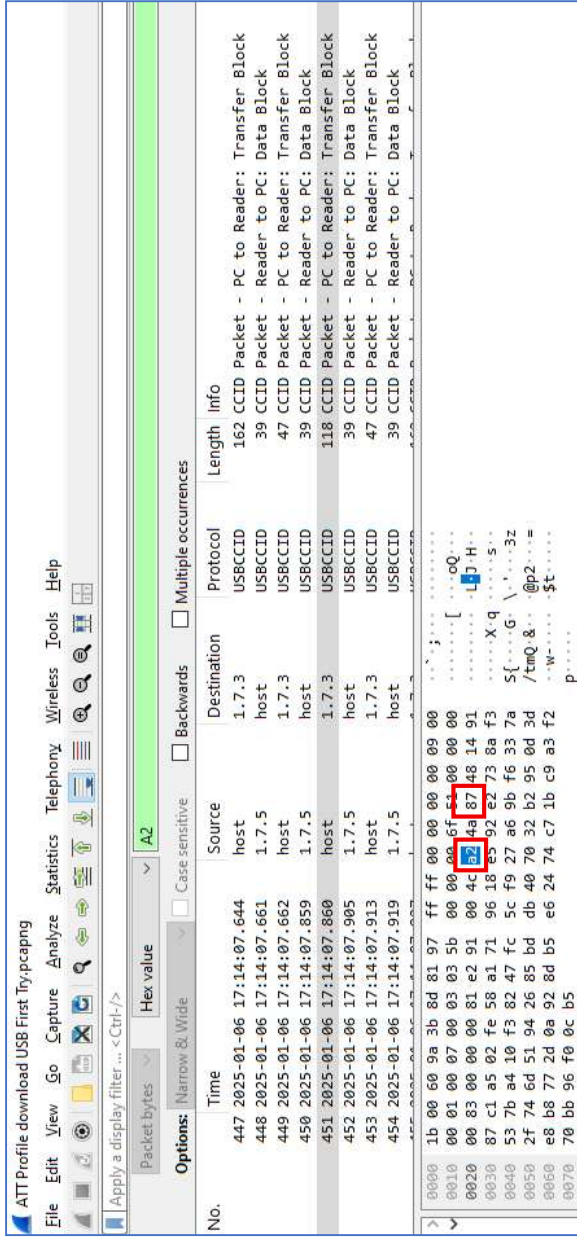
The eSIM specifications further explain that the PPK is symmetric because it is used for both encryption and decryption. Indeed, the eSIM specifications explicitly refer to the algorithms used to protect the Protected Profile Package (*i.e.*, the PPK-ENC) as symmetric algorithms:

- **“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)

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:



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
'A2'	Var.	secondSequenceOf87	
		SHALL be absent if no content	
		'87'	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)
			C
			O

1[D] an eUICC associated with the eUICC identity and configured to:

The Accused Instrumentalities include an eUICC associated with the eUICC identity. More specifically, the accused Samsung mobile devices have an eUICC that is associated with the “EID” eUICC identity.

The eSIM specifications contain this figure that shows a device (gray box) containing an eUICC component (red outline):

- “4. Remote SIM Provisioning System Architecture
This section contains the functional description of the Remote SIM Provisioning system architecture for the Embedded UICC.

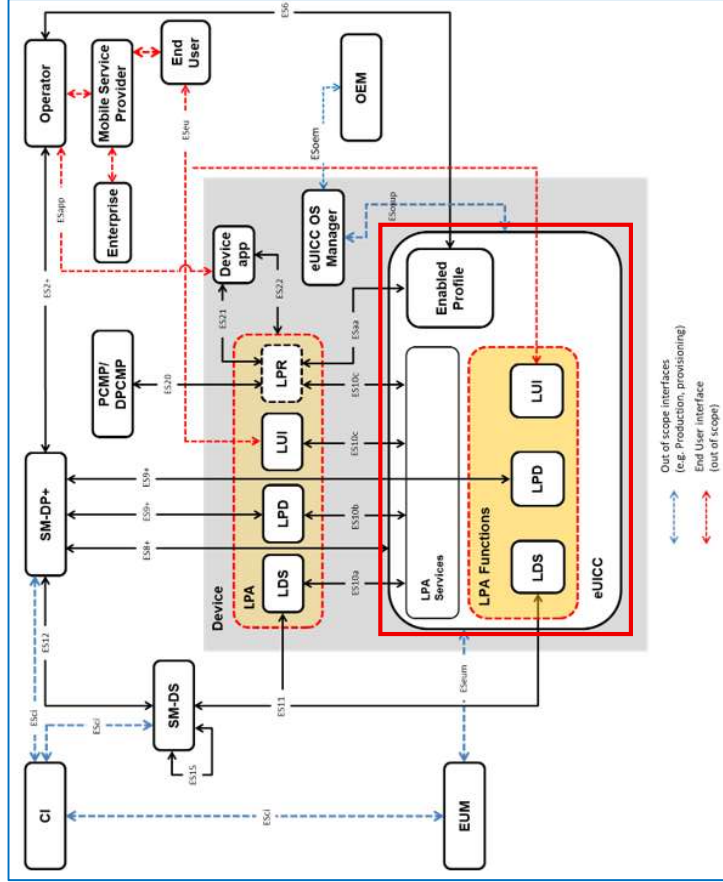


Figure 1: Remote SIM Provisioning System Architecture”

SGP.21-v3.1 at §4 (Remote SIM Provisioning System Architecture)

The eUICC is associated with the eUICC identity for the reasons shown above re claim 1[A].

<p>1[D][a] a. derive a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key;</p>	<p>The Accused Instrumentalities include an eUICC that is configured to derive a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange with the eUICC private key and a subscription manager public key.</p> <p>More specifically, the accused Samsung mobile devices have an eUICC that is configured to derive a profile key called a “Session key” or “S-ENC” profile key using an elliptic curve Diffie Hellman key exchange with the “otSK.EUICC.KA” eUICC private key and the “otPK.DP.KA” subscription manager public key.</p> <p>The eSIM specifications explain that the eUICC uses a Diffie-Hellman Key Agreement, which is elliptic curve key agreement algorithm, to create a shared secret value using the “otPK.DP.KA” subscription manager public key and the “otSK.EUICC.KA” eUICC private key:</p> <ul style="list-style-type: none"> • “2.6.4.1 Key agreement <p><u>An Elliptic Curve Key Agreement Algorithm (ECKA) is used for the establishment of a shared secret value.</u> It shall follow the definition for the Anonymous <u>Diffie-Hellman Key Agreement</u> in BSI TR-03111 [41]. <u>The algorithm is executed</u></p> <ul style="list-style-type: none"> • by the SM-DP+ using otPK.EUICC.KA and otSK.DP.KA, and • <u>by the eUICC using otPK.DP.KA and otSK.EUICC.KA</u> to calculate the shared secret value.” <p>SGP.22-v3.1 at §2.6.4.1 (Key Agreement)</p> <p>The eSIM specifications further explain that the shared secret value (discussed above) is used to derive the session key, such as the “S-ENC” profile key:</p> <ul style="list-style-type: none"> • “2.6.4.2 Key derivation <p><u>Session keys</u> and an initial MAC chaining value <u>are derived from the shared secret value</u> as follows:</p> <ul style="list-style-type: none"> • 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”): <ul style="list-style-type: none"> • 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
--	--

	<p>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:</p> <table border="1" data-bbox="272 541 479 1201"> <thead> <tr> <th style="background-color: #ff0000; color: white;">KeyData</th> <th style="background-color: #ff0000; color: white;">Key</th> </tr> </thead> <tbody> <tr> <td>1 to L</td> <td>Initial MAC chaining value</td> </tr> <tr> <td>L+1 to 2L</td> <td>S-ENC</td> </tr> <tr> <td>2L+1 to 3L</td> <td>S-MAC</td> </tr> </tbody> </table> <p style="text-align: center;">Table 4c: Key Data"</p> <p>SGP.22-v3.1 at §2.6.4.2 (Key Derivation)</p>	KeyData	Key	1 to L	Initial MAC chaining value	L+1 to 2L	S-ENC	2L+1 to 3L	S-MAC
KeyData	Key								
1 to L	Initial MAC chaining value								
L+1 to 2L	S-ENC								
2L+1 to 3L	S-MAC								
<p>1[D][b] b. decrypt a first portion of the eUICC profile using the profile key;</p>	<p>The Accused Instrumentalities include an eUICC that is configured to decrypt a first portion of the eUICC profile using the profile key.</p> <p>More specifically, the accused Samsung mobile devices have an eUICC that can decrypt a first portion of the "Bound Profile Package" eUICC profile using the "S-ENC" profile key.</p>								

The eSIM specifications further provide the below figure, which shows that the first 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)”:

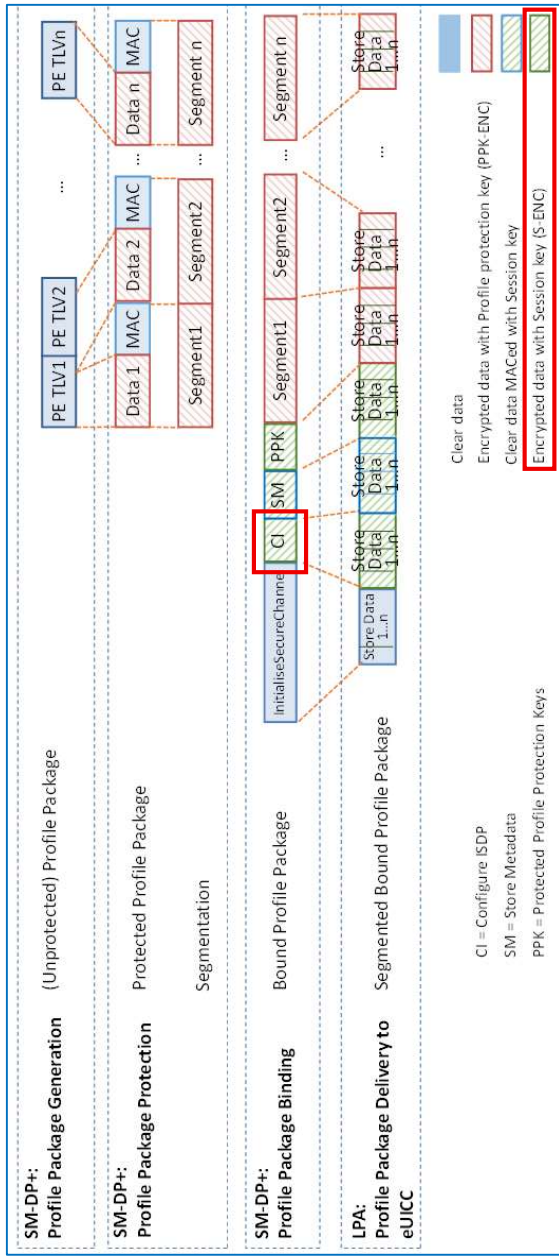
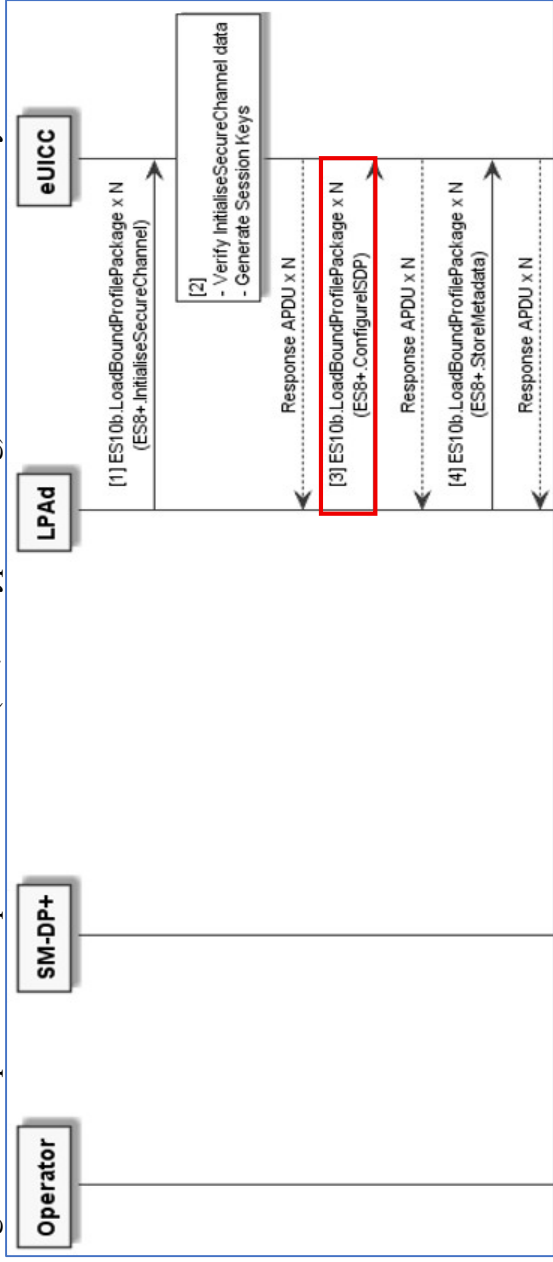


Figure 4: Profile Package stage Description

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

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., encrypted using) a “S-ENC” session key:



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

- “3. The LPA 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.	M

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)

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

<ul style="list-style-type: none"> • “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: <ul style="list-style-type: none"> • 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) <p>Thus, the eUICC decrypts with the “Session key (S-ENC)” data for the “CI” (ConfigureISDP) function to (i) Create the ISD-P and (ii) Store the SM-DP+ proprietary data.</p>	<p>The Accused Instrumentalities include an eUICC that is configured to receive the symmetric key from a network application operating in the mobile device. More specifically, the accused Samsung mobile devices have an eUICC that is configured to receive the “PPK” symmetric key from the “LPAd” network application operating on the mobile device.</p>
	<p>1[D][c] c. receive the symmetric key from a network application operating in the mobile device;</p>

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:

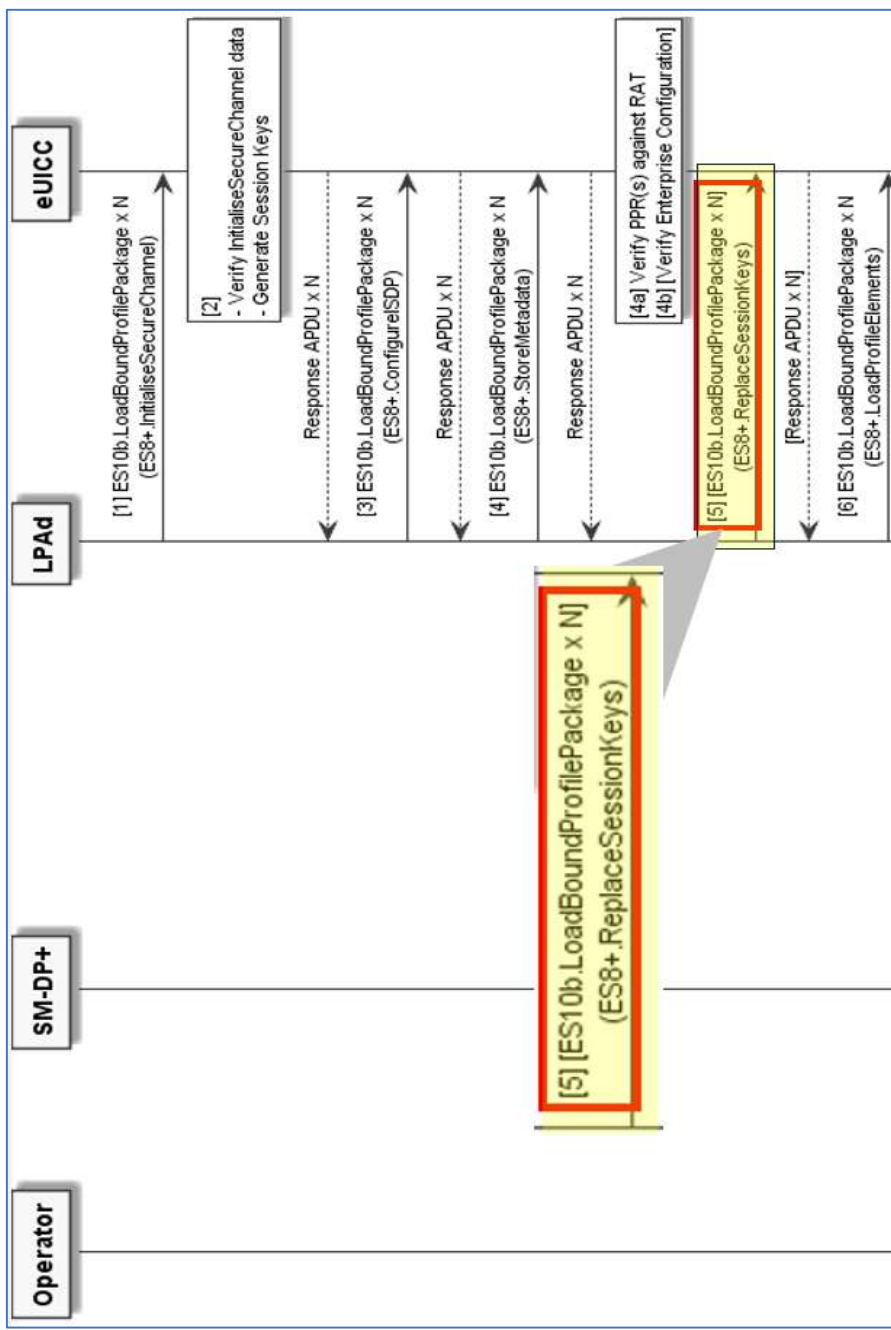


Figure 14: Sub-procedure Profile Installation

“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

<p>SHALL decrypt the Profile Protection Keys and replace the current BSP Session Keys with the decrypted Profile Protection Keys.”</p> <p>SGP.22-v3.1 at §3.1.3.3 (Sub-procedure Profile Installation)</p> <p>The eSIM specification further explain that the portion of the Bound Profile Package having TLVs for the ES8+.ReplaceSessionKeys contains the “PPK” symmetric key:</p> <ul style="list-style-type: none"> • “The following table describes the various sequences of '86', '87' and '88' TLV 	<p>1[D][d] d. decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity,</p>																
<table border="1"> <thead> <tr> <th>Tag</th> <th>Length</th> <th>Value Description</th> <th>MOC</th> </tr> </thead> <tbody> <tr> <td>'A2'</td> <td>Var.</td> <td>secondSequenceOf87 SHALL be absent if no content</td> <td>C</td> </tr> <tr> <td></td> <td>'87'</td> <td>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)</td> <td>O</td> </tr> <tr> <td></td> <td></td> <td>* * * * *</td> <td></td> </tr> </tbody> </table>	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			* * * * *		<p>SGP.22-v3.1 at §2.5.4 (Bound Profile Package)</p> <p>Table 4: Profile Installation sequences of TLV”</p> <p>The Accused Instrumentalities include an eUICC that is configured to decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising the key K and the subscriber identity, wherein the first portion and the second portion are distinct.</p> <p>More specifically, the accused Samsung mobile devices have an eUICC that can decrypt a second portion of the “Bound Profile Package” eUICC profile using the “PPK” symmetric key. Further, the second portion of the “Bound Profile Package” includes the “KI” key K and the “IMSI” subscriber identity. Moreover, the first portion of the “Bound Profile Package” eUICC profile is distinct from the second portion of the “Bound Profile Package” eUICC profile.</p>
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														
		* * * * *															

wherein the first portion and the second portion are distinct; and

The eSIM specifications further provide the below figure, which shows that the second portion of the Bound Profile Package that is colored using red hashes (and labeled “Segment”) is decrypted using the “Profile Protection Key (PPK-ENC)”:

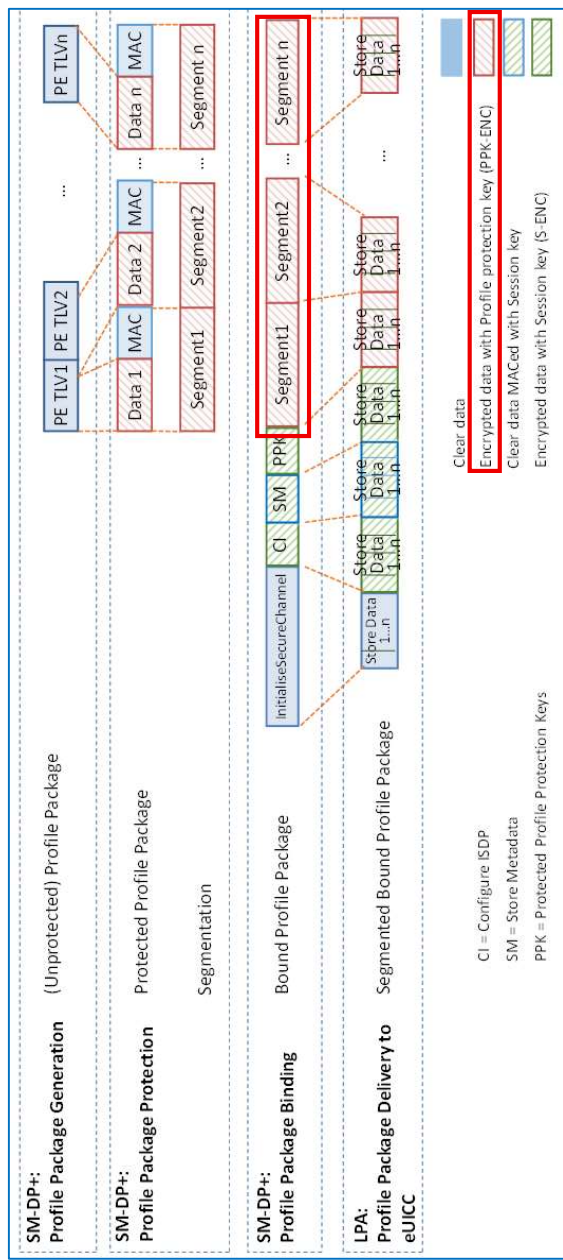


Figure 4: Profile Package stage Description

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

As shown above with respect to claim 1[C][b], the eSIM specifications further explain that this second portion contains the “Ki” key K and the “IMSI” subscriber identity.

Further, the above figure clearly indicates that the first portion of the Bound Profile Package (within the colored area using green hashes) is separate and distinct from the second portion of the Bound Profile Package (colored using red hashes).

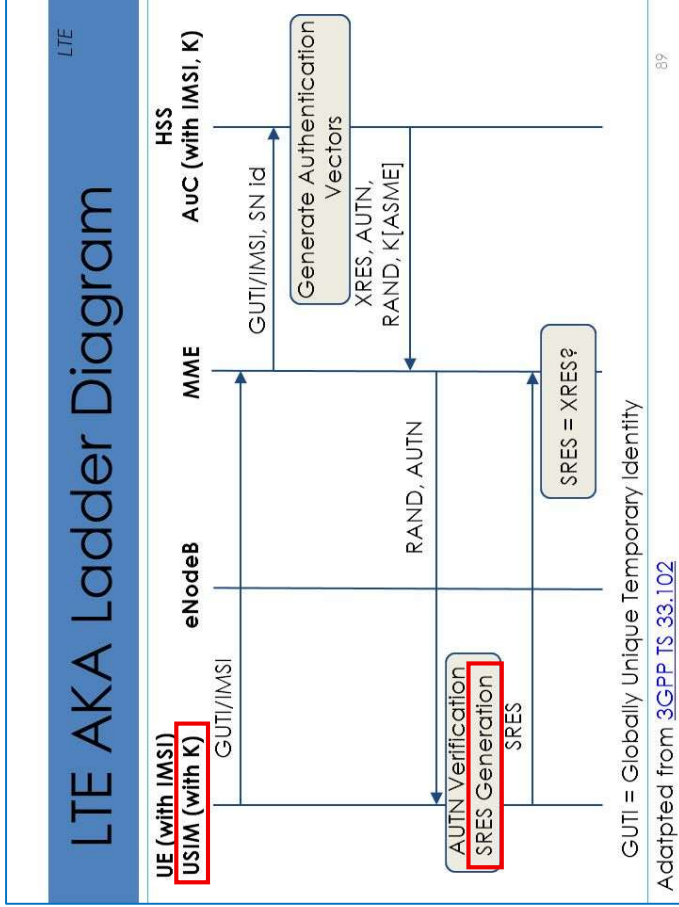
1[D][e] e. generate a response value for authentication of the mobile device with the wireless

The Accused Instrumentalities include an eUICC that is configured to generate a response value for authentication of the mobile device with the wireless network using the key K.

More specifically, the accused Samsung mobile devices have an eUICC that is configured to generate a response value (e.g., “SRES”) using the key K to authenticate the mobile device with the wireless network.

network using the key K.

The following figure shows that the “USIM (with [key] K)” performs “SRES Generation” for authenticating the UE mobile device with the network:



•

https://images.slideplayer.com/12/3359771/slides/slide_89.jpg

CLAIM 2

'893 PATENT V. SAMSUNG

2. The mobile device of claim 1, wherein the eUICC is further configured to receive a profile identity for the eUICC profile as a plaintext.

The Accused Instrumentalities are mobile devices with an eUICC that is further configured to receive a profile identity for the eUICC profile as a plaintext.

More specifically, the accused Samsung mobile devices have an eUICC that can receive an Integrated Circuit Card Identifier “ICCID” profile identity for the “Bound Profile Package” eUICC profile as plaintext or “clear data.”

The eSIM specifications explain that the ICCID is a unique number that identifies an eUICC profile:

- “

Term	Description
ICCID	Unique number to identify a Profile in an eUICC as defined by ITU-T E.118 [14].

”

SGP.21-v3.1 at §1.4 (Definition of Terms)

The eSIM specifications further explain that the ICCID is stored as metadata within the Bound Profile Package:

- “Profile Metadata Requirements

Req no.	Description
META1	All Profiles SHALL have associated Profile Metadata.
META2	Unless specified otherwise in the below requirements, the Profile Metadata SHALL be stored in the eUICC.
META3	The Profile Metadata SHALL be accessible irrespective of the state of the Profile.
META4	The Profile Metadata SHALL include a field for the Mobile Service Provider name. Note: EFSPN is already used in a different context outside of this specification and could be blank.

META5 The Profile Metadata SHALL include a field for the ICCID of the Profile.

SGP.21-v3.1 at §4.8 (Profile Metadata Requirements)

The eSIM specifications further explain that the stored metadata containing the ICCID is “clear data” or plaintext:

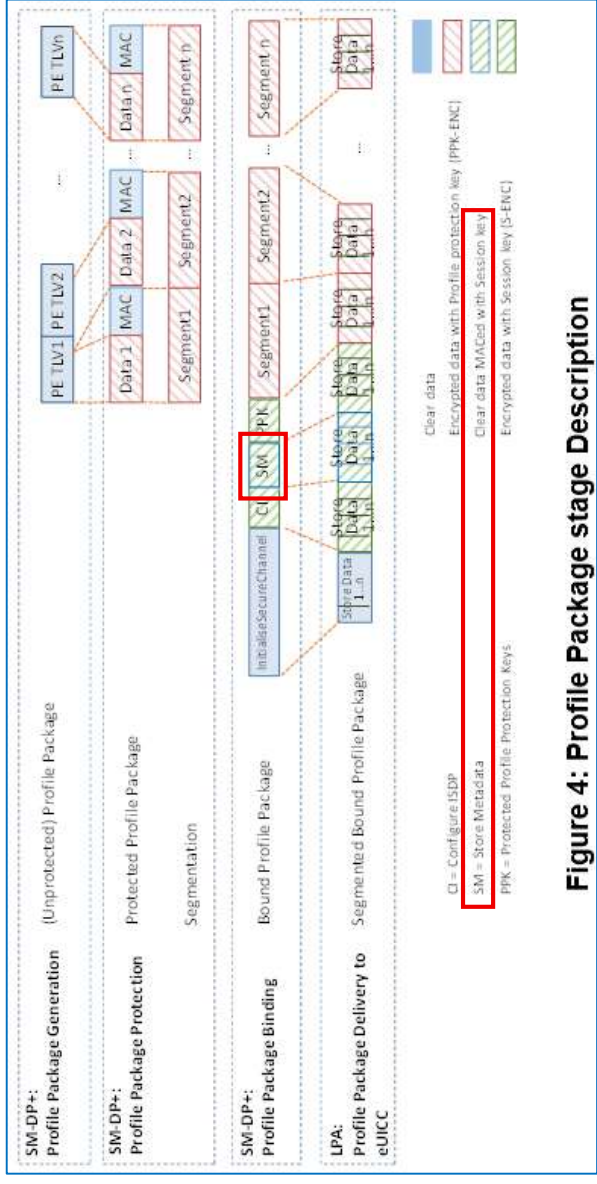


Figure 4: Profile Package stage Description

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

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

-

CLAIM 4

‘893 PATENT V. SAMSUNG

4. The mobile device of claim 1, wherein the random number generator is configured to generate the random number in response to input from at least one of a clock and a sensor.

The Accused Instrumentalities are mobile devices with a random number generator that is configured to generate the random number in response to input from at least one of a clock and a sensor.

More specifically, the accused Samsung mobile devices have a random number generator that can generate a random number in response to input from either a clock or a sensor.

The eSIM specifications require devices to include a random number generator:

- “2.6.8 Random Number Generation
To protect against attacks, a high quality random number generator is required. 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 detail a “True Random Number Generator” for a randomly generated secret, which is an example of a random number:

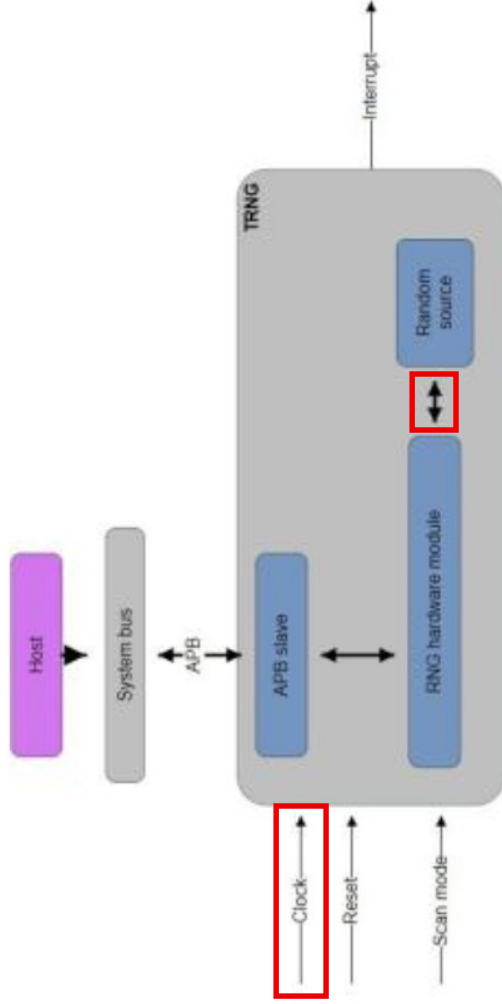
1.1 Definitions

Term	Description
Embedded UICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way
Randomly generated	<u>The secret shall be generated from a True Random Number Generator (TRNG) or from a Deterministic Random Bit Generator (DRBG), the seed of which is generated by a TRNG</u>
Properly derived	The secret shall be generated from a master key using a secure key derivation algorithm. Some secure key derivation algorithms are standardised, as the ones recommended by NIST in SP 800-108

• Official Document FS.27 - Security Guidelines for UICC Profiles, version 2.0

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." Also, in the above diagram, the TRNG generates the random number in response to input from a clock, where the input from the clock is shown. See also evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 5

‘893 PATENT V. SAMSUNG

5. The mobile device of claim 1, wherein the random number generator 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.

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 have a random number generator that can generate a random number from a seed value that includes data from a sensor and a clock.

The eSIM specifications require devices to include a random number generator:

- “2.6.8 Random Number Generation
To protect against attacks, **a high quality random number generator is required.** 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 use a “Deterministic Random Bit Generator” (DRBG) for a randomly generated secret, which is an example of a random number. The randomly generated secret (e.g. random number) is generated from a seed generated by a “True Random Number Generator” (TRNG) :

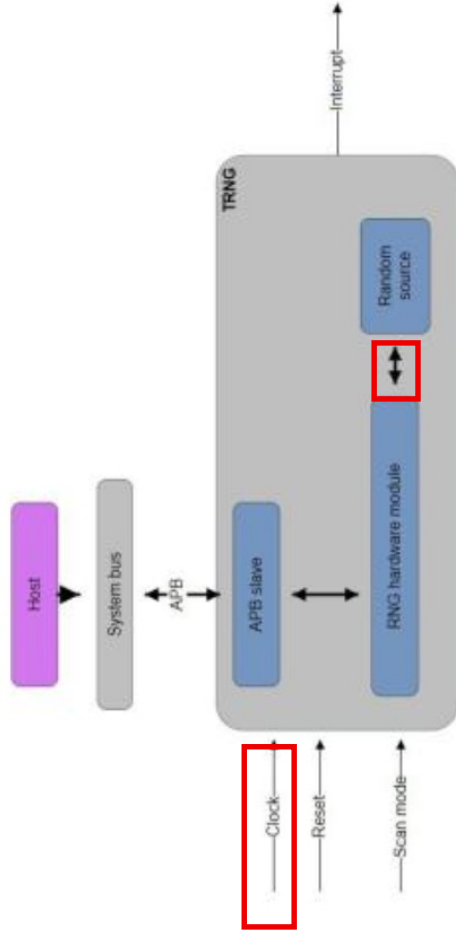
1.1 Definitions

Term	Description
Embedded UICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way
Randomly generated	The secret shall be generated from a True Random Number Generator (TRNG) or from a Deterministic Random Bit Generator (DRBG), the seed of which is generated by a TRNG
Properly derived	The secret shall be generated from a master key using a secure key derivation algorithm. Some secure key derivation algorithms are standardised, as the ones recommended by NIST in SP 800-108

Official Document FS.27 - Security Guidelines for UICC Profiles, version 2.0

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.” Also, in the above diagram, the TRNG generates the random number in response to input from a clock, where the input from the clock is shown. See also evidence and analysis from claim 1, which is incorporated fully herein by reference.

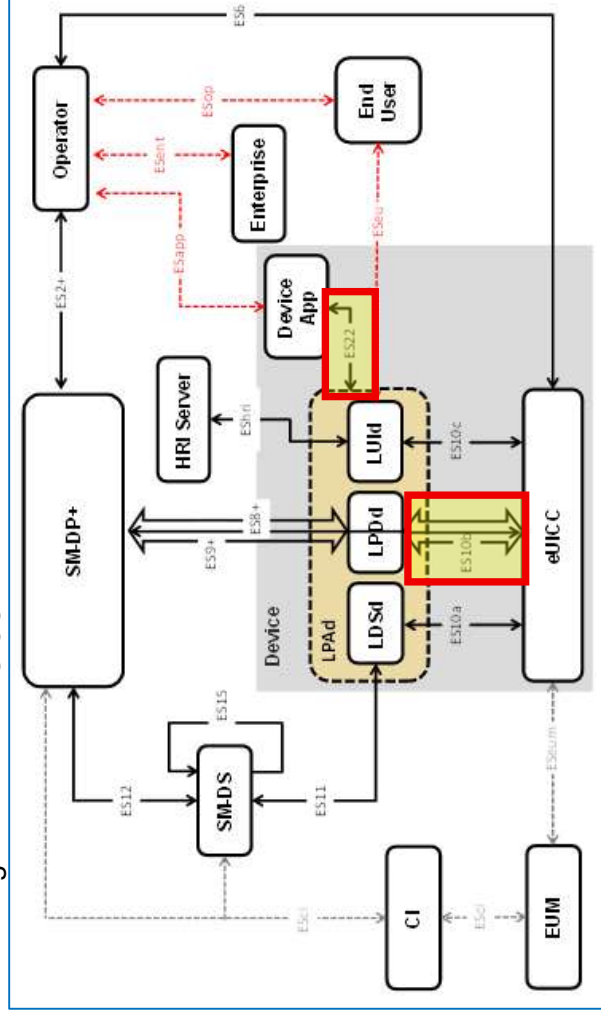
CLAIM 6

'893 PATENT V. SAMSUNG

6. The mobile device of claim 1, wherein the network application is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus.

The Accused Instrumentalities are mobile devices with a network application that is configured to communicate with i) the wireless network and ii) the eUICC in the mobile device using a system bus. More specifically, the accused Samsung mobile devices have a "LPAd" network application that can communicate with the both the wireless network and the eUICC in the mobile device using a system bus. The eSIM specifications require an operator (e.g. wireless network), a network application (e.g. LPAd), and an eUICC, as shown in the General Architecture Diagram:

- "2.1 General Architecture Diagram
This section further specifies the Roles and interfaces associated with the Remote SIM Provisioning and Management of the eUICC for consumer Devices.



SGP.22-v3.1 at §2.1 (General Architecture Diagram)

As shown in the above diagram, the LPAad network application communicates with the Operator wireless network via the interface labeled “ES22.” Similarly, the above diagram shows the LPAad network application communicates with the eUICC via the interface labeled “ES10.” The data for the interfaces labeled “ES22” and “ES10” is transferred over a system bus.

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

CLAIM 7

7. The mobile device of claim 1, wherein the eUICC comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory.

'893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices with an eUICC that comprises computer executable instructions for a processor in the mobile device, and wherein the computer executable instructions are stored within the memory.

More specifically, the accused Samsung mobile devices have an eUICC that includes computer executable instructions (labeled "OS") for a processor (labeled "IC") in the mobile device, and the computer executable instructions (labeled "OS") are stored within a memory (labeled "Memory mng"):

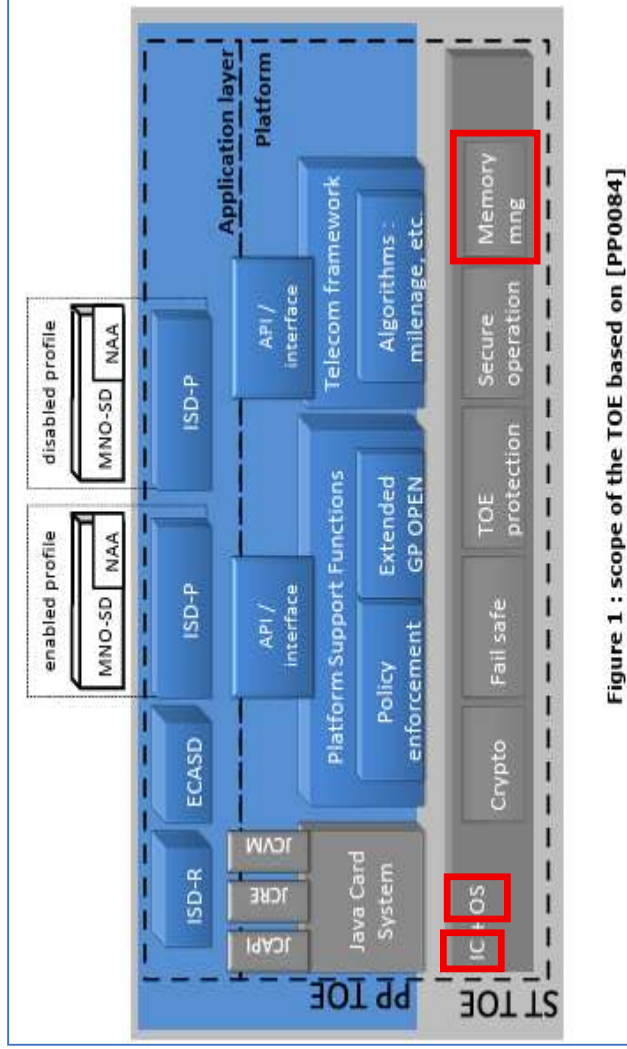


Figure 1 : scope of the TOE based on [PP0084]

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.

CLAIM 8

‘893 PATENT V. SAMSUNG

8. The mobile device of claim 1, wherein the eUICC comprises a package soldered onto a circuit board of the mobile device.

The Accused Instrumentalities are mobile devices with an eUICC that comprises a package soldered onto a circuit board of the mobile device.

More specifically, the accused Samsung mobile devices have an eUICC in the form of a package (e.g. integrated circuit) soldered onto a circuit board of the mobile device:

Step 10



- You've already seen the heavy hitters—here are some bonus chips:
 - Qualcomm SMR526 RF transceiver
 - Qualcomm QDM5872 front end module
 - Skyworks SKY77365-11 quad-band GSM/GPRS/EDGE power amplifier module
 - Qualcomm QET5100 envelope tracker module
 - NXP Semiconductor SN110U NFC controller w/ Secure Element and eSIM
 - NXP Semiconductor BCGU8103 GPS/GLONASS/Galileo/BeiDou low noise amplifier
 - NXP Semiconductor NCX2200 low voltage comparator

<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.

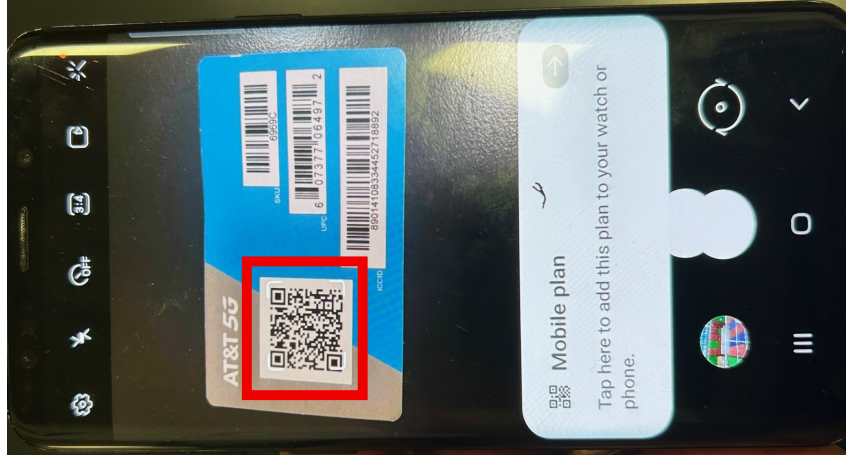
CLAIM 9

9. The mobile device of claim 1, further comprising a user interface configured to receive user identification information before the mobile device receives the symmetric key.

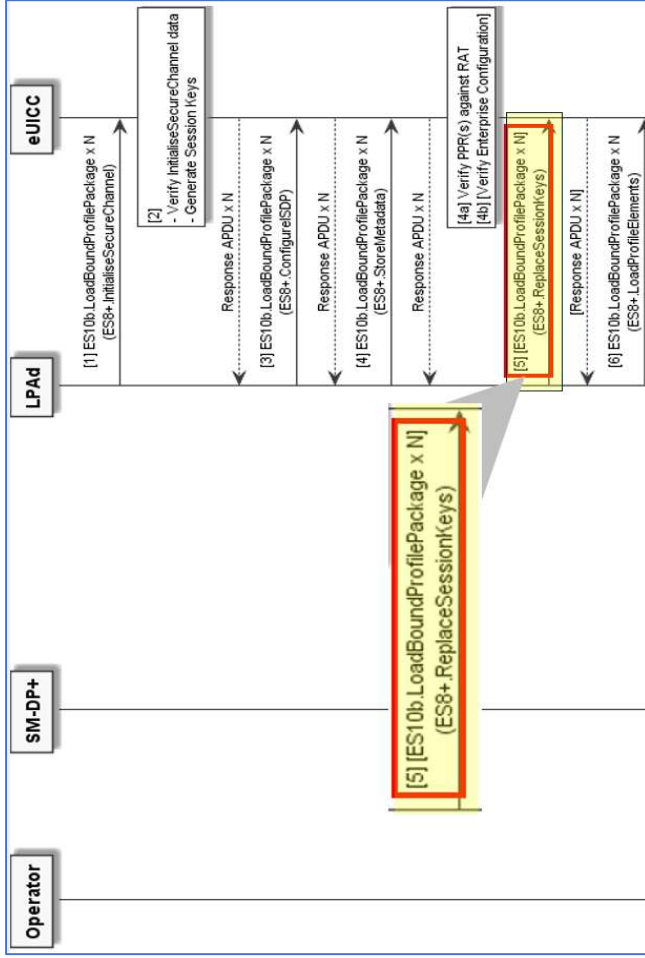
'893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices that comprise a user interface configured to receive user identification information before the mobile device receives the symmetric key.

More specifically, the accused Samsung mobile devices include a user interface that can receive user identification information (e.g. an "Activation Code"). For example, the image below shows the user interface when a Samsung mobile device receives a QR code containing the AT&T activation code:



The eSIM specifications show the activation code “user identification information” is received before the mobile device receives the PPK “symmetric key”:



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)

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

CLAIM 10

10. The mobile device of claim 1, wherein the first portion of the eUICC profile includes the network parameters, the network parameters comprising a list of numbers associated with a mobile network operator

‘893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices that can receive an eUICC profile that includes a first portion with network parameters comprising a list of numbers associated with a mobile network operator. More specifically, the accused Samsung mobile devices receive a Bound Profile Package “eUICC profile” that includes a “first portion” that is colored using green hashes (including at least “CI” or “Configure ISDP”):

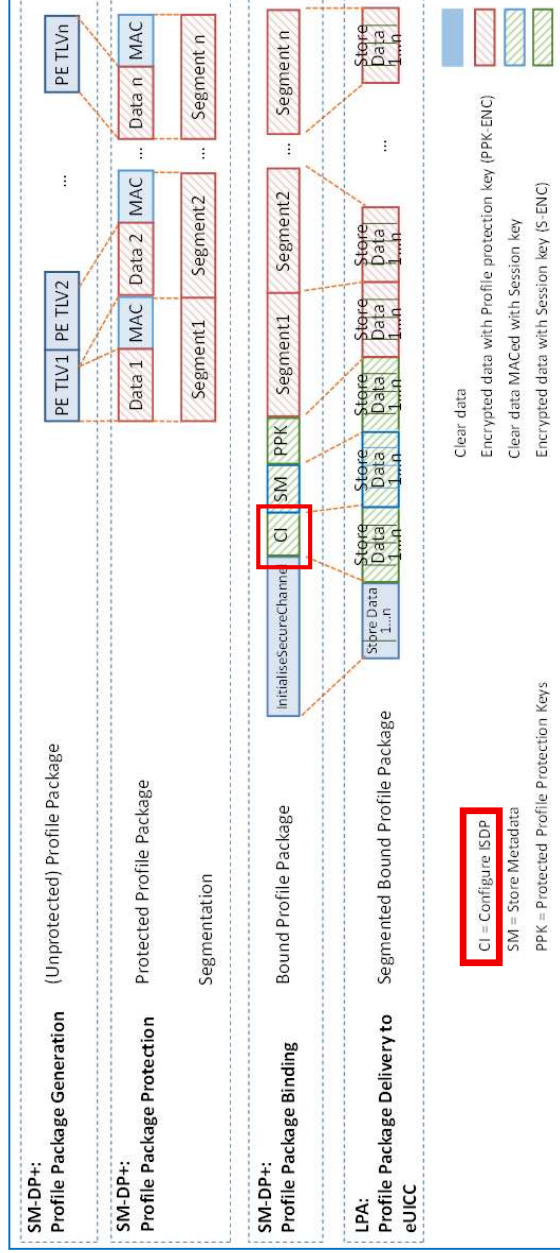


Figure 4: Profile Package stage Description

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

The eSIM specifications explain that the CI/Configure ISDP portion of the eUICC profile contains SM-DP+ proprietary data. On information and belief, the SM-DP+ proprietary data includes network parameters associated with a mobile network operator:

- “5.5.2 Function: ConfigureISDP Related Procedures: Profile Download and Installation

	<p>Function Provider Entity: ISD-R</p> <p>Description: This function is used by the SM-DP+ to provide data to the eUICC for configuring the ISD-P. <u>For this version of the specification, this data element only contains the optional SM-DP+ proprietary data.</u></p> <p>NOTE: Information like the amount of assigned memory MAY be added in future versions.”</p> <p>SGP.22-v3.1 at §5.5.2 (Function: Configure ISDP)</p> <p><i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.</p>
--	---

CLAIM 12

‘893 PATENT V. SAMSUNG

12. The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.

The Accused Instrumentalities are mobile devices with a radio that is further configured to receive, from the subscription manager, the eUICC profile using transport layer security.

More specifically, the accused Samsung mobile devices have radio that can receive, from a “SM-DP+” subscription manager, an eUICC profile “Bound Profile Package” using “TLS” transport layer security. The TLS connection is established during mutual authentication, and the TLS session continues through download of the “Bound Profile Package.”

The eSIM specifications show that the SM-XX subscription manager and the LPAd within the accused mobile device establish an HTTPS connection that uses TLS transport layer security:

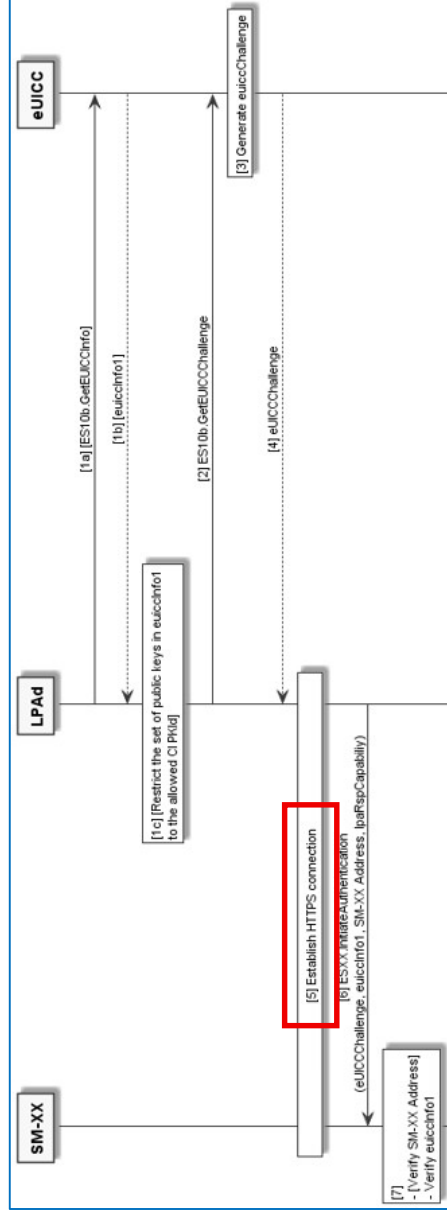


Figure 8A: Common Mutual Authentication Procedure

- “5. The LPAd establishes a new HTTPS connection with the SM-XX in server authentication mode. The **TLS session establishment** SHALL perform a new key exchange (it SHALL NOT reuse keys from a previous session). **During this step, the LPAd SHALL verify that CERT.XX.TLS is valid** as described in section 4.5.2.2. If CERT.XX.TLS is invalid and all retries have been exhausted, the LPAd SHALL stop the procedure. If there is a restriction of the

	<p>allowed eSIM RootCA public key(s), it SHALL NOT affect the establishment of the HTTPS connection.”</p> <p>SGP.22-v3.1 at §3.0.1 (Common Mutual Authentication Procedure)</p> <p><i>See also</i> evidence and analysis from claim 1, which is incorporated fully herein by reference.</p>
--	---

CLAIM 13

‘893 PATENT V. SAMSUNG

13. The mobile device of claim 1, wherein the subscriber identity comprises an International Mobile Subscriber Identity (IMSI).

The Accused Instrumentalities are mobile devices that can receive an eUICC profile that includes a subscriber identity comprising an International Mobile Subscriber Identity (IMSI).

More specifically, the accused Samsung mobile devices have a “Bound Profile Package” eUICC profile containing an “IMSI” subscriber identity.

The eSIM specifications provide example data within the Bound Profile Package specified by the GSMA that includes the “IMSI” subscriber identity:

A	B
1	Default Test SIM Profile
2	
3	
4	
110	IMSI
111	Keys
112	KeysPS
113	DCK
114	HPPLMN
115	CNL
116	ACMMAX
117	UST
118	ACM
119	FDN

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

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

CLAIM 14

14. The mobile device of claim 1, wherein the radio is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key.

‘893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices with a radio that is further configured to receive, from the subscription manager, a ciphertext for the symmetric key, wherein the mobile device is configured to decrypt the ciphertext using at least the eUICC private key.

More specifically, the accused Samsung mobile devices have a radio that can receive from the “SM-DP+” subscription manager, a ciphertext for the Profile Protection Key “PPK” symmetric key. Further, the accused Samsung mobile devices can decrypt that ciphertext using at least the “ofSK.EUICC.KA” eUICC private key.

The eSIM specifications explain that the Bound Profile Package contains a ciphertext Profile Protection Key “PPK” symmetric key (with green hashes for “Encrypted data with Session key (S-ENC),” as shown in the figure below:

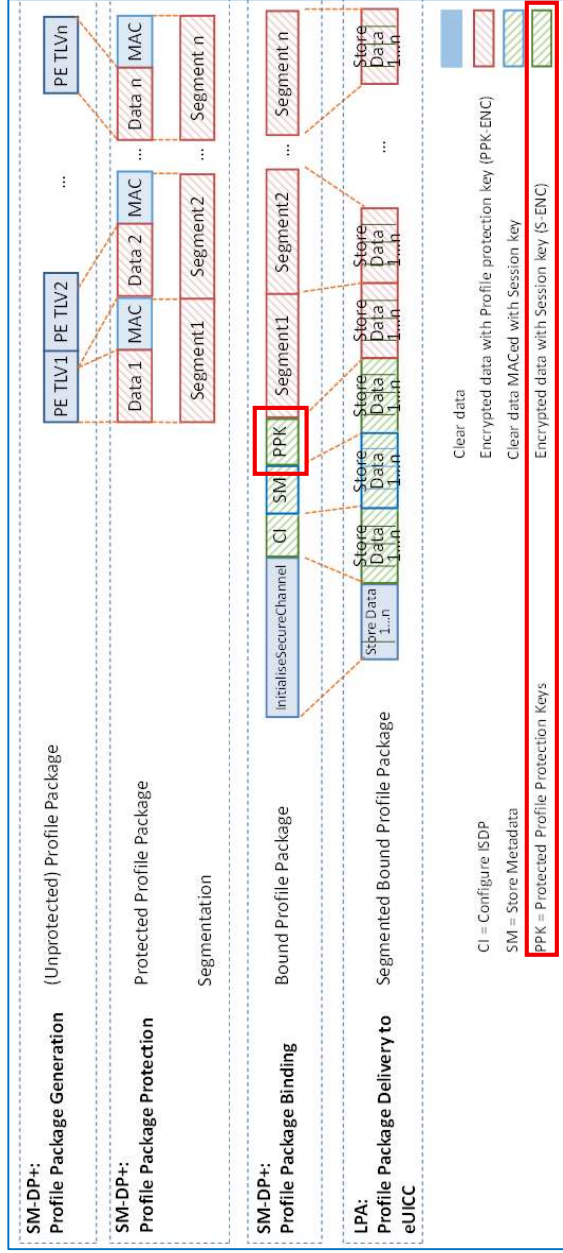


Figure 4: Profile Package stage Description

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

The accused Samsung mobile devices can decrypt the PPK with the “Session key (S-ENC).” The accused Samsung mobile devices derive the Session key (S-ENC) using at least the “otSK.EUICC.KA” eUICC private key.

More specifically, the accused Samsung mobile devices have an eUICC that is configured to derive the “Session key (S-ENC)” using an elliptic curve Diffie Hellman key exchange with at least the “otSK.EUICC.KA” eUICC private key.

The eSIM specifications explain that the eUICC uses a Diffie-Hellman Key Agreement, which is an elliptic curve key agreement algorithm, to create a shared secret value using the “otSK.EUICC.KA” eUICC private 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)

The eSIM specifications further explain that the shared secret value (discussed above) is used to derive the “Session key (S-ENC)”:

- “2.6.4.2 Key derivation
Session keys and an initial MAC chaining value are derived from the shared secret value as follows:
 - 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)

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

CLAIM 15

'893 PATENT V. SAMSUNG

15. The mobile device of claim 1, wherein the mobile device further comprises at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio.

The Accused Instrumentalities are mobile devices that further comprise at least one of a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a tracking device, and a circuit board with the radio.

More specifically, the accused Samsung mobile devices are smartphones, tablets, and laptops, as confirmed by these various Samsung and third-party 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>.

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

CLAIM 16

16. The mobile device of claim 1, wherein the second memory is the same memory as the first memory.

‘893 PATENT V. SAMSUNG

The Accused Instrumentalities are mobile devices with a second memory that is the same as the first memory.
 More specifically, the accused Samsung mobile devices have a single memory that stores an “EID” eUICC identity and is also connected to a processor configured to generate a random number.
 The eSIM specifications explain the “ECASD” stores the “EID” eUICC identity, as shown in 1[A] above, where the memory for the “ECASD” is an example of the first memory:

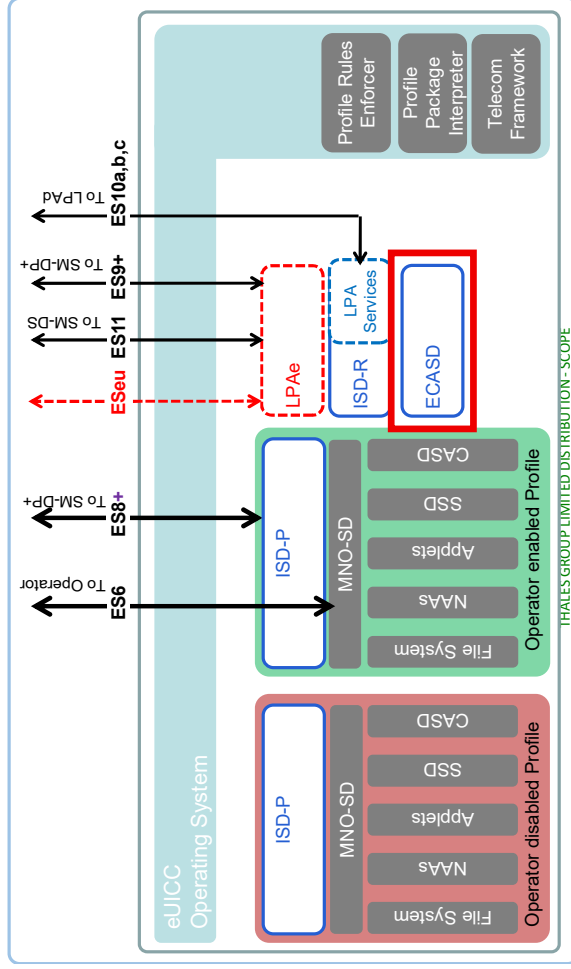


Figure 3: Schematic Representation of the eUICC”

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

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”), which is an example of the second memory:

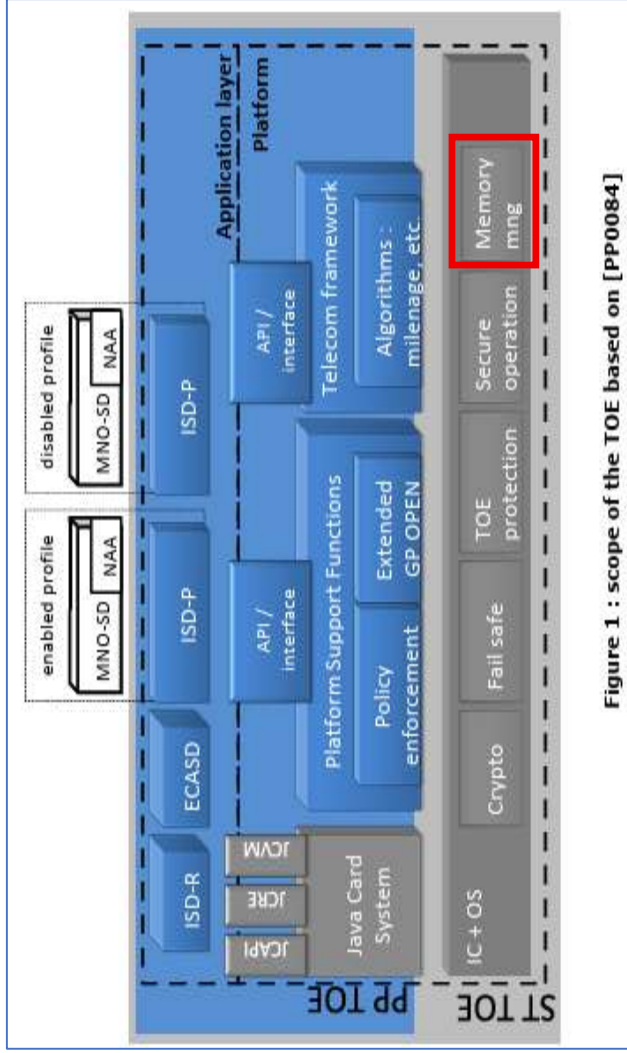


Figure 1 : scope of the TOE based on [PP0084]

SGP.05-v4.0 at §1.2.1 (TOE type)

On information and belief, the (i) first memory for the ECASD and (ii) the second memory (labeled “Memory mng”), are the same memory.

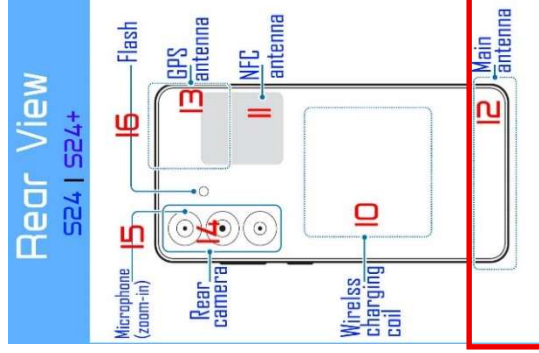
See also evidence and analysis from claim 1, which is incorporated fully herein by reference.

CLAIM 17

'893 PATENT V. SAMSUNG

17. The mobile device of claim 1, wherein the one or more receiving antennas are the one or more transmit antennas.

The Accused Instrumentalities are mobile devices with one or more receiving antennas and one or more transmit antennas, wherein the one or more receiving antennas are the one or more transmit antennas. More specifically, the accused Samsung mobile devices include dual-purpose antennas that can both transmit and receive data:



Rear view of Samsung Galaxy S24 and Galaxy S24+

12. Main antenna

The main antenna on the Galaxy S24 smartphone is located close to the bottom of the device. It serves as a critical component that facilitates wireless communication (e.g., 5G) between the phone and the nearest cellular tower. This ensures that the device can establish a reliable connection with the network and access essential features such as voice calls and mobile data services.

<https://gadgetguideonline.com/s24/layout-of-galaxy-s24-galaxy-s24-and-galaxy-s24-ultra/>

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