

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.;
SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

NETWORK-1 TECHNOLOGIES, INC.,
Patent Owner.

IPR2026-00119
Patent 11,916,893

**PATENT OWNER'S PRELIMINARY RESPONSE TO PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,916,893**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. Introduction1

II. Background2

 A. The ‘893 Patent [EX1001].....2

 B. The ‘893 Prosecution History [EX1004].....7

 C. Petitioner’s References9

 1. Park [EX1005].....10

 2. GlobalPlatform [EX1006]13

 3. AbiChar [EX1007]15

 4. X9.63-Overview [EX1008]17

 5. Nix175 [EX1016]18

 6. Petitioner’s Other References (Haggerty [EX1012], Pierce [EX1013],
 and Konstantinou [EX1014])19

III. Legal Standards20

IV. Level of Ordinary Skill in the Art.....21

V. Claim Construction21

VI. Argument.....22

 A. Grounds 1-2, 6: The Patent Office Allowed The Challenged Independent
 Claim After Considering All Of Petitioner’s References And Petitioner Has
 Not Showed How The Office Erred22

 B. Grounds 1-2: Petitioner’s Art Fails To Present A Reasonable Likelihood Of
 Prevailing Against Independent Claim 124

 1. Petitioner’s References Do Not Teach Or Suggest “Receiv[ing] ... A
 Symmetric Key” From The Subscription Manager And Deriving A
 Profile Key24

2. Petitioner’s References Do Not Teach Or Suggest “Decrypting ... The
Subscriber Identity”30

3. A POSITA Would Not Combine The Park And GlobalPlatform
References As The Petition Proposes.....32

C. Ground 6: The ‘893 Patent Is Entitled To Its Priority Date So Nix175 Is Not
Prior Art37

D. Grounds 3-5: Petitioner’s Art Fails To Present A Reasonable Likelihood of
Prevailing Against The Dependent Claims38

VII. Conclusion.....38

TABLE OF AUTHORITIES

Cases

Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH,
IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....24

Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.,
800 F.3d 1375 (Fed. Cir. 2015).20

Harmonic Inc. v. Avid Tech., Inc.,
815 F.3d 1356 (Fed. Cir. 2016)20

In re Magnum Oil Tools Int’l, Ltd.,
829 F.3d 1364 (Fed. Cir. 2016)20

In re NuVasive, Inc.,
842 F.3d 1376 (Fed. Cir. 2016)20

In re Warsaw Orthopedic, Inc.,
832 F.3d 1327 (Fed. Cir. 2016)21

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) (en banc)21

PUMA N. Am., Inc. v. NIKE, Inc.,
IPR2019-01042, Paper 10 (P.T.A.B. Oct. 31, 2019).....24

Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.,
IPR2025-00632, Paper 20 (P.T.A.B. Nov. 3, 2025).....21

Regulations

37 C.F.R. § 42.100(b)21

EXHIBIT LIST

Exhibit	Description
EX2001	Complaint for Patent Infringement, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667, Dkt. 1 (June 27, 2025)
EX2002	Docket Control Order, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667, Dkt. 26 (Oct. 10, 2025)
EX2003	U.S. Patent No. 11,606,204
EX2004	U.S. Patent No. 11,973,864
EX2005	U.S. Patent No. 12,166,869
EX2006	U.S. Patent No. 11,233,780
EX2007	U.S. Patent No. 12,207,094
EX2008	<i>Reserved</i>
EX2009	Google Patents Page for U.S. Patent No. 11,606,204, https://patents.google.com/patent/US11606204B2/en?q=11606204 (accessed Jan. 13, 2026)
EX2010	Google Patents Page for U.S. Patent No. 11,233,780, https://patents.google.com/patent/US11233780B2/en?q=11%2c233%2c780 (accessed Jan. 13, 2026)
EX2011	September 2, 2016 Rejection of Samsung Patent Application No. 14/803,946
EX2012	U.S. Patent Publication No. 2015/0163056
EX2013	U.S. Patent Publication No. 2015/0121066
EX2014	September 6, 2018 Notice of Allowance and Notice of References Cited for Samsung Patent Application No. 15/350,963
EX2015	U.S. Patent Publication No. 2015/0143125
EX2016	Defendants' Patent Local Rule 3-3 Disclosure of Invalidity Contentions, <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667 (December 9, 2025)
EX2017	U.S. Patent No. 8,761,390
EX2018	Declaration of Eric J. Enger in Support of Patent Owner's Discretionary Denial Brief
EX2019	Declaration of John Nix in Support of Patent Owner's Discretionary Denial Brief
EX2020	Email chain dated September 27, 2016, produced with Bates Nos. NWO SAM 00013288–90
EX2021	Email chain dated December 21, 2016, produced with Bates No.

Exhibit	Description
	NWO SAM 00013295
EX2022	“Patent Portfolio for ‘Embedded SIMs’ and the ‘Internet of Things,’” produced with Bates Nos. NWO SAM 00013436–37
EX2023	Email chain dated January 3, 2017, produced with Bates Nos. NWO SAM 00013296–97
EX2024	U.S. Patent Application No. 14/099,329
EX2025	U.S. Patent Publication No. 2014/0237101
EX2026	<i>Reserved</i>
EX2027	3GPP TS 33.102 “3G security; security architecture,” v10.0.0 (May 2011)
EX2028	3GPP TS 33.401 “Security architecture,” v10.0.0 (March 2011)
EX2029	Declaration of Dr. Karthikeyan Sundaresan In Support of Patent Owner’s Preliminary Responses
EX2030	<i>Reserved</i>

I. Introduction

Patent Owner Network-1 Technologies, Inc. (“Network-1” or “PO”) respectfully requests that the USPTO deny Samsung Electronics Co., Ltd.’s and Samsung Electronics America, Inc.’s (collectively, “Samsung” or “Petitioner”) Petition to institute *inter partes* review of U.S. Patent No. 11,916,893 (“the ‘893 Patent”). For several reasons, Samsung has not shown a reasonable likelihood of prevailing on any of its six grounds that challenge ‘893 claims 1-17.

First, with respect to grounds 1-2 and 6, the Patent Examiner already considered each of Samsung’s five references and concluded that none of them taught or suggested independent claim 1, either alone or in combination. Further, the primary reference relied on during prosecution has the same inventor and a similar disclosure to Samsung’s primary reference in this IPR. The Petition never acknowledges these facts and certainly never explains how the Examiner erred in allowing the ‘893 Patent.

Second, as to grounds 1-2, Samsung’s references fail to teach or suggest several limitations of independent claim 1, including two limitations that the Examiner previously found were undisclosed during prosecution after considering the same art: (1) “receive, from the subscription manager ... a symmetric key”; and (2) “decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising ... the subscriber identity.”

Third, for ground 6, Samsung wrongly alleges the ‘893 Patent is not entitled to its priority date in order to argue that the claims are invalidated by the inventor’s own disclosure from a parent patent. But all of the applications in the priority chain provide written description for each claim limitation. So the inventor’s own patent is not prior art.

Finally, grounds 3-5 only pertain to dependent claims. Because Samsung failed to show that any independent claim was invalid in grounds 1-2 and 6, its challenges to the dependent claims necessarily fail as well.

II. Background

A. The ‘893 Patent [EX1001]

The ‘893 Patent relates to provisioning and authenticating mobile devices that have an embedded subscriber identity module (“eSIM”).¹

Before the ‘893 Patent, mobile devices used a traditional SIM card, *i.e.*, a plastic-encased chip that was physically inserted into the mobile device and could be removed and replaced. EX1001 at 2:38-44. These traditional SIM cards were pre-loaded with various subscriber information for provisioning and authenticating the mobile device, including a set of parameters identifying the mobile device,

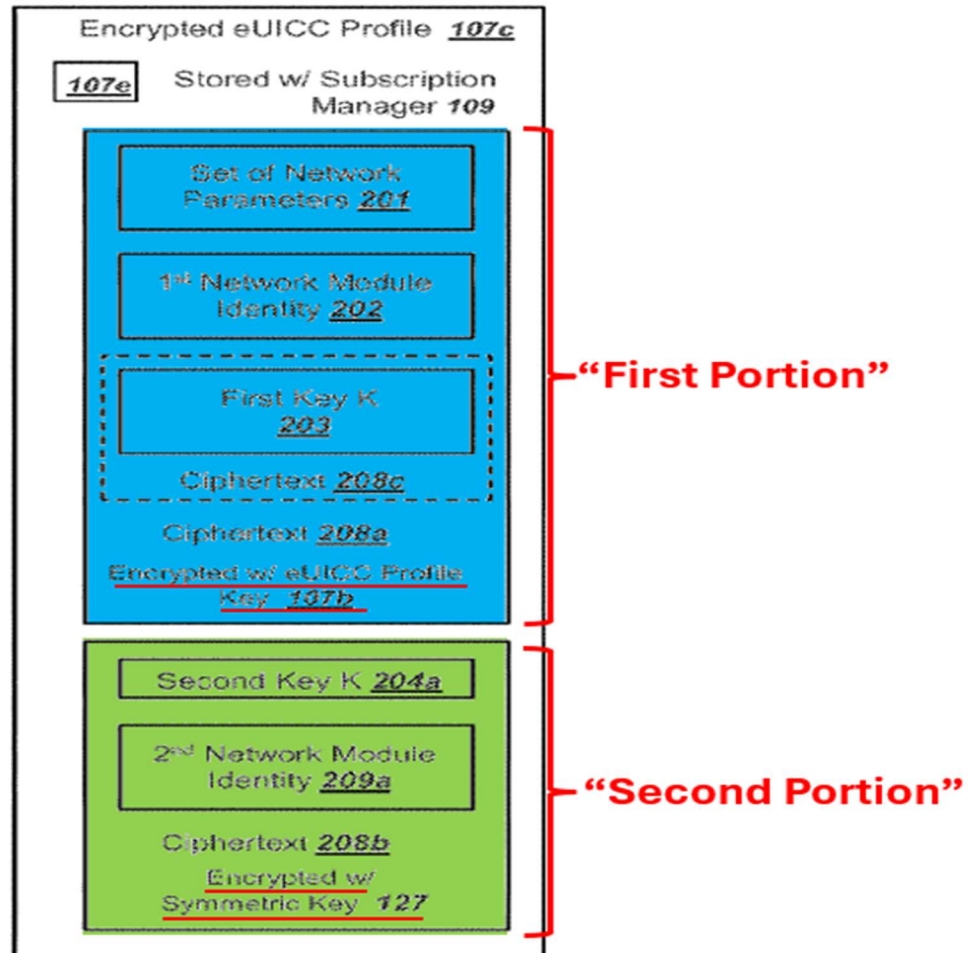
¹ An eSIM may also be referred to as an embedded universal integrated circuit card (“eUICC”). EX1001 at 19:31-33.

information about the network to which the mobile device should connect, and a pre-shared secret key K. *Id.* at 2:45-55. But due to their physical nature, traditional SIM cards had many disadvantages that made them (1) unsuitable for devices in remote locations, (2) less convenient, (3) more costly, and (4) less secure. *Id.* at 2:64-3:15; EX2029 at ¶22.

Because of the drawbacks with physical SIM cards, the industry began to consider replacing them with eSIMs. EX1001 at 3:16-20. With eSIMs, the authentication hardware is permanently embedded within the mobile device and cannot be removed. However, eSIMs are not typically pre-loaded with the subscriber information for provisioning and authenticating the mobile device; rather, that profile information for the subscriber must be electronically transferred to the eSIM. *See id.* at 3:34-4:41. The ‘893 Patent provides a framework for securing that profile information—especially in the context of a distributed network controlled by multiple different parties. *See id.* at 4:45-8:44; EX2029 at ¶23.

The annotated excerpt from Figure 2a (below) illustrates the contents of the exemplary profile information—or encrypted eUICC Profile 107c—that is secured in the eSIM per the ‘893 Patent. The encrypted eUICC profile includes two distinct portions: (1) a first portion (blue); and a second portion (green). EX1001 at 30:35-40. Importantly, as indicated below by the red underlining, the first portion is encrypted with an eUICC profile key 107b, while the second portion is encrypted

with a different symmetric key 127. *Id.* at 11:52-56, 32:46-49. Thus, the first and second portions of the eUICC profile are encrypted differently, to provide enhanced security. EX2029 at ¶24.



To decrypt the first portion, the eSIM derives the eUICC profile key 107b (using, *e.g.*, an Elliptic Curve Diffie-Hellman key exchange with a subscription manager), and then uses that eUICC profile key 107(b) with a deciphering algorithm on the first portion. EX1001 at 38:23-29, 34:42-57. To decrypt the second portion, the eSIM receives a separate symmetric key 127 and then uses it with a deciphering

algorithm on the second portion to identify the network module identity 209a and the key K 204a. *Id.* at 36:56-58, 14-17. At that point, the mobile device is provisioned and can successfully authenticate itself with the network. *Id.* at 36:58-60. This ‘893 approach—which uses two different keys, obtained in two different ways, to decrypt two different portions of the profile—increases security for both the user of the mobile device and the network operator. *Id.* at 35:35-38; EX2029 at ¶25.

Independent claim 1 of the ‘893 Patent typifies the approach discussed above. It recites a “mobile device” comprising an “eUICC” or eSIM. EX1001 at 80:22, 80:37. The eUICC is configured to receive an “eUICC profile” comprising a distinct “first portion” and a distinct “second portion.” *Id.* at 80:42, 80:46, 80:48-49. To decrypt the first portion, the eUICC “derive[s] a profile key using an elliptic curve Diffie Hellman (ECDH) key exchange” and then uses it to decipher the first portion. *Id.* at 80:39-43. To decrypt the second portion, the eUICC “receive[s] the symmetric key” and then uses it to decipher the “key K and the subscriber identity” within that second portion. *Id.* at 80:44-48. Finally, the eUICC “generate[s] a response value for authentication of the mobile device with the wireless network using the key K.” *Id.* at 80:50-52; EX2029 at ¶26.

Here is independent claim 1, highlighted to show (1) the first portion of the profile is decrypted using the derived profile key (blue) and (2) the second portion of the profile is decrypted using the received symmetric key (green):

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

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

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;

a radio including one or more transmit antennas and one or more receiving antennas configured to:

- a. transmit, to a subscription manager, the eUICC identity and the eUICC public key; and
- 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**; and

an eUICC associated with the eUICC identity and configured to:

- 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;
- b. **decrypt a first portion of the eUICC profile using the profile key**;
- c. receive the symmetric key from a network application operating in the mobile device;
- d. **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; and

- e. generate a response value for authentication of the mobile device
with the wireless network using the key K.

EX1001 at 80:22-52 (emphasis and highlighting added).

B. The ‘893 Prosecution History [EX1004]

The application that resulted in the ‘893 Patent was filed on December 10, 2021; however, that application claimed priority to a string of other related continuation applications dating back to December 6, 2013. EX1004 at 361-515. The ‘893 application had fifteen initial claims. *Id.* at 487-489; EX2029 at ¶30.

On January 20, 2022, shortly after filing the ‘893 application, the Applicant disclosed a number of references to the Examiner, including *all five of the references used by the Petitioner to challenge patentability of ‘893 independent claim 1.* EX1004 at 214-351. More specifically, at the very onset of prosecution of this patent, the Applicant disclosed each of Park (*id.* at 341), GlobalPlatform (*id.* at 339), AbiChar (*id.* at 340), X9.63-Overview (*id.* at 350), and Nix175 (*id.* at 275). The Examiner thus considered each of those five references. *Id.* at 169 (Park), *id.* at 167 (GlobalPlatform), *id.* at 168 (AbiChar), *id.* at 178 (X9.63-Overview), and *id.* at 148 (Nix175); EX2029 at ¶31.

On March 27, 2023, the Examiner rejected independent claim 1 under 35 U.S.C. §112, but did issue any §§102(a)-(b) rejections for novelty or obviousness in light of the considered prior art. EX1004 at 117-123; EX2029 at ¶32.

On September 19, 2023, the Applicant and the Examiner had an interview, during which they agreed on minor claim amendments (*e.g.*, explicitly adding a processor, memory, and transceiver) to overcome the §112 rejection. EX1004 at 113-116. A few days later, on September 27, 2023, the Applicant amended independent claim 1 as agreed during the interview. *Id.* at 95. The Applicant also added new dependent claims 16-17. *Id.* at 98; EX2029 at ¶33.

Based on these amendments, the Examiner allowed all the pending claims on October 18, 2023. EX1004 at 75-79. He stated that the ‘893 claims were allowable “since the prior arts taken individually or in combination fails to particularly disclose” all the claim limitations. *Id.* at 76; EX2029 at ¶34.

In the reasons for allowance, the Examiner specifically noted differences between the allowed claims and one prior art reference, U.S. Printed Patent Application No. 2014/0237101 to Park, which he referred to as a “Primary Reference.” *Id.* at 77. Remarkably, the inventor of that “Primary Reference” patent application is the same person that authored the primary reference used in Samsung’s petition—Jaemin Park. *Compare* EX2025 at 1 *with* EX1005 at 1. But that is not where the similarities end; both Park references have similar disclosures. The Park patent application teaches “securely provisioning various profiles” for an eUICC (EX2025 at [0085]), while the Park paper teaches a “secure profile provisioning architecture for eUICCs” (EX1005 at 1). And the Examiner explicitly recognized

that teaching from the Park patent application, noting it “discloses a method for managing a profile in an embedded UICC.” EX1004 at 77; EX2029 at ¶35.

Importantly, the Examiner explained in the reasons for allowance that the Park patent application did not disclose multiple limitations from ‘893 claim 1, including: (1) “receiv[ing], from the subscription manager, ... a symmetric key”; and (2) “decrypt[ing] ... using the symmetric key ... the subscriber identity.” EX1004 at 77; EX2029 at ¶36. As explained below, the Petition’s references similarly fail to teach or suggest those same two claim limitations. *See infra* at §VI(B).

C. Petitioner’s References

The Petition asserts six grounds of invalidity based on combinations of seven references:

Ground	Claims	Statute	References
1	1, 3, 6-11, 13-17	§103	Park + GlobalPlatform + AbiChar
2	1, 3, 6-11, 13-17	§103	Park + GlobalPlatform + X9.63-Overview
3	2, 12	§103	Park + GlobalPlatform + AbiChar + Haggerty <u>OR</u> Park + GlobalPlatform + X9.63-Overview + Haggerty
4	4-5	§103	Park + GlobalPlatform + AbiChar + Pierce <u>OR</u> Park + GlobalPlatform + X9.63-Overview + Pierce
5	10-11	§103	Park + GlobalPlatform + AbiChar +

			Konstantinou <u>OR</u> Park + GlobalPlatform + X9.63-Overview + Konstantinou
6	1-17	§103	Nix175 + Park + GlobalPlatform

Pet., 3. None of those references, either alone or in combination, teach or suggest all the elements of challenged ‘893 independent claim 1.² EX2029 at ¶57.

1. Park [EX1005]

Park, EX1005, is a paper titled “Secure Profile Provisioning Architecture for Embedded UICC” authored in 2013 by Jaemin Park *et al.* EX1005 at 1. Park addresses the security challenges of remotely provisioning profiles onto eUICCs. *Id.* According to Park, because no single mobile network operator (“MNO”) controlled an eUICC, a new component called the Subscription Manager (“SM”) was

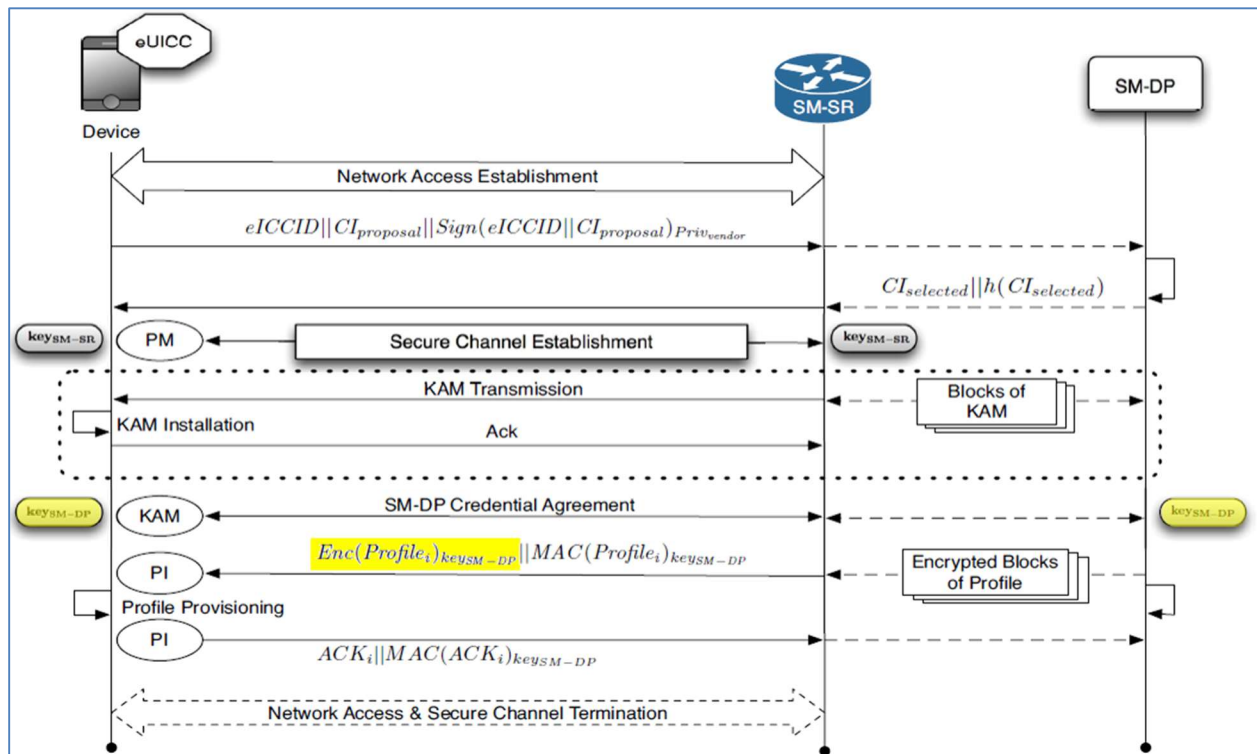
² For the purposes of this preliminary response, Network-1 has only addressed independent claim 1. As shown herein, Samsung failed to demonstrate a reasonable likelihood of success of proving that independent claim 1 is unpatentable. Consequently, Samsung also necessarily failed to show unpatentability of dependent claims 2-17. If the Petition is nonetheless instituted, Network-1 reserves the right to further address the deficiencies in Samsung’s theories, including deficiencies regarding the dependent claims.

introduced, divided into two entities: (1) a data preparation entity (“SM-DP”) that generates profiles; and (2) a secure routing entity (“SM-SR”) that transports profiles to the eUICC. *Id.* However, since profiles often contain sensitive information, this new ecosystem raised security concerns. *Id.*; EX2029 at ¶60.

To combat those security concerns, Park proposes a Secure Profile Provisioning Architecture (“SPA”) that has two phases. EX1005 at 3. In the first pre-provisioning phase, the eUICC vendor installs SM-SR credentials into the eUICC and registers the eUICC’s capability information (*e.g.*, supported cryptographic algorithms, key agreement protocols) with a certification center. *Id.* In the second secure profile provisioning phase, the eUICC connects to SM-SR and sends its ID and capability information signed by the eUICC vendor’s key. *Id.* at 4. The SM-DP verifies this signature using the eUICC vendor’s certificate obtained from the eUICC Certification Center. *Id.* The SM-DP then selects appropriate cryptographic protocols based on the eUICC’s reported capabilities and communicates the selected parameters back to the eUICC. *Id.* A new internal eUICC module called the Key Agreement Module (“KAM”) dynamically performs a key agreement with SM-DP to generate fresh SM-DP credentials on demand. *Id.* SM-DP then encrypts the entire profile using those credentials and transmits them through SM-SR’s secure channel to the eUICC. *Id.* Finally, the eUICC’s profile installer decrypts, verifies, and installs the profile, and then sends acknowledgments back to the SM-DP. *Id.*; EX2029 at

¶61.

Figure 4 illustrates Park’s profile provisioning procedure, discussed above. Notably, as illustrated by the yellow highlighting, Park teaches for both the mobile device and the SM-DP to separately derive the profile key, key_{SM-DP} , and then use it to encrypt/decrypt the entirety of the profile, $Enc(Profile_i)key_{SM-DP}$:



EX1005 at 4-5 (highlighting added); EX2029 at ¶62.

Notably, Park is silent about key aspects of ‘893 claim 1, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) using an elliptic curve Diffie Hellman key exchange to derive a profile key; and (3) decrypting the subscriber identity from within the second portion using the received symmetric key. EX2029 at ¶63.

2. GlobalPlatform [EX1006]

GlobalPlatform, EX1006, is a document titled “Card Specification, version 2.2.1” issued by the GlobalPlatform standards organization and dated January 2011. EX1006 at 1.³ GlobalPlatform defines a standardized architecture for smart card security, including secure channel protocols designed to protect communications between a card and an off-card entity. *Id.* at 39-40, 48, 132. One of those secure channel protocols is called “SCP10.” *See id.* at 254; EX2029 at ¶64.

For confidentiality, GlobalPlatform mostly relies on use of a secure channel encryption key (“C-ENC”) to encrypt message data transmitted to and from the card. EX1006 at 278-279. In addition, SCP10 also imposes an additional level of protection for particularly sensitive data (*i.e.*, keys) transmitted to the card; the sensitive key data is first encrypted with a symmetric Data Encryption Key (“DEK”) and then the entire message—including the already-encrypted sensitive key data—is further encrypted using the C-ENC key. *See id.* at 284. Thus, SCP10 utilizes two-levels of nested encryption for particularly sensitive key data included within the message data. EX2029 at ¶65.

³ Citations in EX1006 are to the bates numbering (bottom right) and not to the internal page numbering (top right) as in the Petition.

GlobalPlatform’s SCP10 teaches two alternative and mutually-exclusive methods by which the card can obtain these keys: (1) the key agreement method; and (2) the key transport method. EX1006 at 255. With (1) the key agreement method, the card and the off-card entity initially exchange secret values and then subsequently use those secrets to compute and *derive* the keys. *Id.* With (2) the key transport method, the card *receives* the keys from the off-card entity and does not have to compute them. *Id.* To select which of the two methods will be used for the session, GlobalPlatform teaches to set the first bit, b1, of the card recognition data to “1” if the key agreement method will be used and “0” if the key transport method will be used. *Id.* at 255, 300-302. Thus, it is impossible within a given session for a card to both derive one key (e.g., C-ENC) and receive another key (e.g., DEK). Table F-1 and its corresponding text confirm as much:

Key transport and key agreement relate to the process of establishing session keys for the Secure Channel Session.

- With **key agreement** the Security Domain and the Off-Card Entity exchange secret values when the Secure Channel is being initiated, and session keys are then **derived** from those secrets using an algorithm known to both the Off-Card Entity and the Security Domain;
- With **key transport** the Security Domain **receives** session keys to be used for the Secure Channel Session from the Off-Card Entity during Secure Channel initiation.

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

Id. at 255 (highlighting added); EX2029 at ¶66.

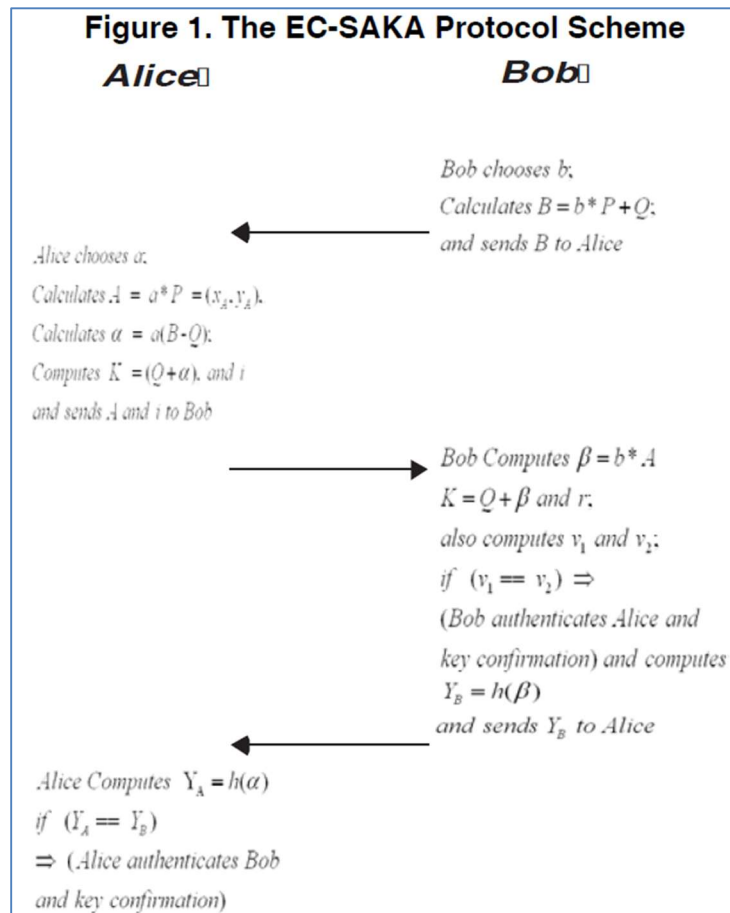
GlobalPlatform fails to teach key parts of '893 claim 1, including: (1) both deriving a profile key *and* receiving a symmetric key at the mobile device/eUICC; (2) decrypting a subscriber identity using the symmetric key; and (3) using an elliptic curve Diffie Hellman key exchange to derive a profile key with a subscription manager. EX2029 at ¶67.

3. AbiChar [EX1007]

AbiChar, EX1007, is a paper titled “A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications” authored in 2007 by Pierre Abi-Char *et al.* EX1007 at 1. To provide secure communication for mobile devices, AbiChar presents “a fast and secure authenticated key agreement protocol based on elliptic curve cryptography” called “EC-SAKA.” *Id.* EC-SAKA is a three-pass authenticated key establishment protocol designed for low-power mobile wireless devices. *Id.*; EX2029 at ¶68.

Figure 1 (below) illustrates the EC-SAKA protocol scheme. As can be seen, the EC-SAKA protocol consists of three message flows between a client (Alice) and a server (Bob). EX1007 at 3. In the setup phase, Alice selects an elliptic curve $E(\mathbb{Z}_p)$, chooses a random base point P of prime order n , and derives a public parameter $Q = h(pw) * P$ from her password pw , then transfers the parameters (E, Q, P, n) to Bob securely. *Id.* In the first flow, Bob chooses a random challenge b and sends $B = b * P + Q$ to Alice. *Id.* In the second flow, Alice chooses a random challenge a , computes

$A = a * P$, derives a shared value $\alpha = a(B - Q)$, computes the shared key $K = Q + \alpha$, and generates an ElGamal signature (A, i) which she sends to Bob. *Id.* And in the third flow, Bob verifies Alice's signature and computes $\beta = b * A$, deriving the same shared key $K = Q + \beta$. *Id.* Upon verification, both parties derive the final session key $K_s = h(ID(Alice) || ID(Bob) || K)$. *Id.* at 3-4; EX2029 at ¶69.



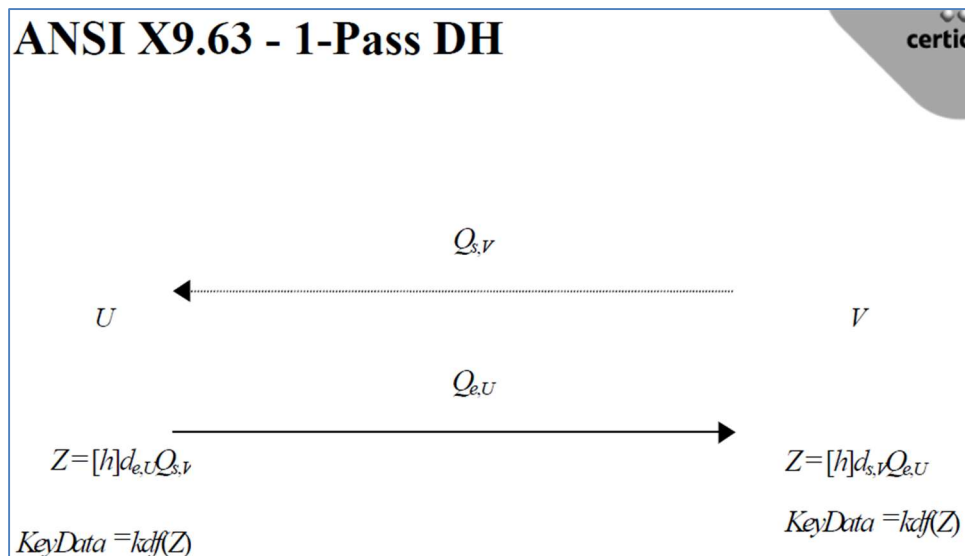
AbiChar fails to teach many key components of '893 claim 1, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) receiving the symmetric key at the mobile

device/eUICC; and (3) decrypting a subscriber identity using the symmetric key.
EX2029 at ¶69.

4. X9.63-Overview [EX1008]

X9.63-Overview, EX1008, is a presentation titled “ANSI X9.63 Overview: Key Agreement and Key Transport Using Elliptic Curve Cryptography” authored in 2007 by Simon Blake-Wilson. EX1008 at 1. It provides a summary of the ANSI X9.63 standard then being developed by the ANSI X9F1 committee. *Id.* at 3. It “specifies key agreement and key transport schemes using elliptic curve cryptography.” *Id.*; EX2029 at ¶70.

One of those schemes is the one-pass Diffie-Hellman scheme, which AbiChar refers to as “1-Pass DH”:



EX1008 at 12. In the one-pass Diffie Hellman scheme, an entity randomly generates an ephemeral private key, computes a corresponding public key, and transmits that

public key to a remote party so that both sides can derive a shared symmetric key. *Id.* at 7, 12. More specifically, one entity (U) generates a fresh ephemeral key pair by randomly selecting an ephemeral private key ($d_{e,U}$) and computing a corresponding ephemeral public key ($Q_{e,U}$). *Id.* at 7, 12. Entity U sends its ephemeral public key to the other party (V), and both entities compute a shared secret (Z) using their respective private keys and the public key received from the other party. *Id.* at 12. That shared secret is then passed through the key derivation function (kdf) to produce shared keying material ($KeyData$). *Id.*; EX2029 at ¶71.

X9.63-Overview fails to teach many key components of ‘893 claim 1, including: (1) a profile with two distinct portions, each of which is decrypted using a different key obtained in a different way; (2) receiving the symmetric key at the mobile device/eUICC; and (3) decrypting a subscriber identity using the symmetric key. EX2029 at ¶72.

5. Nix175 [EX1016]

Nix175, EX1016, is a U.S. Patent titled “Embedded Universal Integrated Circuit Card Supporting Two-Factor Authentication” filed on December 6, 2013 by John Nix. EX1016 at 1. The ‘893 Patent is a continuation of Nix175; both share the same specification and the ‘893 Patent claims priority to Nix175. *Compare* EX1001 *with* EX1016. Nix175 is not prior art to the ‘893 Patent, as explained below.

Samsung concedes Nix175 is only prior art to the ‘893 Patent if it is not entitled to its priority claim. Pet. at 19. According to Samsung, the ‘893 Patent is not entitled to claim priority to Nix175 because the ‘893 Patent claims “receiv[ing] from the subscription manager, ... a symmetric key,” which Nix175 allegedly does not support. *Id.* at 9-10. However, Nix175 explicitly discloses receiving the symmetric key 127 from mobile network operator 104. EX1016 at 57:56-61, Fig 3 at step 309. And Nix175 also teaches that the “mobile network operator 104 could operate the eUICC subscription manager 109.” *Id.* at 11:1-3; *see also id.* at 36:33-34 (“the MNO 104 could also function as a eUICC subscription manager 109”). Thus, because Nix175 teaches the mobile network operator and the subscription manager can be the same, Nix175 also discloses receiving a symmetric key from a subscription manager—thereby providing written description support for the ‘893 claims. So the ‘893 Patent is entitled to its priority date, and Nix175 is not prior art. EX2029 at ¶¶73-75.

6. Petitioner’s Other References (Haggerty [EX1012], Pierce [EX1013], and Konstantinou [EX1014])

The Petition relies on three other references—Haggerty (EX1012), Pierce (EX1013), and Konstantinou (EX1014)—just to invalidate certain dependent claims. Pet. at 61-68. But as explained above, Network-1 only addresses independent claim 1 in this Preliminary Response. So Network-1 reserves the right to explain those three references at another time.

III. Legal Standards

An IPR should not be instituted unless Petitioner has shown a likelihood of success on the invalidity grounds presented in the petition. *See In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016) (“[T]he Board must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.”).

“In an IPR, the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (petitions must identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”); 35 U.S.C. § 312(a)(3). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int'l*, 829 F.3d at 1380. The obviousness inquiry requires considering whether one of skill in the art “would have been motivated to combine the prior art to achieve the claimed invention.” *In re NuVasive, Inc.*, 842 F.3d 1376, 1381 (Fed. Cir. 2016) (quoting *In re Warsaw Orthopedic, Inc.*,

832 F.3d 1327, 1333 (Fed. Cir. 2016)). “[T]he factual inquiry whether to combine references must be thorough and searching...” *Id.*

IV. Level of Ordinary Skill in the Art

For purposes of this Preliminary Response, Network-1 has applied Petitioner’s recitation of the level of skill in the art because, even under that proposed level of skill, Petitioner failed to demonstrate a reasonable likelihood of establishing unpatentability of any challenged claim. *See* Pet. at 9. Network-1 reserves the right to define a person of ordinary skill in the future, if necessary.

V. Claim Construction

Claims are construed according to *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). For purposes of this IPR, Petitioner asserts that no term requires express construction. Pet. at 10. However, Petitioner expressly reserves the right to advance claim constructions in the parallel district court litigation. *Id.* at fn. 2. This stance suggests Petitioner may seek narrow constructions before the District Court for non-infringement purposes while advocating broader constructions in the IPR for patentability determinations. The Board should not entertain such gamesmanship. *See Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.*, IPR2025-00632, Paper 20 at 4 (Squires November 3, 2025) (precedential) (“[T]he rules discourage petitioners from seeking

broader constructions at the Board to support a patentability challenge while seeking narrower constructions in litigation to avoid infringement liability.”).

VI. Argument

The Petition should be denied for multiple independent reasons, as described below.

A. Grounds 1-2, 6: The Patent Office Allowed The Challenged Independent Claim After Considering All Of Petitioner’s References And Petitioner Has Not Showed How The Office Erred

With respect to the sole independent claim 1, Samsung asserts obviousness combinations of five references—*all of which were considered during prosecution of the ‘893 Patent*. Pet. at 3 (grounds 1, 2, 6). As explained above in §II(B), the Applicant disclosed and the Examiner explicitly contemplated each of Park, GlobalPlatform, AbiChar, X9.63-Overview, and Nix175. EX1004 at 169, 341 (Park), *id.* at 167, 339 (GlobalPlatform), *id.* at 168, 340 (AbiChar), *id.* at 178, 350 (X9.63-Overview), and *id.* at 148, 275 (Nix175). Yet even after considering all of those references, the Examiner determined that independent claim 1 was allowable because that art “taken individually or in combination fails to particular[ly] disclos[e], fairly suggest, or otherwise render obvious” numerous limitations of independent claim 1. *Id.* at 76; EX2029 at ¶78.

The Examiner specifically noted differences between the ‘893 claims and one “Primary Reference”: U.S. Printed Patent Application No. 2014/0237101 to Park.

EX1004 at 77; EX2025. That Park patent application has the same inventor and a disclosure similar to Samsung’s Park paper (EX1005), which the Petition relies upon as its primary §103 reference. *Compare* EX2025 with EX1005. For example, the Park patent application teaches “securely provisioning various profiles” for an eUICC (EX2025 at [0085]), while the Park paper teaches a “secure profile provisioning architecture for eUICCs” (EX1005 at 1). And the Examiner specifically identified those teachings from the Park patent application, stating that it “discloses a method for managing a profile in an embedded UICC, and more particularly, to a method for managing a profile in an embedded UICC that enables management information on the profile provided within the embedded UICC to play an essential role for providing communication and additional services, to be provided to a device existing outside the embedded UICC.” EX1004 at 77; EX2029 at ¶79.

Further, the Examiner explained in the reasons for allowance that the Park patent application did not disclose multiple limitations from ‘893 claim 1, including: (1) “receiv[ing], from the subscription manager, ... a symmetric key”; and (2) “decrypt[ing] ... using the symmetric key ... the subscriber identity.” EX1004 at 77. As explained below, the Petition’s references—including the Park paper—similarly fail to teach or suggest those same two claim limitations. *See infra* at §VI(B).

Notwithstanding that (1) independent ‘893 claim 1 was allowed over all five of the Petition’s references and (2) the Examiner performed a detailed analysis and

explained why claim 1 was different from a Park patent application with very similar disclosures to the Petition's Park paper, Samsung has failed to show how the Patent Office erred in applying the prior art and allowing '893 claim 1. Given that the same references were considered by the Examiner, the Board should not institute this IPR absent a clear showing of error in the underlying prosecution. *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020) (precedential) (declining to institute an IPR when the same art was previously presented to the office and the Petition failed to demonstrate the Examiner erred when considering the prior art); *PUMA N. Am., Inc. v. NIKE, Inc.*, IPR2019-01042, Paper 10 (P.T.A.B. Oct. 31, 2019) (informative) (refusing to institute IPR when the office considered the same art and Petitioner did not persuasively demonstrate that the Examiner erred when considering that art). Petitioner has shown no such error in the Examiner's findings.

B. Grounds 1-2: Petitioner's Art Fails To Present A Reasonable Likelihood Of Prevailing Against Independent Claim 1

1. Petitioner's References Do Not Teach Or Suggest "Receiv[ing] ... A Symmetric Key" From The Subscription Manager And Deriving A Profile Key

Claim 1 of the '893 Patent requires that the radio of the claimed mobile device be configured to "receive, from the subscription manager, . . . ii) a symmetric key" and deriving a profile key. EX1001 at 80:30-41. This limitation is not satisfied—or even suggested—by the combination of Park, GlobalPlatform and AbiChar (Ground

1) or the combination of Park, GlobalPlatform and X9.63-Overview (Ground 2). As shown below, none of those references, alone or in combination, discloses or suggests a mobile device *receiving* a symmetric key from a subscription manager and also *deriving* a profile key. EX2029 at ¶81.

(a) The ‘893 Patent Requires Both Receiving A Symmetric Key From A Subscription Manager And Deriving A Profile Key.

The plain language of claim 1 is clear that two different keys must be obtained using two different methods. First, the radio of the mobile device must be configured to *receive*—as an incoming transmission from an external entity identified as a subscription manager—a symmetric key. EX1001 at 80:30-36. This is not a key that is locally derived or computed amongst two parties through a mutual protocol. Rather, it is a key that one party (the subscription manager) sends and the other party (the mobile device) *receives*. EX2029 at ¶82. This symmetric key is used to decrypt one part of the eUICC profile.

Second, claim 1 also separately requires *deriving* a profile key using an elliptic curve Diffie Hellman key exchange. EX1001 at 80:39-41. This profile key is obtained very differently than the symmetric key discussed above; the claim is clear that the profile key is *derived* by mobile device’s eUICC (*i.e.*, calculated from various information), and not simply received like the symmetric key. EX2029 at ¶83. This profile key is used to decrypt a different part of the eUICC profile.

The ‘893 Patent specification confirms there is a difference in how the two claimed keys are obtained. The symmetric key is one that originates externally and is *received* by the mobile device as part of an encrypted communication. *See* EX1001 at 36:56-58 (“the module can receive a symmetric key 127 to decrypt the second key K 204a”); *see also id.* at 6:38-40. Alternatively, the profile key is one that is *derived* using other information according to an elliptic curve Diffie Hellman key exchange. *Id.* at 53:27-60; EX2029 at ¶84.

Thus, one important aspect of ‘893 Patent claim 1 is that the symmetric key and the profile key are obtained via different methods to increase security. One of those keys (the symmetric key) is received by the mobile device as part of an encrypted communication, while the other key (the profile key) is derived at the mobile device the ECDH cryptographic parameters and algorithms. EX2029 at ¶85.

(b) Park Does Not Teach Transmission Of Any Symmetric Key To The Mobile Device.

Park’s Secure Profile Provisioning Architecture (“SPA”) does not disclose a subscription manager that transmits a symmetric key to the eUICC. Rather, Park describes a two-entity Subscription Manager architecture—SM-SR (Secure Routing) for transporting the encrypted profile, and SM-DP (Data Preparation) for generating and encrypting it. EX1005 at 1-2. And in Park’s key agreement framework, the SM-DP and the eUICC establish a shared session key—Park’s *keySM-DP*—through an asymmetric key agreement protocol housed in the eUICC’s

Key Agreement Module (“KAM”). *Id.* at 4-5. The result is that each side independently derives *keySM-DP* through the key exchange; neither side transmits *keySM-DP* to the other. *Id.* at 4. By design, *keySM-DP* is a mutually derived key, not a received one. EX2029 at ¶86.

Park teaches no additional, separate symmetric key that is generated by the SM-DP and then transmitted to the eUICC. And while Park’s profile is encrypted with *keySM-DP* and that profile is subsequently sent over the secure channel—the *keySM-DP* itself is never transmitted; it is independently computed at each endpoint. EX1005 at 4-7. There is no step in Park’s protocol in which the subscription manager transmits a symmetric key to the eUICC. EX2029 at ¶87.

(c) GlobalPlatform Teaches Two Mutually-Exclusive Methods For Obtaining Session Keys; It Does Not Teach Mixing Those Methods Within a Session.

Recognizing the deficiencies of Park with respect to this claim limitation, Samsung turns to GlobalPlatform. Pet. at 38-41, 57. More specifically, Petitioner alleges that GlobalPlatform’s Data Encryption Key (“DEK”) is the claimed “symmetric key” that is received from the subscription manager using GlobalPlatform’s key transport option. Pet. at 40, 57. However, Petitioner fails to note that the key transport option is just one of two mutually-exclusive ways by which the card can obtain keys. *Id.* More specifically, GlobalPlatform teaches using either (1) a key transport option, where the card *receives* session keys from an off-

card entity or (2) a key agreement option, where the card and the off-card entity exchange secret values and then *derive* the session keys using an algorithm. EX1006 at 255; EX2029 at ¶88.

There is no suggestion in GlobalPlatform to use both of these options together to obtain two different keys. Importantly, the two options cannot be used together in GlobalPlatform; rather, for any given session, either the key transport option is used *or* the key agreement option is used (but not both). EX1006 at 255. GlobalPlatform teaches that the choice to use either the key transport option or the key agreement option is recorded as a single bit within the card recognition and security domain management data. *Id.* If the key transport option is selected, then the first bit is a “0.” Alternatively, if the key agreement option is selected, then the first bit is a “1.” *Id.*

Table F1 illustrates this protocol:

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

Id. (highlighting added); *see also id.* at 301-302; EX2029 at ¶89.

This is significant because, for purposes of the claimed “deriv[ing] a profile key” limitation, Samsung alleges the eUICC would derive the session key using its private key and the subscription manager public key (*i.e.*, the key agreement option

is selected). Pet. at 42. But that necessarily means that the GlobalPlatform’s key transport option cannot be selected. *See supra*. Samsung cannot have it both ways. EX2029 at ¶90.

Thus, GlobalPlatform cannot teach or suggest the claimed “receiv[ing] from the subscription manager ... a symmetric key” and deriving a profile key. EX2029 at ¶91.

(d) AbiChar and X9.63-Overview Do Not Cure These Deficiencies

Lastly, neither AbiChar (Ground 1) nor X9.63-Overview (Ground 2) fills the gaps left by Park and GlobalPlatform. Both references merely describe ECDH and elliptic curve key exchange protocols. EX1007, EX1008. And as Petitioner’s own mapping confirms, these references are relied upon only to supply the ECDH algorithm used to derive Park’s *keySM-DP* (*i.e.*, the claimed “profile key” in claim 1). Pet. at 41–45, 57–61. Neither AbiChar nor X9.63-Overview teaches or suggests a mobile device receiving a symmetric key from a subscription manager, as claimed. Rather, Abi-Char’s and X9.63-Overview’s ECDH key exchange, by its very nature, produces a shared key through mutual derivation without transmitting the key itself. The ECDH-derived session key is not a symmetric key that is received from another party; it is one that each party independently computes. AbiChar and X9.63-Overview thus directly reinforce the opposite of what ‘893 claim 1 requires. EX2029 at ¶92.

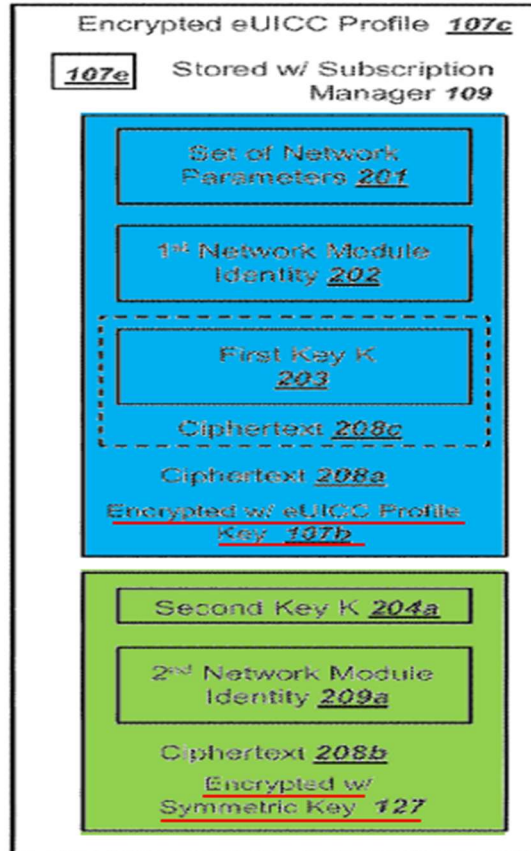
(e) Conclusion

For the foregoing reasons, the combinations asserted in Grounds 1 and 2 do not teach or suggest ‘893 claim 1’s requirement of “receiv[ing], from the subscription manager, . . . a symmetric key” and also deriving a profile key. None of Park, GlobalPlatform, AbiChar, nor X9.63-Overview—whether separately or in combination—discloses that claim limitation. EX2029 at ¶XX. Grounds 1 and 2 should therefore be denied.

2. Petitioner’s References Do Not Teach Or Suggest “Decrypting ... The Subscriber Identity”

Claim 1 of the ‘893 Patent also requires that the eUICC within the mobile device be configured to “decrypt a second portion of the eUICC profile using the symmetric key, the second portion comprising [] the subscriber identity.” EX1001 at 80:46-48.

The ‘893 specification (including annotated Figure 2a below) similarly explains that the eUICC profile contains a second portion 208b (green) that includes a second network module identity 209a. EX1001 at 32:44-46. And the eUICC decrypts the second network module identity 209 using the symmetric key. *Id.* at 60:38-43.



Id. at Fig. 2a (highlighting and red underlining added); EX2029 at ¶94.

As an initial matter, for the reasons described above, none of the references teach or suggest to “receive [] a symmetric key.” *See supra* at §VI(B)(1). So it necessarily follows that none of those references teach or suggest using a received symmetric key to decrypt anything—including a “subscriber identity.” EX2029 at ¶95.

Notwithstanding, with respect to grounds 1-2, Petitioner alleges that Park’s International Mobile Subscriber Identity (“IMSI”) is the claimed “subscriber identity” and that it would be decrypted (and encrypted) using GlobalPlatform’s DEK “symmetric key.” Pet. at 45-46, 57. But GlobalPlatform never teaches to

encrypt/decrypt the IMSI using the DEK. At most, GlobalPlatform teaches to “use[] the relevant data encryption session key (DEK) for sensitive data in command messages or for sensitive data in response messages.” EX1006 at 284 (emphasis added). And according to GlobalPlatform, such sensitive data includes “all keys transmitted to a card.” *Id.* (emphasis added). Thus, GlobalPlatform only teaches to encrypt/decrypt any sensitive key data sent to the card. *Id.*; EX2029 at ¶96.

Unlike key data, the IMSI is not the sort of sensitive data that GlobalPlatform teaches must be encrypted. EX2029 at ¶97. Rather, in the 3G and 4G networks that were available in 2011 when GlobalPlatform was released, the IMSI was transmitted in plain text over the air during initial network attachment. EX2027 at 19 (3G); EX2028 at 21 (4G). Thus, a POSITA would not have understood GlobalPlatform as teaching to encrypt the IMSI using the DEK symmetric key. EX2029 at ¶97. And the Petitioner does not rely on any other reference for this claim element. Pet. at 45-46, 57. Thus, none of Petitioner’s references—whether alone or in combination—teach or suggest “decrypt[ing] ... using the symmetric key ... the subscriber identity,” as per ‘893 claim 1. EX2029 at ¶98.

Grounds 1 and 2 should be denied for this additional reason.

3. A POSITA Would Not Combine The Park And GlobalPlatform References As The Petition Proposes

Petitioner’s theory depends upon a person of skill choosing to layer GlobalPlatform’s DEK mechanism onto Park’s SPA in a particular way that does

not appear and is not taught in either reference. That choice is guided entirely by the hindsight knowledge of the claimed invention itself. Park provides what it deems to be adequate security with full profile encryption using key_{SM-DP} ; there is no articulated need within Park's architecture for an additional symmetric layer providing more security. EX2029 at ¶99.

If a POSITA were to combine Park and GlobalPlatform, he/she would have looked to GlobalPlatform for implementation details of the smart card protocol to aid in realizing Park's scheme. EX2029 at ¶100. Indeed, this is precisely what Park teaches: "consider the way to apply the de-facto standard for profile provisioning, [GlobalPlatform], to the eUICC provisioning ecosystem" in Park. EX1005 at 2. However, that POSITA would have been aware of Park's teaching that a non-conventional application of GlobalPlatform's smart card protocol to Park's profile provision scheme faces numerous drawbacks affecting security and efficiency. EX1005 at 2-3 ("applying the [GlobalPlatform smart card protocol] into [Park's] eUICC provisioning ecosystem has several drawbacks with respect to scalability, efficiency, security, and flexibility"); EX2029 at ¶100. So that POSITA would have looked to the most straightforward application of Park and GlobalPlatform and carefully weighed the effects to security and efficiency when making any modification to Park. *Id.* at ¶100.

For example, a POSITA would have understood that Park’s provisioning ecosystem already provides for security. EX2029 at ¶101. In Park’s provisioning ecosystem, the SM-DP subscription manager locally derives its SM-DP key, key_{SM-DP} , and then uses it to encrypt the entire profile. EX1005 at 4 (the eUICC and SM-DP “dynamically [] generate the SM-DP Credentials (key_{SM-DP}) [and then] SM-DP encrypts each block of [the] profile ($Profile_i$) [before] send[ing] the protected profile blocks to the eUICC”); EX2029 at ¶101. In other words, for security reasons, the SM-DP and eUICC do not transport the SM-DP key, key_{SM-DP} , but rather locally derive it. *Id.* This avoids the need to transport the SM-DP key and expose it to other entities, potentially weakening the overall security. *Id.* Thus, when combining Park and GlobalPlatform, a POSITA would have similarly recognized the need to avoid exposing any session keys to other entities. EX2029 at ¶101.

Accordingly, to retain the security advantage of Park’s proposed design, a POSITA would have used GlobalPlatform’s key agreement option to derive the session keys—in much the same manner as Park derives the SM-DP key. EX2029 at ¶102. More specifically, a POSITA would have set the first bit in parameter i to “1” to utilize the key agreement option (rather than to “0” to utilize the key transport option):

b8	b7	b6	b5	b4	b3	b2	b1	Description
Not available	0	0	0	0	0	-	0	Key Transport
Not available	0	0	0	0	0	-	1	Key Agreement
Not available	0	0	0	0	0	0	-	Signature with message recovery
Not available	0	0	0	0	0	1	-	Signature without message recovery

Table F-1: Values of Parameter "i"

EX1006 at 255 (highlighting added); EX2029 at ¶102. Because of this binary choice, and to maintain consistency with Park’s choice of key agreement for its SM-DP key, this would result in all of GlobalPlatform’s session keys being derived—including the C-ENC key (equivalent of Park’s SM-DP key) used to encrypt the entire profile and the DEK key used to encrypt the sensitive key data. *Id.* Thus, Park implicitly teaches to use GlobalPlatform’s key agreement option to securely derive keys—and not the key transport option that could expose keys to security issues. In this manner, the properly-combined system retains Park’s security advantages. EX2029 at ¶103.

In stark contrast to the straightforward combination discussed above, Samsung proposes a combined Park-GlobalPlatform system that is not taught by either reference and is plainly and improperly motivated by hindsight. EX2029 at ¶104. In Samsung’s combination, the key K and IMSI are considered to be sensitive data that is encrypted by GlobalPlatform’s DEK key, and then the entirety of the profile is further encrypted by another session key (*e.g.*, Park’s SM-DP key or GlobalPlatform’s C-ENC key). *See* Pet. at 20-23. But Park does not teach a second layer of encryption. EX2029 at ¶104. And while GlobalPlatform provides an option

for a second layer of encryption for sensitive key data, it never teaches including the module identity (IMSI) as part of a second layer of encryption. *Id.*

Further, in Samsung's combination, the DEK key is sent using GlobalPlatform's key transport option, while the other session keys are derived using GlobalPlatform's key agreement option. *See* Pet. at 21-23. But GlobalPlatform never teaches to use both options simultaneously to obtain different keys. More specifically, GlobalPlatform does not teach using (1) the key transport option for DEK and (2) the key agreement option for other session keys (like the Command Encryption session key, C-ENC, which Samsung says serves the same function as Park's *key_{SM-DP}*). Pet. at 21; EX2029 at ¶105. Instead, GlobalPlatform specifically states that the card recognition or SD management data will contain a parameter *i* whose first bit *b1* determines whether all the session keys are obtained using either (1) the key transport option (*b1*=0) or (2) the key agreement option (*b1*=1). EX1006 at 255. Thus, Samsung's combination is illogical and goes against the references' teachings. EX2029 at ¶105.

Lastly, when combining Park with GlobalPlatform, a POSITA would not have been motivated to obtain just the DEK using the key transport option, while obtaining the other session keys via a different key agreement option. EX2029 at ¶106. Instead, a POSITA would have viewed using two methods of obtaining session keys (as opposed to one) as inefficient and increasing overhead. *Id.* In short, a

POSITA would not have been motivated to build the combined Park-GlobalPlatform system in the manner set forth in the Petition, absent adopting the inventive insight disclosed only in the '893 Patent. *Id.*

C. Ground 6: The '893 Patent Is Entitled To Its Priority Date So Nix175 Is Not Prior Art

Finally, with respect to ground 6 only, Petitioner alleges the '893 Patent is not entitled to its priority date because none of the applications to which it claims priority provide written description for the claimed "receiv[ing], from the subscription manager ... a symmetric key." Pet. at 9-10. Instead, according to the Petition, the applications only disclose receiving the symmetric key from the mobile network operator. *Id.* And, according to the Petition, if the '893 Patent is not entitled to its priority date, then the inventor's own earlier patent, Nix175, becomes prior art. *Id.*

However, the earliest priority Nix patent application (and all subsequent applications in the chain including the '893 Patent) teach that the "mobile network operator 104 could operate the eUICC subscription manager 109." EX2024 at 25; *see also id.* at 65 ("the MNO 104 could also function as a eUICC subscription manager 109"). Thus, because the '893 priority applications teach the mobile network operator and the subscription manager can be the same, there is ample written description for receiving a symmetric key from a subscription manager. EX2029 at ¶110. Hence, the '893 Patent is entitled to its earliest December 6, 2013 priority date, and Nix175 is not prior art. Ground 6 must fail.

D. Grounds 3-5: Petitioner's Art Fails To Present A Reasonable Likelihood of Prevailing Against The Dependent Claims

Grounds 3-5 challenge only dependent claims of the '893 Patent. Pet. at 3. Because Petitioner failed to present a reasonable likelihood of success of invalidating any independent claim (*see supra*), its challenges to the dependent claims necessarily fail as well.

VII. Conclusion

Network-1 respectfully requests that the Board refuse to institute *inter partes* review for the reasons stated herein.

Dated: March 3, 2026

Respectfully submitted,

/ Michael F. Heim /

Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Network-1 Technologies, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing **Patent Owner’s Preliminary Response**, was served via email to counsel of record for Petitioners as follows:

Counsel for Petitioner	
Lead Counsel	Backup Counsel
William M. Fink (Reg. No. 72,332) O’Melveny & Myers LLP 1625 Eye Street, NW Washington, DC 20006 Telephone: (202) 383-5300 Fax: (202) 383-5414 Email: tfink@omm.com	Benjamin M. Haber (Reg. No. 67,129) O’Melveny & Myers LLP 400 South Hope Street, 19th Floor Los Angeles, CA 90071 Telephone: (213) 430-6000 Fax: (213) 430-6407 Email: bhaber@omm.com Marc J. Pensabene (Reg. No. 37,416) O’Melveny & Myers LLP 1301 Avenue of the Americas, Suite 1700 New York, NY 10019 Telephone: (212) 326-2000 Fax: (212) 326-2061 Email: mpensabene@omm.com Brian Cook (Reg. No. 59,356) O’Melveny & Myers LLP 400 South Hope Street, 19th Floor Los Angeles, CA 90071 Telephone: (213) 430-6000 Fax: (213) 430-6407 Email: bcook@omm.com Caitlin P. Hogan (Reg. No. 61,515) O’Melveny & Myers LLP 1301 Avenue of the Americas, Suite 1700 New York, NY 10019

	Telephone: (212) 326-2000 Fax: (212) 326-2061 Email: chogan@omm.com
--	---

Dated: March 3, 2026

Respectfully submitted,

/Michael F. Heim /

Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Network-1 Technologies, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned hereby certifies that this brief complies with the type-volume limitation of 37 C.F.R. § 42.24 because this brief contains 7,748 words.

Dated: March 3, 2026

Respectfully submitted,

/ Michael F. Heim /
Michael F. Heim (Reg. No. 32,702)
Attorney for Patent Owner
Network-1 Technologies, Inc.