

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.

IPR2026-00118
Patent 12,207,094

**PATENT OWNER'S PRELIMINARY RESPONSE TO PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 12,207,094**

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.	Introduction.....	1
II.	Background.....	2
A.	The ‘094 Patent [EX1001]	2
B.	The ‘094 Prosecution History [EX1004]	7
C.	Petitioner’s References.....	9
1.	Park [EX1005]	10
2.	GlobalPlatform [EX1006]	12
3.	AbiChar [EX1007].....	15
4.	X9.63-Overview [EX1008]	16
5.	Nix175 [EX1016]	18
6.	Petitioner’s Other Reference (Weiss [EX1009]).....	20
III.	Legal Standards	20
IV.	Level of Ordinary Skill in the Art	21
V.	Claim Construction.....	22
VI.	Argument	22
A.	Grounds 1-2, 5: The Patent Office Allowed The Challenged Independent Claim After Considering All Of Petitioner’s References And Petitioner Has Not Showed How The Office Erred	23
B.	Grounds 1-2: Petitioner’s Art Fails To Present A Reasonable Likelihood Of Prevailing Against Independent Claim 1	25
1.	Petitioner’s References Do Not Teach Or Suggest “Receiving The Symmetric Key” And Deriving A Profile Key	25
2.	A POSITA Would Not Have Combined The References As The Petition Proposes	30

C.	Ground 5: The ‘094 Patent Is Entitled To Its Priority Date So Nix175 Is Not Prior Art.....	36
D.	Grounds 3-4: Petitioner’s Art Fails To Present A Reasonable Likelihood of Prevailing Against The Dependent Claims	38
VII.	Conclusion	39

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	23
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	20
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	20
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	20
<i>In re NuVasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016)	20
<i>In re Warsaw Orthopedic, Inc.</i> , 832 F.3d 1327 (Fed. Cir. 2016)	21
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	21
<i>PUMA N. Am., Inc. v. NIKE, Inc.</i> , IPR2019-01042, Paper 10 (P.T.A.B. Oct. 31, 2019).....	24
<i>Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.</i> , IPR2025-00632, Paper 20 (Squires November 3, 2025).....	21

Statutes

35 U.S.C. § 312(a)(3).....	20
----------------------------	----

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	<i>Reserved</i>
EX2008	U.S. Patent No. 11,916,893
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	<i>Reserved</i>
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. NWO SAM 00013295

Exhibit	Description
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	<i>Reserved</i>
EX2026	U.S. Patent Publication No. 2014/0219447
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	U.S. Patent Application No. 14/084,141

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. 12,207,094 (“the ‘094 Patent”). For several reasons, Samsung has not shown a reasonable likelihood of prevailing on any of its five grounds that challenge ‘094 claims 1-22.

First, with respect to grounds 1-2 and 5, 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, a 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 ‘094 Patent.

Second, as to grounds 1-2, Samsung’s references fail to teach or suggest several limitations of independent claim 1, including both: (1) “deriving a profile key” used to “decrypt[] at least a portion of the encrypted profile;” and (2) “receiving the symmetric key” used “decrypt[] at least a portion of the ciphertext” found in another portion of the encrypted profile.

Third, for ground 5, Samsung wrongly alleges the ‘094 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 3-4 only pertain to dependent claims. Because Samsung failed to show that any independent claim was invalid in grounds 1-2 and 5, its challenges to the dependent claims necessarily fail as well.

II. Background

A. The ‘094 Patent [EX1001]

The ‘094 Patent relates to provisioning and authenticating mobile devices that have an embedded subscriber identity module (“eSIM”).¹

Before the ‘094 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 2:45-51. 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,

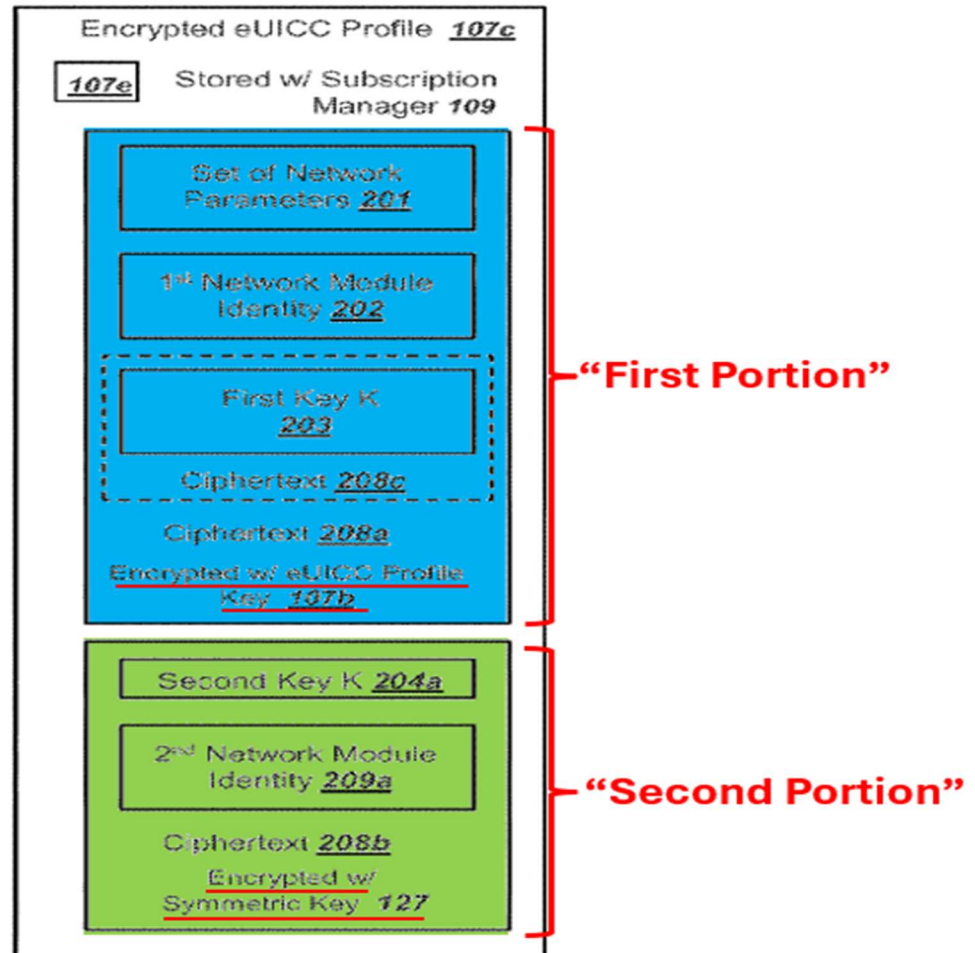
¹ An eSIM may also be referred to as an embedded universal integrated circuit card (“eUICC”). EX1001 at 19:36-38.

information about the network to which the mobile device should connect, and a pre-shared secret key K. *Id.* at 2:52-62. 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 3:4-22; EX2029 at ¶22.

Because of the drawbacks with physical SIM cards, the industry began to consider replacing them with eSIMs. EX1001 at 3:23-27. 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 3:41-4:48. The ‘094 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 4:52-8:50; 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 ‘094 Patent. The encrypted eUICC profile includes two distinct portions: (1) a first portion (blue); and a second portion (green). EX1001 at 30:41-47. 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 11:59-63, 32:52-55. 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 38:30-36, 34:49-64. 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 36:63-65. At that point, the mobile device is provisioned and can successfully authenticate itself with the network. *Id.* at 36:65-67. This ‘094 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 35:42-45; EX2029 at ¶25.

Independent claim 1 of the ‘094 Patent typifies the approach discussed above. It recites a method that can be performed by a mobile device with an eUICC or eSIM. EX1001 at 80:31-67. One of the steps is “receiving from the subscription manager system, an encrypted profile” that comprises a first “ciphertext” portion and a second portion. *Id.* at 80:55-56, 59-64. To decrypt the first portion, the method requires “deriving a profile key using a key exchange algorithm” and then using it to decipher the first portion. *Id.* at 80:47-48, 59-61. To decrypt the second portion, the method requires “receiving the symmetric key” and then using it to decipher the second portion, including the “key K” within that second portion. *Id.* at 80:58, 62-64, 56-57. Finally, the method requires “storing at least the key K in the embedded universal integrated circuit card for use in future communications.” *Id.* at 80:65-67.

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 method comprising:

- (a) generating a first message comprising:
 - (1) an identity of an embedded universal integrated circuit card (eUICC);
 - (2) a nonce; and
 - (3) a first digital signature, generated using a first eUICC private key, wherein the first eUICC private key corresponds to a first eUICC public key;
- (b) sending the first message via a network application to a subscription manager system;
- (c) deriving a second eUICC private key and a corresponding second eUICC public key using a first random number generator and a first set of cryptographic algorithms;
- (d) storing a subscription manager public key which corresponds to a subscription manager private key;
- (e) **deriving a profile key using a key exchange algorithm** based on at least:
 - (i) the second eUICC private key, and
 - (ii) the stored subscription manager public key, wherein the profile key can also be derived at the subscription manager system based at least on: the second eUICC public key, and the subscription manager private key;
- (f) receiving from the subscription manager system, an encrypted profile comprising a ciphertext including a key K encrypted with a symmetric key;
- (g) **receiving the symmetric key**;
- (h) **decrypting, by the embedded universal integrated circuit card, at least a portion of the encrypted profile using the profile key**;

- (i) decrypting, by the embedded universal integrated circuit card, at least a portion of the ciphertext using the symmetric key; and
- (j) storing at least the key K in the embedded universal integrated circuit card for use in future communications.

EX1001 at 80:31-67 (emphasis and highlighting added).

B. The ‘094 Prosecution History [EX1004]

The application that resulted in the ‘094 Patent was filed on January 18, 2024; however, that application claimed priority to a string of other related continuation applications dating back to December 6, 2013. EX1004 at 491-630. The ‘094 application had fifteen initial claims. *Id.* at 620-623; EX2029 at ¶49.

On April 9, 2024, shortly after filing the ‘094 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 ‘094 independent claim 1. EX1004 at 241-318. More specifically, at the very onset of prosecution of this patent, the Applicant disclosed each of Park (*id.* at 292), GlobalPlatform (*id.* at 290), AbiChar (*id.* at 291), X9.63-Overview (*id.* at 310), and Nix175 (*id.* at 252). The Examiner then considered each of those five references. *Id.* at 202 (Park), *id.* at 200 (GlobalPlatform), *id.* at 201 (AbiChar), *id.* at 229 (X9.63-Overview), and *id.* at 174 (Nix175); EX2029 at ¶20.

On September 18, 2024, the examiner rejected all the claims for double patenting and under 35 U.S.C. §112 (for failing to explicitly define “eUICC”).

EX1004 at 130-140. However, the examiner did not issue any §§102(a)-(b) rejections for novelty or obviousness in light of the considered prior art. *Id.* To the contrary, the examiner allowed independent claim 1 over the prior art of record. *Id.* at 135; EX2029 at ¶51.

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. 2014/0219447 to Park (EX2026). EX1004 at 135, 137-139. Remarkably, the inventor of that patent application is the same person that authored the primary reference used in Samsung’s petitions—Jaemin Park. *Compare* EX2026 at 1 *with* EX1005 at 1. And both Park references have similar disclosures. That Park patent application teaches “securely provisioning various profiles” for an eUICC (EX2026 at [0011]), while the Park paper teaches a “secure profile provisioning architecture for eUICCs” (EX1005 at 1). Further, the examiner explicitly acknowledged that teaching from that Park patent application, noting it “discloses a method wherein an [mobile network operator] receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where [the subscription manager] is divided and implemented as SM-SR and SM-DP (data preparation).” EX1004 at 137; EX2029 at ¶52.

On November 4, 2024, the applicant submitted a terminal disclaimer to overcome the double patenting rejection and amended claim 1 to define “eUICC” and overcome the §112 rejection. EX1004 at 110-120; EX2029 at ¶53.

On December 3, 2024, the examiner issued a formal notice of allowance. EX1004 at 74-77. In that notice, the examiner incorporated the prior reasons for allowance from the September 18, 2024 office action. *Id.* at 76; EX2029 at ¶54.

The ‘094 Patent issued on January 21, 2025. EX1004 at 63; EX2029 at ¶55.

C. Petitioner’s References

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

Ground	Claims	Statute	References
1	1-17, 19-22	§103	Park + GlobalPlatform + AbiChar
2	1-17, 19-22	§103	Park + GlobalPlatform + X9.63-Overview
3	18	§103	Park + GlobalPlatform + AbiChar + Weiss
4	18	§103	Park + GlobalPlatform + X9.63-Overview + Weiss
5	1-22	§103	Nix175 + Park + GlobalPlatform

Pet., 3. None of those references, either alone or in combination, teach or suggest all the elements of challenged ‘094 independent claim 1.² EX2029 at ¶59.

1. Park [EX1005]

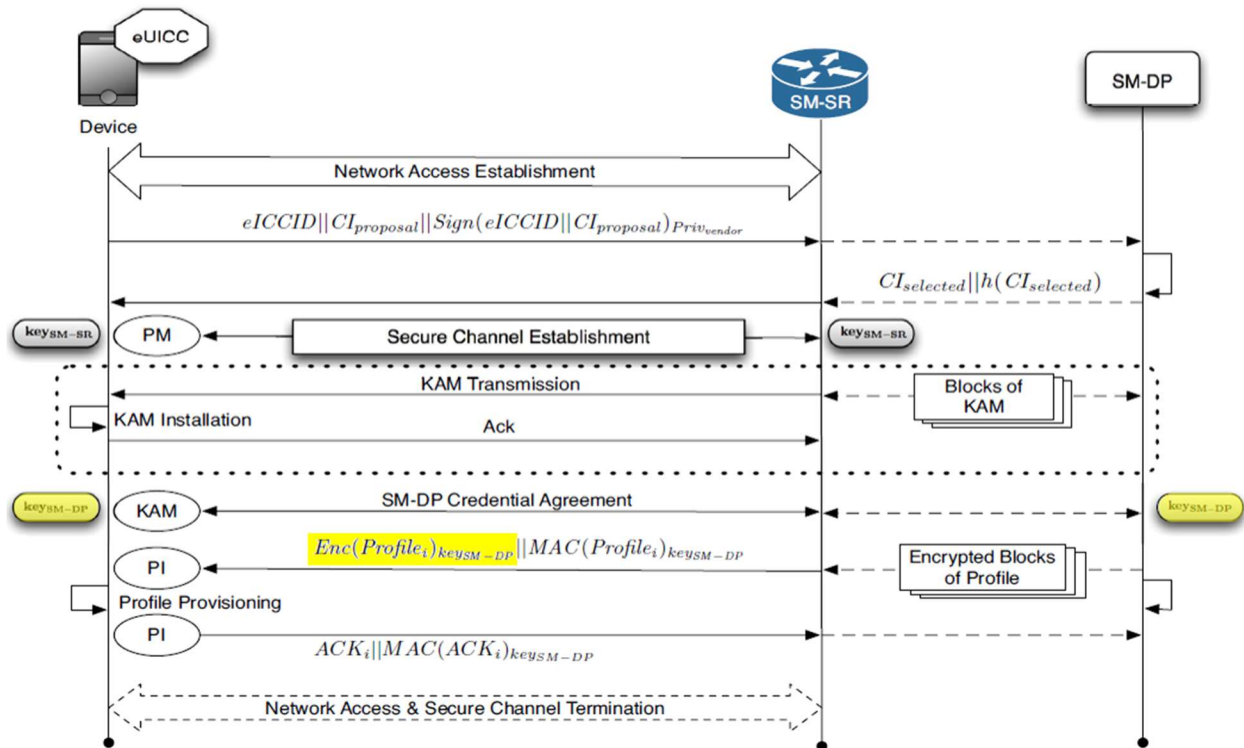
Park, EX1005, is a paper titled “Secure Profile Provisioning Architecture for Embedded UICC” authored in 2013 by Jaemin Park *et al.* EX1005 at 1. Park addresses the security challenges of remotely provisioning profiles onto eUICCs. *Id.* According to Park, because no single mobile network operator (“MNO”)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

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 2-22. 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.

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 important aspects of ‘094 claim 1, including: (1) a profile with two portions, each of which is decrypted using a different key obtained in a different way; and (2) generating a first message comprising a nonce. 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.

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

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

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"

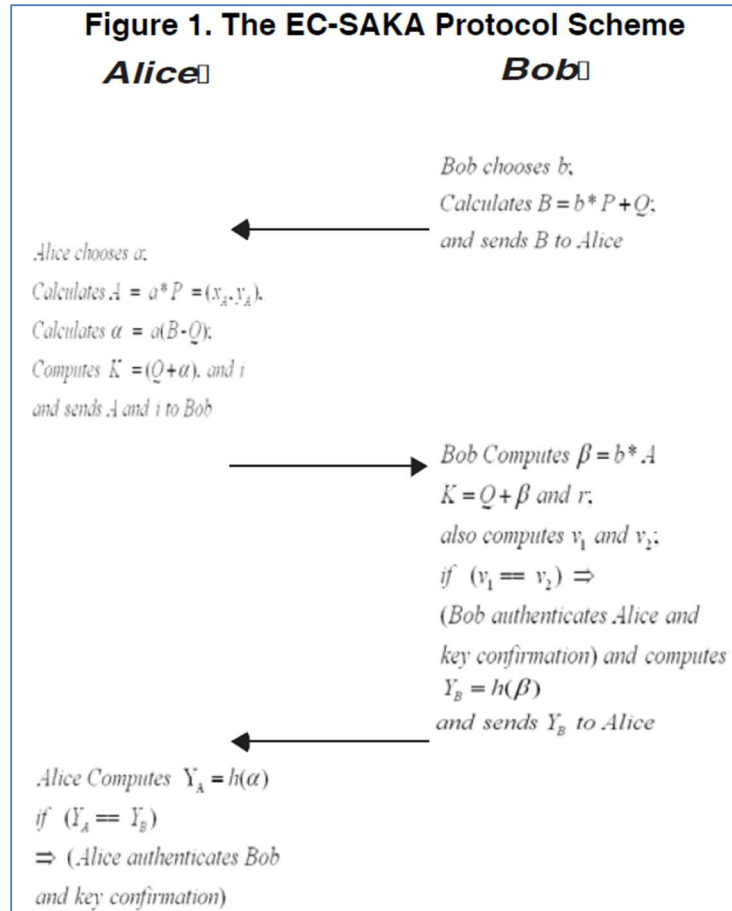
Id. at 255 (highlighting added); EX2029 at ¶66.

GlobalPlatform fails to teach key parts of ‘094 claim 1, including both deriving a profile key and receiving a symmetric key. 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 $E(Z_p)$, 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 $K_s = h(ID(Alice) \parallel ID(Bob) \parallel K)$. *Id.* at 3-4; EX2029 at ¶69.



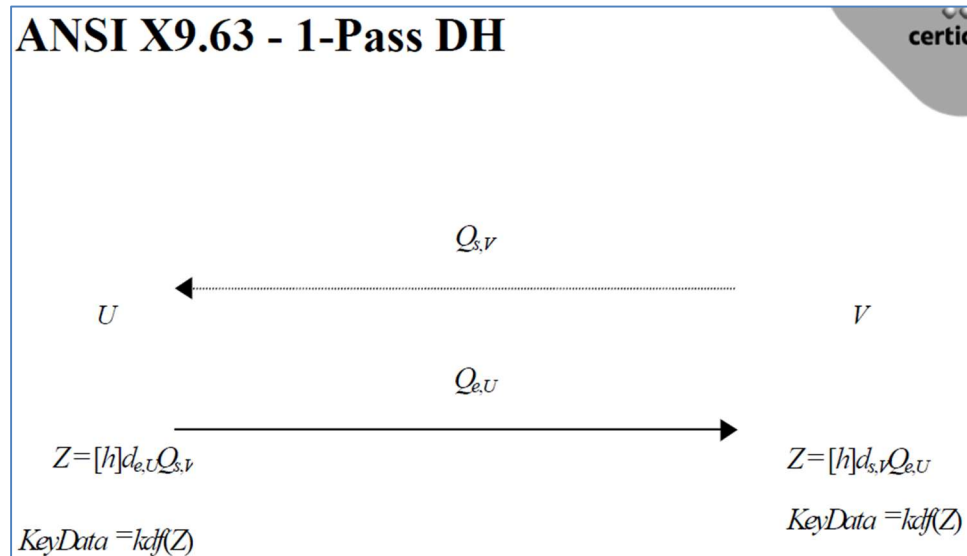
AbiChar fails to teach many key components of ‘094 claim 1, including: (1) a profile with two portions, each of which is decrypted using a different key obtained in a different way; and (2) generating a first message comprising a nonce. EX2029 at ¶69.

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 ‘094 claim 1, including: (1) a profile with two portions, each of which is decrypted using a different key obtained in a different way; and (2) generating a first message comprising a nonce. 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 ‘094 Patent is a continuation of Nix175; both share the same specification and the ‘094 Patent claims priority to Nix175. *Compare* EX1001 *with* EX1016. Nix175 is not prior art to the ‘094 Patent, as explained below.

Samsung concedes Nix175 is only prior art to the ‘094 Patent if it is not entitled to its priority claim. Pet. at 18. According to Samsung, the ‘094 Patent is not entitled to claim priority to Nix175 for two reasons, neither of which has merit. Pet. at 9-10.

First, Samsung alleges there is no priority because the ‘094 Patent claims recite two eUICC public/private key pairs, while Nix175 allegedly discloses only one eUICC public/private key pair. Pet. at 9. However, Nix175 teaches two key pairs: (i) one pair for generating a digital signature used in authenticating; and (ii)

another pair for deriving a profile key used in decryption. Nix175 describes the first key pair at, *e.g.*, EX1016 at 47:17, 54-55 (a first instance of eUICC private key 215 is stored on module 101 within the mobile device and a first instance of eUICC public key 214 is stored on subscription manager 109). This first key pair is used to generate a digital signature that is sent in a first message from the eUICC to the subscription manager. *Id.* at 48:65-49:6. The subscription manager then uses this digital signature to authenticate the eUICC. *Id.* at 49:15-19. Nix175 describes the second key pair at, *e.g.*, 51:65-52:2 (a second instance of eUICC public key 214 and eUICC private key 215). This second key pair is derived using Elliptic Curve Cryptography (ECC) algorithms and a random number generator. *Id.* Then this second key pair is subsequently used with other information to derive a profile key used to decrypt a portion of the eUICC profile. *Id.* at 52:24-32. Thus, because Nix175 teaches two eUICC public/private key pairs, Nix175 provides written description support for the ‘094 claims. EX2029 at ¶76.

Second, Samsung alleges there is no priority because the ‘094 Patent claims “place no limit on the source of the claimed ‘symmetric key’” so they are broad enough to encompass receiving it from the subscription manager, 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 full scope of the ‘094 claims. EX2029 at ¶75.

In sum, the ‘094 Patent is entitled to its priority date, and Nix175 is not prior art. EX2029 at ¶77.

6. Petitioner’s Other Reference (Weiss [EX1009])

The Petition relies on one other reference—Weiss (EX1009)—just to invalidate one dependent claim. Pet. at 65-66. But as explained above, Network-1 only addresses independent claim 1 in this Preliminary Response. So Network-1 reserves the right to explain that other reference 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. 3. 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, 5: 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 ‘094 Patent. Pet. at 3 (grounds 1, 2, 5). 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 202, 292 (Park), *id.* at 200, 290 (GlobalPlatform), *id.* at 201, 291 (AbiChar), *id.* at 229, 310 (X9.63-Overview), and *id.* at 174, 252 (Nix175). Yet even after considering all of those references, the Examiner determined that independent claim 1 was allowable because “it would not have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the teachings of [the] cited prior art to arrive at the claimed invention.” *Id.* at 139; EX2029 at ¶78.

The Examiner specifically noted differences between the ‘094 claims and one reference: U.S. Printed Patent Application No. 2014/0219447 to Park. EX1004 at 135, 137-139; EX2026. 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* EX2026 with EX1005. For example, that Park patent application teaches “securely provisioning various profiles” for an eUICC (EX2026 at [0011]), while the Park paper teaches a “secure profile

provisioning architecture for eUICCs” (EX1005 at 1). And the examiner explicitly recognized that teaching from that Park patent application, noting it “discloses a method wherein an [mobile network operator] receives a secret key allocated to a corresponding embedded UICC (eUICC) through SM-SR (secure routing) in an environment where [the subscription manager] is divided and implemented as SM-SR and SM-DP (data preparation).” EX1004 at 137; EX2029 at ¶79.

Notwithstanding that (1) independent ‘094 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 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 ‘094 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 "Receiving The Symmetric Key" And Deriving A Profile Key

Claim 1 of the '094 Patent recites a method comprising "receiving the symmetric key" while also deriving a profile key. EX1001 at 80:58, 47. 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 and also *deriving* a profile key. EX2029 at ¶81.

(a) The '094 Patent Requires Both Receiving A Symmetric Key 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 method includes *receiving*—as an incoming transmission from an external entity—a symmetric key. EX1001 at 80:58. 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 sends and the other party *receives*. EX2029 at ¶82. This symmetric key is used to decrypt one part of the eUICC profile. EX1001 at 80:62-64.

Second, claim 1 also separately requires *deriving* a profile key using a key exchange algorithm. EX1001 at 80:47. This profile key is obtained very differently than the symmetric key discussed above; the claim is clear that the profile key is *derived* (*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. EX1001 at 80:59-61.

The ‘094 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 36:63-65 (“the module can receive a symmetric key 127 to decrypt the second key K 204a”); *see also id.* at 6:45-47. Alternatively, the profile key is one that is *derived* using other information according to a key exchange algorithm, such as an elliptic curve Diffie Hellman key exchange. *Id.* at 53:35-54:1. EX2029 at ¶84.

Thus, one important aspect of ‘094 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 using, *e.g.*, 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 mobile device. 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 mobile device 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 mobile device. 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 41-42, 60. 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 41, 60. 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 “deriving 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 34-35. 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 “receiving the 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 key exchange

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, 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 '094 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 '094 claim 1's requirement of "receiving the 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 ¶81. Grounds 1 and 2 should therefore be denied.

2. A POSITA Would Not Have Combined The References As The Petition Proposes

a. A POSITA Would Not Have Combined Park and GlobalPlatform To Both "Receiv[e] The Symmetric Key" And Derive A Profile Key

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.*

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.* at ¶103. 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. *Id.* In this manner, the properly-combined system retains Park's security advantages.

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 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 37-42. 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 22; 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.

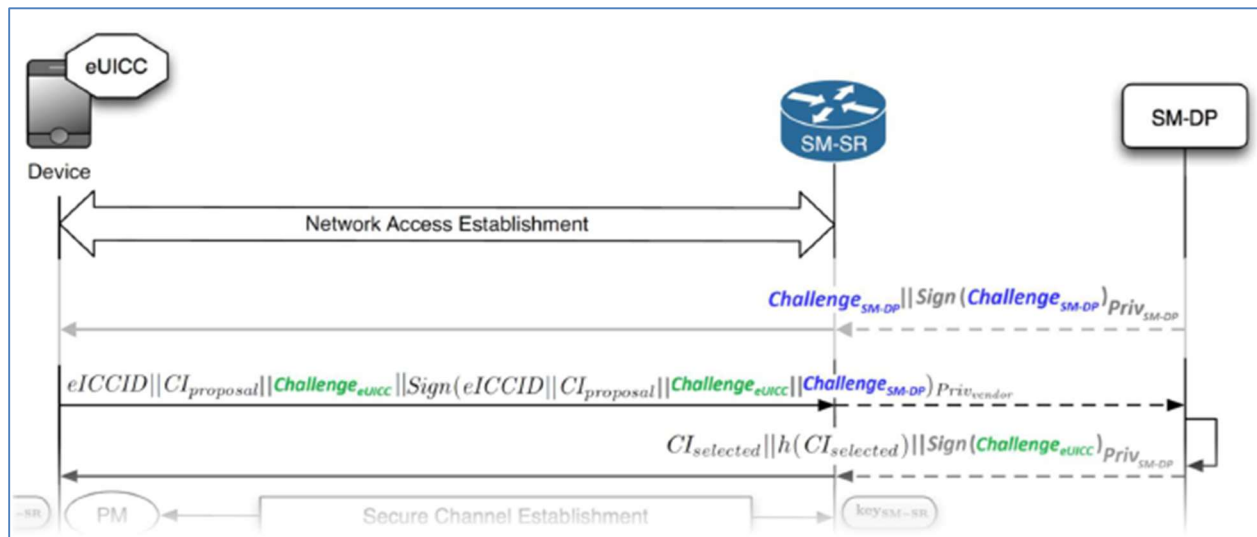
Finally, when combining Park with GlobalPlatform, a POSITA would not have been motivated to obtain just the DEK using the key transport option, while obtaining the other session keys via a different key agreement option. EX2029 at ¶106. Instead, a POSITA would have viewed using two methods of obtaining 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 '094 Patent. *Id.*

b. A POSITA Would Not Have Combined Park And GlobalPlatform To Generate A “First Message Comprising ... A Nonce”

Samsung also argues that a POSITA would have modified Park Figure 4 to include GlobalPlatform's PKI authentication scheme such that the eUICC would generate a message with two nonces. Pet. at 30-32. This was done in hindsight to recreate the claimed “first message comprising ... a nonce.” EX1001 at 80:32-35. But a person of skill would not have combined Park and GlobalPlatform as Samsung suggests. EX2029 at ¶107. Park's PKI authentication scheme is not nonce-based. EX1005 at 4-5. And in light of Park's pre-existing deterministic data authentication,

a POSITA would not have been motivated to include an additional layer of nonce-based authentication (like in GlobalPlatform) that compounds overhead without providing additional utility. EX2029 at ¶107.

More specifically, Samsung modifies Park Figure 4 to include the blue and green “challenges”—neither of which appear in actual Park Figure 4:



Pet. at 31. The above portion of Park Figure 4 illustrates part of the initial capability negotiation between the device and SM-DP. EX2029 at ¶108. Samsung argues that a POSITA would have made this modification to allow for PKI-based authentication between the two entities. However, the existing negotiation exchange in Park already teaches that both entities use PKI; that is, their private keys include and sign deterministic pieces of information ($eICCID$, $CI_{proposal}$, $CI_{selected}$) for various reasons, including to enable authentication. *Id.* In light of Park’s pre-existing PKI based authentication, a POSITA would not have been motivated to include an additional,

redundant layer of signing/authentication that adds to the overhead of authentication, without additional utility. *Id.*

C. Ground 5: The ‘094 Patent Is Entitled To Its Priority Date So Nix175 Is Not Prior Art

Finally, with respect to ground 5 only, Petitioner alleges the ‘094 Patent is not entitled to its priority date because none of the applications to which it claims priority provide written description for two claim limitations. Pet. at 9-10. And, according to the Petition, if the ‘094 Patent is not entitled to its priority date, then the inventor’s own earlier patent, Nix175, becomes prior art. *Id.* Petitioner is wrong. *See* EX2029 at ¶¶110-114.

First, Samsung alleges there is no written description support in the priority applications for the claimed “first eUICC public key” and the claimed “second eUICC public key” because the specification allegedly discloses only one eUICC private/public key pair. Pet. at 9. However, the earliest priority Nix patent application (and all subsequent applications in the chain including the ‘094 application) teaches two key pairs: (i) one pair for generating a digital signature used in authenticating; and (ii) another pair for deriving a profile key used in decryption. EX2029 at ¶111.

The earliest Nix patent application describes the first key pair at, *e.g.*, EX2024 at 82 (77:13) and 83 (78:9) (a first instance of eUICC private key 215 is stored on module 101 within the mobile device and a first instance of eUICC public key 214

is stored on subscription manager 109). This first key pair is used to generate a digital signature that is sent in a first message from the eUICC to the subscription manager. *Id.* at 85 (80:5-10). The subscription manager then uses this digital signature to authenticate the eUICC. *Id.* (80:16-18); EX2029 at ¶112.

The earliest Nix patent application describes the second key pair at, *e.g.*, EX2024 at 89 (84:25-27) (a second instance of eUICC public key 214 and eUICC private key 215). This second key pair is derived using Elliptic Curve Cryptography (ECC) algorithms and a random number generator. *Id.* at 89-90 (84:25-85:3). Then this second key pair is subsequently used with other information to derive a profile key used to decrypt a portion of the eUICC profile. *Id.* at 90 (85:15-20). Thus, because the ‘094 priority applications teach two eUICC public/private key pairs, there is ample written description support for the ‘094 claims. EX2029 at ¶113.

Another Nix patent application no. 14/084,141, which the ‘094 Patent explicitly incorporates by reference (EX1001 at 1:25-30), explicitly discloses both a “first module private key” and a derived “second module private key.” EX2030 at 12:30-13:11. This provides further written description supporting two eUICC public/private key pairs. EX2029 at ¶114.

Second, Samsung alleges there is no written description support in the priority applications for the claimed “receiving a symmetric key” since the claims place no limit on the source of the claimed symmetric key and the claim is broad enough to

encompass receiving it from a subscription manager. Pet. at 9-10. However, according to the Petition, the priority applications only disclose receiving the symmetric key from the mobile network operator. *Id.*

But the earliest priority Nix patent application (and all subsequent applications in the chain including the '094 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 '094 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 '094 Patent is entitled to its earliest December 6, 2013 priority date, and Nix175 is not prior art. Ground 6 must fail.

D. Grounds 3-4: Petitioner’s Art Fails To Present A Reasonable Likelihood of Prevailing Against The Dependent Claims

Grounds 3-4 challenge only a dependent claim of the '094 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 7,889 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.