

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.

IPR2026-00115
Patent 11,606,204

PATENT OWNER'S PRELIMINARY RESPONSE

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. Authentication in Cellular Networks	2
B. The '204 Patent Invention.....	4
C. Effective Filing Date of the '204 Patent	7
D. Level of Ordinary Skill in the Art.....	7
E. Petitioner's References	8
1. Semple [EX1005].....	9
2. Wang [EX1006]	12
III. Claim Construction.....	14
IV. Arguments.....	14
A. Sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity (Claim 1(b)(5), all Grounds).....	15
B. Generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity (Claim 1(b)(4), all Grounds).....	21
C. Secondary considerations show the '204 patent is not obvious.	22
1. The '204 Patent solved a long felt need.....	22
2. The industry has adopted the '204 invention to enable encrypted IMSI transmissions.....	23
V. Conclusion	23

TABLE OF AUTHORITIES

Cases

<i>Tec Air Inc. v. Denso Mfg. Mich., Inc.</i> , 192 F.3d 1353 (Fed. Cir. 1999)	20
---	----

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	<i>Reserved</i>
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	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	U.S. Patent No. 8,391,841
EX2018	Declaration of William B. Collier, Jr. 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
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	Declaration of Dr. Konstantinos Psounis
EX2025	“A Comparative Introduction to 4G and 5G Authentication,” CableLabs, Winter 2019 <i>available at</i> https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication
EX2026	’204 Patent Infringement Contentions from <i>Network-1 Technologies, Inc. v. Samsung Electronics Co., Ltd., et al.</i> , EDTX-2-25-cv-00667 (E.D. Tex. Sept. 30, 2025)
EX2027	Curriculum Vitae of Dr. Konstantinos Psounis

I. Introduction

The invention of the '204 Patent solves a long-felt need in cellular communications: securely identifying and authenticating a mobile device. Prior to the '204 Patent, a mobile device's identity, known as an IMSI, was transmitted "in the clear" and unencrypted. This allowed nefarious actors to intercept the IMSI and potentially identify and track a user.

The invention of the '204 Patent solves this problem by, in part, using an encryption technique known as an elliptic curve integrated encryption scheme in a particular way that allows a mobile device to encrypt and send its IMSI to the cellular network servers before the mobile device is authenticated with the network.

Petitioner's references do not use this method. Petitioner's primary reference, Semple still transmits the IMSI in the clear, and does not describe sending encrypted data in conjunction with a module public key. Wang, which the Petition only uses to argue that Semple could be modified to send the IMSI encrypted, does not use the claimed encryption scheme or keys, instead using a different scheme to encrypt the IMSI. Wang likewise does not suggest sending encrypted data in conjunction with a module public key.

Recognizing that the art does not describe the claims of the '204 Patent, Petitioner, and its expert in a declaration that simply mirror's the language from the Petition, asserts a theory that completely rewrites the security scheme's described

by both of its primary prior art references in a way that can only be explained by hindsight. Petitioner's modifications to these systems weaken their existing security features and fail to improve those systems. This improper argument cannot show a reasonable likelihood that the claims of the '204 Patent are obvious.

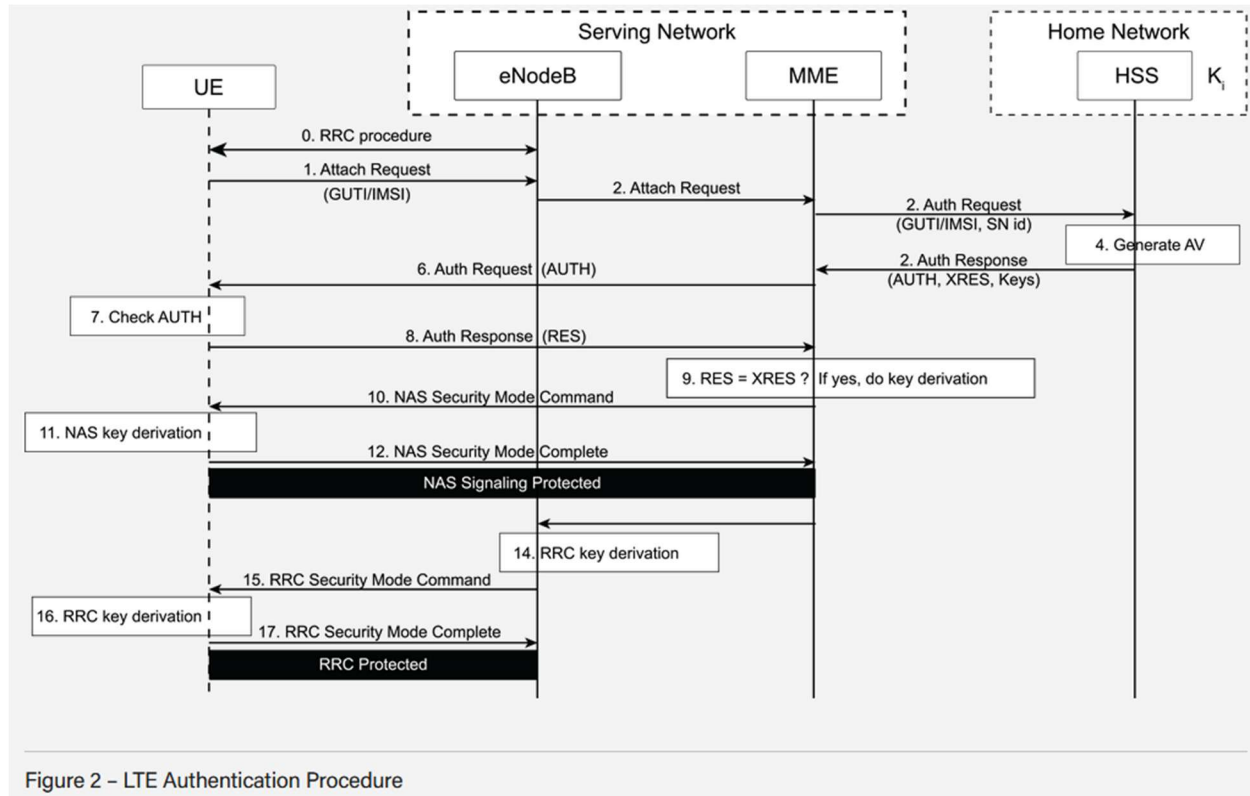
II. Background

A. Authentication in Cellular Networks

Securely authenticating devices and users in a cellular network has always been a challenge. EX2024 ¶¶30-32. Any such system must be able to authenticate a device and allow access to the network. *Id.* ¶¶30-31. One solution, employed in older versions of the cellular standard promulgated by the likes of the ETSI and 3GPP, primarily relied on two pieces of information: a key K and an international mobile subscriber identity ("IMSI"). *Id.* The key K is a secret key used to derive the keys used by the various security functions in mobile networking. *Id.* The key K is historically provided to the mobile device on its SIM card. *Id.* ¶31. Each mobile device has a unique key K that is also known to the device's home network. *Id.* ¶30. In a secure environment, no other devices or entities know this key K. *Id.* The IMSI is a number that uniquely identifies a user of a cellular network. *Id.* ¶30. Like the key K, the IMSI was historically assigned via the SIM card. *Id.*

At the home network, each IMSI is associated with a particular key K. *Id.* ¶30. This association is used in cellular networks to authenticate mobile devices. *Id.* ¶32.

One way to do this is a technique called EPS-AKA used in 4G cellular systems. This approach is illustrated below:



EX2025, 5. In the EAP-AKA procedure, a mobile device attempting to connect to a network first completes the “Radio Resource Control” (“RRC” above) procedure, following which the mobile device sends the “Attach Request.” *Id.*, 4-5 This request includes the device’s IMSI and is forwarded to the device’s Home Network. *Id.*, 4. Using the IMSI, the Home Network identifies the corresponding shared secret key (indicated as K_i in the home network, above). *Id.* Using that key, the Home Network can generate an expected response token, or XRES and an authentication token, or AUTH. *Id.* The AUTH is forwarded to the mobile device, which compares it to its

own token based on Ki to authenticate the network. *Id.*, 5. If the network appears to be authentic, the mobile device generates a response token, or RES, based on Ki and transmits RES back to the network. *Id.* If RES is equal to XRES, then further security keys are generated for future secure transmissions, and the mobile device is allowed access to the network. *Id.*

It had long been recognized that this process was vulnerable to attack because the IMSI was sent in the clear, without encryption. *Id.*, 6; EX2024 ¶32. This allowed nefarious actors to intercept the IMSI to various ends. EX2024 ¶32; EX2025, 6. The inventor of the '204 Patent recognized this problem in existing authentication practice and sought to solve it. EX2024 ¶33; EX1001, 2:48-4:32.

B. The '204 Patent Invention

The '204 Patent is titled “Systems and methods for ‘machine-to-machine’ (M2M) communications between modules, servers, and an application using public key infrastructure (PKI).” EX1001, cover. It was invented by John A. Nix. The '204 Patent was filed on January 12, 2022, and claims priority through a chain of five continuation applications to October 16, 2013. *Id.* cover, page 2. The '204 Patent issued on March 14, 2023. *Id.*

As noted above, the inventor of the '204 Patent recognized a need in the art for better security in wireless network communications. *Id.*, 2:48-4:32. One solution is to “leverage established public key infrastructure (PKI) techniques and

algorithms” in cellular networks. *Id.*, 2:54-56. But, doing so presented a number of technical challenges. *Id.*, 3:51-53; *see id.*, 3:53-4:8. The inventor of the ’204 Patent sought to address these challenges. *Id.*, 4:43-48.

The claimed invention of the ’204 Patent describes a mobile device with certain capabilities that enable the mobile device to complete an authentication process with a mobile network without revealing its IMSI. *Id.*, 100:31-67 (claim 1). These capabilities include storing a public key for a server of the mobile network on the mobile device, in addition to storing the IMSI and key K. *Id.*, 100:40-45. The device can then derive its own public key and private key. *Id.*, 100:46-48. The private key can be used in conjunction with the server public key to derive a symmetric ciphering key. *Id.*, 100:49-53. Using that symmetric ciphering key, the mobile device can generate module encrypted data that includes the IMSI. *Id.*, 100:54-57. The mobile device then sends an encrypted message to a server for a wireless network that includes the IMSI, in addition to the mobile device’s public key. *Id.*, 100:58-65. The device can authenticate itself with the mobile network using a message digest. *Id.*, 100:66-67.

These capabilities are reflected in claim 1, the only independent claim of the ’204 Patent:

1. A mobile device comprising:
 - (a) at least one processor; and

(b) at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:

- (1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;
- (2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;
- (3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;
- (4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;

- (5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and
- (6) authenticating with the wireless network using a message digest with the pre-shared secret key.

Id., 100:31-67 (claim 1).

C. Effective Filing Date of the '204 Patent

The '204 Patent claims priority to October 16, 2013, through a chain of five continuation applications. *Id.*, cover. Petitioner does not dispute that the priority date of the '204 Patent is October 16, 2013. Pet., 7.

D. Level of Ordinary Skill in the Art

For purposes of this Preliminary Response, Patent Owner does not contest Petitioner's recitation of the level of skill in the art, because even under Petitioner's proposed level of skill (Pet., 7), Petitioner has failed to demonstrate a reasonable likelihood of success. Patent Owner reserves the right to propose its own definition of a person of ordinary skill in the art in the future if necessary.

E. Petitioner's References

Petitioner asserts eight grounds of invalidity based on combinations of six references: (1) Semple; (2) Wang; (3) SEC1; (4) Bhuyan; (5) Pierce; and (6) Jorgensen. Pet., 3–4. All eight grounds rely on Semple as the primary reference combined with Wang. Grounds 5–8 add SEC1 as an additional reference but are otherwise identical to Grounds 1–4.

Ground	Claims	Statute	References
1	1–7, 9, 11–12, 14–16, 18–20	§ 103	Semple and Wang
2	5 and 8	§ 103	Semple, Wang, and Bhuyan
3	10	§ 103	Semple, Wang, and Pierce
4	13, 17, and 18	§ 102	Semple, Wang, and Jorgensen
5	1–7, 9, 11–12, 14–16, 18–20	§ 103	Semple, Wang, and SEC1
6	5 and 8	§ 103	Semple, Wang, SEC1, and Bhuyan
7	10	§ 103	Semple, Wang, SEC1, and Pierce
8	13, 17, and 18	§ 103	Semple, Wang, SEC1, and Jorgensen

Pet., 3–4.¹

¹ For the purposes of this preliminary response, Patent Owner has addressed independent Claim 1 because Petitioner has failed to demonstrate a reasonable

1. Semple [EX1005]

Semple is U.S. Patent Publication No. 2010/0174907, titled “Secure bootstrapping for wireless communications.” EX1005, cover. Semple describes a method of authenticating users in a cellular network that is similar to the methods used prior to the invention of the ’204 Patent. Specifically, Petitioner focuses on Semple’s Figure 6 and related discussion:

likelihood of success of showing unpatentability of that claim (and therefore dependent Claims 2-20 as well). If trial is instituted, then Patent Owner reserves the right to further address the deficiencies in Petitioner’s theories, including deficiencies regarding the dependent claims.

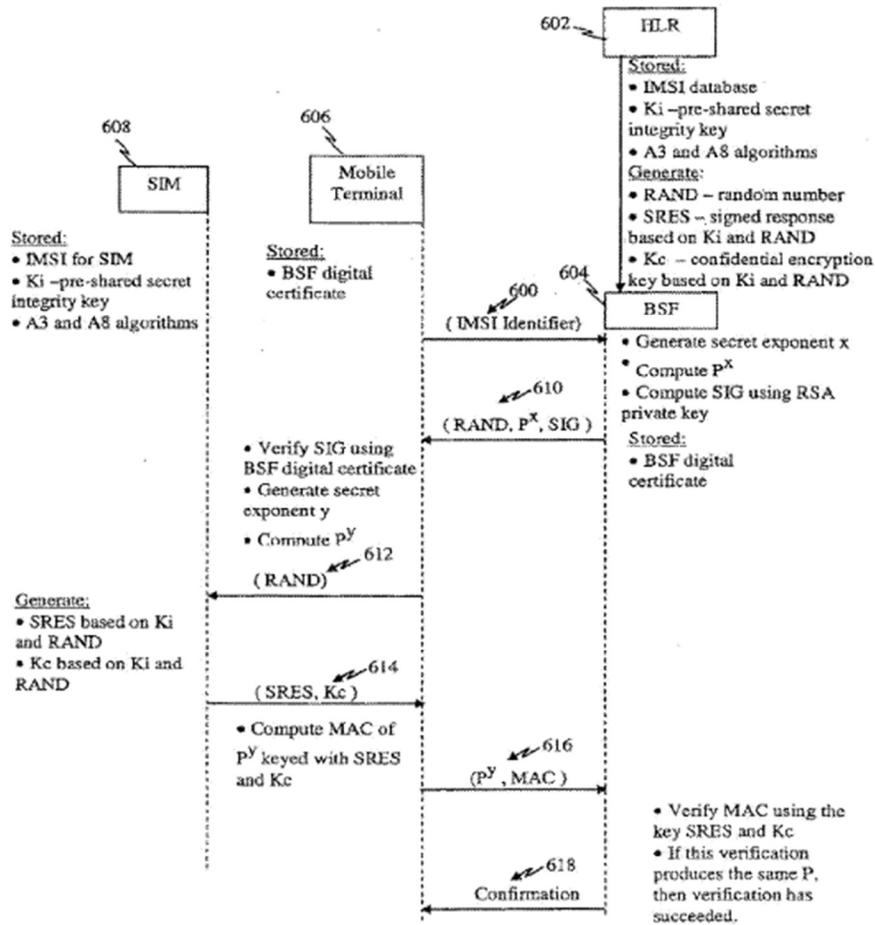


Figure 6

EX1005, Fig. 6; Pet. 8-10. Figure 6 illustrates the interaction of four components: 1) the SIM on the mobile terminal (608); 2) the mobile terminal, itself (606); 3) a bootstrapping server function (BSF), part of the mobile devices home network (604); and 4) the home local register (HLR), also part of the mobile device's home network (602). EX1005 ¶¶24-26, 47. As with the EAP-AKA, Semples begins with the mobile device transmitting its IMSI, in the clear, to the HLR in step 600. *Id.* ¶48. Upon receiving the IMSI, the HLR will identify the key Ki that corresponds to that IMSI. *Id.* Using Ki and a random challenge, RAND, the HLR will generate a signed

response, or SRES. *Id.* This information is provided to the BSF, which generates a public key for itself (Px). *Id.* The BSF then computes a digital signature (SIG) using Px, and sends RAND, Px, and SIG to the mobile terminal. *Id.*

Using this information, the mobile terminal verifies SIG and computes its own key Py. *Id.* ¶49. The mobile terminal also passes RAND to the SIM which computes and returns SRES and Kc based on RAND and Ki. *Id.* The mobile terminal uses this information to generate a message authentication code (MAC) of Py keyed with SRES and Kc and sends a response containing Py and MAC to the BSF. *Id.* The BSF then receives this message and verifies the MAC using the SRES and Kc it previously obtained from the HLR. *Id.* ¶50.

Using this technique, both the mobile terminal and the BSF can mutually authenticate each other, as neither could generate a matching SRES without the correct key Ki. *Id.* ¶50-51. The mobile terminal and BSF can also generate a mutual key Pxy, which can be used in further communications between the two devices. *Id.* ¶51.

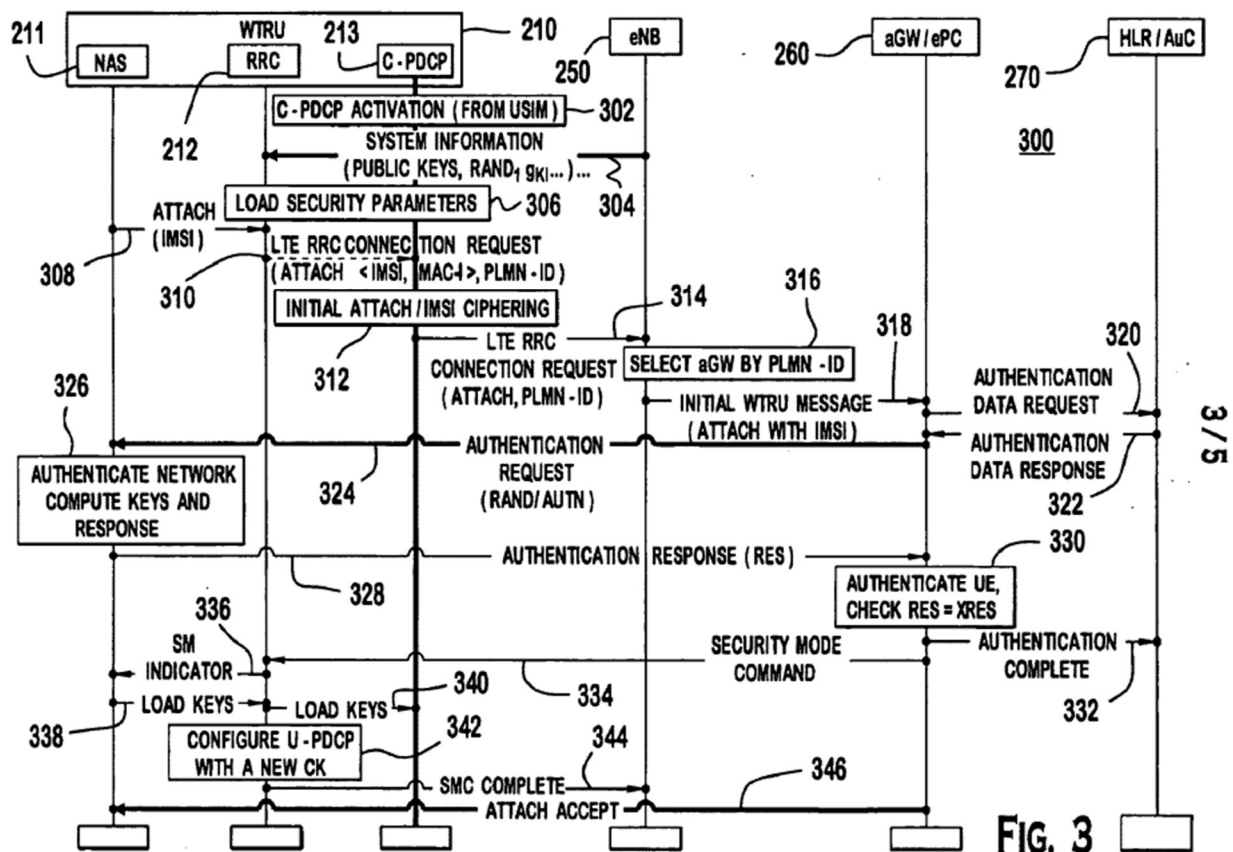
Unlike the invention of the '204 Patent, Semple requires that the IMSI be sent in the clear. Without doing so, Semple's HLR cannot identify the correct key Ki corresponding to the mobile device. There is no teaching in Semple that would allow the IMSI to be sent encrypted during the authentication process. Indeed, no encrypted information is exchanged during that process.

2. Wang [EX1006]

Wang is International Publication Number WO 2008/005162 titled “Method and apparatus for security protection of an original user identity in an initial signaling message.” EX1006, cover.

Wang recognized the need to encrypt the IMSI in cellular communication. *Id.* ¶5. To solve this problem, Wang describes a control-plane packet data convergence protocol (“C-PDCP”) layer in a mobile device (the “WTRU”) that performs ciphering and integrity protection of initial signaling messages. *Id.* ¶¶15, 28.

The Petition focuses on Wang’s process as illustrated in Figure 3:



Id., Fig. 3. Upon WTRU power-up, the C-PDCP layer is activated (step 302) and receives security parameters from the USIM and system information broadcast by the eNode-B (“eNB”) of the network, which includes public keys or key derivation information and random numbers (step 304). *Id.* ¶¶15, 29. Initial security parameters, including a ciphering key (CK) and an integrity key (IK), are then loaded into the C-PDCP layer (step 306), drawn from the USIM and/or derived from the broadcast system information. *Id.* ¶30. The CK may be a public key selected from a broadcast public key set, enabling asymmetric encryption of the IMSI even before any mutual authentication has occurred. *Id.* ¶30.

Next, the NAS layer of the WTRU triggers an RRC connection by sending an ATTACH message with the IMSI to the RRC layer (step 308), which forwards the message along with a MAC-I to the C-PDCP layer (step 310). *Id.* ¶31. The C-PDCP layer ciphers the attach message and the IMSI using the initial CK and sends the ciphered LTE RRC connection request to the eNB (steps 312, 314). *Id.* ¶31. The eNB selects an appropriate access gateway (aGW) based on the PLMN ID (step 316) and forwards the ciphered attach message with the IMSI to the aGW (step 318). *Id.* ¶32. Following the initial ciphered connection is an AKA authentication procedure, which authenticates the WTRU and eNB to each other. *Id.* ¶¶33-36.

Unlike the '204 Patent, Wang's encryption of the IMSI relies on a pre-existing ciphering key CK that is either pre-stored on the USIM or derived from system

information broadcast by the network. *Id.* ¶¶15, 31. Wang does not teach encrypting the IMSI with a key derived from an elliptic curve integrated encryption scheme. Instead, Wang's CK is generated from the pre-shared secret key K and a random value through the conventional 3GPP AKA mechanism. EX1006 ¶¶47–48, Fig. 6.

III. Claim Construction

Petitioner contends that no terms require construction. Pet., 8. For the purposes of this preliminary response, Patent Owner agrees.

IV. Arguments

In each of Petitioner's grounds, Petitioner has failed to show a reasonable likelihood that its proposed combinations teach or disclose the independent claim of the '204 Patent. Accordingly, institution should be denied.

The Petition fails on a fundamental level: each of Petitioner's references are old techniques with failings that the invention of the '204 Patent solves. Semple *requires* that the IMSI be transmitted in the clear and unencrypted, compromising privacy of the IMSI. Petitioner contends that this could be fixed simply by importing Wang's teaching that encrypts an IMSI in a transmission and includes a MAC-I. But, Semple's system does not teach sending encrypted data *at all* during the authentication process, and Petitioner's proposed combination fails to address the fact that this new method is less secure than Semple's teachings. This combination is conjured from hindsight and relies on a fundamental re-design of the security

systems of both Semple and Wang. Unsurprisingly, this combination fails to teach several elements of claim 1 of the '204 Patent.

- A. Sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity (Claim 1(b)(5), all Grounds).**

Element 1(b)(5) requires that the mobile device is capable of “sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key....” As noted above, “the module encrypted data includes the module identity.” The Petition recognizes that this element is not disclosed by Semple. Instead, Petitioner proposes that a POSITA would modify Semple to “encrypt IMSI, as taught by Wang, rather than sending it in the clear....” Pet. 35. Petitioner reasons that “Wang discloses preparing encrypted module data that includes the IMSI, and the encryption would be performed using the symmetric ciphering key in the combined Semple-Wang system.” Pet. 36. For the reasons explained below, the Petitioner fails to show a reasonable likelihood that Semple in view of Wang renders this claim obvious, because neither Semple or Wang describe a “sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key.”

Throughout the Petition, and in reference to element 1(b)(5), Petitioner relies on Semple’s figure 6, which is described above in section II.E.1:

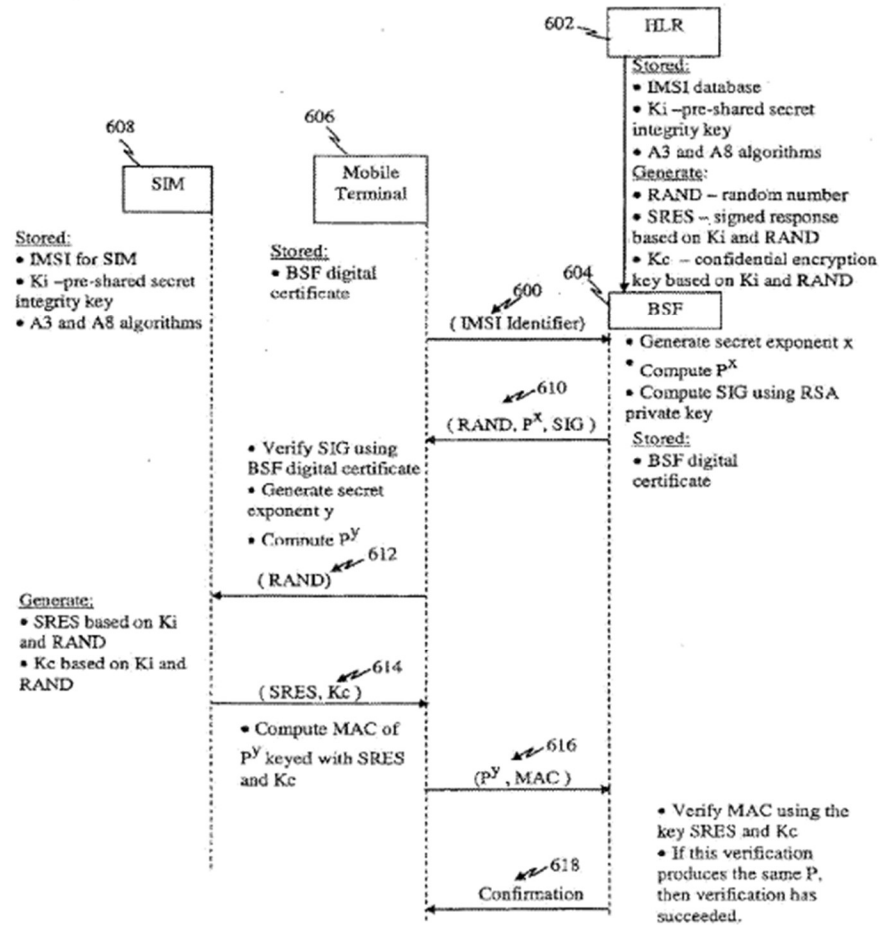


Figure 6

EX1005, Fig. 6; *see* Pet. 36. As illustrated here, Semple describes sending the IMSI from a mobile terminal to a BSF in a first step 600. EX1005, Fig. 6, ¶48. Later, in step 616, Semple transmits a message 616 that includes a public key P^y and a MAC. *Id.* Fig. 6, ¶49. As noted above, Semple never transmits any encrypted data during this process. EX2024 ¶39. In fact, the shared keys required to do so are not generated until the end of this process. EX1005 ¶¶50-51.

Neither Semple nor Wang disclose transmitting an encrypted IMSI with a public module key. EX2024 ¶¶39, 47. *See* Pet. 35 (“Semple by itself describes the

MT sending the IMSI before doing the Diffie-Hellman exchange....”). In fact, neither disclose transmitting even an unencrypted IMSI with a module public key. EX2024 ¶¶47. Recognizing this, Petitioner contends that Semple’s process could be completely re-organized to eliminate step 600 and instead include an encrypted IMSI in step 616. Pet, 35, 37. This modified Semple-Wang system is illustrated by Petitioner annotated version of Semple’s figure 6:

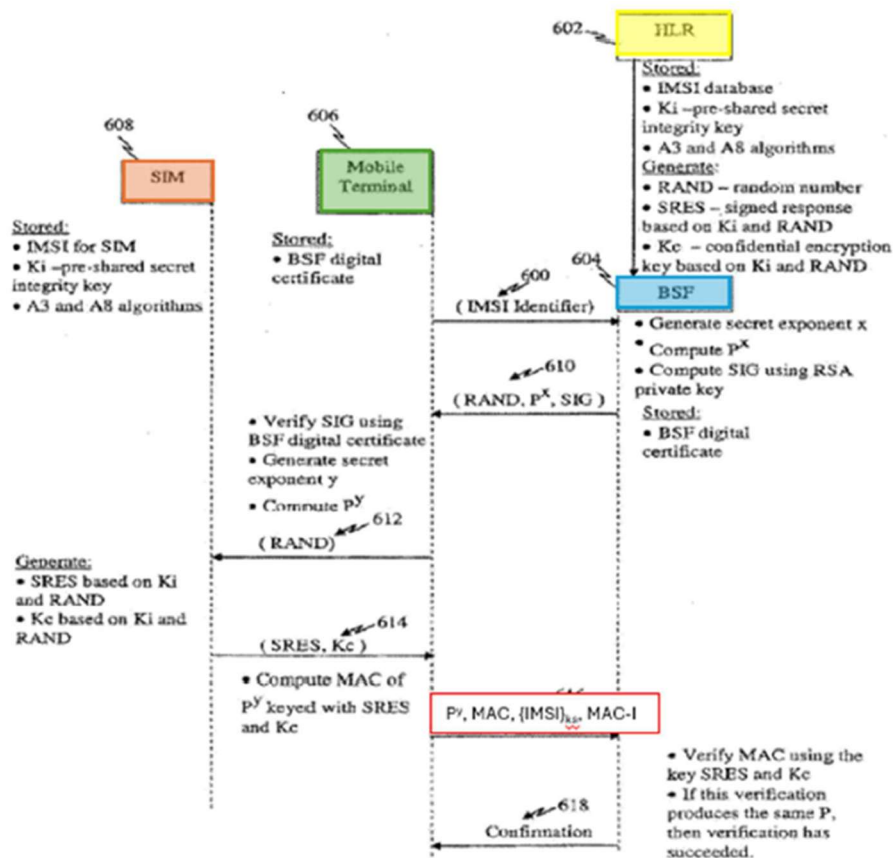


Figure 6

Pet. 39. But, there is no support in Semple or Wang to completely re-work Semple’s security techniques, as Petitioner proposes. EX2024 ¶¶40, 47-48; *see also id.* ¶¶37-57.

The proposed modification moves the IMSI transmission from an initial connection request to the authentication step. Pet. 39, EX2024 ¶¶40-41. Neither Semple nor Wang teach or suggest this change. EX2024 ¶¶42-43. Instead, both teach away from it by requiring their systems to first receive an IMSI before beginning the authentication. *Id.* ¶¶43-47. In Semple, the IMSI is first verified as having a valid subscription to the network before the parameters for authentication are generated and transmitted. *Id.* ¶¶43, 49. In Wang, the authentication vectors cannot be generated without first identifying the IMSI. *Id.* ¶¶43-44, 50.

Moreover, Semple never suggests transmitting any encrypted data during the process of figure 6. Ex2024 ¶49. Instead, each message is sent in the clear, and other than the original IMSI, only contains keys, MACs, and other values used for various security functions, as opposed to any encrypted data and certainly not any data encrypted with an ECIES derived key. *See* EX1025 ¶¶48-50. To the extent Semple does envision transmitting encrypted data, it is only *after* the figure 6 process is complete. EX1025 ¶51; EX2024 ¶38. And as explained further below, sending the IMSI immediately before receiving the RAND, Px, and SIG provides security benefits that Petitioner's proposed changes eliminate. EX2024 ¶¶49, 51-55.

Wang also does not support this modification, which is why the Petition only relies on Wang for the idea of an encrypted IMSI sent with a MAC-I. Pet. at 37. Like Semple, Wang also sends its IMSI *prior to* the authentication request message

containing RAND and AUTN and cannot generate the AUTN without first receiving the IMSI and identifying the corresponding keys. EX1026 ¶¶33-34; EX2024 ¶50.

The Petition glosses over these issues by arguing that sending the IMSI prior to the key exchange “is not necessary since computing x and P_x does not depend on the IMSI or the pre-shared key associated with it.” Pet. 35. This is wrong. In fact, a POSITA would not implement this modification because the change to Semple reduces security of the system. EX2024 ¶48, 57; *see also id.* ¶¶49-56.

Semple’s system relies on the short, sequential timing of its transmissions to prevent attacks on its transmissions. EX1005 ¶53; EX2024 ¶52-53. For example, broadcasting message 610 to any device provides time for nefarious actors to attack the keys used in Semple and attack the security of the BSF. EX1005 ¶53; EX2024 ¶¶52-53. Semple itself recognizes this problem and suggests both that RAND is fresh with each use and that response 616 is received a short time after message 610 is sent. EX1005 ¶53; EX2024 ¶¶52-53. But, this is not guaranteed when message 610 is broadcast to all devices. EX2024 ¶53. The modified system also increases the risk to the terminal device of a compromised BSF, because the mobile device cannot rely on the security of the HLR to ensure it is communicating with its home network. EX2024 ¶54.

Semple’s original design reduces these security risks. EX2024 ¶55. In Semple, the mobile terminal can rely on the fact that the BSF will not transmit message 610

unless it receives an IMSI and identifies a corresponding Ki. *Id.*; EX1005 ¶48. Since RAND, Px, and SIG are computed only in response to message 600, an interloper may still intercept message 610, but the mobile device and network can rely on the short timing of the transmissions to ensure security. EX2024 ¶52, 55; EX1005 ¶53.

Highlighting this, Wang follows a similar approach, sending its IMSI in step 312 before receiving the authentication request message containing RAND and the authentication token in step 324. EX1006 ¶31-34. This allows the WTRU to authenticate the network in step 326. *Id.* ¶34.

Thus, Petitioner's proposal to shoe-horn an IMSI into Semple's message 616 is nothing more than hindsight. EX2024 ¶¶47, 56. The proposed modification reduces the security of both Semple and Wang, and a POSITA would never make that mistake. *See, e.g., Tec Air Inc. v. Denso Mfg. Mich., Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999) (no motivation to make a combination that would render device inoperable for its intended purpose). The actual security systems described by these references teach away from Petitioner's proposed modification for this very reason. In short, the Petition fails to show that Semple and Wang render obvious "a message comprising the module encrypted data and the module public key" under any standard. EX2024 ¶57.

B. Generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity (Claim 1(b)(4), all Grounds).

Element 1(b)(4) requires that the mobile device is able to generate “module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity.” The Petition recognizes that the Semple does not teach encrypted data that includes the module identity. *See* Pet. 32-34. Instead, Petitioner contends that Wang’s encrypted IMSI could be inserted into Semple’s step 616 further using Semple’s key Pxy as an encryption key. *Id.*, 33-34. But this combination fails for a fundamental reason: neither Simple nor Wang teaches encrypting the IMSI using a symmetric ciphering key. EX2024 ¶39. In fact, Semple never suggests encrypting any data during the process illustrated by its Figure 6. *See* EX1005 ¶¶48-53. On the other hand, Wang only teaches encrypting the IMSI with a cipher key (“CK”), which is a public key. EX1006 Abstract, ¶¶15, 29, 38, and 81.

As explained above in section II.E.1, Semple’s figure 6 depicts an authentication process between a mobile device and a mobile network. EX1005, Fig. 6. At the end of this process, both the mobile device and the mobile network will be able to confirm the identity of the other and both will have generated a Pxy key to use in future encryption. *Id.* ¶¶50-51. But, importantly, Semple never suggests transmitting any encrypted data during this process. *See id.* ¶¶48-51. While Semple

posits that its Pxy may be used to generate “a key for further communications,” Semple never actually describes encrypting any data with Pxy, much less encrypting any data during the authentication process which generates Pxy. *Id.* ¶51.

Petitioner’s combination with Wang does not solve this problem. As Petitioner recognizes, Wang does not teach encrypting the IMSI with a symmetric cyphering key. *See* Pet. 33. Instead, Petitioner relies on hindsight to re-construct the claims of the ’204 Patent from thin air, as discussed *supra* section IV.A. This modification is nothing more than hindsight and cannot overcome the fact that neither reference teaches encrypting the module identity using a symmetric cyphering key. EX2024 ¶¶47, 56.

C. Secondary considerations show the ’204 patent is not obvious.

Secondary considerations support the conclusion that the ’204 Patent is not obvious. As explained below, the invention of the ’204 Patent solved a long-felt need and has subsequently been copied by the telecommunications industry.

1. The ’204 Patent solved a long felt need.

The need to securely transmit the IMSI was a long recognized problem in cellular communications that existed well into the 4G and LTE versions of cellular communications standards. EX2025, 1-6; EX2024 ¶58. Other techniques exist to provide some protection to the IMSI, such as the use of GUTI, but even those techniques did not fully protect the IMSI. *Id.*, 6.

The '204 Patent solves this problem. EX2024 ¶59. The claimed invention allows an IMSI to be encrypted during all communications, while also reliably authenticating the mobile device to the network, and vice versa. *Id.* As illustrated by the Petitioner's reliance only on obviousness combinations, this solution did not exist in the art prior to the invention of the '204 Patent. *Id.*

2. The industry has adopted the '204 invention to enable encrypted IMSI transmissions.

Petitioner and others in the industry have adopted the invention of the '204 Patent to provide security to the IMSI. *See generally* EX2026. The invention of the '204 Patent is now implemented in the latest 5G standard promulgated by ETSI and 3GPP. *Id.* These standards describe two authentication procedures, EAP-AKA' and 5G AKA, which encrypt and transmit the IMSI using ECIES encryption and authenticate the mobile device using the claimed invention of the '204 Patent. *Id.*

These factors re-enforce the non-obviousness of the '204 Patent. Despite Petitioner's arguments to the contrary, POSITAs long desired to find acceptable solutions to encrypt the IMSI yet failed to do so prior to the invention of the '204 Patent. After its invention, the techniques claimed by the '204 Patent were widely adopted by the cellular community. The Petitioner's arguments cannot overcome these factors.

V. Conclusion

In all the asserted grounds, Petitioner's proposed combination of Semple and

Wang fails to teach or suggest elements 1(b)(4) and 1(b)(5) of the only independent claim, claim 1. And POSITA would never combine Semple with Wang as proposed by Petitioner in the first place. For these and all of the reasons discussed above, Patent Owner respectfully requests that the Director decline to institute *inter partes* review of the '204 Patent.

Dated: February 20, 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, and exhibits, if any**, were 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: February 20, 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 4594 words as calculated by Microsoft Word, excluding the items exempted under 37 C.F.R. § 42.24.

Dated: February 20, 2026

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