UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

HEADWATER RESEARCH LLC
Patent Owner

Case No. IPR2026-00441
Patent 11,966,464

DECLARATION OF DAVID H. WILLIAMS IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,966,464

AMAZONG-1006
IPR2026-00471

TABLE OF CONTENTS

Page

I. BACKGROUND AND QUALIFICATIONS 1

III. RELEVANT LEGAL STANDARDS 4

A. Claim Interpretation 5

B. Perspective of One of Ordinary Skill in the Art 6

C. Anticipation 6

D. Obviousness 7

IV. SUMMARY OF OPINIONS 9

V. TECHNOLOGY BACKGROUND 10

VI. THE CHALLENGED ’464 PATENT 11

VII. THE ’464 PATENT PROSECUTION HISTORY 11

VIII. LEVEL OF ORDINARY SKILL IN THE ART 13

IX. CLAIM CONSTRUCTION 14

X. OVERVIEW OF THE PRIOR ART REFERENCES 15

A. Khosravi (EX1004) 15

B. Xu (EX1005) 19

C. Frank (EX1022) 19

XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS 20

A. Claims 1, 7-11, and 17-20 Are Rendered Obvious Over Khosravi (EX1004) Alone and/or in View of Xu (EX1005) (Ground 1) 20

1. Claim 1 (Preamble): "A method of operating a wireless end-user device having a secure modem, a secure execution environment and a secure memory partition, the method comprising:" 21

   a. [1.1]: "establishing a connection between the secure modem and a wireless network;" 27

   b. [1.2]: "establishing, through the connection, a secure control channel between the secure execution environment and a network service controller;" 30

   c. [1.3]: "receiving, at the secure execution environment, via the secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more settings;" 34

   d. [1.4]: "storing the one or more settings in the secure memory partition accessible only from the secure execution environment; and" 38

   e. [1.5]: "controlling the wireless end-user device using the one or more settings." 48

2. Claim 7: "The method of claim 1 , wherein the one or more settings include at least one of an access control setting, a traffic control setting, or an admission control setting." 50

3. Claim 8: "The method of claim 1, wherein the one or more settings include a network setting or a device management communication setting." 51

4. Claim 9: "The method of claim 1, wherein the secure execution environment is implemented at least in part as a hardware partition or a software partition." 52

5. Claim 10: "The method of claim 1, wherein the secure execution environment is implemented at least in part in a virtual machine." 53

6. Claim 11 (Preamble): "A wireless end-user device comprising: a secure modem; a secure execution environment; a secure memory partition; and a processor configured to:" 54

   a. [11.1]: "establish a connection between the secure modem and a wireless network;" 56

   b. [11.2]: "establish, through the connection, a secure control channel between the secure execution environment and a network service controller;" 57

   c. [11.3]: "receive, at the secure execution environment, via the secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more settings;" 58

   d. [11.4]: "store the one or more settings in the secure memory partition accessible only from the secure execution environment; and" 59

   e. [11.5]: "control the wireless end-user device using the one or more settings." 60

7. Claim 17: "The wireless end-user device of claim 11, wherein the one or more settings include at least one of an access control setting, a traffic control setting, or an admission control setting." 61

8. Claim 18: "The wireless end-user device of claim 11, wherein the one or more settings include a network setting or a device management communication setting." 61

9. Claim 19: "The wireless end-user device of claim 11, wherein the secure execution environment is

implemented at least in part as a hardware partition or a software partition.” 61

10. Claim 20: “The wireless end-user device of claim 11, wherein the secure execution environment is implemented at least in part in a virtual machine.” 62

B. Claims 2-6 and 12-16 Are Rendered Obvious Over Khosravi in View of Xu and Frank (Ground 2) 62

1. Claim 2: “The method of claim 1, wherein the one or more settings are associated with a service plan for using a service provided by the wireless network.” 62

2. Claim 3: “The method of claim 1, wherein the secure modem further comprises a modem agent accessible only by the network service controller through another secure control channel.” 69

3. Claim 4: “The method of claim 3, wherein the modem agent comprises a service measurement point for use of a service.” 77

4. Claim 5: “The method of claim 4, further comprising: communicating, by the modem agent through the another secure control channel, a first report of the use of the service to the network service controller.” 78

5. Claim 6: “The method of claim 5, further comprising: communicating, using the secure execution environment through the secure control channel, a second report of the use of the service.” 80

6. Claim 12: “The wireless end-user device of claim 11, wherein the one or more settings are associated with a service plan for using a service provided by the wireless network.” 81

7. Claim 13: “The wireless end-user device of claim 11, wherein the secure modem further comprises a modem

agent accessible only by the network service controller through another secure control channel." 82

8. Claim 14: "The wireless end-user device of claim 13, wherein the modem agent comprises a service measurement point for use of a service." 82

9. Claim 15: "The wireless end-user device of claim 14, wherein the processor is further configured to: communicate, by the modem agent through the another secure control channel, a first report of the use of the service to the network service controller." 82

10. Claim 16: "The wireless end-user device of claim 15, wherein the processor is further configured to: communicate, using the secure execution environment through the secure control channel, a second report of the use of the service." 82

XII. SECONDARY CONSIDERATIONS 83

XIII. CONCLUSION.....84

Exhibit No.	**Description**
1001	U.S. Patent No. 11,966,464, issued April 23, 2024 to G. Raleigh ("'464 Patent")
1002	File History of U.S. Patent Application No. 17/867,585 through September 22, 2025
1003	U.S. Provisional Application No. 61/206,354, filed January 28, 2009
1004	U.S. Patent Application Publication No. 2007/0234402, published October 4, 2007 to H. Khosravi *et al.* ("Khosravi")
1005	U.S. Patent Application Publication No. 2007/0061535, published March 15, 2007 to Z. Xu *et al.* ("Xu")
1007	*Curriculum Vitae* of David Williams
1008	U.S. Patent No. 10,694,385, issued June 23, 2020 to G. Raleigh
1009	File History of U.S. Patent Application No. 16/034,362
1011	U.S. Patent No. 6,075,784, issued June 13, 2000 to Frankel *et al.* ("Frankel")
1012	U.S. Patent Publication No. 2001/0053210, published December 20, 2001 to H. Kwon ("Kwon")
1013	U.S. Patent No. 5,999,826, issued December 7, 1999 to N. Whinnett ("Whinnett")
1014	U.S. Patent No. 5,828,663, issued October 27, 1998 to Y. Ikegami ("Ikegami")
1015	U.S. Patent No. 6,931,659, issued August 16, 2005 to H. Kinemura ("Kinemura")
1016	U.S. Patent Publication No. 2007/0123172, published May 31, 2007 to C. Khawand *et al.* ("Khawand")

Exhibit No.	Description
1017	U.S. Patent Publication No. 2005/0079889, published April 14, 2005 to J. Vaglica *et al.* ("Vaglica")
1018	U.S. Patent Publication No. 2007/0269041, published November 22, 2007 to R. Bhatnagar *et al.* ("Bhatnagar")
1019	U.S. Patent Publication No. 2002/0071477, published June 13, 2002 to P. Orava ("Orava")
1020	U.S. Patent Publication No. 2002/0187780, published December 12, 2002 to S. Souissi ("Souissi")
1021	U.S. Patent Publication No. 2005/0123025, published June 9, 2005 to D. Sorrells *et al.* ("Sorrells")
1022	U.S. Patent Publication No. 2006/0165005, published July 27, 2006 to A. Frank *et al.* ("Frank")
1023	Defendant Google LLC's Opening Claim Construction Brief, filed May 13, 2026 in *Headwater Research LLC v. Google LLC*, Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1024	Plaintiff Headwater Research LLC's Responsive Claim Construction Brief, filed June 8, 2026 in *Headwater Research LLC v. Google LLC*, Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1025	Defendant Google LLC's Reply to Plaintiff's Responsive Claim Construction Brief, filed June 22, 2026 in *Headwater Research LLC v. Google LLC*, Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1026	Plaintiff Headwater Research LLC's Sur-Reply to Defendant's Reply to Plaintiff's Responsive Claim Construction Brief, filed July 7, 2026 in *Headwater Research LLC v. Google LLC*, Civ. Action No. 7:25-cv-00369 (W.D. Tex.)

Exhibit No.	**Description**
1027	Joint Claim Construction Statement, filed July 10, 2026 in *Headwater Research LLC v. Google LLC*, Civ. Action No. 7:25-cv-00369 (W.D. Tex.)
1028	U.S. Patent No. 11,405,429, issued August 2, 2022 to G. Raleigh ("'429 Patent")
1029	File History of U.S. Patent Application No. 16/907,887 through September 22, 2025

I, David H. Williams, hereby state as follows:

1. I have been retained by GOOGLE LLC ("Petitioner") as an independent expert consultant in this *inter partes* review ("IPR") proceeding before the United States Patent and Trademark Office ("PTO").

2. I have been asked by Counsel for Petitioner ("Counsel") to consider whether certain references teach or suggest the features recited in Claims 1-20 ("the Challenged Claims") of U.S. Patent No. 11,966,464 ("the '464 Patent") (EX1001). My opinions and the bases for my opinions are set forth below.

3. I am being compensated at my ordinary and customary consulting rate for my work, which is $485 per hour. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other financial interest in this proceeding.

I. BACKGROUND AND QUALIFICATIONS

4. All of my opinions stated in this declaration are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my knowledge and experience in designing, developing, researching, and teaching the technology referenced in this declaration.

5. I am over 18 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein. I understand that a copy of my

current curriculum vitae, which details my education and professional and academic experience, is being submitted as EX1007. The following provides a brief overview of some of my experience that is relevant to the matters set forth in this declaration.

6. I have over 30 years of experience in wireless location services, including experience implementing Wireless 911 (E911) systems and designing, implementing, and managing numerous location-based service (LBS) applications such as family tracking and fleet and asset management. I am currently the President of the company E911-LBS Consulting, and I have been with the company since 2002. As the President of E911-LBS Consulting, I provide services across the entire wireless value chain, particularly with respect to technology and business strategic planning and product design and development associated with LBS, Global Positioning Satellite (GPS) systems, E911, Real-Time Location Systems (RTLS), Radio Frequency Identification (RFID), beacon, and other location determination and sensing technologies and services.

7. I have extensive expertise in all aspects of LBS delivery across the wireless location ecosystem including enabling network, map data, geospatial platform, chipset, data management, device, and location determination infrastructure and integration providers. I am an expert in all related aspects of LBS, including data privacy and security management.

8. For example, I managed the development and launch of several consumer-oriented LBS applications including mobile social networking, family tracking and local search for a major wireless carrier (AT&T). This work included the development of corporate-wide location data privacy policies and their systemic implementation for all LBS customers. My work in both data privacy and mobile social networking resulted in my co-inventing a patent in this field. I also have several other patents related to mobile location and associated applications and architectures.

9. I also have significant experience related to E911 systems. For example, in 2003-2004, I consulted with AT&T Wireless on their implementation of E911 systems. Specifically, I led the development of implementation and monitoring of systems in AT&T Wireless Western Region as part of their deployment of TDOA (Time Difference of Arrival) non-GPS E911 network location infrastructure to meet the wireless E911 location requirements mandated by the FCC. In 2004-2005, I worked with NAVTEQ, a key provider of LBS and E911 location map data, in developing their application developer ecosystem and website, providing developers with access to all of NAVTEQ's product and technical resources for developing location-related applications, including data products involving 911 GIS (Geographical Information Systems).

10. I have authored multiple books on wireless location, including:

- The Definitive Guide to GPS, RFID, Wi-Fi, and Other Wireless Location-Based Services (2005 and 2009 versions);
- The Definitive Guide to Wireless E911; and
- The Definitive Guide to Mobile Positioning and Location Management (coauthor).

11. I received a B.S. degree, in Electrical Engineering, from Purdue University in 1983. I received an MBA degree, in Information Systems Management, from The University of Texas at Austin in 1987.

II. INFORMATION CONSIDERED

12. In preparation for this declaration, I have considered the materials discussed in this declaration, including, for example, the '464 Patent, the references cited by the '464 Patent, the prosecution histories of the '464 Patent and applications from which it derives (including the references cited therein), various background articles and materials referenced in this declaration, and the prior art references identified in this declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

III. RELEVANT LEGAL STANDARDS

13. I am not an attorney and offer no legal opinions. For the purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Claim Interpretation

14. I have been informed that during an *inter partes* review proceeding, claims are to be construed in light of the specification as would be read by a person of ordinary skill in the relevant art at the time the application was filed. I have been informed that claim terms are given their ordinary and customary meaning as would be understood by a person of ordinary skill in the relevant art in the context of the entire disclosure. A claim term, however, will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the claim term in the specification. In that case, the claim term will receive the definition set forth in the patent.

15. I have been informed that certain patent claim terms may be interpreted as "means-plus-function" claim terms. I have been informed that terminology is part of the U.S. Patent Law in 35 USC §112, paragraph 6 (pre-AIA) / 35 USC §112(f) (post-AIA), which states the following: "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof."

B. Perspective of One of Ordinary Skill in the Art

16. I have been informed that a patent is to be understood from the perspective of a hypothetical "person of ordinary skill in the art" ("POSITA"). Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I have been informed that in considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

C. Anticipation

17. I have been informed that a claim is not patentable if it is anticipated. I have been informed that anticipation of a claim requires that every element of a claim is disclosed expressly or inherently in a prior art reference, arranged as in the claim, when considered from the perspective of a person of ordinary skill in the relevant art. I have been informed that when the structure recited in a reference is substantially identical to that of the claims, claimed properties or functions are presumed to be inherent. I have been informed that extrinsic evidence may be used to explain but not expand the meaning of terms and phrases used in the reference relied upon as anticipatory of the claimed subject matter.

D. Obviousness

18. I have been informed that a patent claim is obvious under 35 U.S.C. §103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a POSITA as of the priority date of the patent based on one or more prior art references and/or the knowledge of a POSITA.

19. I have been informed that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long- felt but unmet need, failure of others, copying by others, and skepticism of experts).

20. I have been informed that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. §103. I have been informed that a reference may also be combined with the knowledge of a POSITA, and that this knowledge may be used to combine multiple references. I have been informed that a POSITA is presumed to know the relevant prior art. I have been informed that the obviousness analysis may take into account the inferences and creative steps that a POSITA would employ.

21. In determining whether a prior art reference would have been combined with other prior art or other information known to a POSITA, I have been informed that the following principles may be considered:

- whether the references to be combined involve non-analogous art;
- whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;
- whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;
- whether the combination is of familiar elements according to known methods that yields predictable results;
- whether a combination involves the substitution of one known element for another that yields predictable results;
- whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;
- whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;
- whether the combination is "obvious to try";
- whether the combination involves the known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces, where the variations are predictable to a POSITA;
- whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the

art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;

- whether the combination requires modifications that render the prior art unsatisfactory for its intended use;
- whether the combination requires modifications that change the principle of operation of the reference;
- whether the combination is reasonably expected to be a success; and
- whether the combination possesses the requisite degree of predictability at the time the invention was made.

22. I have been informed that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I have been informed, however, that a teaching, suggestion, or motivation to combine is not required.

IV. SUMMARY OF OPINIONS

23. It is my opinion that Claims 1-20 of the ’464 Patent are unpatentable under 35 U.S.C. §§102 and 103 on the following grounds:

Ground	Reference(s)	Basis	Claims
1	Khosravi (US 2007/0234402) (EX1004) alone and/or in view of Xu (US 2007/0061535) (EX1005)	§103	1, 7-11, 17-20
2	Khosravi and Xu in view of Frank (US 2006/0165005) (EX1022)	§103	2-6, 12-16

V. TECHNOLOGY BACKGROUND

24. The ’464 Patent discloses security techniques for device assisted services (DAS) that include operating a wireless device 100 to control network access using policy settings. These settings are enforced using a “secure execution environment” 114 that communicates with a “wireless cellular network” via a “secure modem” 125. EX1001, Title, Abstract, Claim 1, 1:5-30, 3:9-26, Fig. 1.

25. A “secure control channel” connects the secure execution environment (e.g., 114, 214, 314) with the secure modem to allow for communication over the secure control channel to a network service controller. *Id.*, Fig. 1, Claim 1, 6:61-7:31. “Another secure control channel” connects the secure modem through the wireless cellular network to a network service controller 122 (e.g., via modem secure channel 132, 232 (Figs 1-2)).

26. Secure communication can be achieved using “encrypted communications”. *Id.*, 10:41-43.

27. Secure execution environment 114 includes DAS agents 110 within a secure memory partition to monitor service measurements, provide usage reporting, service policy enforcement, and communication with the network and a network service controller 122. EX1001, 2:41-67, 3:1-67, 4:1-67.

28. The network service controller 122 implements the "service policy" based on monitored service usage/verification of the wireless device. EX1001, 3:9-4:51, 8:8-13.

29. The "secure control channel" and "another secure control channel", and the components they connect, are recited in Claims 1 and 3:

> "establishing, through the connection, a **secure control channel** between the secure execution environment and a network service controller" (claim 1);
>
> "the secure modem further comprises a modem agent accessible only by the network service controller through **another secure control channel**" (claim 3).

30. An exemplary "secure control channel" connects the secure execution environment through the secure modem and the wireless cellular network to the network service controller 122 (e.g., via the "secure control channel"). *See, e.g.,* Figures 1-3.

31. An exemplary "another secure control channel" of Figure 1 connects the secure modem to the network service controller 122.

VI. THE CHALLENGED '464 PATENT

32. The '464 Patent contains 20 claims. I have been asked to opine on the validity of Claims 1-20.

VII. THE '464 PATENT PROSECUTION HISTORY

33. I have reviewed the file history of the '464 Patent.

34. Application No. 17/867,585, that issued as the ’464 Patent, is a continuation of Application No. 16/907,887, that issued as the ’429 Patent (EX1028), which is itself a continuation of Application No. 16/034,362 (*see* EX1009) that issued as U.S. Patent No. 10,694,385 (“’385 Patent”) (EX1008).

35. ***’429 and ’385 Patents:*** No prior art rejection was made during prosecution of the parent ’429 Patent. Only a non-statutory double patenting rejection was raised over the grandparent ’385 Patent.

36. Applicant did not distinguish the claims of the ’429 Patent from the ’385 Patent and instead filed a terminal disclaimer. EX1029, pp.125-129, pp.114-115.

37. The Examiner allowed the ’429 Patent for reasons similar to the ’385 Patent. EX1029, pp.22-31; EX1009, pp.9-14. The reasons for allowance identified three limitations: (1) a “secure modem subsystem connecting to the secure execution environment,” (2) a “secure memory partition accessible only from the secure execution environment,” and (3) a “modem control link.” *Id.* The Examiner mistakenly overlooked Claim 1’s failure to recite a “modem control link”. EX1029, p.30; EX1009, p.13.

38. ***’464 Patent:*** PO obtained allowance by representing to the Office that the claims of the ’464 Patent are allowable “at least for one or more reasons the Examiner found claims of … patent no. 11,405,429, allowable.” EX1002, p.203.

The Patent Office allowed the ’464 Patent in reliance on PO’s representation. *Id.*, p.35 (“The standing claims are viewed as allowable similarly to as found in the now terminally disclaimed Parent Applications”). However, the claims of the ’429 Patent never should have issued as explained above.

39. The independent claims of the ’429 Patent (as well as the independent claims of the ’464 Patent challenged in this IPR) do not even recite the “modem control link” subject matter referenced in the ’429 reasons for allowance. EX1002, p.203.

40. The list of References Cited (EX1001, pp.1-14) includes over 1,000 references submitted by Headwater. The Examiner did not address the listed Khosravi document. Xu and Frank were not cited. The Examiner therefore failed to properly consider Khosravi, Xu, and Frank.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

41. I have been informed that the “priority date” or “earliest effective filing date” of a patent is the date on which it is filed, or the date on which an earlier-filed U.S. or international patent application was filed if the patentee claims the benefit of priority to that earlier-filed U.S. or international patent application. For purposes of this declaration, I have assumed that the ’464 Patent is entitled to a priority date of January 28, 2009, and I have not evaluated or formed an opinion on whether the claims of the ’464 Patent are actually entitled to that date.

42. A person of ordinary skill in the art ("POSITA") as of the earliest possible priority date of the '464 Patent (January 28, 2009) would have been knowledgeable and familiar with wireless device design and architecture.

43. Such a POSITA would have had a bachelor's degree in electrical engineering, computer science, or a related field, and at least 2 years of experience relating to wireless devices and associated communications. Lack of professional experience may be remedied by additional education, and vice versa.

IX. CLAIM CONSTRUCTION

44. For purposes of my analysis in this IPR proceeding, I have been informed that terms that appear in the claims of the '464 Patent should be interpreted according to their plain and ordinary meaning under the *Phillips* standard. In determining the ordinary and customary meaning, I have been informed that the words of a claim are first given their plain meaning that those words would have had to a POSITA at the time of the alleged invention. I also have been informed that the claims, specification, and file history may be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. I have been informed that even treatises and dictionaries may be used under limited circumstances to determine the meaning attributed by a POSITA to a claim term at the time of filing.

45. I also understand that, for terms that evoke a means-plus-function construction, "the construction of the claim must identify the specific portions of the

specification that describe the structure, material, or acts corresponding to each claimed function." 37 C.F.R. §42.104(b)(3). I understand from counsel that construing a means-plus-function claim term is a two-step process that includes (1) identifying the claimed function and (2) then determining what structure, if any, disclosed in the specification corresponds to the claimed function.

46. I have reviewed the '464 Patent and its prosecution history as well as additional documents to construe the claims for performing my validity analysis. It is my understanding no claim term requires express construction apart from the construction set forth below.

47. In the Related Litigation, Petitioner and Patent Owner agreed that the preamble of claim 1 limits the claim. *See* EX1023, EX1024, EX1025, EX1026, and EX1027.

X. OVERVIEW OF THE PRIOR ART REFERENCES

A. Khosravi (EX1004)

48. Khosravi discloses operating a wireless device to control cellular network access by interpreting a policy-based "indication" received from a "policy decision point" 182 ("PDP") to set a policy enforcement configuration following a network access request. EX1004, Title, Abstract, ¶¶[0025], [0066]-[0070], Figs. 1-2.

49. A secure execution environment (e.g., a service operating system (SOS) 125) of the device is associated with a dedicated, partitioned memory resource. *Id*., ¶¶[0020]-[0021], [0033]. Khosravi's method is concerned with policy-based device security stating: "a high amount of trust is needed for computing devices that couple to the network" and the "level of trust" determines "what access the computing device and/or its elements may obtain to the network and or what remediation actions are needed if access is denied." *Id*., ¶¶[0012], [0017], [0023].

50. Khosravi discloses comparing "posture" information which includes policy-relevant settings, integrity measurements and configuration states of the wireless device against a network administrative/service policy profile to provide the "indication" of the device's access rights and remediation actions. EX1004, ¶¶[0027]-[0029],[0046],[0058]-[0059],[0067]-[0068],[0071]-[0072].

51. The "indication" can include information on actions such as updating anti-virus software, and downloading patches. *Id.*

52. Figure 2 illustrates Khosravi's system which includes a connection for connecting a secure modem 240/250 and a wireless network 280. Through the connection, a secure control channel is established between a secure execution environment SOS 225 and the network service controller 282:

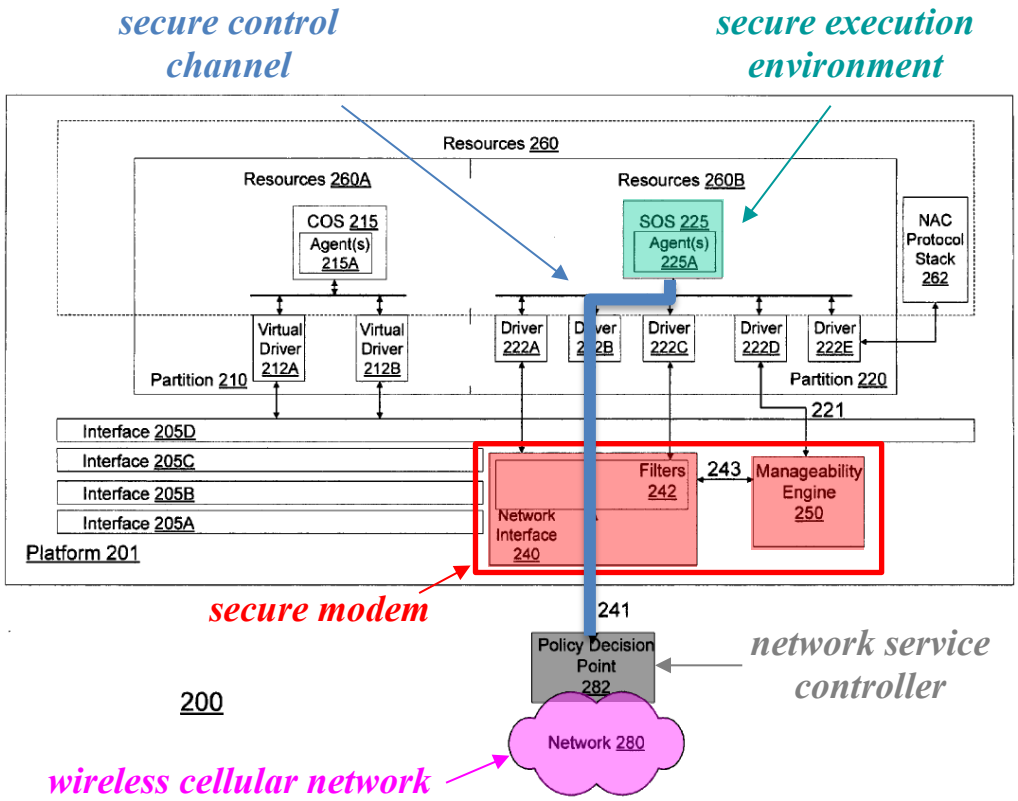


FIG. 2

EX1004, Fig. 2 (Annotated)

See also id., Fig. 1 (and corresponding elements).

53. A network access request is sent from the secure execution environment SOS 125 (e.g., SOS is a secure "intermediary" for a capability operating system (COS) 115/215 request) with "posture" information to a network service controller (i.e., "policy decision point" 182/282). EX1004, Abstract, ¶[0014], ¶[0017], ¶¶[0022]-[0024], Figs. 1-2.

54. Policy enforcement is provided by establishing a secure control channel that connects the secure execution environment SOS 125/225 with the modem to communicate "posture" information to the modem. The policy decision point configures a policy enforcement point to control network access (i.e., filters 142/242). *Id.*

55. To support SOS security, Khosravi "***partitions***" memory resources of the SOS. *Id.*, ¶¶[0021],[0033], Figs. 1-2.

56. The SOS and associated memory "operate separately and independently to other operating systems." *Id.*, ¶[0033].

57. The secure memory partition is accessible only from the SOS's secure execution environment.

58. The "indication" provided in response to the access request is produced at the network's policy decision point using the posture information.

59. The device platform then secures and encodes the indication with a cryptographic key. *Id.*, ¶¶[0062],[0067]-[0068].

60. The manageability engine authenticates/decodes the indication. *Id.*, ¶[0063],¶¶[0067]-[0068].

61. A policy enforcement agent interprets the "indication" and configures the filters for policy enforcement. *Id.*, ¶[0068], ¶¶[0070]-[0072].

62. Network "traffic is blocked by the filters (e.g., circuit broken) if certain criterion associated with the network administrative policies are not met." *Id.*, ¶¶[0039], ¶[0070].

B. Xu (EX1005)

63. Xu discloses a device for wireless connection to a network. EX1005, ¶[0013]; Figs. 2, 3.

64. A "secure memory" contains "policy data" associated with subsystem functions such as "policy management" and "policy enforcement." *Id.*, Abstract. Computer 302 includes a secure execution environment 314 having a secure memory partition 318 that stores service policy settings. *Id.*, ¶¶[0022]-[0023].

65. Network administrative policy data is stored in a secure memory within the secure execution environment. *Id.*, ¶[0003] ("secure storage" allows for "a processing unit that is not reliant on any outside components" to operate "in compliance to a usage policy."), ¶[0023] (improves tamper resistance).

C. Frank (EX1022)

66. Frank discloses a system for provisioning/metering a pay-as-you-go service for a computing device such as a cell phone. EX1022, ¶[0017].

67. A local provisioning module (LPM) architecture having a metering module labelled 454 is shown in Fig. 5.

68. Metering module 454 includes a balance manager 466 and a configuration manager 468. EX1022, ¶[0028].

69. The metering module monitors the use of computing device 400, and measures "input/output (network connectivity)". *Id.,* ¶[0028], ¶[0036].

70. The resulting data is stored in a secure storage accessible only to the LPM. *Id.*; *see also id.* ¶¶[0033]-[0035].

71. The metering includes techniques/measurements referenced by Xu, which cites Frank (as Application No. 11/006,837) for this exact purpose. EX1005, ¶[0025].

XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS

72. In my opinion, the Challenged Claims are unpatentable over the prior art.

A. Claims 1, 7-11, and 17-20 Are Rendered Obvious Over Khosravi (EX1004) Alone and/or in View of Xu (EX1005) (Ground 1)

73. The following sections reference where elements of Claims 1, 7-11, and 17-20 are disclosed and suggested by the prior art.

1. Claim 1 (Preamble): "A method of operating a wireless end-user device having a secure modem, a secure execution environment and a secure memory partition, the method comprising:"

74. Khosravi alone and/or in view of Xu discloses and suggests the Preamble. *See* EX1004, EX1005 in their entireties.

"A method of operating a wireless end-user device"

75. Khosravi discloses "[a] ***method*** that includes initiating a network access request from an access requester on a platform that couples to a ***network***." EX1004, Abstract (emphasis added).

76. Khosravi's "platform" is a "computing device" of a wireless end-user device (e.g., "digital broadband telephony device"). EX1004, ¶¶[0014]-[0015], ¶[0020]. *See also id.*, ¶[0004] ("mobile computing devices"); *id.*, ¶[0020] ("a ***cellular*** or a wireless broadband telephony network") (emphasis added).

"having a secure modem"

77. Khosravi discloses a secure modem (i.e., "network interface" 140/240 and "manageability engine" 150/250) used to connect the platform 101/201 to a wireless cellular network 180/280. EX1004, ¶¶[0024]-[0025], ¶¶[0018]-[0020], ¶[0044], Figs. 1-2.

78. Khosravi's "network interface" 140/240 includes "software, hardware and/or firmware ***to couple platform 101 to a network via wired or wireless***

***pathways**."* EX1004, ¶[0025] (emphasis added). *See also id.* ("wired or wireless…wide area network (WAN/WWAN)"). When a requester initiates a network access request, Khosravi's manageability engine 150/250 forwards "posture information associated with the access requester" to determine network access "based on a comparison of the posture information to one or more network administrative policies." *Id.*, ¶[0017].

79. A POSITA would have understood that a "modem" (i.e., MOdulator/DEModulator) modulates and demodulates data. EX1011, 7:1-4; EX1012, ¶16; EX1013, 2:32-36; EX1014, 3:34-39; EX1015, 5:4-8.

80. A POSITA would have understood Khosravi's network interface in connection with the manageability engine is, and functions as, a part of the secure modem because it includes "the software, hardware and/or firmware to couple platform 101 to a network via wired or wireless pathways" (i.e., a "wireless transceiver"; "wired or wireless…wide area network (WAN/WWAN)"). EX1004, ¶[0004], ¶¶[0014]-[0015], ¶[0025], ¶¶[0018]-[0020], ¶[0049] ("input/output (I/O) interfaces 340"), ¶[0054]. *See also, e.g.*, EX1016, ¶40 (Cellular devices "***typically include modem circuitry***."); EX1017, ¶4; EX1018, ¶58; EX1019, ¶17, ¶11; EX1020, ¶25; EX1021, ¶326; EX1005, ¶[0020].

81. Khosravi's Figure 1 and Figure 2 modem (see annotated Fig. 2 below) includes network interface 240, added filters 242, and manageability engine 250, which function like the '464 secure modem.

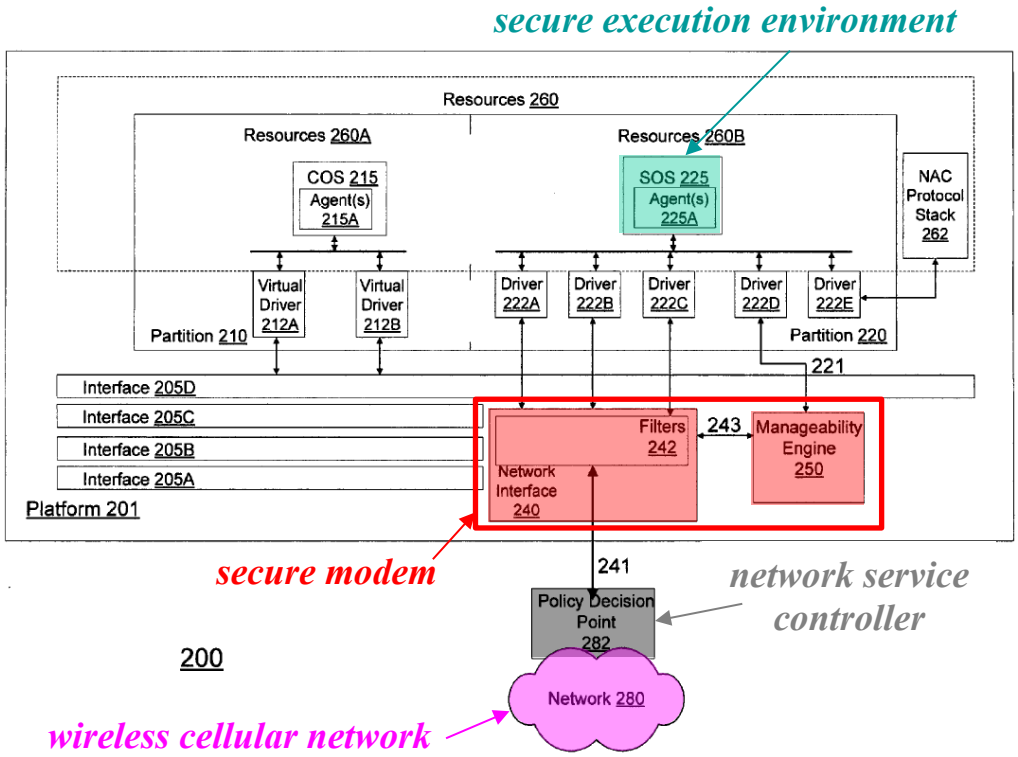


FIG. 2

EX1004, Fig. 2 (Annotated)

82. The '464 Patent's "modem" can include additional components. EX1001, 2:58-59 ("a secured measuring point can be provided in a modem"), 10:31-33 ("modem" includes "DAS agents"), claim 3 ("the secure modem further comprises a modem agent").

83. Khosravi's Figure 1 and Figure 2 (shown above) both depict the secure modem connection to a wireless cellular network.

84. Khosravi's secure modem connects the platform to an access network. EX1004, ¶[0025] ("couple platform 101 to a network"); *cf.* EX1001, 5:14-16.

85. Khosravi's secure modem provides a secure execution partition for access control, security, and service usage. EX1004, ¶[0075] (Manageability engine 150/250 blocks unauthorized network access requests); *cf.* EX1001, 3:39-47 (DAS agents perform "network authorization, network authentication, network admission, access, control" etc.); *see also*, EX1001, 5:27-30 ("modem execution partition"); and 10:49-58.

86. Khosravi's secure modem establishes a separate secure control link with a network element. EX1004 ¶[0047] (manageability engine "establishes a secure communication channel with policy decision point 282"), ¶[0053]; *cf.* EX1001, 11:1-4 ("separate secure modem control channel").

87. Khosravi's secure modem is also secure because the manageability engine employs ***security*** logic 310 in connection with its memory 330. EX1004, ¶¶[0049]-[0053], Figure 3. "[A]t least a portion of memory 330 is ***exclusively accessible*** to security logic 310 or control logic 320 to temporarily store information." *Id.*, ¶[0053] (emphasis added). *See also id.* ("secret key used to cryptographically sign" information).

88. Khosravi's manageability engine 150/250 establishes "a secure communication channel … with a policy enforcement agent". *Id.*, ¶[0026]; *see also id.* ¶[0044] ("Communication link 243" is "an exclusive communication link accessible only to manageability engine 150 to enforce default network administrative policies for platform 201.").

89. Khosravi's "filters" 142/242 of the secure modem facilitate policy enforcement and security via hierarchical trust layers established to access the network. EX1004, ¶[0025].

90. These filters are configured, and can only be modified, by secure logic such as the manageability engine via exclusive link 243. *Id.,* ¶[0044].

91. These filters "control the flow of data traffic to and from platform 101 via communication link 141." *Id.,* ¶[0025]; *see also id.*, ¶[0048]: "access is restricted or limited by manageability engine 150 (e.g., via filters 242)."

92. Alternatively, Khosravi's network interface 140/240 itself satisfies the claimed secure modem given that it "couple[s] platform 101 to a network." EX1004, ¶[0025].

"a secure execution environment"

93. Khosravi discloses that its service operating system (SOS) 125/225 "provides a ***secure execution environment*** … for network access control (NAC)

communication protocols (e.g., IEEE 802.1X and/or RFC 3748)." EX1004, ¶[0023] (emphasis added).

94. The SOS 125/225 "implement[s] authentication procedures to protect platform 101 elements" and to establish "hierarchical trust layers to access a network." *Id. See also* §§XI.A.1.b.-XI.A.1.d. (discussing operation of the secure execution environment).

95. For example, the secure modem and secure execution environment of Khosravi are depicted above (along with the secure control channel, wireless cellular network, and network service controller discussed below):

"a secure memory partition"

96. Khosravi discloses a "secure memory partition accessible only from the secure execution environment." EX1004, ¶[0033]. *See also* §XI.A.1.d.

97. Secure resources 160 include "memory … that [is] ***dedicated to or used independently by***" partition 120. *Id.*, ¶[0021], Figs. 1-2.

98. The memory is "storage" to "support[] one or more functions" or "tasks". *Id.*, ¶¶[0021]-[0023].

99. The memory is partitioned so that the secure execution environment (SOS) "can operate separately and independently to other operating systems." *Id.*, ¶[0033].

100. The memory can be "partitioned" into "memory slots" dedicated to a given OS. *Id.*, ¶[0036].

101. Because SOS 125/225 is contained in a partition, the memory ***"dedicated"*** for that partition is "used ***independently*** by"—and accessible only from—the SOS 125/225. The memory that is "dedicated to or used independently by" a "partition" is accessible only from that partition.

102. Khosravi's memory is "secure" because it is "dedicated" to the SOS's "secure execution environment." *See* §XI.A.1.c. (Element [1.4]). *See also* EX1004, ¶[0023], ¶[0021], ¶[0036].

103. In addition, given that SOS 125/225 is contained in a partition 120/220 (*see* Figs. 1-2), the memory ***"dedicated"*** for that partition would be "used ***independently*** by" — and be accessible only from — the SOS 125/225.

a. [1.1]: "establishing a connection between the secure modem and a wireless network;"

104. Khosravi alone and/or in view of Xu discloses and suggests Element [1.1].

105. Khosravi discloses a secure modem. *See* §XI.A.1.

106. Khosravi discloses establishing a connection ("coupling" via "communication link" 141/241) from the secure modem (i.e., "network interface" 140/240 and "manageability engine" 150/250) of the platform 101/201 to the

wireless cellular network 180/280 (e.g., "cellular or a wireless broadband telephony network"). EX1004, ¶[0025], ¶¶[0018]-[0020], ¶[0044], Figures 1-2.

107. Khosravi's "network interface" 140/240 includes "software, hardware and/or firmware ***to couple platform 101 to a network via wired or wireless pathways***." EX1004, ¶[0025] (emphasis added). *See also id.* ("wired or wireless…wide area network (WAN/WWAN)").

108. When a requester initiates a network access request, Khosravi's manageability engine 150/250 forwards "posture information associated with the access requester" to determine network access "based on a comparison of the posture information to one or more network administrative policies." *Id.*, ¶[0017].

109. Exemplary systems are depicted in Figures 1 and 2 of Khosravi, annotated below to show the secure modem and wireless network:

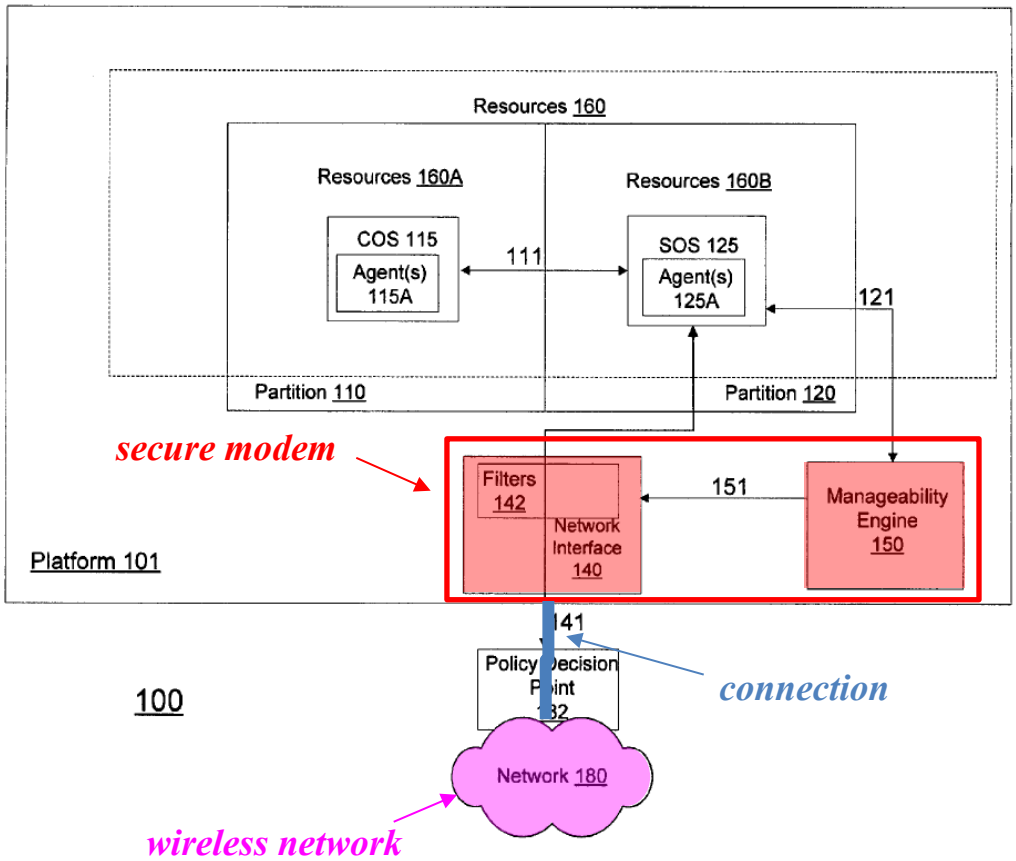


FIG. 1

EX1004, Fig. 1 (Annotated)

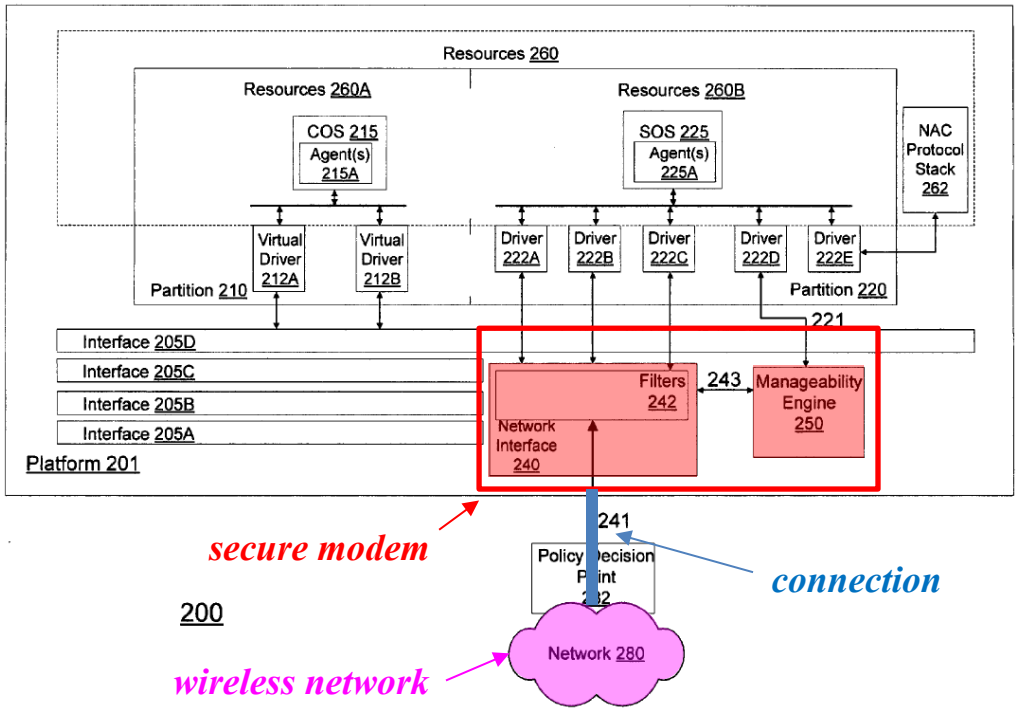


FIG. 2

EX1004, Fig. 2 (Annotated)

EX1004, Figs. 1-2.

b. [1.2]: "establishing, through the connection, a secure control channel between the secure execution environment and a network service controller;"

110. Khosravi alone and/or in view of Xu discloses and suggests Element [1.2].

111. Khosravi discloses "SOS 125 establishes ***a secure communication channel*** … with policy decision point" (PDP) to convey "posture" information sent from the SOS (which is the "secure execution environment") to the PDP (which is a

"network service controller"). EX1004, ¶[0030] (emphasis added), Figs. 1-2. "The policy enforcement agent … 225A [of the SOS] … establishes ***a secure communication channel*** over communication link 241 with policy decision point 282." *Id.*, ¶¶[0062]-[0063] (emphasis added). Khosravi's driver 222B allows SOS 225 access to network interface 240 to communicate with the policy decision point 182/282. *Id.*, ¶[0039].This secure control channel is depicted in the annotated Figure 2, below.

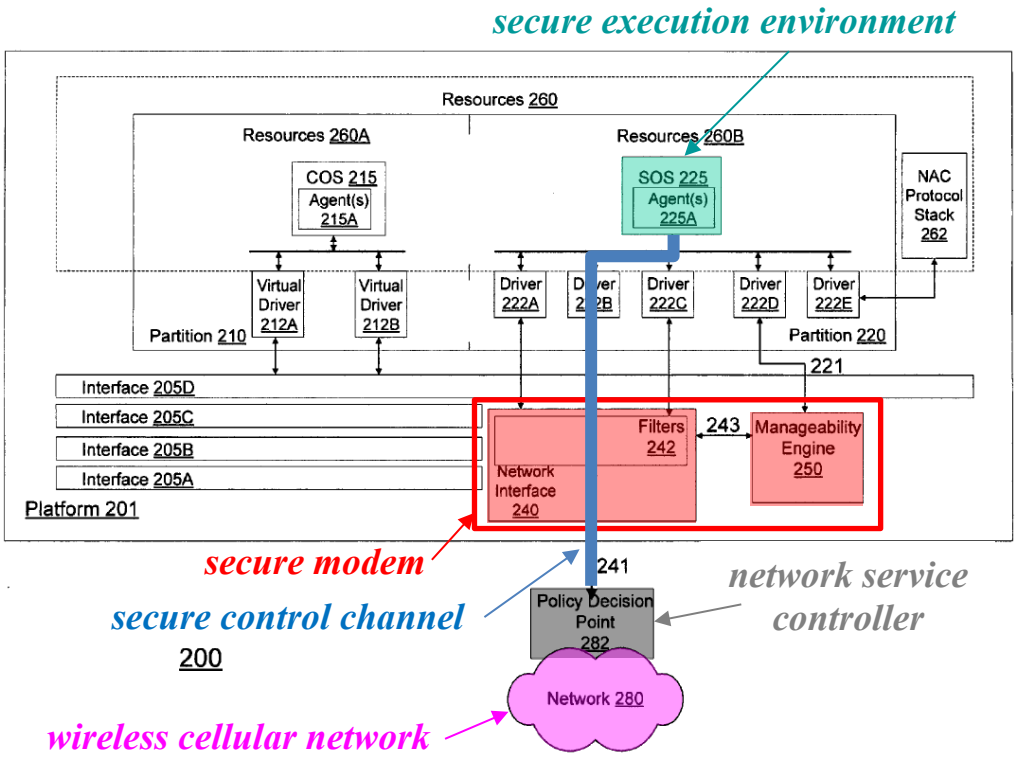


FIG. 2

EX1004, Fig. 2 (Annotated)

112. Khosravi therefore discloses establishing, through the connection (via communication link 141/241), a secure control channel (for sending posture information) between the secure execution environment (SOS 125/225) and a network service controller (PDP 182/282). EX1004, ¶¶[0062]-[0066], Figs. 1-2.

113. This secure channel utilizes "XML signatures and/or PKI certifications." EX1004, ¶¶[0062]-[0063]. The policy enforcement agent 225A "forwards the ***cryptographically signed*** posture information to policy decision point 282." *Id.*, ¶¶[0064]-[0065] (emphasis added).

114. Khosravi's secure communication channel is a "control" channel because it conveys posture information associated with Khosravi's technique for controlling network access rights to an access requester based on "access control policies." EX1004, ¶[0016], ¶[0030]. *See also id.*, ¶[0013], ¶[0044], ¶[0057], §X.A.

115. This channel is a "control channel" for "***control data traffic***" between SOS 225 and policy decision point. EX1004, ¶[0044], ¶[0066]. The PDP 282 compares the posture information to ***network administrative policies*** which include access ***control*** policies for network access. *Id.*

116. Khosravi's secure control channel: (1) links a distinct component of Khosravi's platform (SOS 125/225) with the PDP; and (2) sends posture information (*see, e.g.,* EX1004, ¶[0030] (SOS gathers "posture information about COS 115")), that is distinct from posture information sent from another secure control channel

(*see, e.g., id.*, ¶[0027] ("integrity measurements may also be associated with a manageability engine"), ¶[0042] (ME obtains posture information associated with "itself")).

"through the connection"

117. Khosravi's secure control channel is established through the connection between the secure modem and a wireless network (*see* §XI.A.1.a.). Khosravi's secure control channel is established through the wireless cellular network 180/280 to the policy decision point (PDP) 182/282, with communication link 141/241 providing a "wireless pathway" from the platform's "***network*** interface" 140/240 to the wireless cellular network. EX1004, ¶[0062], ¶[0020], Figs. 1-2.

118. The PDP 182/282 is a "***network*** entity" located in "a ***network*** switch" or "a ***network*** server". EX1004, ¶[0016] (emphasis added).

119. Khosravi discloses and suggests link 141/241 as connecting to the PDP "through the wireless cellular network." *See also* EX1004, ¶[0043]-[0047] ("secure communication channel with policy decision point 282 on network 280").

"network service controller"

120. Khosravi's "policy decision point" 182/282 ("PDP") constitutes a "network service controller." EX1004, ¶¶[0016]-[0017], ¶[0047], Figures 1-2.

121. The '464 Patent's "network service controller" is implemented on a server and performs verification techniques (e.g., "modify[ing] the operation or

service policy settings" (EX1001, 7:21-31); "access control verifications checks to ensure that the device assisted service agents have not been compromised" (EX1001, 7:42-46). *See also* EX1001, 8:8-13, 18:4-54; 17:25-18:64, Figures 1-2.

122. Khosravi's PDP performs these same functions using corresponding server structure. EX1004, ¶[0016].

123. Khosravi's policy PDP 182/282 authenticates the manageability engine 150 using a "PKI private key signature" and provides access policy information back to the manageability engine. *Id.*, ¶[0045].

124. The PDP controls access by deciding "whether to grant network access rights to an access requested based, for example, on a network administrative policy [which] may include one or more access control policies to determine who or what has access to the network." *Id.*, ¶[0016].

c. [1.3]: "receiving, at the secure execution environment, via the secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more settings;"

125. Khosravi alone and/or in view of Xu discloses and suggests Element [1.3].

126. Khosravi discloses receiving at the secure execution environment (Khosravi's "service operating system" (SOS) 125/225), via the secure control channel between Khosravi's SOS 125/225 and policy decision point 282, one or

more messages from the network service controller (Khosravi's "policy decision point" 282), the one or more messages comprising one or more settings (Khosravi's "indication reflect[ing] network administrative policies").

127. Khosravi's manageability engine 150/250 obtains "posture information" from capability operating system (COS) 115/215 and "forward[s]" this information "to the policy enforcement agent" in the SOS. EX1004, ¶¶[0064]-[0065], ¶[0042].

128. The SOS forwards "cryptographically signed posture information to policy decision point 282" over the "secure communication channel." *Id.*, ¶[0065], ¶[0043].

129. The "policy decision point 282 indicates what access COS 215 can have to network 280." EX1004, ¶[0066], ¶[0043].

130. The policy decision point 282 then creates and sends an "indication" (i.e., "one or more messages comprising one or more settings") via the secure control channel which is received by the policy enforcement agent in the SOS ("secure execution environment"), which then forwards the indication to the manageability engine 150. *See* EX1004, ¶¶[0037]-[0038] (via drivers, e.g., driver 222B), ¶[0067], ¶[0083].

131. The SOS 125/225 includes agent(s) 225A including a "policy enforcement agent that enables SOS 225 to act as a policy enforcement point on

behalf of a network administrator for network 280." *Id.*, ¶[0037]. *See also id.*, ¶[0024], ¶[0041].

"one or more messages comprising one or more settings"

132. Khosravi's "indication" constitutes the claimed "one or more messages comprising one or more service policy settings." Khosravi's indication is used to set/enforce network administrative policies. *See, e.g.,* EX1004, ¶[0070] ("indication reflects network administrative policies").

133. Khosravi's indication is used to set/enforce network administrative policies. For example, these messages are used to perform traffic shaping like the '464 Patent. EX1001, 14:54-56.

134. Khosravi's SOS "interprets the indication and configures the data traffic filters on platform 201 based on that interpretation." EX1004, ¶[0070], ¶[0023], ¶[0046].

135. The filters control traffic and "the level of network access." *Id.*, ¶[0070].

136. Khosravi's indication is used by the policy enforcement agent to configure the data traffic filters, *i.e.*, to enforce the service policy settings. *See id.*, ¶[0039].

137. Dependent claim 8 of the '464 Patent specifies that the one or more settings can include "a network setting or a device management communication

setting," and Khosravi discloses such settings. EX1004, ¶[0016] ("*network administrative policies* may include one or more access control policies to determine who or what may *access the network*."; ¶[0025] ("*data traffic filters* … are used to *control the flow of data traffic to and from platform 101* … to facilitate the enforcement of network administrative policies.") (emphasis added). *See also* §XI.A.3.

138. Khosravi's "indication" ***"reflects network administrative policies"*** and is used to configure filters that enforce the policies. EX1004, ¶[0070].

139. Khosravi similarly discloses that its network administrative policies "determine who or what may access the network." EX1004, ¶[0016].

140. Khosravi's policies include "outbreak containing policies," "intrusion detection policies," "monitoring policies," and more. *Id.*

141. Khosravi's indication includes information concerning "updating anti-virus software or downloading patches from specified internal or external servers … or implementing an access control policy … that may result in reconfiguring the data traffic filters." EX1004, ¶[0071].

"from the network service controller"

142. Khosravi's SOS receives the indication ***from the policy decision point*** ("network service controller"). *See, e.g.*, EX1004, ¶¶[0066]-[0067].

143. This matches the reception of service policy settings ***from the network service controller*** in the '464 Patent. Data collected at the wireless device is forwarded to the network service controller for "compar[ing] the [collected data] versus the policy." EX1001, 8:8-13. "[T]he service controller 122 may modify operation or service policy settings for the agents located in the … service control execution partition." *Id.*, 7:25-31.

144. Khosravi's "posture information" is also collected at the device and forwarded to the policy decision point. Khosravi's policy decision point sends the "indication" to its policy enforcement agent to enforce its network administrative policies. EX1004, ¶[0067].

145. The manageability engine forwards a decoded indication to the policy enforcement agent which "interprets whether the decoded indication forwarded from manageability engine 150 grants access requested by the access requester" (e.g., COS 215 via SOS). EX1004, ¶¶[0067]-[0068].

d. [1.4]: "storing the one or more settings in the secure memory partition accessible only from the secure execution environment; and"

146. Khosravi alone and/or in view of Xu discloses and suggests Element [1.4].

Khosravi

147. Khosravi discloses a "secure memory partition accessible only from the secure execution environment." *See* §XI.A.1. (preamble). *See also* EX1004, ¶[0033].[1]

148. Khosravi's stored indication constitutes storage of service policy settings for the "circuit breaker filters" located in the partition that use resources "resident on [the] platform." EX1004, ¶[0039].

149. The policy enforcement agent configures the circuit breaker filters using a criterion "based on… the indication." EX1004, ¶[0039]. *See* §XI.A.1.c.

150. Being implemented on the partition 120/220 comprising Khosravi's SOS, such storage is in the "dedicated" memory that is accessible only to the SOS. EX1004, ¶[0021].

151. Alternately, it would have been obvious to a POSITA based on Khosravi's disclosure to store the service policy settings of the "indication" in the SOS's memory partition, with a reasonable expectation of success. EX1004, ¶[0070].

---

[1] Khosravi's Figure 1 partitions can be part of the Figure 2 virtualization technology enabled platform described in paragraph [0033]. EX1004, ¶[0021].

152. Khosravi's secure memory partition supports the SOS in its handling and use of the received indication to perform assigned functions/tasks. *See, e.g.,* EX1004, ¶¶[0021]-[0023], ¶¶[0068]-[0070].

153. Khosravi motivates storage of settings related to the network administrative policies in secure memory by disclosing such storage in similar contexts, e.g., retrieving "default network administrative policies" from memory 330. EX1004, ¶[0057], ¶[0053] (memory 330 is "exclusively accessible to security logic 310 or control logic 310").

154. At power-up, the manageability engine performs the configuration until the SOS is online. *Id.* It would have been obvious to a POSITA for the SOS to store in its secure memory an indication of new or updated network administrative policies, once the SOS is online and communicating with the policy decision point, just as the manageability engine stores default policies to use at power-up. *Id.*, ¶[0057], ¶[0061], ¶[0070].

155. Additionally, the received indication is secured in various ways; e.g., signed with a cryptographic key, and communicated over secure communication channels. EX1004, ¶[0062], ¶[0063], ¶¶[0067]-[0068].

156. It would have been obvious to a POSITA to store such sensitive information as is contained in Khosravi's "indication" in the secure memory dedicated to the SOS.

157. In contrast, a potentially compromised indication is discarded. EX1004, ¶[0069]. Were the "indication accessible to other components, such as the COS, that component could manipulate its own policies and settings which would compromise Khosravi's entire system.

158. Storing the decoded indication "supports" the SOS applying of the indication. EX1004, ¶[0021], ¶[0068], ¶¶[0070]-[0072].

159. Khosravi contemplates the implementation of multiple remedial actions and, after their completion, obtaining updated posture information. EX1004, ¶[0072].

160. Storing the decoded indication "supports" remedial action implementation (e.g., by allowing the SOS to "interpret" the indication, read it multiple times, and consider appropriate times to implement remedial actions, resource availability, etc.).

161. A POSITA would have been motivated to safeguard the indication by storing it in a secure memory.

<u>Khosravi in view of Xu</u>

162. Even if Khosravi were construed as somehow failing to teach/suggest storing policy settings from the indication in a secure memory partition accessible only from the secure execution environment, this would have been obvious in view of Xu.

163. Xu discloses that "enforcement functions 328 may be loaded into a reserved execution memory 316 and executed when it is determined that the computer 300 is not in compliance with one or more elements of the policy 322." EX1005, ¶[0024]; *see also id.* ¶[0031].

164. Xu discloses the importance of keeping the policy stored in secure memory: "[b]ecause the policy and enforcement functions are maintained within the processing unit 302, some typical attacks on the system are difficult or impossible." EX1005, ¶[0032]. For example, "the policy may not be 'spoofed' by replacing a policy memory section of external memory." EX1005, ¶[0032].

165. Xu teaches that it was well-known to store service policy settings in a secure memory when implementing network policies in a secure execution environment. *See, e.g.,* EX1005, ¶¶[0022]-[0023], ¶[0003].

166. Xu is analogous art to Khosravi and the '464 Patent. Xu seeks to "provid[e] a secure base for enforcing security and/or operating policies" without reliance on external elements and like Khosravi, discloses employing a "secure execution environment 314" to provide the secure base. EX1005, ¶[0003], ¶[0022].

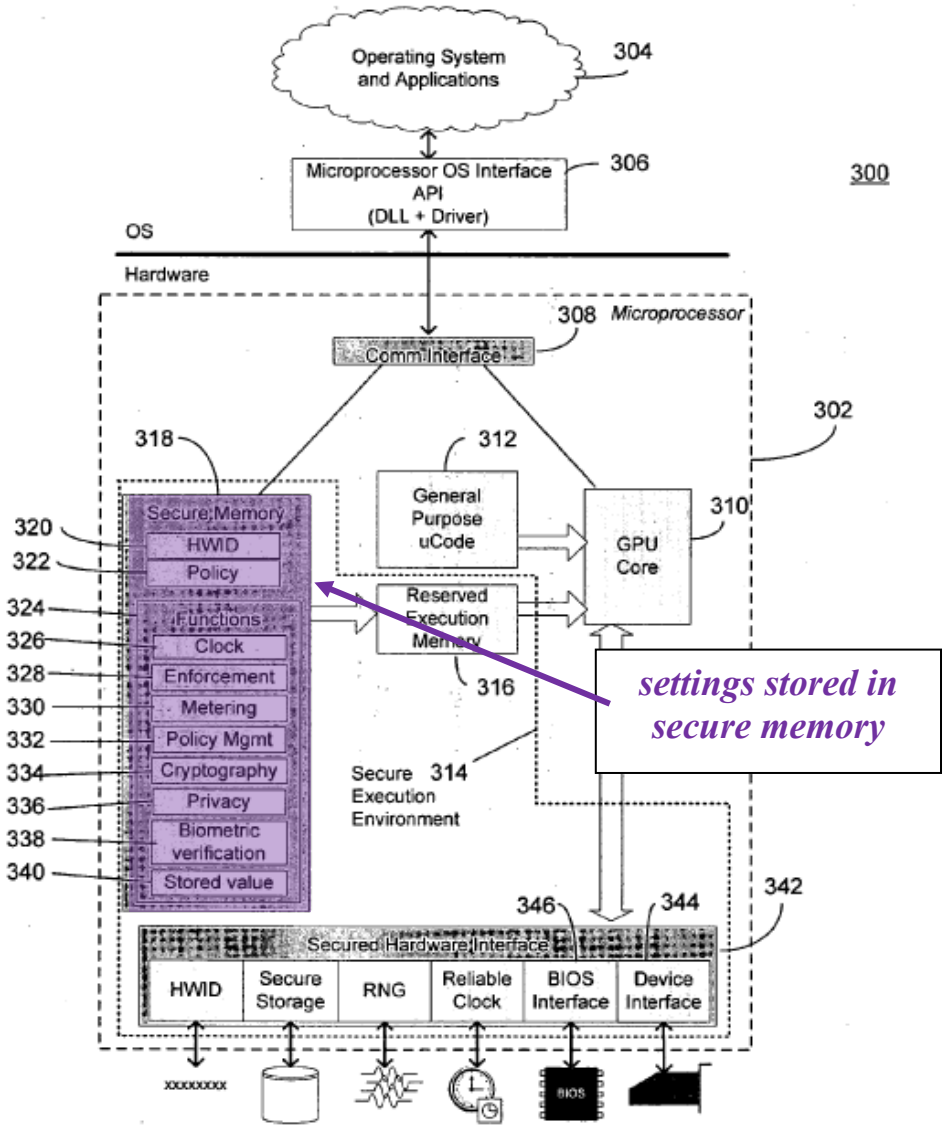
167. Xu's secure execution environment 314 includes a "secure memory 318" which "may store, in a tamper-resistant manner, code and data related to the secure operation of the computer 302." EX1005, ¶[0023]. For example, "[d]ata in the secure memory 318 may include an identification indicia or hardware identifier

320 and ***policy data 322 that may specify policy related operational directives such as metering, reporting, update requirements, etc.***" EX1005, ¶[0023].

168. The secure memory 318 may also include "code or data required to implement "enforcements functions 328, metering 330, policy management 332."*Id*.

169. Like Khosravi, policy data in Xu is used to determine and enforce when a device "is not in compliance with one or more elements of the policy 322" (EX1005, ¶[0024]).

170. Xu's reserved execution memory 316 provides "a highly secure location for the execution of instructions having an elevated privilege level within the processing unit." *Id.*, ¶[0022].



EX1005, Fig. 2 (Annotated)

171. Referencing Figure 2, Xu's "secure memory 318" and "reserved execution memory 316" are accessible only to the secure execution environment.

172. In Xu, the secure execution environment is a part of the processing unit (*see* EX1005, ¶[0014]), and Xu discloses that data elements contained "within the

secure memory ***are not accessible from outside the processing unit.***" *Id.*, abstract (emphasis added). *See also id.*, ¶[0003] ("processing unit … is not reliant on any outside components … to establish the basis for computer capable of being operated in compliance to a usage policy"); ¶[0022] ("the processing unit 302 acts as a full subsystem and does not require any external assets … to build a secure processing environment.").

173. Thus, Xu's processing unit (which includes Xu's secure execution environment) is also itself a secure execution environment.

174. Xu provides implementation details to securely store policy data and to support enforcing such policies via operational directives such as metering, reporting, updating and for remediation. EX1005, ¶[0023].

175. Xu's metering, based on the service policy settings ("whether to meter and what specific items to measure"), is "implemented by the policy management function 332." EX1005, ¶[0023].

176. Xu demonstrates that it was well-known to store network administrative policy data in a secure memory accessible only to the secure execution environment to support the functions/tasks including metering. EX1005, ¶[0003], ¶[0022], ¶[0023] (improves tamper resistance); ¶[0025] (citing EX1022 for disclosing well-known techniques for metering usage for policy management). *See also* EX1022, ¶¶[0025]-[0028].

177. It would have been obvious to a POSITA to modify Khosravi in view of Xu to store policy settings from the indication of network administrative policies (corresponding to "one or more service policy settings") in its secure memory partition accessible only from the secure execution environment.[2]

178. First, a POSITA would have been motivated to do so to support the use and protection of the policy data as taught by Xu and Khosravi. EX1005, ¶[0003] ("secure storage" allows for "a processing unit that ***is not reliant on any outside components***.") (emphasis added); ¶[0023] (improves tamper resistance); abstract (data elements "within the secure memory are not accessible from outside the processing unit."); EX1004, ¶[0021] ("support" functions and tasks).

179. Second, such a modification would have merely constituted combining prior art elements (Xu's secure storage of policy data with storing of Khosravi's "indication" in a secure memory partition) to yield predictable results (e.g., promoting device security, regarding policy setting and enforcement without reliance on outside components, and improved tamper resistance).

---

[2] The subject matter would have been obvious in view of Khosravi alone as noted above.

180. Third, such modification would have merely involved simple substitution of one known element (Khosravi's memory) for another (Xu's technique of storing policy data in secure memory) to obtain predictable results.

181. Fourth, such modification would have involved the use of a known technique (Xu's technique of storing policy data in secure memory) to improve similar devices/methods (Khosravi's devices/methods) in the same way (e.g., avoiding reliance on outside components and improving tamper resistance).

182. Fifth, such modification would have merely involved applying a known technique (Xu's technique of storing policy data in secure memory) to the known device of Khosravi ready for improvement (e.g., promoting device security, avoiding reliance on outside components and improving tamper resistance) to yield predictable results.

183. Khosravi and Xu address the same security goals and operate in compatible architectures.

184. Storing service policy settings in a secure memory of Khosravi according to Xu's teaching would have been straightforward, with a predictable and reasonable expectation of success.

e. [1.5]: "controlling the wireless end-user device using the one or more settings."

185. Khosravi alone and/or in view of Xu discloses and suggests Element [1.5].

186. Khosravi discloses controlling the wireless end-user device (Khosravi's "platform") using Khosravi's "indication reflect[ing] network administrative policies." *See, e.g.,* EX1004, ¶[0070]. *See also* Element [1.3], *supra*.

187. For example, Khosravi controls the wireless end-user device by enforcing the network administrative policies reflected by Khosravi's indication ("one or more message comprising one or more settings") received from Khosravi's policy decision point ("network service controller").

188. Khosravi's enforcement is conducted from the "policy ***enforcement*** agent included in agent(s) 225A" of SOS 125/225 (i.e., Khosravi's secure execution environment). EX1004, ¶[0041] (emphasis added), Figures 1-2. Khosravi's "policy enforcement agent … ***enforc[es]*** network administrative policies when it interprets the indication and configures the data traffic filters on platform 201 based on that interpretation." *Id.*, ¶[0070] (emphasis added).

189. Based on Khosravi's indication, the policy enforcement agent configures the circuit breaker filters to block traffic "if certain criterion associated with the network administrative policies are not met." EX1004, ¶[0039].

190. Configuring device filters and blocking traffic to the device constitutes controlling the device. The policy enforcement is performed by Khosravi's secure execution environment.

191. Khosravi's remediation actions using the indication at the policy enforcement agent also demonstrate "controlling the wireless end-user device."

192. After the agent 225A receives the indication from the policy decision point 282, it "complete[s] the remediation actions." EX1004, ¶[0072].

193. The "indication reflects network administrative policies" and "the policy enforcement agent … ***enforc[es]*** network administrative policies when it interprets the indication." *Id.*, ¶[0070].

194. Khosravi enforces its network administrative policies to control the wireless end-user device. Khosravi's enforcement involves "configur[ing] the data traffic filters." EX1004, ¶[0070]; *see also id.*, ¶[0039] ("circuit breaker filters" block traffic "if certain criterion associated with the network administrative policies are not met.").

195. The enforcement can include remediation actions and configuring the data traffic filters to enforce the access control policy. *Id.*, ¶[0072].

196. These actions control the device's use of a service on the wireless cellular network.

2. Claim 7: "The method of claim 1 , wherein the one or more settings include at least one of an access control setting, a traffic control setting, or an admission control setting."

197. Khosravi alone and/or in view of Xu discloses and suggests Claim 7. *See* Claim 1, *supra*.

198. Khosravi discloses that the one or more settings (Khosravi's "indication" that reflects "network administrative policies") include at least one of an access control setting, a traffic control setting, and/or an admission control setting. EX1004, ¶[0048], ¶[0016].

199. Khosravi discloses that its "network administrative policies may include one or more ***access control policies*** to determine who or what may access the network." *Id.*, ¶[0016].

200. Khosravi also discloses use of "***data traffic filters*** that are used to control ***the flow of data traffic*** to and from platform … to facilitate the enforcement of network administrative policies." EX1004, ¶[0025].

201. Khosravi's network administrative policies include "traffic control settings" given that Khosravi's platform configures the data traffic filters to control the flow of data traffic based on the network administrative policies. *Id.*

202. Khosravi's network administrative policies may include one or more "monitoring policies, and the like" (EX1004, ¶[0016]) such as the monitoring policy

settings taught by Xu which also satisfy the claimed service policy settings. EX1005, ¶[0003], ¶¶[0024]-[0028], ¶[0030].

3. Claim 8: "The method of claim 1, wherein the one or more settings include a network setting or a device management communication setting."

203. Khosravi alone and/or in view of Xu discloses and suggests Claim 8. *See* Claim 1, *supra*.

204. Khosravi discloses that the one or more settings (Khosravi's "indication" that reflects "network administrative policies") include a network setting or a device management communication setting. EX1004, ¶[0048], ¶[0016].

205. Khosravi discloses that its "network administrative policies may include one or more access control policies ***to determine who or what may access the network***." *Id.*, ¶[0016].

206. In addition, Khosravi discloses that circuit breaker filters that "filter the flow of data traffic to or from platform" (i.e., manage network or device communication) are configured based on network administrative policies, i.e., Khosravi's network administrative policies relate to network or device management communication settings. *Id.,* ¶[0039].

207. Khosravi's network administrative policies may include one or more "monitoring policies, and the like" (EX1004, ¶[0016]) such as the monitoring policy

settings taught by Xu which also satisfy the claimed service policy settings. EX1005, ¶[0003], ¶¶[0024]-[0028], ¶[0030].

4. Claim 9: "The method of claim 1, wherein the secure execution environment is implemented at least in part as a hardware partition or a software partition."

208. Khosravi alone and/or in view of Xu discloses and suggests Claim 9. *See* Claim 1, *supra*.

209. Khosravi discloses that the policy enforcement point (one of agent(s) 225A which is a part of Khosravi's secure execution environment) may be implemented at least in part as a hardware partition or a software partition. EX1004, ¶[0015].

210. Further, Khosravi discloses that elements of its system can be implemented via "***software***, ***hardware***, and/or firmware" and elements of the secure execution environment (including SOS 125/225) are contained in "partition" 120/220 as shown in Figures 1 and 2. *Id.*, ¶[0021].

211. Khosravi discloses that the partitioned "resources 160A and 160B" in Figure 1 "represent memory and processing elements that are dedicated to or used independently by partitions 110 and 120, respectively." EX1004, ¶[0021].

212. By dedicating memory and processing elements to the different partitions, Khosravi discloses that the SOS (secure execution environment) is implemented at least in part in a hardware partition.

213. In addition, Khosravi's secure execution environment includes a secure memory partition which constitutes a hardware partition. *See* §XI.A.1.e.

5. Claim 10: "The method of claim 1, wherein the secure execution environment is implemented at least in part in a virtual machine."

214. Khosravi alone and/or in view of Xu discloses and suggests Claim 10. *See* Claim 1, *supra*.

215. The '464 Patent discloses virtual execution partitions as an example software-based approach to creating partitions. EX1001, 8:38-42.

216. Khosravi discloses that the COS and SOS can be partitioned using virtualization (i.e., a software partition).

217. Khosravi discloses an exemplary system "including a ***virtualization*** technology enabled platform" involving a "***virtualization*** technology scheme" which "partitions the resources to support a plurality of operation systems." EX1004, ¶¶[0032]-[0033], Fig. 2. This "virtualization scheme … partitions these resources in such a way that an operating system can operate separately and independently to other operating systems." *Id.*

218. A POSITA would therefore understand that Khosravi's virtualization scheme would implement the Service Operating System, constituting the "secure execution environment," at least in part in a software partition. *Id.*; *see also id.*

¶¶[0033]-[0036] (discussing virtualization technology scheme for partitioning resources).

219. Khosravi discloses that the policy enforcement point (one of agent(s) 225A which is a part of Khosravi's secure execution environment) may be implemented at least in part as a software partition. EX1004, ¶[0015].

220. Khosravi discloses that elements of its system can be implemented via "***software***, hardware, and/or firmware" and elements of the secure execution environment (including SOS 125/225) are contained in "partition" 120/220 as shown in Figures 1 and 2. *Id.*, ¶[0021].

6. Claim 11 (Preamble): "A wireless end-user device comprising: a secure modem; a secure execution environment; a secure memory partition; and a processor configured to:"

221. To the extent the Preamble is limiting, Khosravi alone and/or in view of Xu discloses and suggests the Preamble. *See* EX1004, EX1005 in their entireties.

222. Khosravi discloses a wireless end-user device (Khosravi's platform) that comprises "a secure modem; a secure execution environment; [and] a secure memory partition" as claimed. *See* §XI.A.1. (Preamble).

223. Khosravi discloses that its platform includes at least one processor configured to perform the functions recited in Elements [11.1]-[11.5].

224. Khosravi specifies that its "platform 101 includes the software, ***hardware***, and/or firmware ***to support one [or] more functions for a computing device***," these functions including "***storage***" and "***general processing tasks***." EX1004, ¶[0021].

225. Khosravi discloses that "[a]t least a portion of this software, hardware, and/or firmware is depicted in FIG. 1 as resources 160…represent[ing] memory and ***processing elements*** that are dedicated to or used independently by partitions 110 and 120, respectively." *Id.*

226. Such "hardware" and "processing elements" are used by other individual components of Khosravi's platform. *Id.,* ¶[0025] ("Network interface 140 may include the software, ***hardware*** and/or firmware to couple platform 101 to a network via wired or wireless pathways (e.g., a media access controller, wireless transceiver, ***digital signal processor***, antennae, radio, fabric interface, etc.)."), ¶[0027] ("Manageability engine 150, for example, has direct access to ***hardware services*** or resources resident on platform 101 (not shown)").

227. Khosravi discloses that "[t]hese hardware resources may include ***processing elements***, chipset registers, memory, busses, firmware, etc." *Id.,* ¶[0027].

228. Khosravi discloses that "[f]or example, security logic 310 and control logic 320 each or collectively represent any of a wide variety of logic device(s) or executable content to implement the features of manageability engine 150" and

"[t]hese logic device(s) may include a ***microprocessor, network processor, service processor***, microcontroller, field programmable gate array (FPGA), application specific integrated circuit (ASIC), sequestered thread or core of a ***multi-core/multi-threaded microprocessor***, special operating mode of a ***processor*** (e.g., system management mode) or combination thereof."). EX1004, ¶[0049].

229. The '464 Patent discloses that the term "processor" encompasses multiple processing devices, thus encompassing multiple processing elements disclosed by Khosravi. EX1001, 2:22-24 ("the term 'processor' refers to ***one or more devices***, circuits, ***and/or processing cores configured to process data***, such as computer program instructions.").

230. Khosravi's "processing elements" that "support[] one or more functions for a computing device" satisfies a "processor configured to" perform the functions of Elements [1.1]-[1.5]. *See* §XI.A.1.

a. [11.1]: "establish a connection between the secure modem and a wireless network;"

231. Khosravi alone and/or in view of Xu discloses and suggests Element [11.1]. *See* §XI.A.1.a., *supra*, discussing Element [1.1].

232. Khosravi discloses "a processor configured to" perform the function of Element [11.1]. *See* §XI.A.11. (preamble).

233. Khosravi discloses that its "[n]etwork interface may include the software, ***hardware*** and/or firmware to couple platform 101 to a network via wired or wireless pathways (e.g., a media access controller, wireless transceiver, ***digital signal processor***, antennae, radio, fabric interface, etc.)." EX1004, ¶[0025]. Khosravi's "platform" can connect ("couple") to "a cellular or a wireless broadband telephony network." *Id.*, ¶[0020]. *See also id.* ("wired or wireless … wide area network (WAN/WWAN)").

234. As such, the "digital signal processor" included in the hardware of Khosravi's "network interface" represents a processor configured to establish a connection between the secure modem at the network interface and a wireless network.

b. [11.2]: "establish, through the connection, a secure control channel between the secure execution environment and a network service controller;"

235. Khosravi alone and/or in view of Xu discloses and suggests Element [11.2]. *See* §XI.A.1.b., *supra*, discussing Element [1.2].

236. Khosravi discloses "a processor configured to" perform the function of Element [11.2]. *See* §XI.A.11. (preamble).

237. Khosravi discloses a "policy enforcement agent from among agent(s) 225 establish[ing] a secure communication channel over communication link 241 with policy decision point 282." EX1004, ¶[0062].

238. The "agent(s) 225A" of Khosravi, including the "policy enforcement agent," are included on the "service operating system" (SOS) 125/225 using "resources" 160/260 "represent[ing] memory and ***processing elements*** that are dedicated to or used independently by partitions 110 and 120, respectively." EX1004, ¶[0021].

239. As such, the "processing elements" located in "partition" 120/220 including the "policy enforcement agent" represent a processor configured to establish, through the connection, a secure control channel between the secure execution environment and a network service controller.

c. [11.3]: "receive, at the secure execution environment, via the secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more settings;"

240. Khosravi alone and/or in view of Xu discloses and suggests Element [11.3]. *See* §XI.A.1.c., *supra*, discussing Element [1.3].

241. Khosravi discloses "a processor configured to" perform the function of Element [11.3]. *See* §XI.A.11. (preamble).

242. Khosravi discloses a policy decision point 282 that creates and sends an "indication" (i.e., "one or more messages") which is received by the policy enforcement agent via communication link 241 and then forwarded to the manageability engine. *See* EX1004, ¶[0067].

243. Therefore, the "policy enforcement agent" receives the indication representing the one or more messages.

244. As referenced above, the "agent(s) 225A" of Khosravi, including the "policy enforcement agent," are included on the "service operating system" (SOS) 125/225 using "resources" 160/260 "represent[ing] memory and ***processing elements*** that are dedicated to or used independently by partitions 110 and 120, respectively." EX1004, ¶[0021]; *See* §XI.A.11.b., *supra*.

245. As such, the "processing elements" located in "partition" 120/220 including the "policy enforcement agent" represent a processor configured to receive, at the secure execution environment, via the secure control channel, one or more messages from the network service controller, the one or more messages comprising one or more settings.

d. [11.4]: "store the one or more settings in the secure memory partition accessible only from the secure execution environment; and"

246. Khosravi alone and/or in view of Xu discloses and suggests Element [11.4]. *See* §XI.A.1.d., discussing Element [1.4].

247. Khosravi discloses "a processor configured to" perform the function of Element [11.4]. *See* §XI.A.11. (preamble).

248. Khosravi discloses that the "resources 160A and 160B represent memory and ***processing elements*** that are dedicated to or used independently by partitions 110 and 120" for performing "***storage***" tasks. EX1004, ¶[0021].

249. The "processing elements" located in "partition" 120/220 including the "policy enforcement agent" represent a processor configured to store the one or more settings in the secure memory partition accessible only from the secure execution environment.

e. [11.5]: "control the wireless end-user device using the one or more settings."

250. Khosravi alone and/or in view of Xu discloses and suggests Element [11.5]. *See* §XI.A.1.e., *supra*, discussing Element [1.5].

251. Khosravi discloses "a processor configured to" perform the function of Element [11.5]. *See* §XI.A.11. (preamble).

252. Khosravi discloses that the "policy enforcement agent … interprets whether the decoded indication forwarded from manageability engine 150 grants the access requested by the access requester." EX1004, ¶[0068].

253. As referenced above, the "agent(s) 225A" of Khosravi are included on the "service operating system" (SOS) 125/225 using "resources" 160/260 "represent[ing] memory and ***processing elements*** that are dedicated to or used

independently by partitions 110 and 120, respectively." EX1004, ¶[0021]; *See* §XI.A.11.b., *supra*.

254. As such, the "processing elements" located in "partition" 120/220 including the "agent(s) 225A" represent a processor configured to control the wireless end-user device using the one or more settings.

7. Claim 17: "The wireless end-user device of claim 11, wherein the one or more settings include at least one of an access control setting, a traffic control setting, or an admission control setting."

255. Khosravi alone and/or in view of Xu discloses and suggests Claim 17. *See* §XI.A.2. (claim 7).

8. Claim 18: "The wireless end-user device of claim 11, wherein the one or more settings include a network setting or a device management communication setting."

256. Khosravi alone and/or in view of Xu discloses and suggests Claim 18. *See* §XI.A.3. (claim 8).

9. Claim 19: "The wireless end-user device of claim 11, wherein the secure execution environment is implemented at least in part as a hardware partition or a software partition."

257. Khosravi alone and/or in view of Xu discloses and suggests Claim 19. *See* §XI.A.4. (claim 9).

10. Claim 20: "The wireless end-user device of claim 11, wherein the secure execution environment is implemented at least in part in a virtual machine."

258. Khosravi alone and/or in view of Xu discloses and suggests Claim 20. *See* §XI.A.5. (claim 10).

B. Claims 2-6 and 12-16 Are Rendered Obvious Over Khosravi in View of Xu and Frank (Ground 2)

259. The following sections reference where elements of Claims 2-6 and 12-16 are disclosed and suggested by the prior art.

1. Claim 2: "The method of claim 1, wherein the one or more settings are associated with a service plan for using a service provided by the wireless network."

260. Khosravi in view of Xu and Frank discloses and suggests Claim 2. *See* Claim 1, *supra*.

261. As discussed for Elements [1.3] and [1.5], Khosravi's "network administrative policies" indicated by the policy decision point and enforced by the policy enforcement agent (EX1004, ¶[0070])) satisfies the claimed "one or more settings." *See* §§XI.A.1.c, XI.A.1.e.

262. For example, Khosravi expressly discloses that the received "indication reflects network administrative policies" and the "policy enforcement agent… is enforcing network administrative policies when it interprets the indication and configures the data traffic filters." EX1004, ¶[0070].

263. Khosravi's policy decision point "indicates what ***access*** the access requester can obtain to the network based on a comparison of the posture information to one or more network administrative policies." EX1004, ¶[0017] (emphasis added).

264. Thus, Khosravi's indication (reflecting network administrative policies) is associated with access to the service provided by the wireless cellular network.

265. Khosravi does not expressly disclose that its network administrative policies are associated with a "service plan."

266. However, Xu discloses service plans for device usage (e.g., "pay-per-use", "pay-as-you-go" plans). EX1005, ¶[0003], ¶¶[0024]-[0028], ¶[0030].

267. Xu discloses policies associated with such plans for using a service provided by the network, such as policies for metering. EX1005, ¶[0025] (discussing policies such as "[w]hether to meter and what specific items to measure"). Xu discloses that policy data 322 "may specify policy related operational directives such as metering, reporting, update requirements, etc." EX1005, ¶[0023].

268. Xu expressly refers to Frank for "techniques and measurements" relating to metering. EX1005, ¶[0025].[3] Thus, Xu explicitly motivates combination with Frank.

269. Frank discloses that "usage plans" are "[c]losely related to metering." EX1022, ¶[0036].

270. Similar to Xu's "pay-as-you-go" plans, Frank's usage plans "may include both actual use, i.e. time of operation or activations of a resource." *Id.* Frank further discloses that "usage plans may include unlimited use for a period of calendar time, use for a number of hours, use by application…, ***use by input/output (network connectivity)***," or combinations of the above. *Id.* Frank's service plans provide for access to the service provided by the wireless cellular network.

271. The "service provider 210" provides the usage plan "for determining operation of the computer." EX1022, ¶[0044]; *see also id.*, Fig. 6 (access to service denied at 520 based on lack of funds).

---

[3] Frank is the publication corresponding to Application No. 11/006,837 referenced at EX1005, ¶[0025].

272. Frank is analogous art to Khosravi, Xu, and the '464 Patent, as it relates to enforcement and security of policies on a computing device. EX1022, ¶[0004], ¶[0023] (local provisioning module provides security); ¶[0029].

273. It would have been obvious to implement Frank's techniques (including the "usage plan" that is "[c]losely related to metering") disclosed by Frank with a reasonable expectation of success in Khosravi-Xu given Xu's express teaching to use Frank for details about metering.

274. Xu discloses that metering "may include a variety of techniques and measurements" (EX1005, ¶[0025]) including monitoring user usage of the device as disclosed by Frank (EX1022, ¶[0028]).

275. It would have been obvious to associate Khosravi's network administration policies with a service plan as disclosed in Xu and Frank. Khosravi teaches that its network administrative policies may include one or more "monitoring policies, and the like" (EX1004, ¶[0016]) and a POSITA would have recognized that Xu's and Frank's metering/measuring policies are types of monitoring policy. EX1005, ¶[0025] ("Whether to meter and what specific items to measure may be a function of the policy….").

276. Xu motivates associating Khosravi's network administrative policies with usage-based service plans, e.g., policies associated with "paying for time on a

pay-per-use computer" and where "usage is charged per period or by activity." EX1005, ¶[0028], ¶[0030].

277. Frank refers to specific types of plans, including pay-as-you-go plans for accessing a network. EX1022, ¶[0036].

278. A POSITA would have several additional reasons to combine Frank with Khosravi and Xu.

279. First, a POSITA would have been motivated to do so to enforce business policies (as in Xu and Frank) in addition to security policies (as in Khosravi and Xu) when granting access to a network. Khosravi establishes trust to ensure that a device has the required posture before being given access to a network. EX1004, ¶[0077].

280. Frank and Xu disclose that business policies, including usage plans, need to be enforced in a secure manner. EX1022, ¶[0029], ¶[0033], ¶[0036]; EX1005, ¶[0023].

281. Such business policies, supplied by the service provider (EX1022, ¶[0044] ("service provider 210 may typically provide… at least one usage plan")), constitute an important policy that a POSITA would have been motivated to enforce in the secure manner provided by Khosravi.

282. For example, Xu discloses that a "stored value function 340" is implemented "for use in paying for time on a pay-per-use computer". EX1005, ¶[0027].

283. Xu discloses that "when usage is charged per period or by activity, a stored value balance may be maintained using the stored value function 340." *Id.*, ¶[0030].

284. Xu's stored value function 340 includes a balance associated with "pay-per-use" plans and plans where "usage is charged per period or by activity", and thus are associated "with a service plan that provides for access to the service" as claimed.

285. It would have been obvious to implement Khosravi's system to enforce security to maintain and monitor the stored value balance associated with the service plan as taught by Xu.

286. Khosravi discloses that its network administrative policies may include one or more "monitoring policies, and the like" (EX1004, ¶[0016]), and monitoring usage as taught by Xu would have been one obvious implementation.

287. Additionally, Xu expresses a need to "establish[] trust" in a multi-operating system environment (EX1005, ¶¶[0001]-[0002]), and establishes "hierarchical trust" for "posture reporting and policy enforcement" in relation to network access using multiple operating systems (EX1004, Title, ¶¶[0022]-[0023]).

288. Second, such modification would have constituted mere combination of prior art elements (Khosravi's network administration policies associating with Xu and Frank's pay-as-you-go service plans) according to known methods (e.g., Xu's technique of storing stored value function in secure memory and Khosravi and Frank's technique of the service provider providing the policies/plans) to yield predictable results (e.g., providing means to securely implement policies associated with the service plan).

289. Third, such modification would have involved the use of a known technique (Xu and Frank's enforcing business policies in a secure environment) to improve similar devices/methods (Khosravi's enforcing of network access based on network policies) in the same way (e.g., maintaining and monitoring a stored value balance associated with the service plan based on policies provided by a service provider).

290. Fourth, such modification would have involved mere application of a known technique (Xu and Frank's technique of metering to enforce a service plan) to the known device of Khosravi ready for improvement to yield predictable results. Khosravi, Xu, and Frank express the same security goals and operate in compatible architectures.

291. Employing Xu and Frank's teachings in Khosravi's system would have been straightforward and predictable and a POSITA would have had a reasonable expectation of success.

2. Claim 3: "The method of claim 1, wherein the secure modem further comprises a modem agent accessible only by the network service controller through another secure control channel."

292. Khosravi in view of Xu and Frank discloses and suggests Claim 3. *See* Claim 1, *supra*.

"the secure modem further comprises a modem agent"

293. As discussed for Claim 2, it would have been obvious to implement Khosravi's techniques to enforce network administrative policies associated with service plans in view of Xu and Frank. *See* §XI.B.1.

294. Khosravi discloses that its network administrative policies may include one or more "monitoring policies, and the like" (EX1004, ¶[0016]) and it would have been obvious to apply the monitoring of service usage of Xu and Frank to Khosravi's system, as further detailed below (EX1005, ¶¶[0003], [0025], [0028], [0030], [0038]; EX1022, ¶¶[0025]-[0028], [0036]).

295. Xu discloses techniques for enforcing policies based on monitored usage of the device, e.g., where "usage is charged per period or by activity" such as "paying for time on a pay-per-use computer." EX1005, ¶[0028], ¶[0030]. *See also*

id., ¶[0003] ("pay-per-use, pay-as-you-go, or other metered operation[s]"), ¶[0025], ¶[0038]. Xu teaches using monitoring techniques as described in Frank that involve a "metering module." EX1005, ¶[0025]; EX1022, ¶¶[0025]-[0028] ("metering module … for monitoring how often, how much, or over what period the computing device … or components thereof, are used."). *See also* EX1022, ¶[0028] ("metering module may … count application starts … when metering usage by application…."; ¶[0036] ("metering or usage data created or used by the metering module").

296. Xu/Frank's metering module as applied to Khosravi's platform constitutes the claimed "modem agent." For example, the metering module is a service measurement point, just like the modem agent in the '464 Patent. EX1001, 12:26-37 ("modem agent … provides a service measurement point … for measuring service usage by the device"); *see also id.*, 12:37-38 ("the service measure provided by the modem agent"), 14:26-31; EX1022, ¶¶[0025]-[0028] (device "monitor[s] how often, how much, or over what period the computing device … or components thereof, are used"), ¶[0036].

297. It would have been obvious to apply Xu/Frank's teachings concerning its metering module to Khosravi's secure modem to arrive at the claimed modem agent. For example, it would have been obvious to employ the metering module (i.e., the part of the metering module which monitors and reports user device usage, discussed herein) as part of Khosravi's manageability engine because that engine

"monitors platform 101" and meets the security requirements of metering noted by Frank. *See* §XI.A.1.a. *See also* EX1004, ¶[0078], Figure 6; EX1022, ¶[0036].

298. A POSITA also would have been motivated to include the metering module in the modem because it monitors "input/output (network connectivity)," which takes place in the modem and is therefore monitored in the modem. EX1022, ¶[0036] (disclosing metering use of "input/output (network connectivity)"), ¶[0017] (computing device may be "a cell phone" or "PDA"), ¶[0048] (service provider can be "a telephone company" that provides "an Internet connection"), ¶[0016] (account types include a "prepaid account" as well as "a telephone postpaid account"); *see also id.* ¶[0028] ("The metering module 454 may provide the mechanism for monitoring how often, how much, or over what period the computing device 400, or components thereof, are used.").

299. Additionally, Frank discloses that the metering module includes components (e.g., balance manager) that are "very sensitive and important to the secure operation of the" local provisioning module (LPM) and "therefore they are likely to be under various security attacks during the operation of the LPM." EX1022, ¶[0029].

300. Further, Frank discloses that "[m]etering or usage data created or used by the metering module 454 may need" to be stored in secure memory. EX1022, ¶[0036]. A POSITA therefore would have been motivated to protect the metering

module and related data, e.g., by executing it as part of the manageability engine's security logic in Khosravi and storing its data in secure memory. *See* EX1004, ¶[0053] ("at least a portion of memory 330 is memory that is exclusively accessible to security logic 310"); EX1022, ¶[0033] (LPM "store[s] balance data in a secured manner so that it cannot be tampered with by a user and so that it is accessible only by the LPM").

301. Frank's "local provisioning module (LPM)", like Khosravi's manageability engine, "may perform the function of enforcing a particular state on the computing device". EX1022, ¶[0025]. Frank's LPM further includes a communication module that "allows the LPM [] to communicate with the network". EX1022, ¶[0039], ¶[0024] ("the LPM [] is communicatively coupled to the service provider"). These similarities would have reinforced to a POSITA the motivation and reasonable likelihood of success in implementing the metering module as part of the modem.

"… accessible only by the network service controller through another secure control channel"

302. It would have been obvious for the modem agent (Xu/Frank's "metering module") to be "accessible only by the network service controller through another secure control channel" as claimed. Khosravi discloses connecting the manageability engine (ME) and policy decision point (PDP) via "***a secure***

communication channel… via communication links 243 and 241." EX1004, ¶[0047]; *see also id.*, ¶¶[0018]-[0020], ¶¶[0024]-[0027], ¶[0029], Figures 1-2.

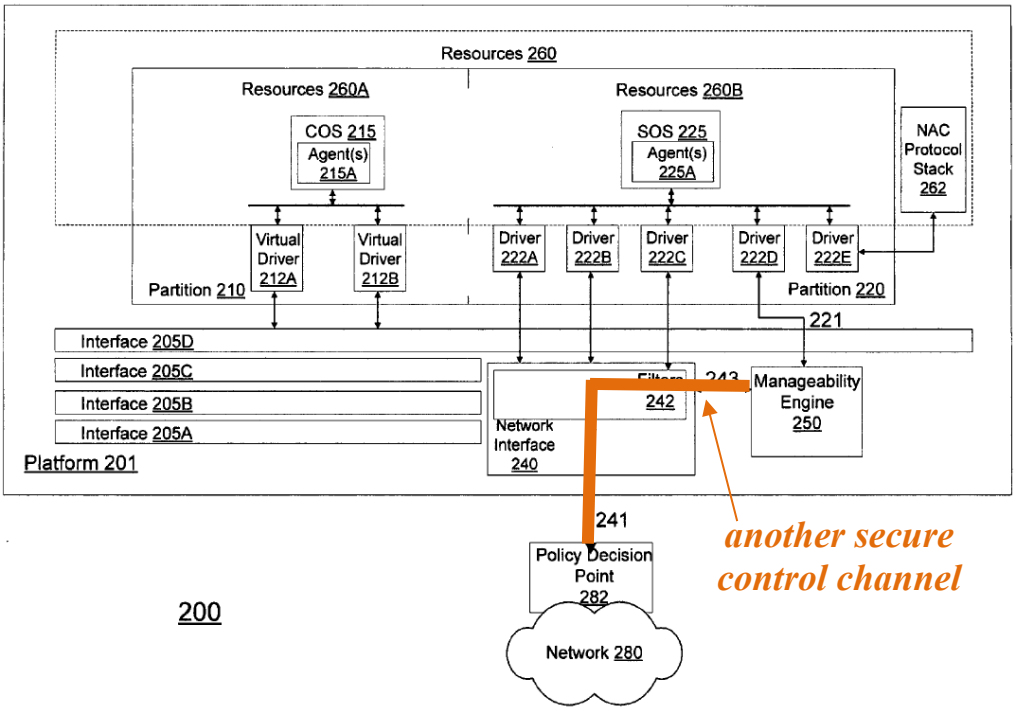


FIG. 2

Khosravi's "Another" Secure Control Channel
EX1004, Fig. 2 (Annotated)

303. As seen above, this "another secure control channel" includes communication link 243 and constitutes a distinct channel from the "secure control channel" recited in Element [1.2] which connects the SOS 125/225 to the policy decision point 182/282.

304. In the '464 Family, the term "channel" encompasses channels that overlap and go through each other. *See, e.g.,* EX1028, claim 3 ("the first secure

control channel connects the modem control link to the network service controller ***through the modem local channel***").

305. This manageability engine-to-policy decision point (ME-PDP) channel is a control channel because Khosravi discloses that the out-of-band, secure communication channel can be used for "remediation" when, for example, the SOS does not meet default network policies. The ME-PDP channel "has no data traffic from entities on platform 201 other than manageability engine 150" and is therefore a control channel. EX1004, ¶[0047].

306. Khosravi's dedicated, "out-of-band" channel is suited for avoiding unnecessary exposure to components (such as the SOS), sending data securely from the manageability engine to the policy decision point, without traversing or trusting other components. EX1004, ¶[0047] (out-of-band channel using links 241-243 "has no data traffic from entities on platform 201 other than manageability engine 150").

307. A POSITA would have utilized this dedicated channel between the metering module (modem agent) and PDP (network service controller) as an obvious choice to accommodate the PDP's access to the metering module with a reasonable expectation of success. Khosravi expressly discloses that the out-of-band channel is a "secure" channel between the ME and PDP. *Id.*, ¶[0047].

308. It is a "control" channel because the metering/usage data is for controlling the user's usage of device service plans. EX1005, ¶[0003], ¶¶[0024]-

[0028], ¶[0030], ¶[0036]. *See also* EX1022, ¶[0033] (data related to "controls for pay-per-use or pre-pay operation"). The out-of-band channel is conveyed via link 141/241 which passes through the wireless network. *Id.*, ¶[0062], ¶[0020]. Thus, Khosravi's out-of-band channel satisfies the claimed "another secure control channel."

309. Frank motivates accessing the metering module by the service provider at least through the use of "provisioning packets" that can be used to "update a balance in the balance manager" of the metering module. EX1022, ¶[0030].

310. Frank's metering module collects measurements/empirical data, i.e., user device usage data (EX1022, ¶[0028]), and would be located in the manageability engine in the obvious combination given that it collects the same type of data as Khosravi's posture feature.

311. Because the modem agent (Xu/Frank's "metering module") would constitute a part of the manageability engine, a POSITA would have looked to the direct ME-PDP channel as an obvious choice to accommodate the service provider's access to the metering module in the secure modem. Frank describes that the service provider uses such a link 212 "to send provisioning packets to add value to the computer". EX1022, ¶[0016]; *See* §§XI.A.1.a.-XI.A.1.b. *See also* EX1004, ¶¶[0016]-[0017], [0047], Figures 1-2.

312. In the combined system, the metering module would have been "accessible only by the network service controller through another secure control channel." In the combined system, the metering data itself would not be accessible to any part of the device outside of the manageability engine (EX1004, ¶[0053]; EX1022, ¶[0033] (metering data "accessible only by the LPM")).

313. To ensure security and control of communication between the metering agent and the network service controller, a POSITA would have been motivated to use the direct channel between the manageability engine (over links 243-241) and the policy decision point, which is the "another" secure control channel.

314. The only other channel between the PDP and the manageability engine would unnecessarily route information through other components like the SOS 225, thereby potentially increasing risk of exposure to potentially untrusted entities. *See* EX1004, ¶¶[0046], [0057]-[0058], Fig. 6 (ME monitoring is first Trust Layer exclusive of SOS).

315. To avoid unnecessary exposure, Khosravi's dedicated, "out-of-band" channel is suited specifically for this purpose: sending data securely from the manageability engine to the policy decision point, without traversing or trusting other components. EX1004, ¶[0047] (out-of-band connection using links 241-243 "has no data traffic from entities on platform 201 other than manageability engine 150").

316. A POSITA would have utilized this dedicated channel between the metering module (modem agent) and PDP (network service controller) as an obvious choice to accommodate the PDP's access to the metering module with a reasonable expectation of success.

317. A POSITA would have recognized that there is no need for multiple channels to communicate between the metering module and the network service controller, and as such using only one channel between the PDP and manageability engine would have been an obvious implementation.

3. Claim 4: "The method of claim 3, wherein the modem agent comprises a service measurement point for use of a service."

318. Khosravi in view of Xu and Frank discloses and suggests Claim 4. *See* Claim 3, *supra*.

319. Khosravi in view of Xu and Frank renders obvious the use of a modem agent (Xu/Frank's "metering module") comprising a service measurement point for use of a service. *See* §§XI.B.1.-XI.B.2. Xu/Frank's metering module comprises a service measurement point for measuring use of the service, as claimed. *Id. See, e.g.,* EX1022, ¶¶[0025]-[0028].

320. The '464 Patent specifies that the "modem agent" can be the "service measurement point." EX1001, 12:26-38.

4. Claim 5: "The method of claim 4, further comprising: communicating, by the modem agent through the another secure control channel, a first report of the use of the service to the network service controller."

321. Khosravi in view of Xu and Frank discloses and suggests Claim 5. *See* Claim 4, *supra*.

322. As explained for claim 3, Xu/Frank's metering module as applied to Khosravi's platform would satisfy the claimed modem agent. In the obvious combination, the modem agent (Xu/Frank's metering module) communicates through the another secure control channel, a first report (user device usage data collected by the metering module) of the use of the service to the network service controller. *See* §§XI.B.1.-XI.B.2.

323. Khosravi's manageability engine reports "posture information" which "includes integrity measurements that refer to empirical data collected from the hardware, software, and/or firmware of" the platform. EX1004, ¶[0027]. *See also id.*, ¶[0047] (information is conveyed between manageability engine and policy decision point via the ME-PDP secure control channel).

324. For example, integrity measurements can include "empirical data" and "log/trace files." *Id.* ¶[0028]. *See also id.*, ¶¶[0047] (manageability engine sends a request to policy decision point), [0053], [0059].

325. In the combined system, such log files and "empirical data" collected from the manageability engine would have included Frank's "[m]etering or usage data created or used by the metering module". EX1022, ¶[0036].

326. This information would have been sent via Khosravi's "another secure control channel" ("out-of-band network connection") which provides for direct communication between Khosravi's manageability engine and policy decision point. In particular, this direct ME-PDP path would have been obvious for this report in the combined system because Frank's metering or usage data are not needed or accessible from other components of the device, such as the SOS. EX1022, ¶[0033]. *See also* §§XI.B.2.-XI.B.3.

327. The metering/usage data ("first report") conveyed from the metering module to the PDP via the another secure control channel is distinct from the posture information sent from the SOS ("second report"), e.g., associated with operation of the COS (*see* §XI.A.1.b. (Element [1.2]) and §XI.B.5. (claim 6)) to the PDP via the secure control channel of Element [1.2].

328. The obvious combination employs repeated instances of a report, thereby satisfying "first" and "second" reports. Thus, the information communicated from the metering module to the policy decision point in Khosravi comprises a first report of the use of the service in the combined system.

329. Xu further motivates such reporting with its disclosure of a "reporting" operation. EX1005, ¶[0023] ("policy related operational directives such as metering, reporting" etc.).

330. By saving this metering or usage data in secure memory (e.g., in a log file), thereby allowing the manageability engine to include it in the reported posture information, the metering module communicates the usage data to the service controller. Thus, in the obvious combination, the modem agent (Xu/Frank's "metering module") communicates a first report of the use of the service ("metering or usage data created … by the metering module," *see* EX1022, ¶[0036]) to the network service controller (Khosravi's policy decision point) through the "another" secure control channel. *See* §XI.B.2.

5. Claim 6: "The method of claim 5, further comprising: communicating, using the secure execution environment through the secure control channel, a second report of the use of the service."

331. Khosravi in view of Xu and Frank discloses and suggests Claim 6. *See* Claim 5, *supra*.

332. Khosravi discloses that the secure execution environment (SOS 225 which includes agent(s) 225A) communicates a second report ("posture information") of the monitored use of the service through the secure control channel (communicated via "communication link" 141/241). For example, the SOS

"monitors communications between [policy decision point] 182 for network 180 and COS 115" in order to "enforce the policies and protect the COS." EX1004, ¶[0080]. *See also id.*, ¶[0030] (posture information is conveyed from SOS to policy decision point via the secure control channel).

333. Posture information related to such monitoring (constituting a "second report") is sent to the network service controller (i.e., policy decision point) by the SOS. EX1004, ¶[0082] ("[P]osture information may be provided by manageability engine 150 ***and/or SOS 125***."). EX1004, ¶¶[0043]-[0044] ("the posture information obtained and forwarded by manageability engine 150 ***and/or agent(s) 225*** is also forwarded to policy decision point 282 over a secure communication channel that is established via communication link 241.").

334. The second report is distinct from the first report given that (1) the second report is sent from the SOS whereas the first report is sent from the secure modem, and (2) they are communicated over distinct channels (the "secure control channel" and the "another secure control channel"). *See* §XI.A.1.b. and §XI.B.2.

6. Claim 12: "The wireless end-user device of claim 11, wherein the one or more settings are associated with a service plan for using a service provided by the wireless network."

335. Khosravi in view of Xu and Frank discloses and suggests Claim 12. *See* §XI.B.1. and §XI.A.6. (Claims 2 and 11).

7. Claim 13: "The wireless end-user device of claim 11, wherein the secure modem further comprises a modem agent accessible only by the network service controller through another secure control channel."

336. Khosravi in view of Xu and Frank discloses and suggests Claim 13. *See* §XI.B.2. and §XI.A.6. (Claims 3 and 11).

8. Claim 14: "The wireless end-user device of claim 13, wherein the modem agent comprises a service measurement point for use of a service."

337. Khosravi in view of Xu and Frank discloses and suggests Claim 14. *See* §XI.B.3. and §XI.B.7. (Claims 4 and 13).

9. Claim 15: "The wireless end-user device of claim 14, wherein the processor is further configured to: communicate, by the modem agent through the another secure control channel, a first report of the use of the service to the network service controller."

338. Khosravi in view of Xu and Frank discloses and suggests Claim 15. *See* §XI.B.4. and §XI.B.8. (Claims 5 and 14).

10. Claim 16: "The wireless end-user device of claim 15, wherein the processor is further configured to: communicate, using the secure execution environment through the secure control channel, a second report of the use of the service."

339. Khosravi in view of Xu and Frank discloses and suggests Claim 16. *See* §XI.B.5. and §XI.B.9. (Claims 6 and 15).

XII. SECONDARY CONSIDERATIONS

340. As discussed herein, all elements of the Challenged Claims were known in the art, and any differences would have been obvious to a POSITA based on the disclosures of the applied references and the knowledge in the art.

341. I am not aware of any secondary considerations that would alter my opinion.

342. Any secondary considerations evidence Owner may offer in this proceeding would be insufficient to overcome the strong evidence that the Challenged Claims are obvious.

XIII. CONCLUSION

343. For the reasons set forth above, it is my opinion that all elements of the Challenged Claims of the ’464 Patent are disclosed or suggested by the prior art. In my opinion, the Challenged Claims of the ’464 Patent are anticipated by and/or would have been obvious over the prior art.

344. In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

345. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: August 26, 2026

David H. Williams