

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,

Petitioner,

v.

TELCOM VENTURES LLC,

Patent Owner.

Case No. IPR2025-00973

U.S. Patent 9,462,411

DECLARATION OF CHUCK EASTTOM

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	QUALIFICATIONS	2
III.	MATERIALS CONSIDERED	6
IV.	SCOPE OF OPINIONS	6
V.	RELATED MATTERS	7
VI.	LEGAL STANDARDS	9
	A. Claim Construction.....	10
	B. Obviousness.....	11
	C. Motivations to Combine.....	13
VII.	LEVEL OF ORDINARY SKILL IN THE ART	14
VIII.	CLAIM CONSTRUCTION	15
IX.	TECHNOLOGY BACKGROUND.....	16
	A. Near Field Communications (“NFC”)	16
	B. Session Initiation Protocol (“SIP”)	18
X.	U.S. PATENT NO. 9,462,411 (“’411 Patent”) (Ex. 1001)	19
	C. Priority Date	19
	D. ’411 Patent Overview	19
	E. The ’411 Patent’s Prosecution History	21
XI.	ASSERTED REFERENCES	22
	A. Jain (Ex. 1017)	22
	B. Dua (Ex. 1018)	30

XII.	THE CHALLENGED CLAIMS OF THE '411 PATENT ARE NOT OBVIOUS.....	34
A.	Petitioner's Ground 1 Fails Because the Claims Are Not Obvious in View of Jain.....	34
i.	<i>Jain Does Not Disclose or Render Obvious the Claimed “communicating [by the smartphone] using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating.”</i>	34
ii.	<i>Jain Does Not Disclose or Render Obvious “detecting that a proximity criterion is satisfied between the smartphone and an entity.”</i>	42
iii.	<i>Jain Does Not Disclose or Render Obvious “selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor.”</i>	43
B.	Petitioner's Ground 2 Fails Because the Claims Are Not Obvious in View of Dua.....	49
iv.	<i>Dua Does Not Disclose or Render Obvious “selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor.”</i>	50
v.	<i>Dr. Almeroth Fails to Establish that Dua Discloses or Would Have Rendered Obvious “detecting that a proximity criterion is satisfied” and “selectively communicating . . . responsive to the proximity criterion having been detected as being satisfied.”</i>	55

XIII. SUMMARY AND OTHER REMARKS 65

Table of Exhibits

Exhibit No.	Description
2001	Interim Processes for PTAB Workload Management, Acting Director Memorandum (March 26, 2025)
2002	FAQs for Interim Processes for PTAB Workload Management
2003	EDTX Litigation Second Amended Docket Control Order (Jan. 29, 2025)
2004	Docket Navigator Statistics for Judge Rodney Gilstrap
2005	Samsung's Preliminary Invalidity Contentions (Feb. 3, 2025)
2006	Exhibit 411-C (Samsung's Subject Matter Eligibility Contentions)
2007	Telcom Ventures Complaint for Patent Infringement
2008	Non-Final Office Action, Application No. 17/730,174
2009	Declaration of Dr. Chuck Easttom
2010	<i>Curriculum Vitae</i> of Dr. Chuck Easttom
2011	Chiradeep BasuMallick, "What is NFC (Near Field Communication)? Definition, Working, and Examples" (Sept. 29, 2022), https://www.spiceworks.com/tech/networking/articles/what-is-near-field-communication/
2012	Liu et al., "Near-Field Communications: A Comprehensive Survey," IEEE (June 2025)
2013	"The Creation of the NFC Forum and its Vision" (2011) https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/NFCChips/nfcforum.html
2014	McHugh & Yarmey, "Near Field Communication: Introduction and Implication," ERIC (2012)
2015	Coskun et al., "The Survey on Near Field Communication," Sensors (June 5, 2015)
2016	"Cisco SIP IP Phone Administrator Guide, Release 7.5," Cisco https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7960g_7940g/sip/7_5/english/administration/guide/ver7_5/sipaxa75.pdf
2017	Rosenberg et al., RFC 3261 SIP: Session Initiation Protocol (June 2002), https://www.ietf.org/rfc/rfc3261.txt
2018	Schulzrinne et al., RFC 3550 RTP: A Transport Protocol for Real-Time Applications (July 2003), https://datatracker.ietf.org/doc/html/rfc3550

2019	Baughner et al., RFC 3711 The Secure Real-time Transport Protocol (SRTP) (Mar. 2004), https://www.rfc-editor.org/rfc/rfc3711.html
2020	Kurose et al., Computer Networking: A Top Down Approach, Chapter 7.4 (March 2012, 6th ed.) https://gaia.cs.umass.edu/kurose_ross/retired/protocols_real_time_interactive.pdf
2021	Rosenberg & Shockey, The Session Initiation Protocol (SIP): A Key Component for Internet Telephony, Computer Telephony, June 2000, at 124 https://gaia.cs.umass.edu/kurose_ross/retired/protocols_real_time_interactive.pdf
2022	Mealling & Daniel, RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record (Sept. 2000) https://www.cs.columbia.edu/sip/articles/SIP_tutorial_CT_Magazine_June2000.pdf
2023	Jeremy George, DNS Configuration, SIP.edu Cookbook (May 12, 2003), https://web.mit.edu/sip/sip.edu/dns.shtml
2024	Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International Telecommunication Union (Nov. 2010), https://www.itu.int/rec/t-rec-e.164-201011-i/en

I. INTRODUCTION

1. My name is Dr. Chuck Easttom, and I have been retained as a technical expert by counsel for Patent Owner Telcom Ventures LLC (“Telcom Ventures” or “Patent Owner”) to investigate and opine as to the validity of U.S. Patent No. 9,462,411 (“the ’411 Patent”) in view of Petitioner Samsung Electronics Co., LTD.’s (“Petitioner” or “Samsung”) Petition for *Inter Partes* Review (the “Petition”) (Paper 1).

2. This declaration is based on information currently available to me. To the extent that additional information becomes available, I reserve the right to continue my investigation and study, and thus may expand or modify my opinions as my investigation and study continues. I may also supplement my opinions in response to any additional information that becomes available to me, any matters raised by Petitioner and/or opinions rendered by Petitioner’s experts, or in light of any relevant orders from the Board.

3. My opinions are based on my years of education, research, and experience, as well as my investigation and study of relevant materials.

4. I am being compensated at the rate of \$550 per hour for my work in this case, including time spent testifying. I am also being reimbursed for reasonable fees and expenses, including hotel and travel expenses, incurred as a result of my work in this case. Neither I nor my company have received any additional compensation

for my work in this inter partes review. My compensation is not tied in any way to the substance of my testimony or the outcome of this proceeding. I have no other financial interest in this *inter partes* review or to the parties. I am available to offer these opinions at deposition and at trial if called upon to do so.

II. QUALIFICATIONS

5. I have summarized in this section my educational background, work experience, and other relevant qualifications. A true and correct copy of my curriculum vitae is attached as Ex. 2010 to Patent Owner's Preliminary Response which includes a list of all other cases in which, during the previous four years, I have testified at trial or by deposition.

6. I have over thirty years of experience in the computer science industry including extensive experience with computer security, mobile devices, and related topics. I have authored forty-five computer science books, including books on mobile devices and on cryptography. I also have authored over eighty research papers and am an inventor with twenty-seven computer science patents.

7. I hold a Doctor of Science (D.Sc.) degree in Cyber Security from Capitol Technology University (Dissertation Topic: "A Comparative Study of Lattice Based Algorithms for Post Quantum Computing"). I also hold a Doctor of Philosophy (Ph.D.) in Technology focused on nanotechnology (Dissertation Topic: "The Effects of Complexity on Carbon Nanotube Failures") from Capitol

Technology University. I also have a Doctor of Philosophy (Ph.D.) in Computer Science from the University of Portsmouth (Dissertation Topic: “A Systematic Framework for Network Forensics Using Graph Theory”). I also hold four Master’s degrees—one in Applied Computer Science, one in Education, one in Defense and Strategic Studies, and one in Systems Engineering.

8. I am currently an Adjunct Lecturer for Georgetown University teaching graduate courses in requirements engineering, artificial intelligence, cybersecurity, and cryptography. I am also an adjunct for Vanderbilt University teaching graduate computer science courses in quantum computing, digital forensics, algorithms, and cybersecurity. I also developed a graduate course in digital forensics for the University of Dallas and taught that course from 2019 to 2022.

9. I am a Senior Member and Distinguished Speaker for the Association of Computing Machinery (“ACM”) and a Senior Member and Distinguished Visitor of the Institute for Electrical and Electronics Engineering (“IEEE”). The IEEE is the world’s largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards for a wide range of engineering disciplines, including software development. I am also a Distinguished Visitor of the IEEE. I have been involved in IEEE standards creation for several years.

10. I have extensive experience with smart cards, Near Field Communications (“NFC”), the ISO/IEC 7810 standard for identification cards, the

ISO/IEC 7816 standard for electronic cards for identification, the ISO/IEC 14443 standard for contactless integrated circuit cards, the EMV standard, and related standards and technologies.

11. I have worked with smart cards as an authentication method since the Department of Defense began using the Common Access Card in the early 2000s. Near Field Communications were covered in networking courses that I took as part of my second Master's degree and in some of the networking certifications I hold. I have also worked with NFC since at least 2005. Specific certifications I hold that are relevant to NFC and/or mobile devices include:

- Associate of Systems Engineering (ASEP) from INCOSE (International Council on Systems Engineering) 275062
- CompTIA Network + Certified COMP10163630
- CompTIA Network Infrastructure Professional – CNIP COMP10163630
- EC Council Certified Security Administrator (ECSA) ECC947248
- EC Council Certified Encryption Specialist (ECES)
- CISSP – ISSAP – Certified Information Systems Architecture Professional #387731
- CISSP – ISSEP Information Systems Security Engineering Professional #387731

- Oxygen Phone Forensics Certified
- CompTIA Security+ COMP001021522764
- SC-300 - Microsoft Identity and Access Administrator

12. Specific publications that I have authored or participated in related to NFC, chip design, and/or mobile devices include the following:

- Easttom, C. (2005). Introduction to Computer Security. New York City, New York: Pearson Press.

- Easttom, C. & Dulaney, E. (2015). CompTIA Security+ Study Guide: SY0-401. Hoboken, New Jersey: Sybex Press.

- Easttom, C. & Roberts, R. (2018). Networking Fundamentals, 3rd Edition. Goodheart-Wilcox Publishing.

- Easttom, C. (2020). Modern Cryptography: Applied Mathematics for Encryption and Information Security 2nd Edition. New York City, New York: Springer Press.

- Easttom, C. (2021). An In-Depth Guide to Mobile Device Forensics. CRC Press.

- Easttom, C., Mei, N. (2019). Mitigating Implanted Medical Device Cybersecurity Risks. IEEE 10th Annual Computing and Communication Conference UEMCON.

- Easttom, C., Sanders, W. (2019). On the Efficacy of Using Android Debugging Bridge for Android Device Forensics. IEEE 10th Annual Computing and Communication Conference UEMCON.

13. I am qualified to render the opinions set forth herein. Under my definition of a POSITA, or Dr. Almeroth's definition, set forth below, I am and was as of the priority date of the '411 Patent, at least one of ordinary skill in the art.

III. MATERIALS CONSIDERED

14. I have reviewed the '411 Patent, including the challenged claims, prosecution history, and relevant patent family. The '411 Patent was marked as Exhibit 1001, and its prosecution history was marked as Exhibit 1005.

15. I also reviewed the Petition, and each of Exhibits 1001-1047 attached to the Petition.

16. In forming my opinions, I have considered the materials listed above and any other documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

17. I have also considered the understanding of a person of ordinary skill in the art around the time of the invention of the '411 Patent.

IV. SCOPE OF OPINIONS

18. I set forth my opinions throughout this declaration.

19. I understand that Petitioner argues that the challenged claims would have been obvious over U.S. Patent Application Publication No. 2009/0069049 (“Jain”) (Ground 1) and U.S. Patent Application Publication No. 2006/0165060 (“Dua”) (Ground 2).

20. I disagree. It is my opinion that the challenged claims of the ’411 Patent would not have been obvious in view of the asserted references, alone or in combination, for the reasons discussed herein.

V. RELATED MATTERS

21. Patent Owner filed a complaint against Petitioner in the Eastern District of Texas, styled *Telcom Ventures LC v. Samsung Electronics Co., Ltd. et al*, Case No. 2:24-cv-00691-JRG (filed August 21, 2024).

22. I understand Patent Owner asserted a total of eight patents against Petitioner in that action, U.S. Patent Nos. 9,462,411, 9,832,708, 10,219,199, 10,674,432, 11,770,756, 11,924,743, 11,937,172, and 12,028,793.

23. I understand that a jury trial for the suit between Patent Owner and Petitioner is expected to begin on June 1, 2026. Ex. 2003 at 1.

24. I understand that Petitioner filed IPR petitions against all eight patents asserted by Patent Owner. These are:

- IPR2025-00957, regarding U.S. Patent No. 11,937,172
- IPR2025-00972, regarding U.S. Patent No. 10,219,199

- IPR2025-00973, regarding U.S. Patent No. 9,462,411 (the instant Petition)
- IPR2025-00974, regarding U.S. Patent No. 10,674,432
- IPR2025-00975, regarding U.S. Patent No. 9,832,708
- IPR2025-00976, regarding U.S. Patent No. 11,924,743
- IPR2025-00977, regarding U.S. Patent No. 11,770,756
- IPR2025-00978, regarding U.S. Patent No. 12,028,793

25. I also understand Patent Owner is asserting the '411 Patent against Apple Inc., in the Northern District of California, styled *Telcom Ventures LLC v. Apple Inc.*, Case No. 5:25-cv-05041 (filed October 4, 2024).

26. I understand Patent Owner asserted the same eight patents against Apple Inc. in that action.

27. I understand that Apple Inc. has filed IPR petitions against all eight patents asserted by Patent Owner. These are:

- IPR2025-01232, regarding U.S. Patent No. 9,462,411
- IPR2025-01233, regarding U.S. Patent No. 9,832,708
- IPR2025-01234, regarding U.S. Patent No. 10,219,199
- IPR2025-01235, regarding U.S. Patent No. 10,674,432
- IPR2025-01236, regarding U.S. Patent No. 11,770,756
- IPR2025-01237, regarding U.S. Patent No. 11,924,743

- IPR2025-01238, regarding U.S. Patent No. 11,937,172
- IPR2025-01239, regarding U.S. Patent No. 12,028,793

28. I understand Google LLC has filed IPR petitions against seven of the eight patents asserted by Patent Owner in the above litigations. These are:

- IPR2025-01349, regarding U.S. Patent No. 11,924,743
- IPR2025-01389, regarding U.S. Patent No. 11,937,172
- IPR2025-01401, regarding U.S. Patent No. 12,028,793
- IPR2025-01408, regarding U.S. Patent No. 9,832,708
- IPR2025-01409, regarding U.S. Patent No. 11,770,756
- IPR2025-01419, regarding U.S. Patent No. 10,219,199
- IPR2025-01421, regarding U.S. Patent No. 10,674,432

29. As of the signing of this declaration, I have been retained to provide an opinion in all eight IPRs filed by Petitioner against the patents asserted by Patent Owner. I have also been retained to provide an opinion in each of the IPRs filed by Apple, Inc. and Google LLC.

VI. LEGAL STANDARDS

30. For purposes of this Declaration, I use the legal principles below as a guide in formulating my opinions. I am not an attorney, and I am not offering any opinions regarding legal matters; however, I have been informed by Telcom

Venture's counsel of the legal principles relevant to the issues herein and have the following understanding.

31. In an *inter partes* review proceeding, I understand that a party seeking to invalidate a claim must prove invalidity by a preponderance of the evidence, which I understand to mean evidence that convinces you that it is more likely than not that the particular proposition is true. I understand that the preponderance of the evidence standard applies to all aspects of an allegation of anticipation or obviousness, including the prior art status of the relevant reference(s).

A. Claim Construction

32. I understand the first step in determining whether or not a patent claim is valid is to properly construe the claims. I understand that the words of a claim are generally given their ordinary and customary (sometimes referred to as their plain and ordinary) meaning as understood by a person of ordinary skill in the art at the time of the invention. I also understand that, as a general matter, a claim should not be limited to a preferred embodiment, but that in certain cases, the scope of the right to exclude may be limited by a narrow disclosure or by positions taken, such as by statements made during patent prosecution. I also understand the claims must be supported by the specification. Also, to the extent that a patent claims priority to an earlier filed application, the claims must be supported by the disclosure in that

application. For terms that have not been construed, I understand that they should be afforded their plain and ordinary meaning to one of ordinary skill in the art.

33. I understand that the plain and ordinary meaning of a claim term is the meaning that a person of ordinary skill in the art would have understood at the time of the effective date in view of the specification and the prosecution history.

B. Obviousness

34. I understand that a claimed invention is not patentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as I understand it, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and objective indicia of non-obviousness to the extent they exist.

35. I understand that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the art at the time of the invention. A person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill is not an automaton, and may be able to fit together the teachings of multiple patents employing ordinary

creativity and the common sense that familiar items may have obvious uses in another context or beyond their primary purposes.

36. I understand that if a reference or proposed combination of references does not disclose or suggest all of the elements of a claim, the combination cannot render the claim obvious. I also understand that in order to combine prior art references to show obviousness, a person of ordinary skill in the art, without knowledge of the claimed invention, or without the use of hindsight, must have been motivated to combine the prior art by some suggestion or teaching in the prior art, the knowledge of one of skill in the art, or the nature of the problem to be solved.

37. I understand that an invention would have been obvious if a designer of ordinary skill in the art, facing the wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may have been obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would have recognized that it would improve similar devices in the same way, using the technique may have been obvious. I understand, however, that routine experimentation does not necessarily preclude patentability.

38. I understand that obviousness of a patent claim cannot properly be established through hindsight, and that elements from different prior art references, or different embodiments of a single prior art reference, cannot be selected to create the claimed invention using the invention itself as a roadmap. I understand that the claimed invention as a whole must be compared to the prior art as a whole, and courts must avoid aggregating pieces of prior art through hindsight that would not have been combined absent the inventors' insight.

C. Motivations to Combine

39. I understand that in deciding obviousness, it is appropriate to consider whether some teaching, suggestion, or motivation would have led a person of ordinary skill in the art to combine the invalidating references. I also understand that a reason to combine the teachings is needed even in a single-reference obviousness ground. I understand that there must be a showing of a suggestion or motivation to modify the teachings of that reference. I also understand that it is appropriate to look to a variety of factors when evaluating reasons to combine teachings or modify the teachings of a reference in an obviousness analysis, and that it is important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine or modify the prior art elements in the manner claimed. I understand that in determining obviousness, it may be helpful to consider whether there is some teaching, suggestion, or motivation to combine or modify

teachings and a reasonable expectation of success in doing so. I understand, however, that the teaching, suggestion, or motivation to combine inquiry is not required and may not be relied upon in lieu of the obviousness analysis outlined above. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was independently known in the prior art. I also understand that this is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.

VII. LEVEL OF ORDINARY SKILL IN THE ART

40. I understand that patent claims are to be interpreted from the viewpoint of one of ordinary skill in the relevant art. To determine the level of skill that would be “ordinary,” I understand that a person of ordinary skill in the art (“POSITA”) must generally have the capability of understanding the general principles that are applicable to the pertinent art.

41. In my opinion, a POSITA would have had at least a bachelor’s degree in electrical engineering, computer engineering, or a related field, with about two years of experience in wireless communications. More work or practical experience may qualify one not having the requisite education as a person with ordinary skill in the art while a higher level of education could offset less experience. I was at least a

person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under this definition.

42. I have reviewed Dr. Almeroth's Declaration (Ex. 1002). I understand that Dr. Almeroth contends that a POSITA would have had "at least a Bachelor of Science in electrical engineering, computer engineering, or similar fields and at least two years of practical experience in the field of secure wireless communication applications." Ex. 1002 ¶75. I disagree that there is a requirement for any experience in secure wireless communications. The claims of the '411 Patent do not have any requirement that the communications be "secure" such as encryption or encoding of the wireless communications. *E.g.*, Ex. 1001 at Cl. 1. I was at least a person of ordinary skill in the art as of the effective filing dates of the Asserted Patents under Dr. Almeroth's definition. Thus, I met the requirements of a POSITA under either my definition or Dr. Almeroth's definition as of the priority date of the '411 Patent.

VIII. CLAIM CONSTRUCTION

43. I understand that unless claim terms are provided an express construction, the terms must be given their plain and ordinary meaning.

44. I understand that Petitioner contends the "[n]o express constructions are required to find the '411 patent claims invalid." Pet. at 8. Other than explaining the plain and ordinary meaning, which I do below, I do not offer an opinion on the correct construction of any disputed terms, because, in my opinion, the Challenged

Claims are not taught or suggested by the prior art. I reserve the right to respond to any future claim construction argument asserted by Petitioner or Dr. Almeroth.

IX. TECHNOLOGY BACKGROUND

45. Below, I provide a brief overview of the history of contactless smart cards, or proximity cards, and the use of the same technologies in devices.

A. Near Field Communications (“NFC”)

46. Near Field Communication (“NFC”) is a broad term for short-range wireless communication technology that allows devices to exchange data when they are brought very close together. It is an extension of Radio Frequency Identification (“RFID”) technology, designed for secure, quick, and convenient data transfer.

47. NFC-capable devices can communicate with other NFC-capable devices in either active or passive mode. In active mode, both devices generate their own radio frequency field to transmit data. Ex. 2011 at 4. In passive mode, one device generates the radio frequency field while the other responds without a power source. *Id.*

48. A paper by Liu et al. provides a history of NFC, stretching back to the first understanding of the wave theory of light. Ex. 2012 at 4. That paper includes an overview of NFC history which is shown here:

TABLE I: Timeline of NFC Milestones

1678		•	Huygens presented his “Wave Theory of Light”.
1801		•	Young presented the double-slit diffraction experiment.
1815		•	Fresnel presented a series of memoirs about his understanding of diffraction.
1821		•	Fraunhofer constructed the first diffraction grating.
1887		•	Hertz demonstrated the existence of radio waves.
1891		•	Lord Rayleigh calculated the Rayleigh distance $\frac{A^2}{2\lambda}$.
1947		•	Cutler <i>et al.</i> reformulated the Rayleigh distance as $\frac{2A^2}{\lambda}$.
1956		•	Polk calculated the Fresnel distance.
1983		•	The first patent on RFID-based NFC was granted.
1984		•	Winters formulated the initial theory of MIMO.
1994		•	The first patent on MIMO was granted.
1996		•	Foschini laid down crucial theoretical foundations for MIMO.
1999		•	Driessen and Foschini utilized a spherical wave-based model to characterize LoS MIMO.
2003		•	Jiang <i>et al.</i> proposed to use spherical wave-based models to describe short-range MIMO.
2010		•	Marzetta proposed the concept of massive MIMO.
2015		•	Channel measurement results on massive MIMO necessitated the use of a spherical wave-based channel model.
2016		•	Prather proposed the concept of holographic MIMO.
2017		•	Hu <i>et al.</i> re-showed the potential of large intelligent surfaces in enhancing wireless transmissions.
2018		•	Amiri <i>et al.</i> proposed the concept of ELAA.
2023		•	The first tutorial review of NFC was presented.

49. Despite the long history of the physics and technology supporting NFC, NFC itself is relatively new. For example, the NFC Forum was created in 2004 to ensure maximum compatibility across all implementations of NFC technology. Ex. 2013 at 1. But the NFC Forum was not even founded until many years after the first standards related to smart cards were published. As late as 2012, *see* Ex. 2014 at 1, and even 2015, some sources still referred to NFC as an “emerging technology.” Ex. 2015 at 1.

50. Within the umbrella of NFC, there are numerous individual standards that are more specific. One such standard is ISO/IEC 14443. The ISO/IEC 14443

standard has four parts. Part 1 defines the physical properties of the card (e.g., size, durability, environmental tolerance). Part 2 specifies how the card is powered by the RF field of the reader and how modulation/coding are done for transmitting and receiving signals. Part 3 describes card initialization and how multiple cards in the field are identified and selected (anti-collision protocol). Part 4 defines higher-level data exchange protocols, including how commands and responses are structured.

51. The specificity of individual NFC standards means that any such standard is self-sufficient. In other words, a POSITA consulting one of these standards, such as ISO/IEC 144443, would have a complete solution for near field communications and would not need to look to other standards or technologies.

B. Session Initiation Protocol (“SIP”)

52. One of the prior art grounds identified by Petitioner, Dua, makes extensive reference to Session Initiation Protocol. *E.g.*, Dua ¶[0042]. A brief background of that protocol is provided for reference.

53. The standard SIP is the Session Initiation Protocol is an Internet Engineering Task Force (“IETF”)-standardized application-layer protocol defined in RFC 3261. Ex. 2016 at 1. It sets forth standards for establishing, managing, and terminating real-time multimedia communication sessions over IP, including VoIP. It functions as a request-response protocol, similar to HTTP, and uses text-based messages to control calls involving voice, video, and other digital media.

54. RFC 3261 describes SIP technology as

an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility [27] - users can maintain a single externally visible identifier regardless of their network location.

Ex. 2017 at 5.

55. SIP itself does not transmit media (like voice or video). Instead, protocols such as Real-Time Transfer Protocol (“RTP”) and secure RTP (“sRTP”) are used to transmit data. Ex. 2018 at 1 (describing RTP); Ex. 2019 at 1 (describing sRTP).

X. U.S. PATENT NO. 9,462,411 (“’411 Patent”) (Ex. 1001)

C. Priority Date

56. The ’411 Patent was filed as U.S. Patent Application No. 12/264,711, on November 4, 2008 and issued on October 4, 2016.

57. I understand that Petitioner does not challenge this priority date for purposes of the Petition, and I have assumed that each of the challenged claims is entitled to a priority date of November 4, 2008. Pet. at 6.

D. ’411 Patent Overview

58. The ’411 Patent describes mobile wireless devices and methods of using a mobile wireless device to engage in one or more communications modes,

but only when certain conditions or criteria are met, such as the satisfaction of a proximity condition and a value of a parameter, e.g., a physiological parameter, satisfying a criterion. Ex. 1001, 1:7-12; 5:65-6:16. The specification recognizes that the devices in the art were rigidly configured to perform a predetermined number of functions. *Id.*, 1:20-37. The '411 Patent addresses this rigidity problem by providing devices and methods that “may be used to enable adaptively one or more modes/functions of a device” based upon the satisfaction of certain criteria. *Id.*, 1:32-35. The specification explains that the invention advantageously allows “a mobile wireless device [to] act as a ‘wallet’ (over and above other functions) only when it is time to pay for an item and not act as a wallet when there is no need to do so.” *Id.*, 1:26-29.

59. The '411 Patent also describes estimating “a value of at least one other parameter that may be associated with the wireless communications device . . . and/or an entity (living or otherwise) that is associated with and/or is proximate to the wireless communications device.” *Id.*, 5:67-6:4. Such parameters include “velocity, acceleration, ToD, ToM, ToY, humidity, temperature, height, level of brightness, level of darkness, a blood pressure, a heart rate, a blood content, a physiological state, a psychological state, etc.” *Id.*, 6:5-9. These parameters can be estimated using “sensors that may, according to some embodiments, be device-based and/or network assisted/based means and/or sensors.” *Id.*, 6:13-15. The disclosed

wireless communications devices may be “configured to selectively enable a first communications mode/function” responsive to a value of such a parameter. *Id.*, 6:22-35.

E. The ’411 Patent’s Prosecution History

60. I have reviewed the prosecution history of the ’411 Patent.

61. U.S. Patent Application No. 12/264,711 was filed on November 4, 2008 and issued as U.S. Patent No. 9,462,411 on October 4, 2016.

62. The ’411 Patent issued after a total of nine rejections during prosecution. Ex. 1005 at 73, 126, 195, 239, 294, 329, 381, 419, 452. Applicant amended the claims in response to the first eight rejections, but did not make an amendment and traversed the ninth rejection. Ex. 1005 at 115-123 (amendments in response to the first Office Action); 157-165 (amendments in response to the second Office Action); 220-224 (amendments in response to the third Office Action); 266-269 (amendments in response to the fourth Office Action); 316-320 (amendments in response to fifth Office Action); 346-350 (amendments in response to the sixth Office Action); 407-409 (amendments in response to seventh Office Action); 431-433 (amendments in response to eighth Office Action); 478-485 (remarks in response to ninth Office Action).

63. In traversing the ninth Office Action, Applicant noted that the identified prior art did not disclose “refraining from communicating.” Ex. 1005 at 482.

Applicant also noted that the identified prior art relied upon in the Office Action stated that “mobile phones with Near Field Communication (NFC) transceivers and biometric authentication [sic] with a fingerprint sensor did not exist yet.” Ex. 1005 at 483 (emphasis in the original). Applicant noted that proposed Claim 1 assumes a smartphone with a first air interface and a sensor for physiological data that can sense a value of physiological data. Ex. 1005 at 483. Applicant noted that “[f]or at least these reasons, independent Claims 1 and 26 are patentable.” Ex. 1005 at 484.

64. The Examiner entered an Examiner’s Amendment coinciding with the Notice of Allowability. Ex. 1005 at 496-500. The Examiner’s Amendment introduced the final two limitations of the issued independent claims. (“selectively sending...” and “communicating by the smartphone using a second air interface...”). *Id.* The Examiner credited Applicant’s remarks in its final argument for allowability, filed on April 6, 2016, and the Examiner’s Amendment, with placing the application in position for allowance. Ex. 1005 at 500.

XI. ASSERTED REFERENCES

A. Jain (Ex. 1017)

65. United States Patent Application No. 2009/0069049 to Jain is titled “Interfacing Transaction Cards with Host Devices.” Jain was published on Mar. 12, 2009 and filed on Sep. 5, 2008. Jain focuses throughout on the functionality in a transaction card and independence from any particular mobile device to support

transaction capabilities. One example is the following: “[f]or example, the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110a.” Jain ¶[0023].

66. Figure 3 of Jain shows an exemplary transaction card.

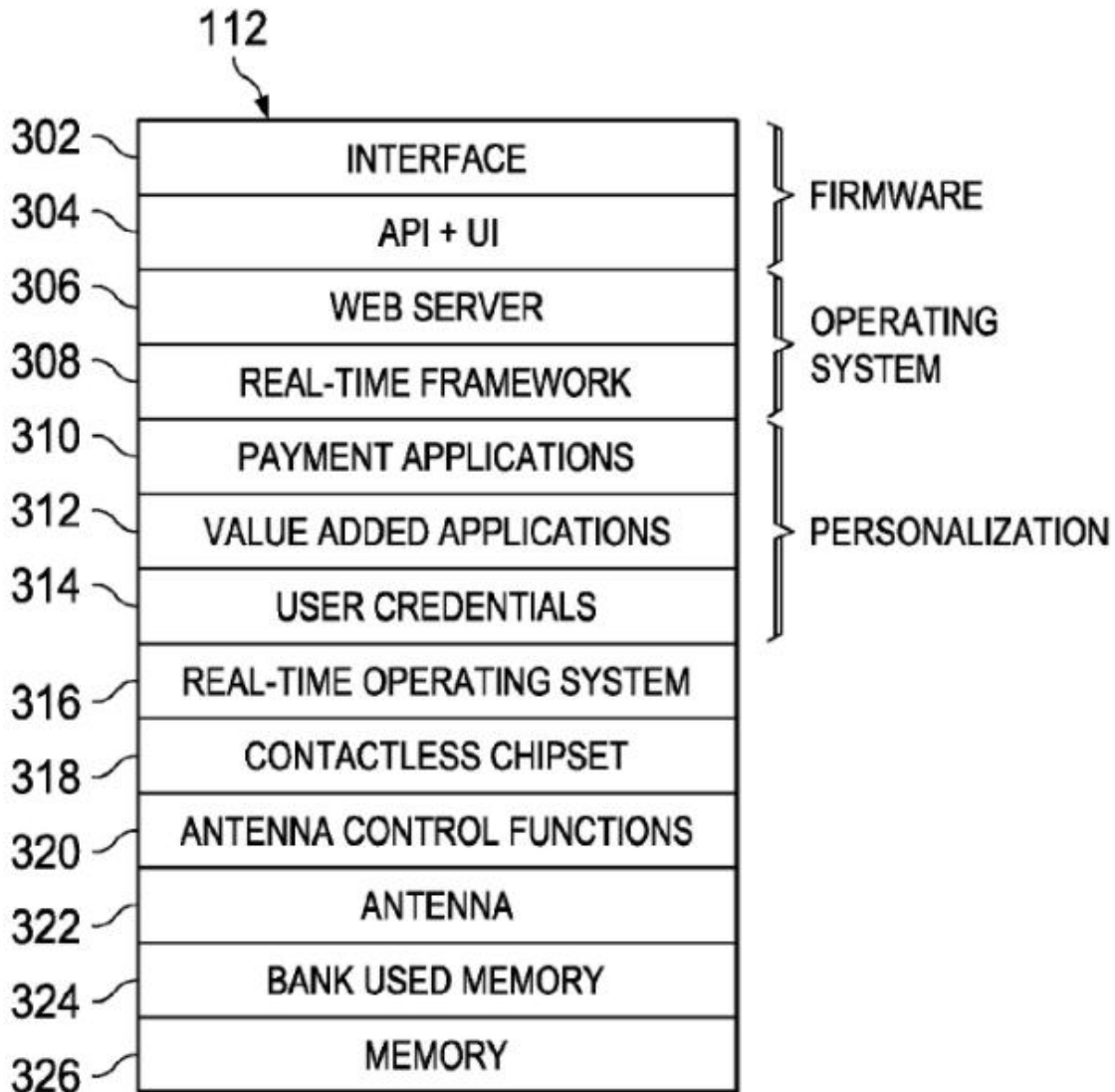


FIG. 3

Jain, Fig. 3; ¶¶[0009], [0049].

67. Jain focused on the relevant technology being in the transaction card so that the card could be used with a wide range of mobile devices. An example in Jain is the following: “[a]s used in this disclosure, the mobile devices 110 are intended to encompass cellular phones, data phones, pagers, portable computers, SIP phones,

smart phones, personal data assistants (PDAs), digital cameras, MP3 players, camcorders, one or more processors within these or other devices, or any other suitable processing devices capable of communicating information with the transaction card 112.” Jain ¶[0021].

68. Throughout multiple disclosures in Jain, the transaction card operates independently of any mobile host device. Jain, Abstract; ¶¶[0005], [0018], [0023], [0049], [0076]; cls. 1, 16. This approach allows Jain’s transaction card to interact with a wide range of mobile devices, and the mobile devices need not be altered in any way to support transactions.

69. Figure 1 of Jain explains how Jain’s transaction system functions using an intelligent card independent of any mobile device: “FIG. 1 is a block diagram illustrating an example transaction system 100 for wirelessly executing transactions using an intelligent card independent of a host device.” Jain ¶[0018].

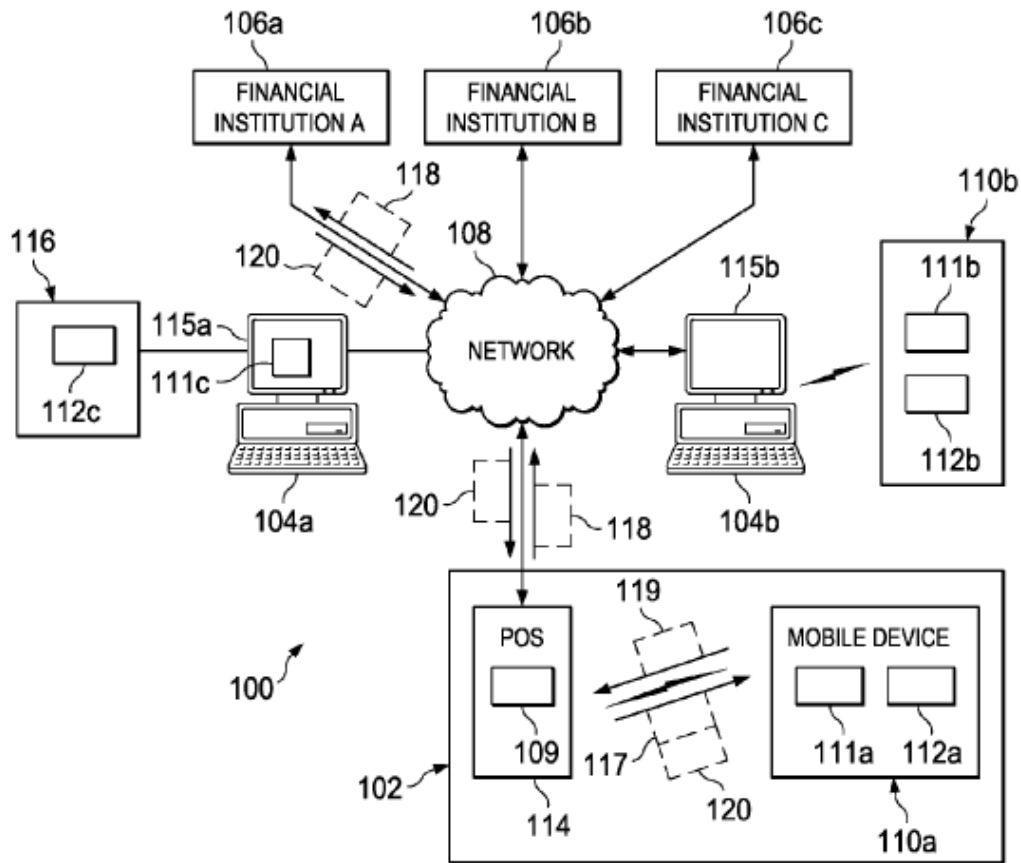


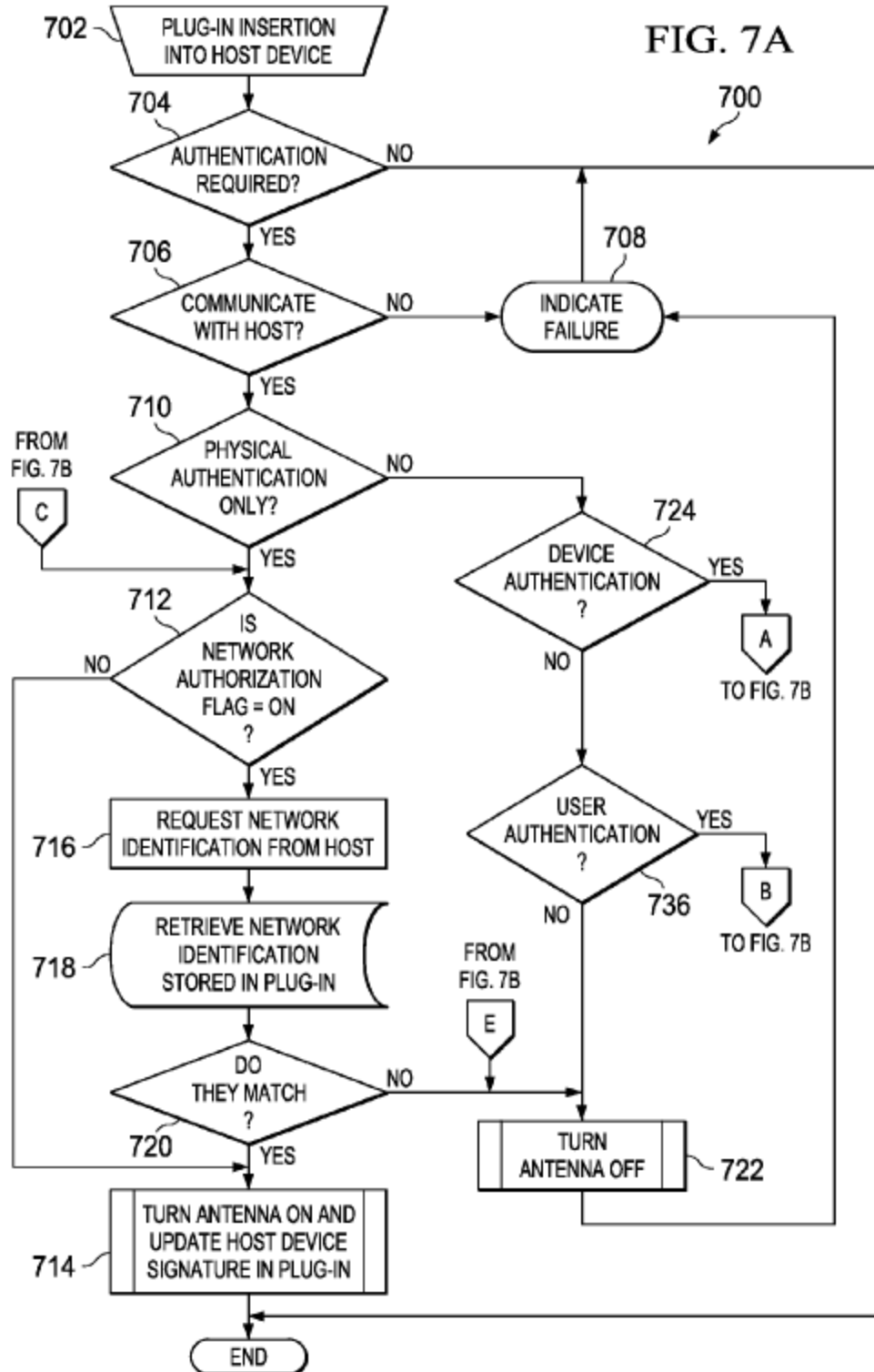
FIG. 1

70. The independence of the transaction card is perhaps most clearly disclosed in the following: “[i]n other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110.” Jain ¶[0022].

71. The independence of the transaction card is further disclosed in the following: “In some implementations, the transaction card 112 can be implemented differently. The transaction card 112 may be implemented as a Key FOB and remains live outside the mobile device 110 as a FOB. In this case, the transaction

card 112 may be passive and powered from an induction magnetic field generated by the POS 114.” Jain ¶[0029]. In fact, Jain discusses the transaction card as a master, and the mobile device as a slave. Jain ¶[0018].

72. Jain begins with connecting the transaction card to a mobile device which initiates a bootstrap process. Jain ¶¶[0065], [0072], [0077]. Figure 7 of Jain depicts that bootstrapping process:



73. This process only occurs when the transaction card is connected to the mobile device. After that point, the mobile device has been authenticated, and transactions can proceed.

74. The mobile device can be a cell phone, pager, portable computer, PDA, MP3 player, camcorder, digital camera, or other mobile device. Jain ¶[0021]. The mobile device provides a graphical user interface for the user to see and provide information. Jain ¶[0022].

75. There is a POS system that transmits a request to execute a transaction to the transaction card. Jain ¶[0019].

76. Jain provides an even more detailed description of the transaction card and its relationship to the mobile device in the following:

The transaction card 112 can include any software, hardware, and/or firmware configured to wirelessly execute transactions with the POS device 114. For example, the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110 a. In other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110. The transaction card 112 may execute transactions with the POS device 114 using short range signals such as NFC (e.g., ISO 18092/ECMA 340), ISO 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals (e.g., POS 114). In some implementations, the transaction card 112 may include one or more chipsets that execute an operating system and security processes to independently execute the transaction. In doing so, the mobile device 110 does not require additional hardware, software, and/or firmware to wirelessly execution a transaction with the POS 114 such as an NFC transaction.

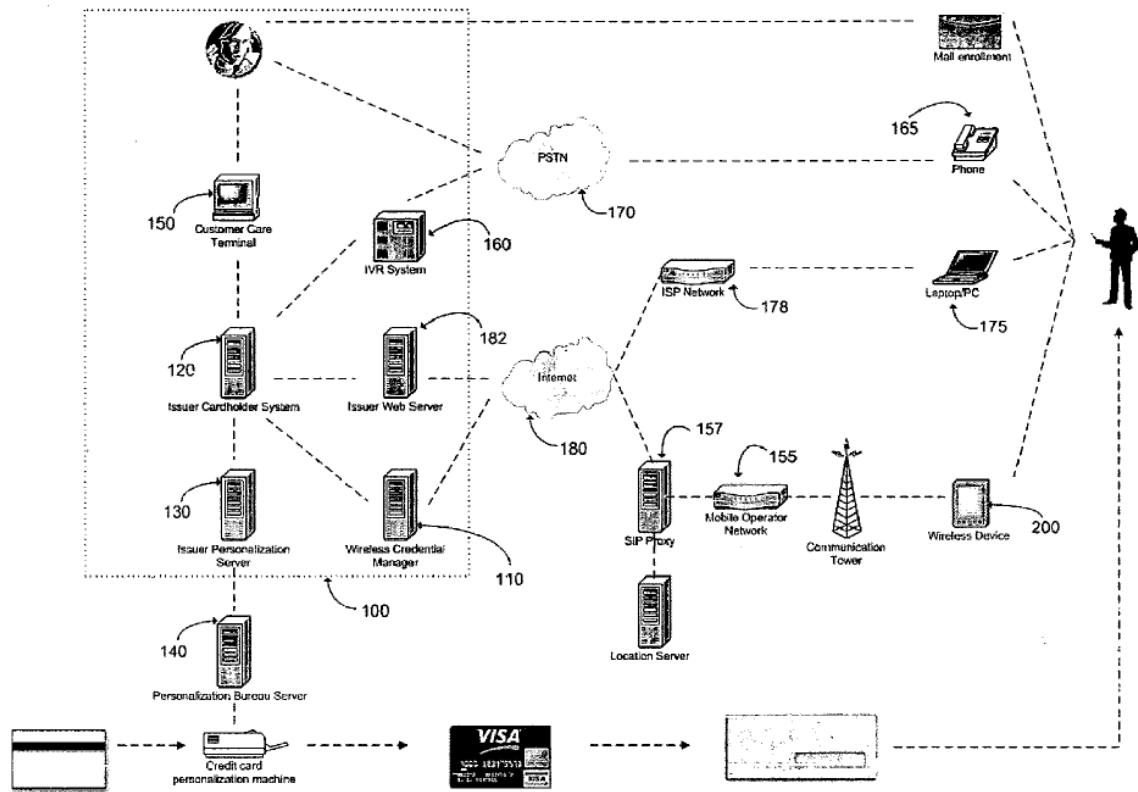
Jain ¶[0023].

77. The mobile device is essentially a host for Jain's transaction card. The mobile device provides a GUI so the user can see information, *see* Jain ¶¶[0019], [0022], and interfaces with the transaction card. Jain ¶¶[0021], [0022], [0025]. The mobile device may also provide access to cellular communications. Jain ¶¶[0021], [0023], [0042], [0043], [0068].

B. Dua (Ex. 1018)

78. United States Patent Application No. 2006/0165060 to Dua is titled "Method and Apparatus for Managing Credentials Through a Wireless Network." The Examiner considered Dua during the prosecution of two other applications that depend from the '411 Patent. Dua was considered during prosecution of U.S. Patent No. 10,674,432. Ex. 1009 at 169. The Examiner also considered Dua during the prosecution of U.S. Patent No. 10,660,015. Ex. 1008 at 212.

79. Dua was filed on Jan. 21, 2005 and published on July 27, 2006. Dua describes a methodology for conducting transactions, including financial, over a wireless network. Dua, Abstract. Dua describes itself as follows: "[t]he ultimate goal of the present invention is to securely, accurately and rapidly distribute credentials to the proper wireless devices based upon the actions of credential issuers." Dua ¶[0038]. Figure 1 of Dua provides an overview of the system according to one embodiment:



Dua, Fig. 1.

80. Figure 2 of Dua provides a flowchart illustrating the steps in the process for issuing a credential according to a preferred embodiment:

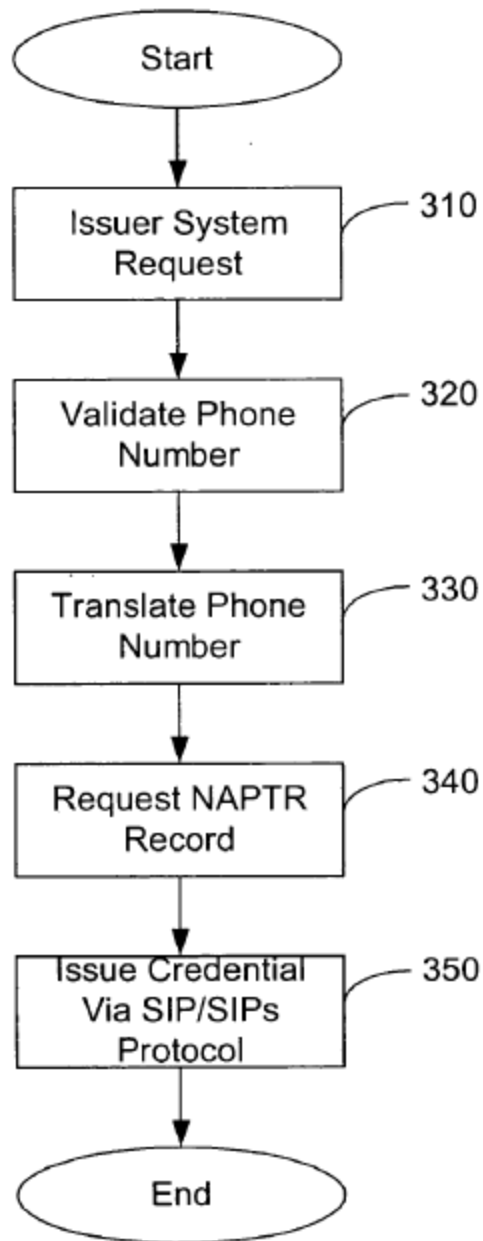


FIG. 2

Dua, Fig. 2.

81. Dua depends heavily on SIP (Session Initiation Protocol). SIP is mentioned 375 times in Dua. RFC 3261 was the active standard for SIP at the time

that Dua was filed. SIP focuses on establishing communication. Ex. 2017 at 1. Once said communication is established, then another protocol such as RTP or sRTP is used to transmit any data. Ex. 2020 at 10; Ex. 2021 at 3-4. In fact, Dua itself makes this clear:

Associated with SIP is the SDP, defined in RFC 2327. SIP is used to invite one or more participants to a session, while the SDP-encoded body of the SIP message contains information about what media encodings (for example, voice, video) the parties can and will use. After this information is exchanged and acknowledged, all participants are aware of the participants' IP addresses, available transmission capacity, and media type. Then, data transmission begins, using an appropriate transport protocol. Typically, the RTP is used.

Dua ¶[0110].

82. In Dua, credentials are issued by the issuer's system and then transmitted to the wireless device. Dua ¶[0040]. Credentials are distributed by the Wireless Credential Manager. Dua ¶[0043].

83. Dua makes frequent reference to Naming Authority Pointer ("NAPTR"). NAPTR records provide a mapping from a domain to the Service Records ("SRV") record for contacting a server with the specific transport protocol in the NAPTR service field. Ex. 2022 at 3-4; Ex. 2023 at 3. NAPTR is closely related to E.164, an international public telecommunication numbering plan. Ex. 2024 at 3.

XII. THE CHALLENGED CLAIMS OF THE '411 PATENT ARE NOT OBVIOUS

A. Petitioner's Ground 1 Fails Because the Claims Are Not Obvious in View of Jain

84. The following paragraphs address examples of why certain limitations of claims are not obvious in view of Jain.

85. While I address certain limitations to demonstrate that each of the challenged claims are not unpatentable, I reserve the right to supplement this declaration to include additional information and opinions related to any and all challenged claims and claim elements.

i. Jain Does Not Disclose or Render Obvious the Claimed "communicating [by the smartphone] using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating."

86. Independent claim 1 requires a "a smartphone." Independent claim 3 is an apparatus claim for "a smartphone." Both dependent claims of the '411 Patent depend from one of these independent claims, and therefore all claims of the '411 Patent require a "smartphone." The claimed smartphone has the functionality of "communicating [by the smartphone] using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating." '411 Patent, Cls. 1, 3.

87. The '411 Patent contemplates a smartphone or "wireless communication device" that is itself capable of both a first and second

communications mode. '411 Patent, 2:60-3:2, 7:14-31. Similarly, it is the “mobile subscriber device 14” of the '411 Patent that itself can “authorize and complete a financial transaction such as the payment of a toll and/or of an item at a check out line.” '411 Patent, 9:15-22. It is also the “wireless communications device” which may be “configured to estimate a value of at least one other parameter that may be associated with... an entity (living or otherwise) that is associated with and/or is proximate to the wireless communications device.” '411 Patent, 5:65-6:4. But rather than point to a single mobile device in Jain that meets these limitations, Dr. Almeroth points to two separate pieces of hardware that purportedly meet these limitations. *E.g.*, Ex. 1002 ¶96 (pointing to the “smartphone’s touch screen or keypad” as a smartphone-based sensor); ¶111 (pointing to the reader mode of the transaction card as detecting that a proximity criterion is satisfied); ¶¶128-129 (pointing to the “special NFC hardware” of transaction card 112 as the first air interface); ¶150 (pointing to the cellular capabilities of the mobile device 110 as the second air interface).

88. Whenever the '411 Patent does refer to multiple devices engaged in short-range communications, it is two separate, fully functional devices. For example:

The entry of the first device 14 within area 22 can selectively enable a mode and/or a function at device 14 and can optionally enable a mode and/or a function at device 15 based, according to some embodiments, on a proximity criterion to area 24. For example, if device 14 owned

and/or operated by a user is at a first store within area 22 and the device 15 owned/operated by, for example, the user's spouse is at a second store within area 24, then the user's spouse at device 15 can complete a purchase within area 24 based on the user's presence with device 14 within area 22.

'411 Patent, 10:29-39.

89. Thus, whenever the '411 Patent refers to multiple devices, they are still both inherently capable of performing both short-range wireless communications, and a second mode of communication such as cellular communications.

90. Dr. Almeroth argues that Jain renders obvious “selectively communicating by the smartphone using a first air interface” because Jain “discloses a plurality of air interfaces with which the smartphone is capable of communicating, including: (1) a first air interface for short-range communications (such as for contactless transactions) with POS device 114; and (2) a second air interface for cellular and other communications with a cellular network, for example.” Ex. 1002 ¶¶128, 159. I disagree. Jain does not disclose and would not have rendered obvious “communicating [by the smartphone] using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating” of claims 1 and 3 because Jain does not disclose a single device, i.e., a smartphone, capable of communicating over multiple air interfaces in which one of those air interfaces is a short-range link, as required by the claim.

91. Unlike the claims at issue, which rely on a single device—a smartphone—to perform a series of steps, Dr. Almeroth switches between the mobile device of Jain and the transaction card of Jain when rendering his opinions. Dr. Almeroth’s position that the claimed “smartphone” can be met by capabilities of the transaction card 112 of Jain is incorrect. Dr. Almeroth alleges that “Jain’s first air interface may utilize ‘NFC (e.g., ISO 18092/ECMA 340), ISO 14443 type A/B, ISO 51693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals.’” Ex. 1002 ¶129 (citing Jain ¶[0022]). But this first air interface capability is available with “special NFC hardware with reader mode capability as part of the transaction card 112.” Jain ¶[0030]. The “mobile device 110” and the “transaction card 112” of Jain are separate and distinct pieces of hardware.

92. Jain touts that the “mobile device 110 does not require additional hardware, software, and/or firmware” *because* the transaction card itself already has the required functionality, such as NFC. Jain ¶[0023], *see also* ¶[0018] (“An intelligent card is a device configured to . . . access or otherwise execute services (e.g., transactions) independent of the host device.”). In fact, Jain discloses a transaction card that “include[s] any software, hardware, and/or firmware configured to wirelessly execute transactions with the POS device 114” *independent of the*

mobile device. Jain ¶[0023] (explaining that “the transaction card 112 may include one or more chipsets that execute an operating system and security processes to independently execute the transaction”). For example, the Jain transaction card itself includes hardware to transmit short-range signals, such as NFC, and the mobile device does not. *Id.* In fact, Jain uses the phrase “independent of the mobile device” or “independent of the host device” several times. Jain, Abstract, ¶¶[0005], [0018], [0023], [0049], [0076], cls. 1, 16). A POSITA would understand that the independence of the transaction card from the mobile/host device is an essential element of Jain.

93. Dr. Almeroth never alleges that the independent mobile device 110 and transaction card 112 of Jain disclose using a single device to perform the claimed communications. Nor does he allege that Jain renders such a device obvious. Jain specifically requires a *distinct* transaction card that is “*independent*” of the mobile device. Jain ¶[0076] (“The intelligent card 806 is configured to . . . execute transactions *independent of the host device 810*.”) (emphasis added); *see also id.* ¶[0023] (“[T]he transaction card 112 may wirelessly execute transactions *without aspects of the transaction being executed by the mobile device 110*.”) (emphasis added). Jain also makes clear that the transaction card alone, rather than the combination of the transaction card and mobile device, is essential to executing transactions. *See id.* ¶[0018] (“*By providing the intelligent card*, the system 100

may wirelessly execute transactions”) (emphasis added). Accordingly, because Jain discloses an independent transaction card separate from the mobile device which completes the claimed short-range communications, the transaction card cannot be considered part of the mobile device such that the combination of the two devices discloses the claimed “smartphone.” This is even more true because the mobile device, on its own, does not have the capability to perform short range communications.

94. Dr. Almeroth also argues that “mobile device 110 having transaction card 112 therefore selectively communicates with POS device 114 over NFC or other short-range communication medium” Ex. 1002 ¶135. But there is in fact no requirement in Jain that the smartphone be involved in the disclosed transactions or communications at all. Jain ¶[0023] discloses that “transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110a. In other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110.” Jain ¶[0023]. It is this independent transaction card which “may execute transactions” using “short range signals such as NFC (e.g., ISO 18092/ECMA340), ISA 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals.” *Id.* It is the

transaction card and the transaction card alone that performs any transactions or communications using signals that Dr. Almeroth alleges correspond to the first air interface. Ex. 1002 ¶129. Dr. Almeroth also points to Figure 1 of Jain as showing the claimed “first air interface.” Ex. 1002 ¶¶129-130. But Figure 1 describes a system where the transaction card is connected to—not subsumed into the mobile device to create a smartphone. This retained independence is clear in the full context of Figure 1, which shows both the transaction card placed within the mobile device, but also the mobile device within the store 102. Applying Dr. Almeroth’s logic, the mobile device located within the store would itself become a part of the store—a result not contemplated by Jain. The transaction card remains independent.

95. Not only does Dr. Almeroth fail to allege that the “communicating by the smartphone using a first air interface of a plurality of air interfaces would have been rendered obvious by Jain, he admits that the hardware responsible for communicating on the first air interface is separate from the smartphone itself. In his background discussion of Jain, Dr. Almeroth admits that “[t]he transaction card works together with a smartphone to provide a user with the ability to wirelessly execute transactions with financial institutions and point-of-sale (POS) retail terminals to enable users to use the smartphone for mobile payments.” Ex. 1002 ¶86 (citing Jain ¶[0019]).

96. Jain in fact teaches away from a smartphone having the capabilities of the transaction card. Jain emphasizes that an independent transaction card capable of executing transactions allows for greater versatility in the types of host mobile devices—a benefit that would be lost if the transaction card were integrated into the mobile device. *See* Jain ¶[0021] (identifying digital cameras, pagers, MP3 players, camcorders and portable computers as possible mobile devices); *see also id.* ¶[0035] (“For example, the user may want to re-personalize the transaction card 112 ***to change host devices, to have multiple host devices***, and/or other reasons.”) (emphasis added); ¶[0041] (“financial institutions 106 may assign one or more mobile host devices 110 to a transaction card 112”). Assigning a transaction card to multiple host devices, to devices that are not phones, and using the transaction cards independently, are benefits that would be lost if Jain’s mobile device and transaction card were one. Any integration of the transaction card with the mobile/host device would be entirely contrary to Jain and would make Jain unable to work with multiple devices.

97. Therefore, Jain fails to disclose or render obvious at least “communicating [by the smartphone] using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating” of independent claims 1 and 3.

ii. Jain Does Not Disclose or Render Obvious “detecting that a proximity criterion is satisfied between the smartphone and an entity.”

98. Independent claims 1 and 3 require “detecting that a proximity criterion is satisfied between the smartphone and an entity.” All dependent claims depend from one of these claims, and thus incorporate this limitation.

99. Dr. Almeroth argues that Jain discloses this limitation. Ex. 1002 ¶111. I disagree.

100. In support of his position, Dr. Almeroth first misstates Jain. Dr. Almeroth alleges that “*the smartphone* (mobile device 110 having transaction card 112) first ‘wirelessly receive[s] a request from the POS device 114 to execute a transaction and/or provide a response.’” Ex. 1002 ¶111 (emphasis added) (quoting Jain ¶[0023]). That is not what Jain says. Jain says that “*the transaction card 112* may execute one or more of the following: wirelessly receive a request from the POS device 114 to execute a transaction and/or and [sic] provide a response.” Jain ¶[0023] (emphasis added). Jain describes *the transaction card* as capable of “execut[ing] transactions with the POS device 114 using short range signals such as NFC.” Jain ¶[0023]. Because the transaction card has the NFC capability, “the transaction card 112 may wirelessly execute transactions *without aspects of the transaction being executed by the mobile device 110*. *Id.* But the claimed “detecting that a proximity criterion is satisfied” step must be met between the smartphone and the entity. Jain

discloses the proximity criterion being met by the transaction card 112, not the mobile device 110. For the same reasons as above with respect to Section XII.A.i, Jain similarly does not disclose the claimed “proximity criterion having been satisfied between the smartphone and the entity.” *See supra* Section XII.A.i..

101. Next, Dr. Almeroth argues that Jain renders this limitation obvious. Ex. 1002 ¶¶112-117. But Dr. Almeroth fails to explain why a POSITA would contravene the teaching of Jain to implement an NFC capability on the mobile device rather than the transaction card. *See* Jain ¶[0023]. Furthermore, implementing the transaction cards capabilities in the smartphone would be contrary to the teachings of Jain. It would also prevent Jain from being used on multiple mobile devices. Therefore, Jain fails to disclose or render obvious “detecting that a proximity criterion is satisfied between the smartphone and an entity” of independent claims 1 and 3.

iii. Jain Does Not Disclose or Render Obvious “selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor.”

102. Jain does not disclose and would not have rendered obvious limitation 1.c, which claims “selectively communicating by the smartphone ... responsive to the proximity criterion having been detected as being satisfied **and responsive** to a value of the **physiological data** associated with a living organism that was **sensed by the smartphone using the smartphone-based sensor**” (emphasis added), nor the

similar limitation of 3.c, which claims “selectively communicating using a first air interface of a plurality of air interfaces with which the smartphone is capable of communicating, responsive to the proximity criterion having been detected as being satisfied *and responsive* to a value of the *physiological data* associated with a living organism that was *sensed by the smartphone using the smartphone-based sensor*” (emphasis added). Petitioner alleges that “mobile device 110 also does not communicate with POS device 114 unless its user has been authenticated.” Pet. at 27. However, this allegation relies on impermissibly mixing and matching various processes disclosed in Jain, none of which actually disclose “selectively communicating . . . responsive to the proximity criterion having been detected as being satisfied *and responsive* to a value of the *physiological data* associated with a living organism that was *sensed by the smartphone using the smartphone-based sensor*.”

103. Dr. Almeroth sets forth the majority of his analysis of this limitation by reference to limitation 1[a]. Ex. 1002 ¶134. There, Dr. Almeroth alleges that “Jain discloses [sensing by a smartphone using a smartphone-based sensor] in at least two instances.” Ex. 1002 ¶93. I disagree.

104. Dr. Almeroth first points to the “initial bootstrapping” process of Figure 7B as disclosing “authenticating a user using a PIN number or biometrics.” Ex. 1002 ¶94. However, the bootstrapping of Figure 7B does not meet the limitation

communicating . . . responsive to a value of the physiological data . . . sensed by the smartphone using the smartphone-based sensor.

105. Dr. Almeroth first asserts that a user's PIN, if input using the touch screen of a mobile device, satisfies the physiological limitation. Ex. 1002 ¶¶96. I disagree, as a PIN is not "physiological data." Even if a PIN is input via a touch screen, thus utilizing a physiological process (touch), the data internalized by the smartphone is the PIN itself, not any data regarding the touch. *See* Jain ¶[0075] (checking a provided PIN against a locally stored PIN). The use of a touch screen to provide a PIN thus does not meet the limitation "sensing by a smartphone, using a smartphone-based sensor, physiological data" of limitation 1[a] nor "communicating . . . responsive to a value of the physiological data . . . sensed by the smartphone using the smartphone-based sensor" of limitation 1[c]. A capacitive touch screen is not physiological data.

106. Further, to the extent the process disclosed in Figure 7B contemplates alternative inputs such a "biometric information," the entire process disclosed in Figure 7B still fails to disclose or obvious the limitations of the '411 Patent, which claim communicating by the smartphone *in response to both* a proximity criterion *and* a value of the physiological data associated with a living organism.

107. The process described in Figure 7B is the process of "automatically bootstrapping an intelligent card in response to at least insertion into a host device."

Jain ¶[0072]. This bootstrapping process of Jain is done independently of any process involving the first air interface, alleged to be NFC, or any process regarding a proximity criterion. Instead, the PIN and/or “biometric information” of Jain is input through GUI 111 and is checked against “a locally stored PIN” on the on the “intelligent card.” Jain ¶[0075]. This authentication process does not trigger any connection using the first air interface. Jain ¶[0072]. Because the bootstrapping is completely separate from the process to initialize communication responsive to the parameter and the proximity criterion, the initial bootstrapping process of Jain does not disclose and would not have rendered obvious this limitation.

108. In a second theory, Dr. Almeroth then alleges that Jain renders this limitation obvious utilizing the “automatic[] bootstrapping” process in connection “each individual transaction after transaction card 112 has been bootstrapped onto and is part of mobile device 110.” Ex. 1002 ¶104 (citing Jain ¶[0029]). This is incorrect because Dr. Almeroth is again conflating two different processes—the “bootstrapping process” that it relies on with respect to Figure 7B and the distinct transaction process that Dr. Almeroth alleges is disclosed in Jain ¶[0029].

109. Dr. Almeroth alleges that “during payment, the merchant terminal may ‘prompt the user to authorize a transaction such as by entering a PIN.’” Ex. 1002 ¶104 (quoting Jain ¶[0029]). First, this PIN entry could very well be through a traditional, non-touchscreen keypad. Second, as discussed above, the use of a

capacitive touchscreen to enter a PIN does not disclose or render obvious sensing a physiological parameter, as the data sensed is not physiological. Third, this excerpt from Jain never contemplates the use of the GUI 111¹ of the wireless device (or the wireless device at all) for providing user authentication in a manner contemplated by the bootstrapping process of Jain ¶[0075].

110. Instead, Jain ¶[0029] discusses an alternative embodiment of the overall intelligent card system, in which the intelligent card of Jain is physically embodied in a periphery device such as a “Key FOB and remains live outside the mobile device 110 as a FOB.” Jain ¶[0029]. In this embodiment, “[a]fter the antenna of the transaction card 112 is activated in this mode, a merchant terminal may detect the presence of a host device with the transaction card 112 and prompt the user to authorize the transaction such as by entering a PIN, signing on a terminal interface, confirm the amount of the transaction, and/or other action.” *Id.* The transaction card 112 acts “as a contactless plastic payment card.” *Id.*

111. It is my opinion that Dr. Almeroth completely misreads Jain when he states that the authentication process of ¶[0029] “is as opposed to incorporating PIN

¹ Jain discloses: “Again returning to the example, the transaction card 112 may present a request for the user to enter a PIN through the GUI 111.” Jain ¶[0075].

authorization on the POS device.” Ex. 1002 ¶105. Jain could not be clearer, the authentication options include “*signing on a terminal interface*.” Jain ¶[0029] (emphasis added). Jain does not teach away from authorization via the POS device, but in fact directly discloses it. This error explains the fatal flaw in his analysis – Dr. Almeroth misunderstands Jain, and thus does not appreciate that these authentication steps are contemplated as actions between the user and the *merchant terminal* via the transaction card and are unrelated to the wireless device itself.

112. Dr. Almeroth does get one portion of his analysis right here - nowhere does Jain contemplate making modifications to merchant terminals such that they could *accept biometric information*. Such modifications would significantly complicate the system and incur material additional costs. Jain instead contemplates utilizing more traditional terminals, capable of performing “a normal card-present transaction. In other words, the POS 114 may perceive the transaction card 112 as a contactless plastic payment card and may communicate with the transaction card 112 as a contactless plastic payment card to execute payment transactions.” Jain ¶[0029]. Jain expressly discloses that “in this implementation, neither the terminal nor the financial institution may require additional software to execute the transaction.” Jain ¶[0029]. Even if Jain had provided teachings to modify the POS, those teachings still would not render obvious a “smartphone-based sensor.”

113. Jain does not disclose, and would not have rendered obvious, at least “selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor” of independent claim 1, nor “selectively communicating . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor” of independent claim 3.

B. Petitioner’s Ground 2 Fails Because the Claims Are Not Obvious in View of Dua

114. The following paragraphs address examples of why certain limitations of claims are not obvious in view of Dua.

115. While I address certain limitations to demonstrate that each of the challenged claims are not unpatentable, I reserve the right to supplement this declaration to include additional information and opinions related to any and all challenged claims and claim elements.

- iv. ***Dua Does Not Disclose or Render Obvious “selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor.”***

116. The '411 Patent claims “selectively communicating [by the smartphone] . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor” in both independent claims 1 and 3. Dr. Almeroth alleges that “Dua’s wireless device also does not communicate with a POS terminal unless its user has been authenticated-both as part of initial credential acquisition and each individual transaction-by entry of a PIN on the wireless device touchscreen or through biometric/fingerprint scan (responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor).” Ex. 1002 ¶207. I disagree.

117. I am aware that the Petitioner has alleged that the Examiner “seemingly overlooked” disclosures of Dua regarding “biometric technologies. Pet. at 41-42. I disagree with Petitioner’s interpretation. During the prosecution of the related '432 Patent, Applicant successfully and correctly argued that Dua did not “teach or suggest ‘enabling a mode to communicate . . . responsive to at least one physiological

parameter . . . ’ as recited in amended claim 1.” Ex. 1009 at 253. The Examiner stated in the notice of allowance that:

Dua alone or in combination fails teaches or fairly suggest [sic]; responsive to at least one physiological parameter having been sensed by at least one sensor of the smartphone, enabling a mode to communicate by the smartphone information requesting an authorization; while the mode is enabled, transmitting by the smartphone first data to a first device, the first data relating to a plurality of financial transactions to be conducted; . . . independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface, wherein said transmitting by the smartphone first data and said receiving by the smartphone second data are performed over an air interface that differs from the first air interface.

Ex. 1009 at 275-276 (emphasis in the original).

118. Dua’s disclosure of “biometric technologies” alone, as set forth below, does not disclose and would not have rendered obvious “selectively communicating... responsive to the value of physiological data that was sensed.”

119. Dr. Almeroth’s discussion of Dua’s disclosure of this limitation boils down to a single paragraph in which he points to his discussion of limitation 1[a]. Ex. 1002 ¶207. But Dr. Almeroth’s discussion of limitation 1[a] is directed to that limitation, which merely claims “sensing by a smartphone, using a smartphone-based sensor, physiological data.” Dr. Almeroth’s analysis of limitation 1[a] does not establish that the devices in Dua “*selectively communicat[e]*... responsive to a value of physiological data.”

120. In fact, Dr. Almeroth's analysis of limitation 1[a] expressly includes disclosures in Dua in which there is communication between the smartphone and the entity, such as a POS terminal, in advance of any authentication such as a PIN or other credential check. Instead, the use of a PIN or other authentication in Dua identified by Dr. Almeroth is to protect the security of Dua's disclosed "wallet application and data contained in the electronic wallet." Ex. 1002 ¶172.

121. For example, Dr. Almeroth focuses on a process in Dua under which the user must enter a PIN to issue a credit card to the wallet application. *Id.* (citing Dua ¶¶[0128]-[0129], [0178], [0180], [0250]). But the disclosure of those paragraphs explicitly contemplates communication between a Wireless Credential manager (WCM) and a "SIP-enabled mobile device 500 via the Internet" in which the "WCM 510 may initiate communication with a wallet application on Bob's wireless device 500." Dua ¶¶[0128]-[0129]. This disclosure permits "direct communication between the end-points (WCM and wallet application) for the purpose of transferring confidential information." Dua ¶[0178]. And most critically for my disagreement with Dr. Almeroth, "[t]he established session may initially be used to exchange encryption keys and/or other security information. ***Subsequent to that***, the issuer's system will authenticate the mobile user's identity in real-time to ensure that the person on the receiving end is in fact the person that requested the digital credential." Dua ¶[0180] (emphasis added). The connection is established and

communication between the wallet application and the WCM has begun prior to the disclosed authentication.

122. Dr. Almeroth's discussion in paragraph 171 of his declaration fares no better. There, he points to the use of biometric sensors for authentication and decryption, but provides no discussion of such authentication as a prerequisite for communication. Ex. 1002 ¶171 (citing Dua ¶¶[0366], [0414], [0534], [0050], [0399], [0429]). His identified citations themselves again speak to authenticating the user for the transaction, not "selectively communicating by the smartphone . . . responsive to the proximity criterion having been detected as being satisfied and responsive to a value of the physiological data associated with a living organism that was sensed by the smartphone using the smartphone-based sensor." *E.g.*, Dua ¶[0366] ("[d]ata in the wallet application is encrypted and protected with a special wallet PIN code which is set by the wireless device owner during the setup of the application"); ¶[0414] ("online PIN verification also gives certain credential issuers a stronger means by which to validate a person's identify during a transaction."); ¶[0534] ("the user would be required to provide a E.164 number for a wireless device in order to establish the wallet account on a server hosted and managed by the wallet service provider."). Similarly, Dua ¶[0395] discloses "pressing buttons" or "hold[ing] down either button 1 or 2" enable RF communication, which fails to disclose selectively communicating responsive to a proximity criterion and responsive to a value of the

physiological data. In fact, these citations again make reference to the use of a connection to provide authentication. Dua ¶[0050] (“the resolved Internet address is used to establish secure real-time communication between WCM 110 and the wallet application on wireless device 200 using the Session Initiation Protocol (SIP)... to transfer encrypted credentials.”). The connection via SIP is used to exchange credentials and thus the communication is not responsive to such credentials.

123. The use of credentials to, for example “open the wallet application prior to card issuance” or “[m]aking significant changes in the wallet application” also fails to establish that “selectively communicating by the smartphone using a first air interface . . . responsive to a value of the physiological data associated with a living organism.” *See* Ex. 1002 ¶173.

124. Additionally, Dr. Almeroth again alleges that the entry of a PIN into a capacitive touch screen itself would meet the limitation of “sensing by a smartphone, using a smartphone-based sensor, physiological data associated with a living organism.” Ex. 1002 ¶177. For the reasons set forth above in my discussion of Ground 1, the entry of a numerical value into a capacitive touch screen is not sensing “physiological data associated with a living organism.” A capacitive touch screen is not physiological data. *Supra* ¶105.

125. Dr. Almeroth’s appeals to the knowledge of a POSITA with respect to limitation 1[a] also fail to establish that “selectively communicating by the

smartphone using a first air interface . . . responsive to a value of the physiological data associated with a living organism.” Instead, he remains focused on the general concept of protecting “sensitive functionalities” via “authentication or verification process.” Ex. 1002 ¶¶174-175. Dr. Almeroth remains focused on the authentication serving as a predicate for accessing the wallet application, rather than for communicating using the first air interface. E.g., Ex. 1002 ¶¶176-177. Whether Dua contemplates using a biometric for such authentication, Dr. Almeroth never establishes, in his discussion of limitation 1[a] nor his discussion of limitation 1[c], that any form of authentication is done and in response the smartphone selectively communicates.

v. ***Dr. Almeroth Fails to Establish that Dua Discloses or Would Have Rendered Obvious “detecting that a proximity criterion is satisfied” and “selectively communicating . . . responsive to the proximity criterion having been detected as being satisfied.”***

126. The ’411 Patent claims “detecting that a proximity criterion is satisfied between the smartphone and an entity” and “selectively communicating . . . responsive to the proximity criterion having been detected as being satisfied” in both independent claims 1 and 3.

127. Dr. Almeroth asserts that Dua discloses this limitation. Ex. 1002 ¶180. I disagree.

128. Dr. Almeroth points to high level disclosures in Dua regarding the use of a “short range wireless link,” but those disclosures do not disclose or render obvious the claimed proximity criterion. *See* Ex. 1002 ¶¶180-183. As such, Dr. Almeroth alleges that “[a] POSITA would understand that short-range RFID links, including in particular the NFC communication link disclosed by Dua, are established responsive to detecting that a proximity criterion is satisfied.” Ex. 1002 ¶184. Dr. Almeroth alleges that “receipt of a short-range RFID or NFC signal . . . corresponds to and teaches detecting that a proximity criterion has been satisfied between the smartphone and an entity.” Ex. 1002 ¶185. He then points to specific disclosures regarding NFC as disclosing “detecting that a proximity criterion is satisfied and then establishing a short-range link that is used for subsequent communications.” Ex. 1002 ¶¶189-190. However, Dua does not contemplate the use of NFC for its short-range connections, and Dr. Almeroth’s analysis fails to tie the disclosures of NFC to Dua’s disclosures.

129. In his attempt to address this limitation, Dr. Almeroth notes that Dua discloses the use of a “short-range link between Dua’s wireless device 800 (*the smartphone*) and an RF reader 820 of a merchant POS terminal 860 (*an entity, wherein the entity is not the living organism*).” Ex. 1002 ¶181 (emphasis in the original). However, the disclosures surrounding these short-range connections do not actually disclose the use of a proximity criterion, and thus, Dr. Almeroth pivots

to disclosures in the ECMA 340 standard for NFC – disclosures that are not incorporated into Dua, are not referenced in Dua, and which Dr. Almeroth never establishes would be obvious to combine with Dua.

130. Dr. Almeroth alleges that Dua “discloses the RFID chip can be an NFC chip – thus disclosing NFC transactions.” Ex. 1002 ¶183. Not so. The sole reference to NFC in Dua is in the background of the technology section. Dua ¶[0016] (“Wireless devices with integrated RFID proximity chips or Near Field Communication (NFC) technology may also provide users the ability to transfer information to a reader device.”). Even after acknowledging its existence, Dua then omits NFC entirely from the list of network protocols contemplated by the invention of Dua, which include “GSM/GPRS, CDMA2000, W-CDMA, EDGE, HDR, 1xRTT, UMTS, IMT-2000, 802.11a, 802.11b, 802.11g, or BLUETOOTH.” Dua ¶[0041]. In fact, in every example where Dua discusses available “wireless” protocols, Dua omits any discussion or even mention of NFC. *See* Dua ¶[0318] (“Connectivity between the wireless device and the reader/POS terminal could be made via 802.11a/b/g, Bluetooth, or other RF protocols.”); *see also id.* ¶[0457] (“The user may accomplish [transferring credentials between devices] using . . . the short-range transmission capability of both devices (e.g. Bluetooth, infra-red, etc); *see also id.* ¶[0101] (listing Internet protocols such as “Transmission Control Protocol (TCP), Transmission Layer Security (TLS), User Datagram Protocol (UDP), Internet

Protocol (IP), Domain Name System (DNS), and others.”); *see also id.* ¶[0103] (“SIP can provide a set of services that is more diverse, compelling and profitable than any of the contemporary wireless protocols including WAP, SMS and MMS.”); *see also id.* ¶[0263] (“As such, WCM 110 is preferably compatible with IPv4 and IPv6 networks. WCM 110 also supports the following transport protocols: UDP/TCP/TLS/SCTP. WCM 110 also supports multiple domain names.”); *see also id.* ¶[0429] (“A number of server authentication and data encryption protocols may be employed to secure credentials and other confidential information such as Wireless Transport Layer Security (WTLS), Transport Layer Security (TLS), and Secure Socket Layer (SSL). Wireless Identity Module (WIM) could be used for digital signatures enabling authenticated payments.”); *see also id.* ¶[0494] (“The connection between the wallet application and the storage service could utilize an application protocol such as HTTP, SIP, or others.”).

131. In fact, while Dua only makes a passing mention of NFC in the background section, Dua frequently embraces the use of Bluetooth, but Dr. Almeroth does not rely on this disclosure. As one example:

For example, if a user wants a digital debit card, the user may be prompted by a bank employee to bring his wireless device in proximity of an RFID reader, which will send a command to the wallet application signifying that it is going to receive a new credential via Bluetooth. The bank system and the wireless device may exchange encryption keys via RF in order to establish a secure Bluetooth connection with the bank network (the process for establishing Bluetooth connectivity is similar to what is outlined later in the Wallet Transfer section).

Dua ¶[0321].

132. Another example is found in the following excerpt from Dua:

The user would first login to his existing wallet application using his PIN or biometric ID. From the settings menu, the user would choose the "secure wallet transfer" option. The user might be given the ability to select which short-range transmission capability to use for communication with the new device (in case the device supports different types). For this example, we will assume that the user selects Bluetooth. The wallet application on the existing device will display a randomly generated 20 digit key that the user will be required to enter in the wallet application on the new device in order to authenticate the existing device and wallet.

Dua ¶[0458].

133. Using Bluetooth for short-range communications is disclosed in Dua, *see* Dua ¶¶[0463]-[0465], [0468], [0485]; however, NFC is never disclosed for any communication in Dua. It is my understanding that neither Petitioner nor Dr. Almeroth point to or rely on the Bluetooth disclosures in Dua with regard to this claim limitation.

134. Dr. Almeroth points Dua's "proximity transaction" as disclosing a transaction that could be NFC. Ex. 1002 ¶183. In fact, the "local environment," also referred to as a "proximity environment," of Dua does not contemplate NFC. *See* Dua ¶¶[0314]-[0315]. The "proximity environment" disclosed "serve[s] as a replacement for single-purpose cards and tokens" during which the device "can transmit . . . information to a reader using the short range transmission capability of the wireless device (e.g. RF)." Dua ¶[0315]. Dua explains that this proximity

environment can allow “a wireless device loaded with a wallet application, *that also has an integrated RFID chip* can simply be waved slowly in close proximity to a reader device to facilitate a transaction.” *Id.* (emphasis added). Despite Dr. Almeroth’s claims that a POSITA would find it obvious to implement NFC, Dua specifically omits NFC from this embodiment even though Dua previously referenced NFC in the background.

135. The “personal environment” pointed to by Dr. Almeroth at Dua ¶[0321] also does not disclose NFC. Ex. 1002 ¶183. That environment discloses peer-to-peer connectivity and identifies “802.11a/b/g, Bluetooth, or other RF protocols” for providing that connectivity. Dua ¶[0318]. It does not mention NFC. In fact, the only use of RFID references in the “personal environment” is an initial step in setting up a two-way communication exchange like Bluetooth. Dua ¶[0321]. The fact that the credentials will be exchanged via Bluetooth and not RFID again confirms that Dua does not contemplate a complex two-way exchange using RFID, which thus also indicates that Dua was not contemplating using NFC in this environment. And Dr. Almeroth does not allege that Bluetooth itself meets the proximity criterion of the claim limitations.

136. Dr. Almeroth points to other examples in Dua as disclosing “the detection of proximity between a smartphone and POS reader.” Ex. 1002 ¶186.

These examples fail to disclose selectively communicating responsive to a proximity criterion.

137. Dua ¶¶[0383] [0384] does not disclose selectively communicating responsive to a proximity criterion being met. Dua considers the security concerns of constant transmission by a device with an RFID chip (Dua ¶[0382]) and proposes a solve in which the transmission capable device has “a single button embedded on the wireless device that can be used to activate the wallet application and to control the transmission of information to an external device via RFID.” Dua ¶[0383]). It is the activation of this wallet button that “enables communication via the RFID interface”, not the proximity criterion itself. Dua ¶[0383]. Dua notes that “the user is prompted to press and release the ‘wallet button’ in order to enable RF communication on the device.” Dua ¶[0385]. Dua also proposes an embodiment where “RF communication may only be enabled during the period while the button is pressed down.” Dua ¶[0386]. It is the wallet button that initiates RF communication in Dua ¶¶[0383] [0384], and therefor Dua ¶¶[0383] [0384] do not disclose “selectively communicating . . . responsive to a proximity criterion having being detected.”

138. With respect to Dua ¶[0321] as discussed above, the disclosure states that “the user may be prompted by a bank employee to bring his wireless device in proximity of an RFID reader, which will send a command to the wallet application

signifying that it is going to receive a new credential via Bluetooth.” Dua ¶[0321].

Dr. Almeroth alleges that this discloses this limitation because the “RFID reader would not know to send a command specifically to a specific user’s wireless device... unless the RFID reader has detected said proximity with the wireless device.” This is an overstatement. This disclosure in Dua does not indicate that the proximity criterion must be detected as being satisfied before the wireless device begins communicating, as it is entirely possible that the RFID reader discussed is sending “a command” due to an external input such as an instruction from the bank employee. There is no indication in this paragraph that the communication is responsive to a proximity criterion.

139. With respect to Dua ¶[0009], this is discussion in the Background of the Invention section, and discusses the use of “[a] contactless smart card.” The disclosed range is based on “non-battery powered cards”, confirming that this background disclosure is not about a device or smartphone at all. This disclosure does not call for a proximity criterion being satisfied, nor would it have rendered such a criterion obvious.

140. Dr. Almeroth then argues that a POSITA would find it obvious to implement Dua’s “NFC communications” as Dr. Almeroth discloses them. Ex. 1002 ¶192. First, as discussed above, Dua does not disclose the use of NFC communications. Second, Dr. Almeroth alleges this is because “Dua tells a POSITA

to look to ‘ISO/IEC 14443’ RF proximity standard (Dua ¶[0013]), which would motivate a POSITA to also look to the standard for NFC.” Ex. 1002 ¶192. But a “standard for NFC” is not referenced in Dua, and Dr. Almeroth never explains why a POSITA would have been motivated to combine the disclosure of this undisclosed “standard for NFC” with Dua, nor reasonable expectations of success in doing so. And Dr. Almeroth admits that Dua does not point to the NFC standard, but to ISO/IEC 14443. *See* Dua ¶[0013].

141. Dr. Almeroth’s statement that a POSITA would have found a “standard for NFC”, based simply on a background mention of NFC that is unrelated to (and excluded from) the actual system of Dua, does not set up any relationship between the proximity requirements of NFC and the disclosure of Dua itself, as Dua does not contemplate the use of NFC, but of the one-way RFID communication systems actually disclosed in ISO/IEC 14443. In other words, with nothing in Dua itself to rely on, Dr. Almeroth instead provides paragraphs of discussion of the ECMA 340 standard without establishing that a POSITA would have combined the disclosures of these two documents. Ex. 1002 ¶¶189–191.

142. Further, Dua contradicts Dr. Almeroth as it specifically recites its own concepts for protocols that could be used for connectivity instead of relying on NFC. For example, Dua discloses that for short range communications, “[c]onnectivity could initially be established by exchanging encryption keys via RFID that allow the

devices to establish connectivity via an alternate channel securely so no other device can listen in to the communication. Keys could also initially be exchanged via infrared technology.” Dua ¶[0318]. Dua identifies a process by which connectivity is established by a button and subject to 30-second connectivity time out, the type of independent connectivity requirement that indicates a POSITA, reading Dua, would not go searching to re-implement un contemplated technologies like NFC. Dua ¶¶[0383], [0384]. Dua also proposes providing security by establishing exclusive connectivity when utilizing its disclosed wallet. Dua ¶[0478]. These disclosures in solve the concerns surrounding security or indiscriminate transmission noted by Petitioner. These examples also illustrate that it would not have been obvious to a POSITA to seek out and rely on undiscussed NFC standards relating to proximity.

143. In sum, Dua does not disclose “detecting that a proximity criterion is satisfied between the smartphone and an entity” and “selectively communicating... responsive to the proximity criterion having been detected as being satisfied” of the ’411 Patent, and so Dr. Almeroth provides pages of discussion of how NFC itself does have such a criteria. But Dua ultimately does not contemplate NFC as part of its claimed invention. And Dr. Almeroth’s efforts to combine the Dua system with NFC boil down to an unsupported bare allegation that a single reference to NFC in Dua’s background would have motivated a POSITA to disregard Dua’s disclosures of separate peer-to-peer communication protocols and look to an NFC standard. This

is impermissible. Dr. Almeroth has not established that Dua discloses nor renders obvious “detecting that a proximity criterion is satisfied between the smartphone and an entity” of independent claims 1 and 3.

XIII. SUMMARY AND OTHER REMARKS

144. It is my opinion that Petitioner has failed to show that any of the Challenged Claims set forth in Grounds 1 and 2 are unpatentable as obvious as explained above.

145. My opinions expressed in this Declaration are based on the information available to me at this time. To the extent any additional information becomes available, I reserve the right to supplement my opinions contained herein.

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.

Executed on September 17, 2025.



Chuck Easttom