

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP. AND KIA CORPORATION,
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner

Case IPR2024-00785
U.S. Patent 10,407,026

**DECLARATION OF DR. SAM MALEK IN SUPPORT OF PATENT
OWNER'S PRELIMINARY RESPONSE**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND BACKGROUND	3
II. QUALIFICATIONS	4
III. MATERIALS CONSIDERED	10
IV. LEGAL PRINCIPLES	10
V. PERSON OF ORDINARY SKILL IN THE ART (“POSITA”).....	15
VI. BACKGROUND	17
A. Overview of the ’026 Patent.....	17
B. Prosecution History of the ’026 Patent	18
VII. SUMMARY OF ZAID (EX1005).....	19
VIII. DETAILED ANALYSIS OF PETITION GROUNDS	20
A. Dr. Almeroth fails to show that Zaid discloses or suggests “a request ... for unlocking of the vehicle” that “include[s] a unique access code.”	21
B. Dr. Almeroth fails to show that Zaid discloses or suggests “the “request from the mobile device including a unique access code obtained by the mobile device from the server.”	24
C. Dr. Almeroth fails to show that Zaid discloses or suggests the claimed “unique access code.”	30
D. Dr. Almeroth fails to show that Zaid discloses or suggests a “vehicle [that] is configured to receive information from the server to authenticate the request by the mobile device.”	34
E. The Additional References Do Not Cure the Deficiencies of Zaid.....	38
IX. CONCLUSION.....	38

I, Dr. Sam Malek, declare under penalty of perjury as follows:

I. INTRODUCTION AND BACKGROUND

1. I have been retained as an expert witness on behalf of Emerging Automotive LLC (“Emerging Auto”) to provide information and assistance regarding U.S. Patent No. 10,407,026 (“the ’026 patent”). Specifically, I have been asked to consider the Petition for Inter Partes Review numbered IPR2024-00785 (“the Petition”) regarding the ’026 patent, and specifically the Declaration of Dr. Almeroth (EX1004) that accompanies the Petition.

2. In this declaration I provide my independent analysis of the ’026 patent in light of the materials cited below and discussed herein and my knowledge and experience in this field during the relevant time frame. I have been asked to consider what one of ordinary skill in the art at the time of the invention of the ’026 patent (a “POSITA,” see Section V below) would have understood from the specification, including scientific and technical knowledge related to the patent. I have also been asked to consider whether certain references anticipate or would have rendered obvious the inventions described in the claims of the ’026 patent.

3. My findings, as explained below, are based on my study, experience, and background in the fields discussed below, informed by my education and my extensive experience in the field of cloud-based processing systems. I have also relied on my review and analysis of the references identified by Dr. Almeroth,

information provided to me, and information that I have independently reviewed. I have personal knowledge of the facts and opinions set forth in this declaration, and, if called upon to do so, I would testify competently thereto.

4. I am being compensated for my independent analysis as an expert with respect to this inter partes review proceeding. My compensation is not contingent in any way on the content of my analysis, the opinions that I offer, or the outcome of this proceeding. I have no financial interest in either Petitioner (Toyota or Kia) or Patent Owner (Emerging Auto) and I have no financial interest in the '026 patent.

II. QUALIFICATIONS

5. My qualifications for forming the opinions given in this declaration are summarized here and are addressed more fully in my curriculum vitae, which is submitted as EX2002. That exhibit also includes a list of my publications.

6. I have approximately 25 years of experience in the general area of computer and software technology in a variety of roles, including as a software engineer, software architect, and programmer at a variety of companies, as well as a researcher and professor at several universities.

7. I am currently a Full Professor of Software Engineering with tenure in the Informatics Department within the School of Information and Computer Sciences at the University of California, Irvine. I am also the Director of the

Software Engineering and Analysis Laboratory (“SEAL”). My general research interests are in the field of software engineering, and to date my focus has spanned the areas of software analysis and testing, mobile computing, architecture and design, and software dependability and security. The underlying theme of my research has been to devise techniques and tools that aid with the construction, analysis, and maintenance of largescale software systems.

8. I received my Ph.D. and M.S. degrees in Computer Science from the University of Southern California and my B.S. degree in Information and Computer Science from the University of California, Irvine. I have received numerous awards for my research contributions, including the Test of Time Award from the Association for Computing Machinery Special Interest Group on Software Engineering (2020), National Science Foundation CAREER award (2013), GMU Emerging Researcher/Scholar/Creator award (2013), and the GMU Computer Science Department Outstanding Faculty Research Award (2011).

9. I have authored over 130 peer-reviewed research publications. These publications have been highly cited (more than 11,000 times according to scholar.google.com). Many of my publications have dealt with the topics that are related to this proceeding, including distributed software systems, cloud computing, client-server architecture, and software settings and configuration. I provide a few examples here.

10. My Ph.D. dissertation resulted in novel algorithms for optimizing the deployment architecture of a distributed software system. The deployment architecture of a distributed software system is the allocation of its software components to its hardware devices. There are many deployments of a software system possible, but some may be superior to others with respect to certain quality of service objectives (e.g., latency, availability, security). One application of my dissertation work was in the context of cloud computing, because in most cloud-based software systems there are many geographically distributed nodes (servers) available for the deployment of software components.

11. I have also worked on techniques to leverage cloud computing for software testing. For instance, in an article titled “A Whitebox Approach for Automated Security Testing of Android Applications on the Cloud,” I showed how the resources in the cloud can be effectively harnessed to facilitate security testing at scale.

12. In another article titled “GLIDE: A Grid-based Lightweight Infrastructure for Data-intensive Environments,” I described the results of my work with colleagues from NASA in the development of a new distributed software system for sharing large amounts of data generated by NASA. This capability was the first of its kind in the realm of Grid Computing, which is a precursor to Cloud Computing.

13. A significant focus of my work has been on computer security, including electronic forms of access control and management of privileges in software systems. For instance, I led a team of researchers in a project sponsored by the Defense Advanced Research Project Agency (DARPA) to develop a novel approach for protecting Android applications from various form of access control attacks. The project resulted in the development of a tool called COVERT. I have published extensively on this work, including a highly cited manuscript that appeared in the IEEE Transactions on Software Engineering in 2015. In another project, I developed DelDroid, which at the time was the first approach for automated determination and enforcement of least privilege architecture in Android. This work was published in the Journal of Systems and Software in 2019.

14. I have received numerous research grants from a variety of organizations, including the National Science Foundation (NSF), Federal Bureau of Investigation (FBI), Air Force Office of Scientific Research, Department of Homeland Security (DHS), National Security Agency (NSA), Defense Advanced Research Projects Agency (DARPA), Office of the Director of National Intelligence, and Army Research Office among others. Software systems and results produced in my research lab have been adopted for use by various organizations in both private (e.g., Boeing, Bosch) and public (e.g., NASA, DHS, FBI) organizations. Many of the above-mentioned projects and software systems involved analysis and design of

client-server software systems deployed on the cloud. For instance, in a project called “RASS: Resilient Autonomic Software Systems” funded by Air Force Office of Scientific Research, I led a team of researchers to develop a new method of automatically adapting Air Force’s software systems to fluctuations in communication networks, thereby making them resilient to network interruptions.

15. I also have several years of experience as a software engineer, software architect, and programmer at a variety of companies, namely the Boeing Company, PricewaterhouseCoopers Consulting (later acquired by International Business Machines (“IBM”) Corporation), FieldCentrix, and Neural Computing Systems Lab. During my tenure in the industry, I gained professional experience in the design, development, and management of largescale software engineering efforts. Among the software systems that I designed and developed were commercial ecommerce and enterprise software systems. Many of the software systems developed in the context of my professional experience were built according to the general client-server architectural style and deployed on the cloud or cloud-like environments. In most of these systems, the server held the state of the distributed application, allowing for that state, such as the preferred user settings, to be transferred to client at runtime.

16. I have taught software engineering and computer science courses on a regular basis at the B.S., M.S., and Ph.D. levels at the universities where I have been

employed. I cover concepts related to cloud computing, distributed software, client-server architectural style, authentication, encryption techniques, access control mechanisms, and protocols for exchange of electronics credentials (e.g., electronic keys, passwords, and tokens) in many of the courses that I teach at the university. Notably, I have regularly taught distributed software engineering courses at UC Irvine and previously at George Mason University (GMU). In these courses, I cover concepts such as the client-server architectural style, cloud computing principles, and server-side storage of user-defined preferences.

17. I have been a frequent speaker at scientific conferences, symposia, workshops, and gatherings of software engineering academics and professionals. I have served as chair, committee member, and reviewer for numerous software engineering journals, magazines, and conferences. I have served on the editorial board of the ACM Transactions on Software Engineering and Methodology, IEEE Transactions on Software Engineering, the ACM Transactions on Autonomous and Adaptive Systems, the Springer Journal of Automated Software Engineering, and the Springer Journal of Computing. I am a member of the Association for Computing Machinery (ACM), ACM Special Interest Group on Software Engineering (SIGSOFT), and the Institute of Electrical and Electronics Engineers (IEEE). I have testified at trial and deposition as an expert witness in numerous cases in the past five years.

III. MATERIALS CONSIDERED

18. In preparing this declaration and forming my opinions, I have considered: the claims, specification, and prosecution history of the '026 patent; the Petition and declaration by Dr. Almeroth (including all materials cited in each); and all materials cited and discussed in this declaration. In addition, I have considered the relevant legal standards, as they have been explained to me by counsel and as I understand them. I have also considered the knowledge and understanding of a person of ordinary skill at the time of the invention of the '026 patent, of which I am familiar. As part of my analysis for this matter, I have also considered my own knowledge and experience, including my work and experience with cloud-based processing systems.

IV. LEGAL PRINCIPLES

19. In forming my opinions here, I have applied the following understanding of certain legal concepts related to anticipation, obviousness, combinations of references, and knowledge of one of ordinary skill in the art. Counsel for Patent Owner has informed me of legal principles that apply in this proceeding.

20. It is my understanding that assessing the validity / patentability of a U.S. patent claim based on a prior art analysis requires two essential steps. First, one must analyze the terms of the patent claims to understand what meaning one of

ordinary skill in the art would give the terms. Second, one may then assess validity by comparing a patent claim to the “prior art.” I understand that the teaching of the prior art is viewed through the eyes of a person of ordinary skill in the art at the time the invention was made. My opinion as to what constitutes a relevant person of ordinary skill in the art is set forth below.

21. I have been informed that in order for a patent claim to be invalid as anticipated by a prior art reference under 35 U.S.C. § 102, each and every element of that patent claim must be found disclosed in that reference, explicitly or inherently, to a person of ordinary skill in the art. Inherent disclosure requires that the claimed element be the only possible option given the other disclosures of the reference, and that it would be so recognized by persons of ordinary skill in the art. I also understand that the missing descriptive material cannot merely be probably or possibly present. If any single element of a claim is not disclosed in the reference, the entire claim is not anticipated. I understand that a prior art reference merely capable of being modified so as to operate in the same manner as the patented device or system does not anticipate. I further understand that obviousness is not inherent anticipation, and that it is insufficient that a missing limitation is so similar to a limitation actually disclosed in the reference that one of ordinary skill in the art would see the substitution as obvious. I also understand that, if it is necessary to reach beyond the boundaries of a single reference to provide missing disclosure of

the claimed invention, the proper ground for asserting invalidity is not anticipation, but obviousness.

22. I understand that a claim is invalid as obvious under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art.

23. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and the claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

24. I have been informed that the following factors are used to determine whether or not the claimed subject matter would have been obvious: (i) the scope and content of the prior art; (ii) the differences between the prior art and the claimed invention; (iii) the level of ordinary skill in the field of the invention; and (iv) any relevant objective considerations of non-obviousness, such as commercial success, long-felt but unresolved needs, failure of others, etc.

25. I also understand that in considering the scope and content of the prior art, references must be reasonably related (i.e., analogous) to the claimed invention of that patent. I understand that the test for determining whether a prior art reference constitutes analogous art to the claimed invention is (1) whether the reference is from

the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference is still reasonably pertinent to the particular problem the inventor is trying to solve.

26. I understand that a party asserting obviousness based on a combination of prior art references must demonstrate that one of ordinary skill in the art would have been motivated to combine the teachings of those references to achieve the claimed invention and that the skilled artisan would have had a reasonable expectation of success in doing so. It is my understanding that it is not enough to show that one skilled in the art could combine elements of multiple references, but instead there must be some reason that would have prompted a person of ordinary skill in the art to combine the elements in the way the claimed invention does. I understand that there must be some reasoned explanation as to why one of ordinary skill in the art would combine the references. The reason cannot come from hindsight.

27. I understand that in considering whether a claimed invention is obvious, one may but is not required to find obviousness if at the time of the claimed invention there was a reason that would have prompted a person having ordinary skill in the field of the invention to combine the known elements in a way the claimed invention does, taking into account such factors as: (1) whether the claimed invention was merely the predictable result of using prior art elements according to their known

function(s); (2) whether the claimed invention provides an obvious solution to a known problem in the relevant field; (3) whether the prior art teaches or suggests the desirability of combining elements claimed in the invention; (4) whether the prior art teaches away from combining elements in the claimed invention; (5) whether it would have been obvious to try the combinations of elements, such as when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions; and (6) whether the change resulted more from design incentives or other market forces. To find it rendered the invention obvious, the prior art must provide a reasonable expectation of success. Obvious to try is not sufficient in unpredictable technologies.

28. I understand that each claim must be evaluated separately for obviousness, and that it is improper to use hindsight. I understand that the disclosures in a patent or a prior art reference are viewed from the perspective of a person of ordinary skill in the art at the time of the invention. The obviousness analysis by a person of ordinary skill in the art must consider only what was known at the time of the invention.

29. It is my further understanding that obviousness cannot be based on a hindsight combination of components selected from one or more prior art references. I also understand that an invention would not have been obvious simply because all of the elements of the invention may have been known separately in the prior art.

30. I understand that a combination of disclosures or references would not have been obvious if the alleged modification(s) to be made to the reference(s) would have been inconsistent with the reference's stated goals or would have rendered the combination inoperable for its intended purpose. I further understand that for something to have been obvious, the party asserting obviousness must explain why a POSITA would have selected components or features for combination in the manner claimed.

31. I have been informed that a prior art reference must be considered in its entirety, i.e. as a whole, including portions that would lead away from the claimed invention.

32. I understand that with respect to claim construction, the proper construction is considered in the context of, and must be consistent with, the specification and that the claim language should be read in light of the specification and file history as it would be interpreted by one of ordinary skill in the art.

V. PERSON OF ORDINARY SKILL IN THE ART ("POSITA")

33. Counsel for Patent Owner has informed me that a person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. In my opinion, the relevant field of art for the '026 patent is that of cloud-based processing systems.

34. For the purpose of this Declaration, and based on my opinions herein, the time of invention for the '026 patent is April 2011. However, I understand that Dr. Almeroth opines that the time of the invention is October 2013. Any invention date from the early-to-mid-2010s would not alter my opinion regarding a person of ordinary skill in the art. Thus, my opinion regarding a POSITA applies to either a date of invention in April 2011 or a date of invention in October 2013.

35. I have been informed by counsel for Patent Owner that the person of ordinary skill is generally familiar with the type of problems encountered in the field and the prior art solutions to those problems and possesses an ordinary level of creativity.

36. I understand that Petitioners' expert, Dr. Almeroth, opined that a person of ordinary skill in the art "would have had at least a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the fields of access control systems, vehicle electronics, and/or cryptography. Additional education could substitute for professional experience and vice versa." EX1004, Almeroth Decl., ¶ 72.

37. For purposes of this declaration, I apply Dr. Almeroth's definition. However, I note that the opinions I set forth below are applicable under any

reasonable definition of a POSITA. I also note that I qualify as a POSITA under Dr. Almeroth's proposed definition.

VI. BACKGROUND

A. Overview of the '026 Patent

38. United States Patent Number 10,407,026 (the "'026 patent") is titled Vehicles and Cloud Systems for Assigning Temporary E-Keys to Access Use of a Vehicle. EX1001, Face Page. The '026 patent "relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems." *Id.* at 1:54-57.

39. In embodiments, a vehicle owner or administrator may request a vehicle for personal use or to share an e-key with "any number of users." *Id.* at 43:23-26. "Each e-key will include a unique access code," and "[t]he unique generation of access codes enables each electronic key[] to be different for each user." *Id.* at 43:38-58. "Each unique code can then be used to associate those e-keys with the same vehicle, but assigned to different devices/people with different privileges." *Id.* at 46:4-6. Claim 1 of the '026 patent recites a "unique access code," requiring that the "the unique access code is associated with privileges for use of the vehicle, [and that] the privileges are defined for the unique access code." *Id.*, claim 1.

40. The '026 patent describes a vehicle is “configured to communicate with a server of a cloud system to enable access to use of the vehicle via one or more electronic keys.” *Id.* The vehicle includes communications circuitry “configured to receive a request from [a] mobile device for unlocking of the vehicle,” and the request includes “a unique access code.” *Id.* “[T]he vehicle is configured to receive information from the server to authenticate the request from the mobile device.” *Id.*

B. Prosecution History of the '026 Patent

41. As part of my analysis, I reviewed the file history of the '026 patent. The applicants filed the application for the '026 patent on May 26, 2017. EX1002, 133. On March 4, 2019, the Examiner issued an office action, for double patenting and as allegedly obvious in view of the Ehrman reference. *Id.* at 169-173. In response, the applicants argued that Ehrman did not disclose the claimed “unique access code.” *Id.* at 207. Ehrman disclosed providing a rental car user a unique vehicle identifier (VID) and a password. *Id.*, 206. The applicants explained that Ehrman’s “VID is unique to the car, not something that is unique to access.” *Id.* at 207. A user could identify a car using a VID, but Ehrman “does not teach that privileges are defined for the unique access code.” *Id.*

VII. SUMMARY OF ZAID (EX1005)

42. United States Publication Number 2011/0112969 by Zaid et al. (EX1005, “Zaid”) is titled “Vehicle Access Control Services and Platform.” Zaid disparages against vehicles having direct communication with a “central server.” EX1005, ¶ 16 (“cellular and satellite communication service fees can be expensive. Also, if the car is out of satellite communication range, such as in an underground parking garage, or downtown in a city with major high rises, or other locations, this can prevent proper authorization to the central server to verify granting of access to the vehicle and to receive the latest car access control information with minimum latency. In addition, the satellite communication can completely drain the car battery, particularly when the car is parked for a long period of time.”). Zaid proposed communicating with a vehicle with a user’s “wireless communications device.” *See Id.*, ¶ 82. In Zaid, a “vehicle reservation [can be] booked at [a] server.” *Id.*, ¶ 80. The reservation may be encrypted and then “communicated to a wireless communication device of the user.” *Id.*, ¶¶ 125-126. The wireless communication device decrypts the reservation, using a private key. *Id.*, ¶ 126. Decryption using the private key is to “ensure and authenticate that the intended wireless communication device is receiving the vehicle reservation rather than one that intercepts the vehicle reservation.” *Id.* The wireless communication device then forwards the decrypted reservation to the vehicle. *Id.* at 128. After the vehicle

receives and authenticates the reservation, the vehicle is then reserved; thereafter, “the vehicle access control system begins to accept commands from the wireless communication device such as commands to open the door.” *Id.*, ¶ 129.

43. As shown above, Zaid’s system discloses sending various messages, including reservation messages from the server to the wireless communication device, reservation messages from the wireless communications device to the server, and command messages from the wireless communication device to the vehicle. Zaid discloses that each of the messages may include a “unique increment” to “avoid repeat message attack,” such as a “counter and/or time stamp.” *Id.*, ¶ 130. A unique increment such as a counter and/or time stamp can help prevent an unauthorized person from intercepting a message and “repeating it.” As an example, a command message to unlock a vehicle may include a timestamp of 10 a.m. If an unauthorized person intercepts the message and later attempts to use the message to unlock the car (say at 1 p.m.), the system may recognize the discrepancy in the time stamp and the time and deny the request, preventing an unauthorized unlocking of the vehicle.

VIII. DETAILED ANALYSIS OF PETITION GROUNDS

44. As I describe in detail below, it is my opinion that Dr. Almeroth and the Petition fail to demonstrate any reasonable likelihood of success that any claim of the ’026 patent is invalid.

A. Dr. Almeroth fails to show that Zaid discloses or suggests “a request ... for unlocking of the vehicle” that “include[s] a unique access code.”

45. Claim 1 of the '026 patent includes the following two limitations: “wherein the communications circuitry of the vehicle is configured to receive a request from the mobile device for unlocking of the vehicle,” (1[e]) and that the request “includ[es] a unique access code” (1[f]). In my opinion, Dr. Almeroth does not demonstrate that a POSITA would have understood Zaid to disclose or suggest any request for unlocking of the vehicle that includes a unique access code. Particularly, for this claimed requirement, Dr. Almeroth relies on Zaid’s “reservation” as including the “unique access code.” Almeroth Decl., ¶ 108. Even if this request did include the claimed “unique access code,” (which in my opinion, it does not, as explained below in Section VIII.C), Zaid’s “reservation” is not “a request ... for unlocking of the vehicle,” as Zaid discloses that any request to unlock is separate from a “reservation.”

46. Dr. Almeroth identifies only Zaid’s “vehicle reservations,” as the claimed “request ... for unlocking of the vehicle.” Almeroth Decl., ¶ 108. For this limitation, Dr. Almeroth points to Zaid at paragraph 124 and Fig. 4. *Id.* But as demonstrated by these portions of Zaid—and indeed, throughout Zaid—the “reservation” is for reserving a vehicle. It is not a request to unlock the vehicle. See EX1005, ¶ 124.

47. Zaid discloses that a user may book a reservation for a vehicle at a central server. *Id.* at ¶ 125. As the central server does not have direct communication with the vehicle, the reservation information is provided to the vehicle via a wireless communication device. *Id.* at ¶¶126-128. I understand Dr. Almeroth to agree with this explanation. Almeroth Decl., ¶ 86 (opining that “[t]he server generates and transmits a vehicle reservation ... to the wireless communication device ... which passes the request to a ‘vehicle access component.’”).

48. In my opinion, passing of reservation information, as described by Dr. Almeroth, is not “a request ... for unlocking of the vehicle,” as claimed. A POSITA would understand from Zaid that any request for unlocking of a vehicle would be separate from and only occur after the vehicle is reserved. As Zaid describes in paragraph 124, “a reservation for a vehicle is received from a wireless communication device” and “vehicle access is provided based on the reservation.” EX1005, ¶ 124. As Zaid discloses, it is only “once vehicle access is provided, [that] the user can send commands from the wireless communication device to a vehicle access control component coupled to the vehicle to accurately [actuate] various vehicle functionalities.” *Id.* Zaid further discloses that instructions for the car function, such as unlocking doors, is received through direct commands—not the separate request for reservation. EX1005, ¶ 100. In my opinion, a POSITA

would understand that a “vehicle reservation” provides a user access to the vehicle allowing them to send control commands for the vehicle (including, e.g., unlocking the vehicle).

49. While Zaid discloses a separate command for unlocking the doors, this command is not the “reservation.” See EX1005, ¶ 124. Dr. Almeroth does not identify anything in this separate command as a unique access code and does not opine that the separate command for unlocking includes any unique access code. Almeroth Decl., ¶¶ 113-116.

50. While I understand that Dr. Almeroth does not opine that it would be obvious to modify Zaid’s “reservation” to be a request for unlocking of the vehicle, it is nevertheless my opinion that a POSITA would not have found it obvious and, indeed, would have been dissuaded from making such a modification to Zaid. A POSITA would have recognized that unlocking a car in response to receiving a reservation would result in security and safety concerns. A POSITA would understand that generally, a reservation would be for a future period. The reservation being a request for unlocking of the vehicle would allow unauthorized access to the vehicle before the reservation period. As yet another apparent security concern, a user may reserve a vehicle, making it available, but may wait a period of time before unlocking and entering the vehicle. Unlocking the door before a user is ready to access the vehicle (e.g., if the user reserves a vehicle to save it, but

steps away to order a coffee) presents security concerns such as theft. While I do not understand Dr. Almeroth to offer an opinion to the contrary, it is my opinion that a POSITA would not modify Zaid's reservation to include a request for unlocking of a vehicle.

B. Dr. Almeroth fails to show that Zaid discloses or suggests “the “request from the mobile device including a unique access code obtained by the mobile device from the server.”

51. In my opinion, Dr. Almeroth does not demonstrate that a POSITA would have understood that Zaid discloses or suggests a “request from the mobile device including a unique access code *obtained by the mobile device from the server*,” as recited in claim 1. Claim 1 recites that “a unique access code [is] obtained by the mobile device from the server.” Claim 1 further requires that the unique access code must also be included in “the request from the mobile device.” In my opinion, a POSITA would understand that in Zaid's disclosure, any purported “unique access code” identified by Dr. Almeroth is not both “obtained by the server” and included in “the request from the mobile device,” as required.

52. Here, Dr. Almeroth identifies the “unique increment” or “incremental number” of Zaid as the purported “unique access code.” Almeroth Decl., ¶ 112. In my opinion, Zaid does not disclose or suggest that any “unique increment” that is sent from the mobile device was “obtained ... from the server.”

53. Dr. Almeroth does not identify any portion of Zaid that discloses where the “unique increment” comes from or how it is generated. I reviewed Zaid, and the reference discusses the “unique increment” in only three instances, in paragraphs 81 and 130 and in claims 21-22. *See generally* EX1005. I reproduced those portions of Zaid below:

In various embodiments, communications, including vehicle reservation communications, received from the wireless communication device by the vehicle access control system for vehicle access control includes a unique increment for each message to avoid repeat message attack. In various embodiments, the unique increment is in the form of a counter and/or time stamp that indicate the uniqueness of the message to avoid a repeat message attack.

EX1005, ¶ 81

This statement does not disclose or suggest a server providing a unique increment to the mobile device. Or that any unique increment received from the server is then sent from the mobile device.

54. Next is paragraph 130:

In various embodiments, each message for exchanging information such as vehicle reservation and updates include a unique increment for

each message to avoid repeat message attack. In various embodiments, the unique increment may be in the form of a counter and/or time stamp that indicate the uniqueness of the message to avoid a repeat message attack. *Id.* at ¶ 130.

This statement likewise does not disclose or suggest a server providing a unique increment to the mobile device. Indeed, as discussed below, a POSITA would understand this statement to indicate that the unique increment is associated with “each message,” and, as such, any increment would be “unique” to a single message, and not to a “reservation.”

55. Zaid’s claims 21 and 22 say that “the vehicle reservation includes a unique increment” and that “the unique increment is selected from the group consisting of counter and time stamp.” EX1005, claims 21-22. Zaid’s claims, however, do not recite a server, obtaining any unique increment from a server, or sending any received unique increment from the mobile device.

56. It is therefore my opinion that there is no explicit disclosure of Zaid that the request from the mobile device includes any unique increment obtained from the server. It is also my opinion that the functionality is not inherent or necessary in Zaid’s system because the mobile device could generate a “unique increment” on its own (and in fact, a POSITA would understand that it does). It is

therefore my opinion that Dr. Almeroth fails to show that Zaid discloses any unique access code that was obtained by the mobile device. And even if Zaid did, it is further my opinion that Zaid does not disclose that any unique access code obtained by a server is included in a request from the mobile device.

57. While Dr. Almeroth did not opine that these features would have been obvious, it is nevertheless my opinion that they would not be. In my opinion a POSITA would have understood that the mobile device itself generates any “unique increment,” (a counter or timestamp) that it sends. As Zaid explains, “each message” includes a “unique increment.” EX1005 ¶¶ 81, 130. The messages sent from the mobile device to the vehicle include, not only reservations, but also “commands (e.g., unlock doors, start engine, and/or other commands).” *Id.* at ¶ 100; *see also id.*, ¶ 124. And Zaid states that all of these messages include the “unique increment.” The subsequent commands, e.g., for unlocking, do not originate at the server, but at the mobile device itself. *Id.* at ¶ 124 (“once vehicle access is provided, the user can send commands from the wireless communication device to a vehicle.”). As such, a POSITA would have understood that for these later command messages to include the “unique increment,” the mobile phone would generate it for the message.

58. A POSITA would have also understood that the “unique increment” sent from Zaid’s mobile device would not be obtained from the server because,

Zaid's "unique increment" is unrelated to the underlying content of the messages.

As claimed in the '026 patent, the "unique access code is associated with privileges" and "the privileges are defined for the unique access code." '026 Pat., claim 1. As described in the '026 patent, the unique access code can be used to distinguish different users, and thus their respective privileges. '026 Pat., 43:46-50 ("unique generation of access codes enables each electronic keyed to be different for each user.").

59. Far different from the "unique access code" described in the '026 patent, Zaid's "unique increment" is unrelated to privileges or even specific users. Zaid's "unique access code" is used "to avoid repeat message attack." EX1005, ¶¶ 81, 130. A repeat message attack, also known as replay attack, is a type of network attack consisting of three steps: (1) An attacker eavesdrops on network communication and intercepts a valid, typically encrypted message, that is intended to authenticate a sender to a recipient. (2) The attacker saves the message. (3) The attacker transmits the message to the recipient at a later time to impersonate the original sender, and thereby gain unauthorized access. A common solution to overcome this type of attack is to include a timestamp or a unique increment (counter), to prevent an intercepted message from being "repeated" or "replayed." The recipient can check the timestamp or the counter included in the message against the current time or counters received previously to determine

whether the message is a replayed message. A POSITA reading Zaid would have understood that this is the purpose of the “unique increment” included in “each message” of Zaid. A POSITA would have known that in a system like that disclosed in Zaid, using the same unique increment in a message sent from a server to the mobile device and from a message sent by the mobile device to the vehicle would make the system more susceptible to repeat message attacks because the system would not be using a unique increment for “each message,” as described in Zaid. Indeed, Zaid describes that a “wireless communication device receives and caches the reservation” before it “forward[s] [the] reservation ... to [the] vehicle access kit.” Zaid, Fig. 5. A POSITA would have understood that such caching and forwarding could have an unknown delay, which would substantially eliminate the purpose of using a timestamp to defeat repeat message attacks. Further, Zaid discloses that the vehicle will synchronize with the counter of the *remote key*—not a server that sends a message reserving the vehicle. *Id.*, ¶ 53.

60. Dr. Almeroth also opines that encrypting Zaid’s reservation discloses the “unique access code” limitation. Almeroth Decl. ¶¶ 114-116. I disagree. This theory fails because in Zaid, the encrypted reservation from the server—what Dr. Almeroth opines makes it “unique”—is not sent from the mobile device to the vehicle. As Zaid explains, “decryption is required at each communication relay station to authenticate the vehicle reservation.” EX1005, ¶¶ 70, 99, 125. The

wireless communication device decrypts the message before sending the reservation to the vehicle. EX1005, ¶ 125. Thus, even if encrypting the message made it a “unique access code obtained by the mobile device from the server,” Dr. Almeroth’s alternative theory nevertheless fails because—since the mobile device performs decryption—that encrypted message is not sent “from the mobile device,” as required by claim 1.

C. Dr. Almeroth fails to show that Zaid discloses or suggests the claimed “unique access code.”

61. Claim 1 of the ’026 patent recites a “unique access code” that “is associated with privileges for use of the vehicle” and where “privileges are defined for the unique access code.” It is my opinion that Dr. Almeroth does not demonstrate that a POSITA would have understood Zaid’s “unique increment” to be “associated with privileges.” Moreover, it is my opinion that Dr. Almeroth does not show that a POSITA would have understood that Zaid’s alleged privileges are “defined by” the unique increment, as required by claim 1.

62. As described in the ’026 patent, the unique access code can be used to distinguish different users, and thus their respective privileges. ’026 Pat., 43:46-50 (“unique generation of access codes enables each electronic key to be different for each user.”). However, Zaid’s “unique increment” does not and cannot be used for this purpose.

63. Dr. Almeroth identifies Zaid’s “incremental number” as the purported “unique access code” of claim 1 of the ’026 patent. Almeroth Decl., ¶ 112. As I described above in Section VIII.B, Zaid’s “unique increment” is unrelated to any underlying content of the messages, including any purported privileges in the message. In fact, as I discuss above, Zaid discloses that a “unique increment” is included on all messages in the system, regardless of whether the message includes any of the “alleged privileges.” See EX1005, ¶¶ 81, 130.

64. Dr. Almeroth opines that “the unique increment in *Zaid* is a unique access code.” Almeroth Decl., ¶ 112. However, for element 1[g], which requires that “the unique access code is associated with privileges for use of the vehicle,” Dr. Almeroth does not rely on any portion of Zaid discussing the “unique increment,” and instead relies on Zaid’s discussion of the “reservation,” which Dr. Almeroth had previously identified as the purported “request” of claim 1. Almeroth Decl., ¶¶ 108, 119. Dr. Almeroth opines that the reservation has a “unique access code” and a different reservation would result in a different unique access code. *Id.*, ¶ 119. In my opinion, based on these facts, a POSITA would not have understood the “unique access code” to be “associated with privileges” as claimed.

65. As Zaid discloses in its “unique increment” embodiments, every communication in the system, regardless of its underlying content, includes a

“unique increment” to “avoid a repeat message attack.” EX1005, ¶¶ 81, 130. As I described above, the “unique increment” of Zaid is to limit the ability of an attacker to intercept and “repeat” a message. An example of how this “unique increment” may be implemented in practice follows. If a first message has a “unique increment” of “3” and a second message also has a “unique increment” of “3,” it signals that the second message may be an unauthorized “repeat message.” It is therefore my opinion that Zaid’s “unique increment” is associated with each “message” or “communication” in the system, but it has no association with the underlying information of the message. Indeed, the fact that the unique increment continuously changes would inform a POSITA that it cannot be associated with privileges for use of a vehicle that are unlikely to change frequently, or at least as frequently as each sent message in the system. It is my opinion that a POSITA would understand that Zaid’s “unique increment” is not “associated with” the alleged privileges, as required by claim 1.

66. Moreover, Dr. Almeroth offers no explanation of how “the privileges are defined for the unique access code,” as recited in claim 1. In his analysis for claim 1[g], Dr. Almeroth only uses the word defined once, in a conclusion sentence that repeats the claim language:

Therefore, the unique access code is associated with privileges of use for the vehicle, and the privileges are defined for the unique access code. Almeroth Decl., ¶ 119.

67. In my opinion, this conclusion sentence is insufficient to demonstrate that a POSITA would have understood Zaid to disclose or suggest that the privileges are defined for the unique access code.

68. Moreover, it is my opinion that Zaid’s alleged privileges are not “defined for the unique access code.” As I explained above, the “unique increment” of Zaid is unrelated to any purported privileges.

69. Dr. Almeroth’s alternative theory—that the “encrypted reservation” is a unique access code, also fails in my opinion. In my opinion, encrypting the reservation does not transform it to being associated with underlying privileges of the message or make the privileges defined for the encryption. As a POSITA would have been aware, encryption is a scheme that converts the message from one form to another. Encryption by itself does not make a message unique. If a message is not unique to begin with, encryption, alone, does not make it unique either, as encrypted versions of two identical messages are also identical. Realizing this, Dr. Almeroth opines that the encrypted message (“secret code”) is unique to the reservation request. Almeroth Decl., ¶115. The claim, however, requires the request to include a unique access code, not that the access code be unique to the

request. A system in which an access code is not unique, rather it is only unique to the request, is fundamentally different from the claimed system requiring the request to include a unique access code. Moreover, just like the “unique increment” of Zaid, the encryption scheme is agnostic to the actual content of the underlying message—not “associated with” it. *Id.* And as discussed above, Petitioners offer no reason how the alleged privileges are “defined for” the encryption. Petitioners cannot demonstrate any likelihood of success for element 1[g].

D. Dr. Almeroth fails to show that Zaid discloses or suggests a “vehicle [that] is configured to receive information from the server to authenticate the request by the mobile device.”

70. In my opinion, Dr. Almeroth does not demonstrate that a POSITA would have understood Zaid to disclose or suggest that the vehicle of claim 1 be “configured to receive information from the server to authenticate the request by the mobile device.” Dr. Almeroth opines that the vehicle “receives a private key from the server” to “‘authenticate’ the reservation.” Almeroth Decl., ¶ 122. In my opinion, Dr. Almeroth does not accurately describe Zaid’s disclosure, and nevertheless, a POSITA would have understood that no “private key” of Zaid authenticates any request **by** the mobile device.

71. As an initial matter, the disclosure of Zaid relied upon by Dr. Almeroth is unrelated to any request **by** the mobile device. Dr. Almeroth relies on

Zaid’s paragraph 126 for the purported “authentication” disclosure. Almeroth Decl., ¶ 122. Specifically, Zaid at paragraph 126 states that “decryption is used to ensure and ***authenticate that the intended wireless communication device is receiving*** the vehicle reservation rather than one that intercepts the vehicle reservation.” Almeroth Decl., ¶ 122 (quoting EX1005, ¶ 126) (I modified emphasis). As shown in the emphasized portion quoted above, the decryption authenticates that an authorized wireless device received the message. It does not authenticate a request ***by*** the mobile device, or any request at all. As paragraph 126 of Zaid discloses, “the vehicle reservation is communicated ***to*** a wireless communication device.” EX1005, ¶ 126 (emphasis added). “[T]he wireless communication device receives and caches the reservation.” *Id.* The wireless communication device decrypts the reservation using “a locally stored private key of the wireless communication device.” *Id.* A POSITA would understand that this functionality discloses what Zaid explicitly says it does, to authenticate that the correct mobile communication device ***receives*** the reservation. *Id.* Dr. Almeroth does not identify or discuss how any public key authenticates any request ***by*** the mobile device.

72. A POSITA would understand that Zaid’s decryption using private keys would not authenticate any message at all. In asymmetric cryptography, such as that discussed in Zaid, an entity has two keys: private key and public key. Any

information encrypted using the private key can be decrypted only using the corresponding public key, and conversely, any information encrypted using the public key can be decrypted only using the private key. As the names suggest, private keys are intended to be kept secret, while public keys are intended to be shared openly. Asymmetric cryptography can be used to achieve confidentiality or authentication. A message encrypted using an entity's public key is only readable by that entity, since only that entity has the private key to decrypt the message, ensuring confidentiality of that message. A message encrypted using an entity's private key can be read by anyone that has the entity's public key, but ensures the authenticity of that message, because only that entity has the private key to create such a message.

73. Zaid discloses that after receiving a message, the wireless communication device decrypts the first layer of encryption encrypted using the public key of the wireless communication device using a locally stored private key of the wireless communication device. In various embodiments, decryption is used to ensure and authenticate that the intended wireless communication device is receiving the vehicle reservation rather than one that intercepts the vehicle reservation. EX1005, ¶ 126. Accordingly, Zaid is disclosing the wireless device decrypting a received message using its private key, thus ensuring that only the wireless device can read the message and further protecting against a situation in

which the message is intercepted by another device. As I discussed above, a POSITA would not understand this to disclose or suggest authenticating the request by the mobile device, as required by the claim.

74. Zaid further discloses that “the vehicle reservation with its first layer of encryption stripped out is forwarded from the wireless communication device to the vehicle access kit. EX1005, ¶ 128. The vehicle access kit receives the vehicle reservation and decrypts the vehicle reservation. *Id.* Here, the second layer of encryption encrypted using a **public key** of the vehicle access kit is decrypted using a **private key** of the vehicle access kit stored locally on the vehicle access kit. *Id.* Given the understanding of how asymmetric encryption works, a POSITA would know that the authenticity of the wireless device cannot be determined solely based on the vehicle using its private key to decrypt a message encrypted using its public key, since any device can use the vehicle’s public key to send it an encrypted message. Since the private keys received by Zaid cannot be used in authenticating the request by the mobile device, Zaid does not disclose that the vehicle receives information from the server to authenticate the request by the mobile device, as required by the claim.

75. I also note that Dr. Almeroth’s proposed obviousness modification for this limitation does not cure Zaid’s deficiencies. Dr. Almeroth offers a modification of the vehicle receiving the private keys directly from the server.

Almeroth Decl., ¶ 123. Regardless of whether the vehicle receives private keys directly from the server, a POSITA would understand that private keys cannot “authenticate the request by the mobile device,” as claimed. As I described above, the private keys instead can only be used for confidentiality to ensure that only the intended recipient can access the messages—messages that can or cannot be authentic.

E. The Additional References Do Not Cure the Deficiencies of Zaid.

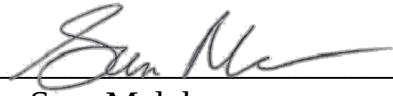
76. For Grounds 2-4, Dr. Almeroth proposes adding different references in combination with Zaid. However, Dr. Almeroth only proposes doing so as related to dependent claims 10, 13, and 15. The added references do not cure any deficiencies of Zaid discussed above, and Dr. Almeroth offers no opinion to the contrary.

IX. CONCLUSION

77. This declaration reflects my opinions as currently held. However, my analysis may continue such that I may consider additional information that may result in additional observations.

78. 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 this 30th day of August, 2024, at Irvine, California.



Dr. Sam Malek