IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC
Patent Owner

Case No. IPR2024-00405
U.S. Patent No. 10,073,960 BI
Case No. IPR2024-00407
U.S. Patent No. 9,679,289 B1

DECLARATION OF MARKUS JOKOBSSON, PH.D
EXHIBIT

I. INTRODUCTION AND SCOPE OF ENGAGEMENT

1. My name is Markus Jakobsson. I have been retained by counsel for Patent Owner Proxense, LLC ("Proxense") to provide my opinions regarding whether claims of U.S. Patent Nos. 9,679,289 (hereafter the "289 Patent") and 10,073,960 (hereafter the "960 Patent) recite terms understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure enabling an application, function or service, absent an algorithm disclosed in the Specifications of the respective patents.

II. QUALIFICATIONS AND COMPENSATION

2. I make this Declaration based upon my own personal knowledge, information, and belief, and I would and could competently testify to the matters set forth in this Declaration if called upon to do so.

3. Attached hereto as **Appendix A** is a true and correct copy of my Curriculum Vitae (CV). I am being compensated at the rate of $875 per hour for my time, plus reasonable out-of-pocket expenses. My compensation does not depend upon the outcome of the IPR proceedings, the contents of this Declaration, any testimony that I may provide, or the ultimate outcome of this litigation.

4. I am currently the Chief Scientist at Artema Labs, a crypto startup concerned with the security and confidentiality of digital representations of ownership. My research relates to how to make online transfers of ownership secure against abuses of various types, among other things.

5. I have founded or co-founded several successful computer security companies. I am the CEO at ZapFraud, a cybersecurity company that develops techniques to detect deceptive emails, such as Business Email Compromise emails. At ZapFraud, my research studies and addresses abuse, including social engineering, malware and privacy intrusions. My work primarily

involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches.

6. I am also the founder of Carbyne Biometrics, a biometric authentication company; Secure Technology, a target advertising company; RavenWhite Security, a device authentication company; FatSkunk, a mobile malware detection company (acquired by Qualcomm in 2013); Extricatus, a security consulting company (now defunct); CSExpert, a security consulting company; and RightQuestion, a telecom security company.

7. I received a Master of Science degree in Computer Engineering from the Lund Institute of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a Researcher at the San Diego Supercomputer Center, where I did research on authentication and privacy.

8. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and prevention. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. During that time I predicted the rise of what later became known as phishing. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols.

9. From 2004 to 2016, I held a faculty position at the Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of

Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to 2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books.

10. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, Chief Scientist at Agari from 2016 to 2018, Chief of Security and Data Analytics at Amber Solutions from 2018 to 2020, and Chief Scientist at ByteDance from 2020 to 2021.

11. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing countermeasures, including technological countermeasures, user interaction and education.

12. Amber Solutions is a cybersecurity company that develops home and office automation technologies. At Amber Solutions, my research addressed confidentiality, user interfaces and authentication techniques in the context of ubiquitous and wearable computing, and involved the tracking of users, for purposes of personalization and emergency response, using wireless technologies such as Bluetooth and Bluetooth Low Energy (BLE).

13. ByteDance is a media company concerned with secure processing of data, and is the owner of TikTok. At ByteDance, my research addressed fraud prevention, confidentiality, user interfaces and authentication techniques in the context of the many products offered by ByteDance.

14. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of the technical advisory board at Cequence Security (an anti-fraud company, previously named Stealth Security). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

15. I have authored six books and over 100 peer-reviewed publications, and have been a named inventor on over 300 patents and patent applications.

16. My work has included research in the area of applied security, mobile security, cryptographic protocols, authentication, malware, social engineering, usability and fraud.

17. I have been engaged as a technical expert in over 75 computer-related cases, including numerous cases involving Internet security, mobile security, encryption and/or authentication.

III. SUMMARY OF OPINIONS

18. As discussed in detail below, I do not believe the terms "RDC communicating wirelessly with [] at least one external device within [a] proximity zone", "integrated, wireless communication interface communicating wirelessly with [] at least one external device within [a] proximity zone", "local, secured information stored by [] integrated, secure memory", and "enablement signal" are understood by person of ordinary skill in the art to have a sufficiently

definite meaning as the names of structures for "enabling one or more of an application, a function and service." The terms, rather, connote the general and generic abilities of general purposes computers or are a completely meaningless nonce defined only by the intended action to be performed. Absent a control logic or some other type of algorithm executed by a controller or another type of processor, there would be no structure for the foregoing to perform the function of "enabling one or more of an application, a function and a service." The shared specification of the 289 and 960 Patents discloses a control logic that can be used by an "RDC," "wireless communication interface," and "local, secured information" to "enable one or more of an application, a function and service." The same control logic generates "an enablement signal enabling one or more of an application, a function and a service." Consequently, absent the control logic disclosed in the shared specification, the claims of the 289 and 960 Patents would be meaningless.

IV. UNDERSTANDING OF LEGAL PRINCIPLES

19. I have been advised on certain legal principles as they relate to forming my opinions presented herein. I set forth my understanding below.

A. Claim Construction

20. I understand that claims terms should be accorded the plain and ordinary meaning they would be ascribed by a person of ordinary skill in the art as of the effective filing date of the application for the patent at issue.

21. Generally speaking, I understand that to ascertain the meaning of a claim term, one of ordinary skill in the art primarily looks at intrinsic evidence, such as the words of the claims themselves, the specification, and the prosecution history. I understand that certain types of extrinsic evidence—such as general purpose and scientific dictionaries, relevant scientific principles, and references illustrating the meaning of technical terms and the state of the art—may

also be relevant to claim construction.

22. I further understand that a patentee may choose to define a term differently than the term's plain and ordinary meaning in the art and that, under such circumstances, the patentee's own definition controls. Additionally, a claim term is not entitled to its plain and ordinary meaning in the art when the patentee has expressly disclaimed the scope under such plain and ordinary meaning through descriptions in the specifications or statements made during prosecution of the patent applications.

23. I have been informed that a person of ordinary skill in the art is deemed to read a claim term not only in the context of the particular claim in which the term appears, but also in the context of the entire patent, including the specification, other claims, and prosecution history.

24. I further understand that when a claim term recites a function performed by a general-purpose computer, the corresponding structure is the computer as programmed to perform an algorithm, such as a control logic, disclosed in the patent for performing the function.

25. I understand that a dependent claim is a claim that incorporates by reference all limitations of its independent claim and of any intervening claims. As a general guideline, the scope of a dependent claim is narrower than that of its independent claim.

26. For the purpose of my opinions expressed herein, I have been asked to assume the 289 and 960 Patents have an effective filing date of December 6, 2007, which is the filing date of U.S. Provisional Application No. 60/992,953 to which both Patents claim priority.

B. Person of Ordinary Skill in the Art

27. When interpreting a patent, I understand that it is important to view the disclosure and claims of that patent from the level of a person of ordinary skill in the relevant art at the time of the invention. My opinion of the level of ordinary skill in the art of the Asserted Patents is based on my personal experience working in the fields of electrical engineering and computer science,

my knowledge of colleagues and others working in those fields as of and for several years prior to the applicable time frame applicable to each of those patents, my study of those patents and their file histories, and my knowledge of:

- The level of education and experience of persons actively working in the above fields at the time the subject matter at issue was developed;
- The types of problems encountered in the art at the time the subject matter was developed;
- The rapidity with which innovations are made in those fields;
- Prior art patents and publications;
- The activities of others working in those fields;
- Prior art solutions to the problems addressed by the relevant art; and
- The sophistication of the technology at issue in this case.

28. I have also been informed that these factors are not exhaustive and are merely a useful guide to determining the level of ordinary skill in the art.

29. With those factors in mind, in my opinion a Person of Ordinary Skill in the Art ("POSITA") with respect to the 289 and 960 Patents would have been a person with a Bachelor of Science degree in Computer Science, Computer Engineering, or a related discipline, and two years of experience in designing, developing, implementing, and/or deploying systems or applications on portable computing devices such as mobile phones and laptops, including programming of software and/or firmware for such devices.

V. OVERVIEW OF THE 289 AND 960 PATENTS

30. The 289 and 960 Patents disclose and claim a technical improvement to solve a technical problem of not being able to expand proximity systems to new and third-party

applications, by providing a novel control logic allowing memory to be used as secured local storage for external applications. The technical problem is highlighted in the Background sections of the 289 and 960 Patents:

> However, most proximity systems and location tracking systems have limited capabilities. Typically, the proximity sensor, RFID tag or similar device is a dumb device, in the sense that the device is designed and has the capability only to report its location. For example, such devices typically do not have the capabilities to run different applications or to even interact with different applications. Furthermore, these systems typically are proprietary and narrowly tailored for a specific situation, thus preventing easy expandability to other situations or third party applications.

289 Patent, 2:11-20; 960 Patent, 2:19-28.

31. The 289 and 960 Patents disclose a novel control logic solving the above problem. The control logic controls "service blocks" within device memory:

> The memory 210 also stores the various service blocks 112A-N… In other cases, the issuer may allow any third party service 120 to use available service blocks 112. If a new service block is created, then memory for that service block is allocated.., Regardless of how created, once created, external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding access key 118.

289 Patent, 6:42-60; 960 Patent, 6:49-67.

32. The control logic controlling the service blocks allows for isolated storage and selection of different credentials for different applications. This provides improved data security, as a breach in one third-party application would not affect the keys used by other applications. This is detailed, for example, with reference to Fig 6 (reproduced below):

> Also shown is a device 510Y with two applications 120Y1 and 120Y2, each of which accesses a different service block. In some cases, the first application 120Y1 is enabled from a first service block 112C, thus allowing a second application 120Y2 to operate using a second service block 112F (although the two applications need not be on the same device 510.

289 Patent, 6:42-60; 960 Patent, 6:49-67.

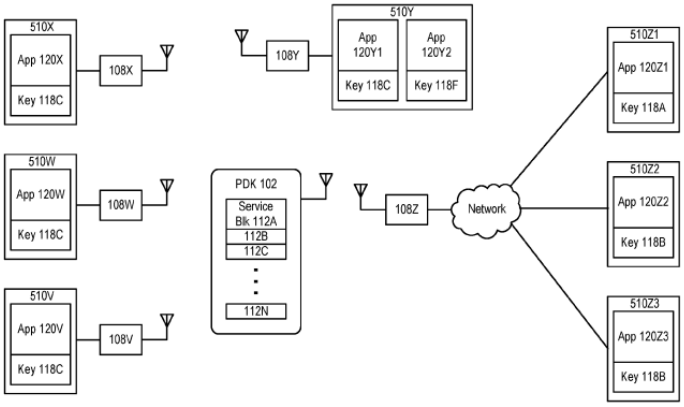


FIG. 6

33. The 289 and 960 Patents further detail how the control logic may be utilized in various general-purpose computers, such as cell phones, servers, personal computers, and credit card terminals. For example, again with reference to Fig. 6, the 289 and 960 Patents detail the simultaneous use of the control logic by different applications as a user accesses the website of his credit card provider:

> [T]he first application **120**Y**1** might be the auto login/logoff, where a user logs in to a personal computer via a service block **112**C that provides a username and password. Now that the user is logged in, the user wishes to attach to his credit card company. The user types in the web address of the credit card provider, where the credit card provider requests the user's credentials. First, the user may have to provide some live biometric information.

> Application **120**Y**2** compares this against a biometric stored in a second service block **112**F on the PDK. After the sensor **108**Y verifies the correct biometrics, the sensor indicates to the PDK that external services may now access their service blocks. The credit card provider **120**Z**1** then sends its service block access key **118**A to the PDK where this third service block **112**A is retrieved and sent back to the credit card issuer. The credit card issuer then verifies the data and authorizes the user's transaction.

289 Patent, 9:43-63; 960 Patent, 9:56-10:3.

34. As the above illustrates, when implemented, the control logic generates an enablement signal enabling one or more of an application, a function and a service by having the application, function or service to be enabled authenticate by exchanging an access key for the ability to store, retrieve and/or modify data in a service block of local secured memory.

VI. CLAIMS AT ISSUE

35. I understand the Petitioner is challenging is challenging claims 1-20 of the 289 Patent and claims 1-20 of the 960 Patent. Claims 1 and 14 of the 289 Patent are independent claims. Likewise, claims 1 and 14 of the 960 Patent are independent claims.

VII. THE CLAIMS FAIL TO RECITE A STRUCTURE FOR ENABLING ONE OR MORE OF AN APPLICATION, A FUNCATION AND A SERVICE

36. Having reviewed the challenged claims and the shared specification of the 289 and 960 Patents, it is my opinion that the structures recited for performing the function of "enabling one or more of an application, a function and a service" recited in claims 1 and 14 of the 289 Patent and claims 1 and 14 of the 960 Patent are not used in common parlance or by persons of skill in the pertinent art to designate structure or a class of structures recognized for performing the function. Rather, the structure "local, secured information stored by the integrated, secure memory," recited it claims 1 of the 289 Patent and claim 1 of the 960, is nothing more than a

computer readable media providing the general and generic ability of general-purpose computers to securely store information within tamper-proof memory. Likewise, the "integrated wireless communication interface communicating wirelessly with the at least one external device within a proximity zone," recited in claim 1 of the 960 Patent, is nothing more the general ability of general-purpose computers to receive data using standards protocols such a Bluetooth, Wi-Fi, and the like. Similarly, the "integrated RDC communicating wirelessly with the at least one external device within the proximity zone," recited in claim 1 of the 289 Patent, is nothing more than the general ability of general-purpose computers to decode encrypted data received via Bluetooth, Wi-Fi, and similar connection. Finally, the "enablement signal," recited in claim 14 of the 289 Patent and claim 14 of the 960 Patent, is a completely meaningless nonce defined only by the intended action to be performed.

A. Local, Secured Information Stored by the Integrated, Secure Memory

37. On its face, the term "local, secured information stored by the integrated, secure memory" recites nothing more than a computer readable media providing the general and generic ability of general-purpose computers to securely store information within tamper-proof memory. This ability is commonly employed within computers to securely store data at rest. However, the secure storage of data does not provide a structure for "enabling one or more of an application, a function and a service." Instead, an algorithm or control logic defining how the data is to be accessed and made usable to application, function, or service would be required. Such an algorithm is provided within the shared specification of the 289 and 960 Patents.

38. One instance of the algorithm is provided within the definition of "local secured information" provided in the shared specification:

> "The service block access keys 118 allow the sensor 108 to unlock information stored in the corresponding service blocks 112, which

information is used as ***local secured information***."

289 Patent, 3:45-50; 960 Patent, 3:54-57 (emphasis added).

39. The shared specification explicitly defines "local secured information" with an algorithm. Per the algorithm, an "access key" is exchanged to "unlock information stored within a service block." Accordingly, local, secured information is defined in the specification as information unlocked in exchange for an access key.

40. The algorithm defining "local, secured information" is repeated in the shared specification with reference to "control logic 250," again clarifying that it means information unlocked (made accessible) in exchange for (by proving) an access key.

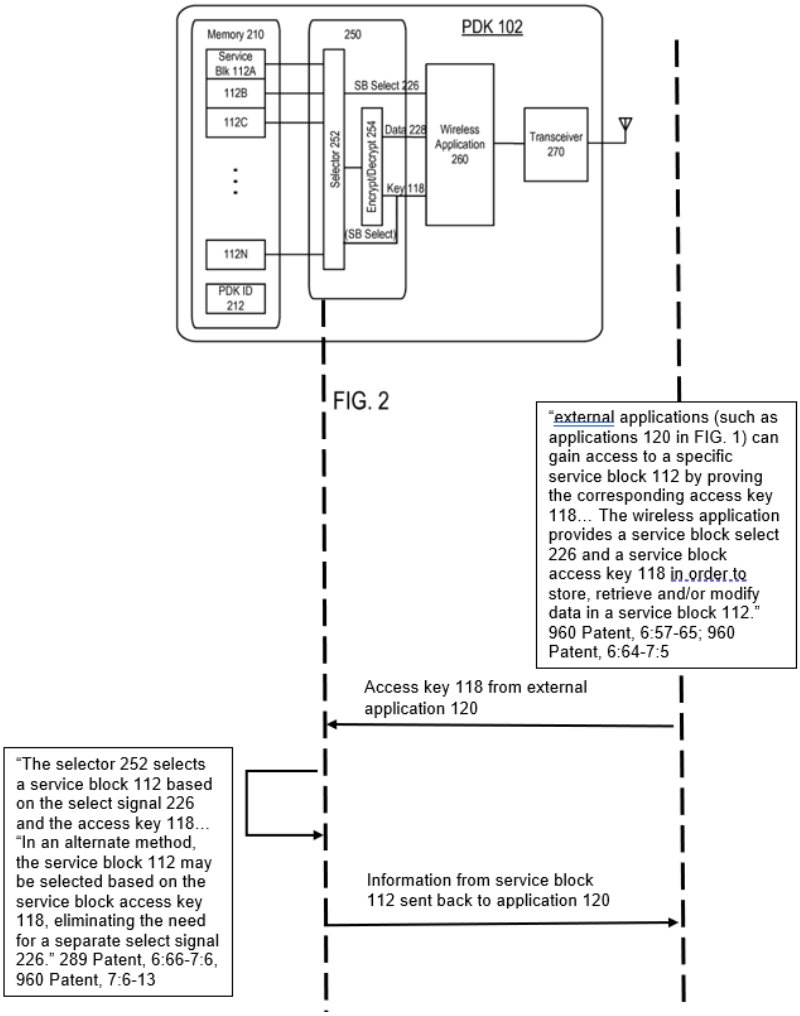
> [O]nce created, external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding access key 118. In FIG. 2, this is shown conceptually by control logic 250.

289 Patent, 6:57-62; 960 Patent, 6:64-7:1.

41. After summarizing the operation of algorithm of control logic 250 as "external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding ***access key 118***," the shared specification goes on to state:

> The wireless application ***provides*** a service block select 226 and ***a service block access key*** 118 in order to ***store, retrieve and/or modify data*** in a service block 112. The selector 252 selects a service block 112 based on the select signal 226 and the access key 118.… In an alternate method, the service block 112 may be selected based on the service block access key 118, eliminating the need for a separate select signal 226."

289 Patent, 6:63-7:6; 960 Patent, 7:3-13.



42. The operation of the algorithm of control logic 250 is graphically represented in the above figure. When executed, the algorithm exchanges an "access key" provided by an application for the information held within "service block". The detailed function of the "access key" is consistent with its plain and ordinary meaning. "Access" means "[t]o store data on and retrieve data from a disk or other peripheral device." The algorithm thus describes exchanging an access key provided by an application to retrieve, store and/or modify data. A POSITA would recognize that this as being similar to a database key, which along with an access control mechanism is a key used to determine what records of the database to allow access to. Such keys are also referred to

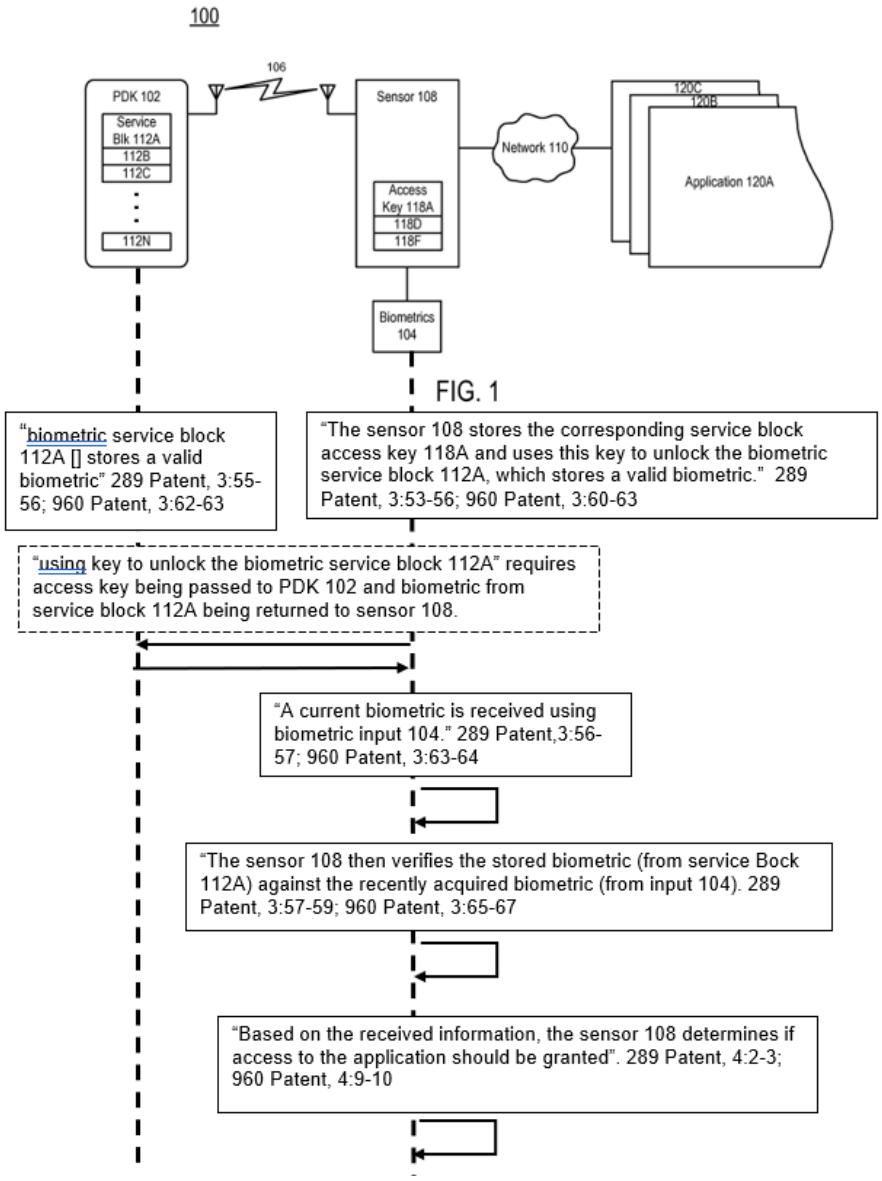
as “data access keys,” or as in the specification of the 289 and 960 patents, simply “access keys”.

43. The algorithm is further repeated in the shared specification with reference to Figures 1 and 4-6. With reference to Figure 1, the shared specification details use of the algorithm in which an access key held by an external application is exchanged to unlock biometric information held within a service block to enable function of biometric authentication.

> In one example, a biometric is required in order to access specific service blocks 112 in the PDK102. Verification of the biometric is achieved by using service block 112A. The sensor 108 stores the corresponding service block access key 118A and uses this key to unlock the biometric service block 112A, which stores a valid biometric. A current biometric is received using biometric input 104. The sensor 108 then verifies the stored biometric (from service block 112A) against the recently acquired biometric (from input 104). Upon proper Verification, various applications 120 are per mitted to connect to the PDK102 via the sensor 108 and/or to gain access to other service blocks 112.
>
> The system 100 can be used to address applications 120 where it is important to authenticate an individual for use. Generally, the sensor 108 wirelessly receives information stored in the PDK 102 that uniquely identifies the PDK 102 and the individual carrying the PDK102. The sensor 108 can also receive a biometric input 104 from the individual. Based on the received information, the sensor 108 determines if access to the application 120 should be granted. In this example, the system 100 provides authentication without the need for PINs or passwords (although PINs and passwords may be used in other implementations).”

289 Patent, 3:51-4:6; 960 Patent 3:58-4:13.

44. The flow of such a process is shown in the figure below.



45. As the above shows, the biometric authentication by sensor 108 is enabled by the sensor exchanging an access key to unlock and retrieve a biometric held within a service block.

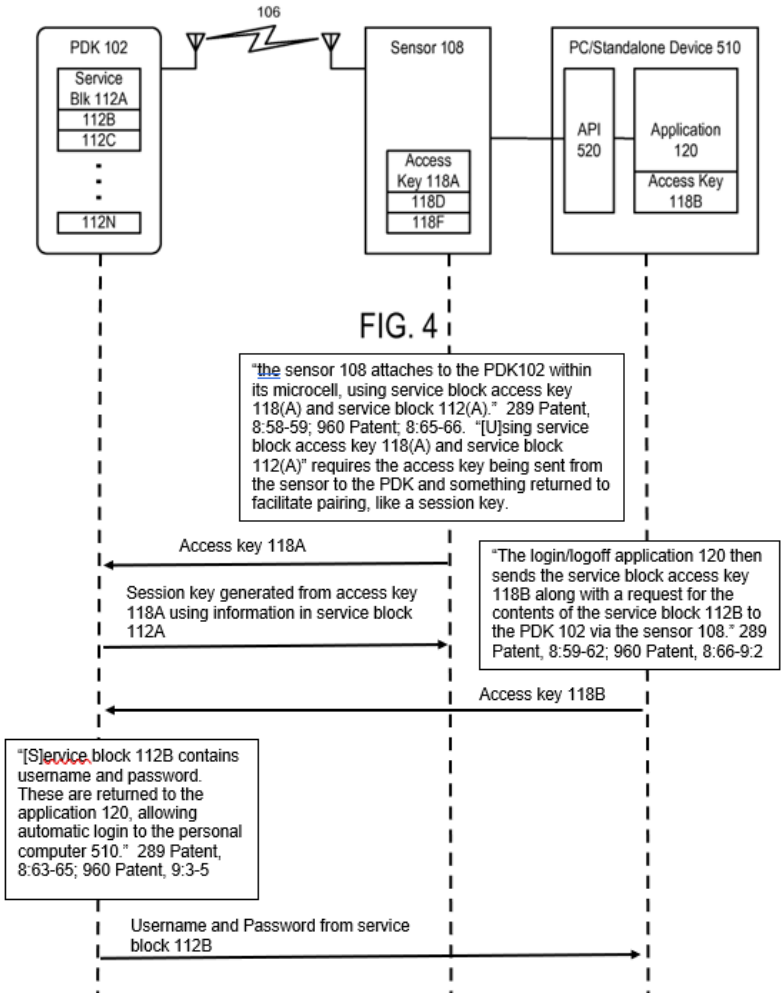
46. With reference to Figure 4, the shared specification details how the algorithm of exchanging an access to retrieve information held within service block enables an auto login/logoff application.

> An example of a local application (FIG. 4) is an auto login/logoff of a personal computer. When a PDK 102 is within the proximity of

the personal computer 510, the PDK 102 is detected and the sensor 108 attaches to the PDK 102 (using service block112A). The login/logoff application 120 then sends the service block access key 118B along with a request for the contents of the service block 112B to the PDK 102 via the sensor 108. For example, a standard may specify that particular service block 112B contains username and password. These are returned to the application 120, allowing automatic login to the personal computer 510

289 Patent, 8:55-65; 960 Patent, 8:62-9:5

47. The flow is shown in the figure below.



48. The flow begins by "the sensor 108 attach[ing] to the PDK 102 within its microcell,

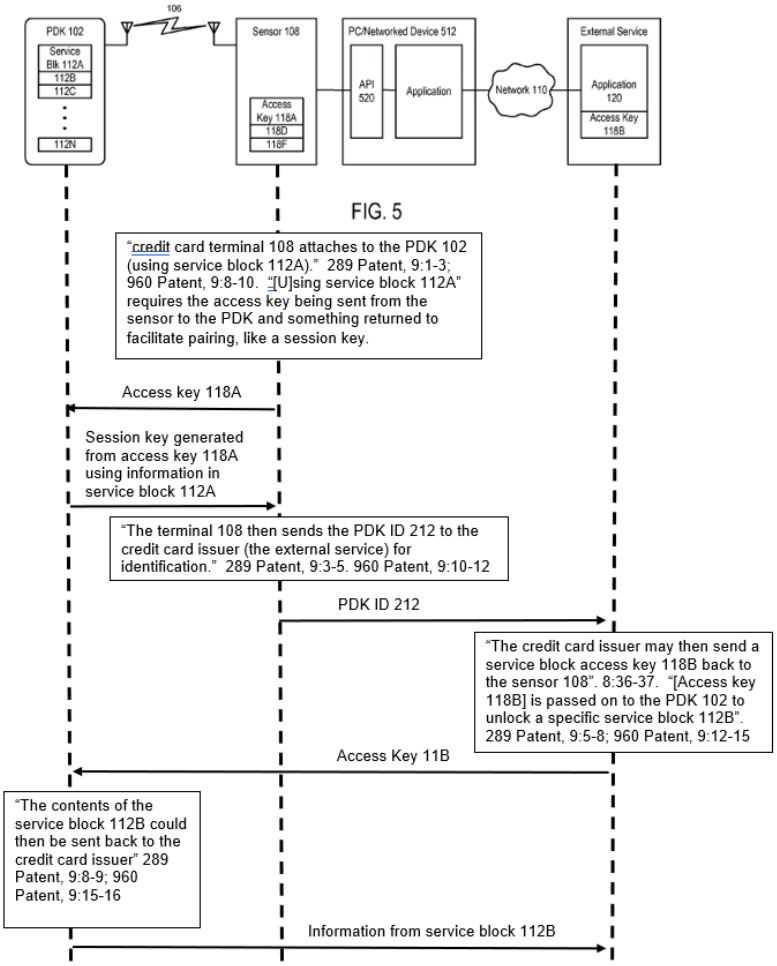
using the service block access key 118(A) and service block 112(A)." While this entails the exchange of an access key 118(A) for a derivation of information held within the service block 112(A), such a session key generated from the access key, it does not enable the login/logoff application 120. Rather, it merely creates a wireless link between the sensor 108 and the PDK 102 facilitating wireless communication between the sensor 108 and PDK 102. As the example makes clear, the link itself does not enable login/logoff application 120 because subsequent steps are required after establishing wireless communication between sensor 108 and PDK 102. Rather, application 120 is not enabled until it exchanges an access key 118(B) to unlock and retrieve a username and password held within service block 112(B).

49. The shared specification also details how the algorithm of exchanging an access to retrieve information held within a service block enables service of using a credit card to purchase goods. With reference to Figure 5, the shared specification states:

> An example of a remote application (FIG.5) is a credit card transaction. The sensor 108 in this case could be a credit card terminal. When the PDK 102 is brought in close proximity, the credit card terminal 108 attaches to the PDK 102 (using service block112A). The terminal 108 then sends the PDKID 212 to the credit card issuer (the external service) for identification. The credit card issuer may then send a service block access key 118B back to the sensor 108, where it is passed on to the PDK102 to unlock a specific service block 112B. The contents of the service block 112B could then be sent back to the credit card issuer where further decryption could occur and the credit cardholder could be verified. Once verified, the credit card terminal displays that the transaction is approved.

289 Patent, 8:66-9:12; 960 Patent, 9:6-19.

50. The flow for enabling the service of charging a credit card is shown in the below figure.



51. As with the enabling login/logoff application 120, the flow begins by "credit card terminal 108 attach[ing] to the PDK 102 (suing service block 112A)." While this entails the exchange of an access key 118(A) for a derivation of information held within the service block 112(A), such a session key generated from the access key, it does not enable the service of using the credit card to complete the transaction. Rather, it merely creates a wireless link between the credit card terminal 108 and the PDK 102 facilitating wireless communication between the credit card terminal 108 and PDK 102. As the example makes clear, the link itself does not enable service of charging the credit card because subsequent steps are required after establishing wireless

communication between credit card terminal 108 and PDK 102. Rather, the service of charging the credit card is not enabled until credit card issuer sends an access key 118B to unlock and retrieve the contents of service block 112B.

52. "FIGS. 4 and 5 illustrate a basic case where a single application accesses a single service block on a single PDK via a single sensor." 289 Patent, 9:20-22; 960 Patent, 9:27-29. However, as noted above, the algorithm of control logic 250 defining local, secured memory is not limited to use with single applications. Rather, as detailed with reference Figure 6, the algorithm can be used with multiple applications, sensors, and service blocks.

> FIG. 6 illustrates a case with multiple applications, sensors, and service blocks. This illustrates the sharing of service blocks. As shown, service blocks may be limited to a single service or source or may be shared across multiple services and Sources. A service block 112 is a protected memory element which allows an application 120 with the right credentials to access it. In this example, applications 120W. 120X and 120Y1 can each access service block 112C since each application has access to service block access key 118C. Similarly, applications 120V, 120Z2 and 120Z3 can each access service block 112B. Although not shown in FIG. 6, it is also possible for an application to access more than one service block. FIG. 6 also shows a situation where applications 120Z1-3 running on different devices 510Z1-3 all access the PDK 102 through the same sensor 108Z. Each sensor 108 covers a certain proximity Zone (i.e., microcell). The presence of the PDK 102 within a microcell indicates proximity of the PDK to that particular sensor.
>
> Also shown is a device 510Y with two applications 120Y1 and 120Y2, each of which accesses a different service block. In some cases, the first application 120Y1 is enabled from a first service

block 112C, thus allowing a second application 120Y2 to operate using a second service block 112F (although the two applications need not be on the same device 510). For example, the first application 120Y1 might be the auto login/logoff, where a user logs in to a personal computer via a service block 112C that provides a username and password. Now that the user is logged in, the user wishes to attach to his credit card company. The user types in the web address of the credit card provider, where the credit card provider requests the user's credentials. First, the user may have to provide some live biometric information. Application 120Y2 compares this against a biometric stored in a second service block 112F on the PDK. After the sensor 108Y verifies the correct biometrics, the sensor indicates to the PDK that external services may now access their service blocks. The credit card provider 120Z1 then sends its service block access key 118A to the PDK where this third service block 112A is retrieved and sent back to the credit card issuer. The credit card issuer then verifies the data and authorizes the user's transaction.

289 Patent, 9:23-63; 960 Patent, 9:30-10:3.

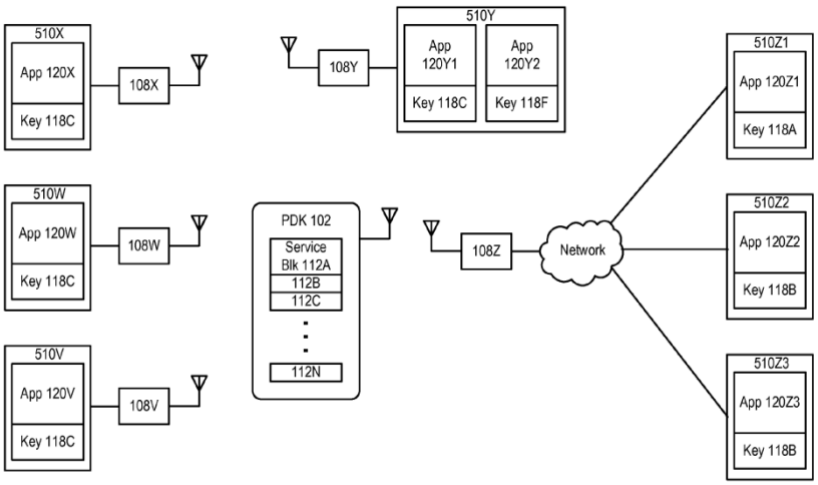


FIG. 6

53. Again, the shared specification details that access to a service block is dependent on being able to exchange the right access key to unlock and retrieve the information held within the service block. Thus, "applications 120W. 120X and 120Y1 can each access service block 112C since each application has access to service block access key 118C." 289 Patent, 29-32; 960 Patent, 9:36-39. The algorithm of control logic 250, which defines local, secured information, allows multiple applications to simultaneously use the same PDK. As detailed above, "the first application 120Y1 might be the auto login/logoff, where a user logs in to a personal computer via a service block 112C that provides a username and password." 289 Patent, 9:47-50; 960 Patent, 9:54-57. As shown in Figure 6 above, application 120Y1 has a copy of access key 118C, and thus can exchange access key 118C to unlock and retrieve the username and password in service block 112C. Once logged in to the computer, the example continues with the user authenticating via biometric verification application 120Y2, such that "Application 120Y2 compares this against a biometric stored in a second service block 112F on the PDK." 289 Patent, 9:55-56; 960 Patent, 9:62-63. Application 120Y2 can make the comparison because it has access key 118F which can be exchanged to unlock and retrieve a biometric stored in service block 112F. Finally, the "credit card provider 120Z1 then sends its service block access key 118A to the PDK where this third service block 112A is retrieved and sent back to the credit card issuer." 289 Patent, 9:59-62; 960 Patent, 9:66-10:2. Yet again, something is enabled by exchanging an access key to unlock and retrieve information held within service.

54. As the foregoing examples demonstrate, the shared specification discloses several instances of how the algorithm defining local, secured information is used to "enable one or more of an application, a function and a service." Absent this algorithm, "local, secured information stored by the integrated, secure memory" would be nothing more than the general ability of

computers to store data in a tamper-proof formation. Absent the algorithm, local, secured information would be unable to "enable one or more of an application, a function and a service" and claim 1 of the 289 Patent and claim 1 of the 960 Patent would be meaningless.

B. The Integrated RDC / Wireless Communication Interface Communicating Wirelessly with the At Least One External Device within the Proximity Zone

55. A "wireless communication interface" are nothing more than the general ability of computers to receive information via wireless protocols, such as Bluetooth, Wi-Fi, and the like. The claims themselves say as much. Both claim 1 of the 289 Patent and claim 1 of the 960 state each is "communicating wirelessly with the at least one external device within the proximity zone." This is exactly what happens when devices communicate over Bluetooth or Wi-Fi, they receive/send information from/to other devices within range (i.e., proximity zone). But just receiving information is insufficient to "enable one or more of an application, a function and service." An algorithm must be executed instructing how to use the received information.

56. The shared specification also does not provide any significant structure for the receiver decoder circuit (RDC). Rather, RDC is merely described as follows:

> The RDC 304 provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306.

289 Patent, 7:45-48; 960 Patent, 7:52-55.

57. Per the above, the RDC is just a wireless interface that can decode or decrypt received data. But Bluetooth, Wi-Fi, and most other communication protocols utilize some form of data encryption to protect data in transit. Accordingly, neither an RDC nor a wireless communication interface provides anything more than the general ability of a computer to receive

data. However, just receiving data does not "enable one or more of an application, a function and service." Absent an algorithm, the received information would be meaningless. The shared specification does provide an algorithm defining local, secured memory that is implemented as control logic 250. Absent the algorithm, RDC or wireless communication interface "communicating wirelessly with the at least one external device within the proximity zone" would not "enable one or more of an application, a function and a service" and claim 1 of the 289 Patent and claim 1 of the 960 Patent would be meaningless.

C. Enablement Signal Enabling One or More of an Application, a Function and a Service

58. The claim term "enablement signal" has a plain and ordinary meaning described directly in the shared specification. This term has no other defined meaning and would not be recognized by a person of ordinary skill in the art outside of the definition provided for it by the shared specification. In other words, there was no meaning or definition in the art at the time, outside of the context provided by the specification, to designate a structure or class of structures for "enabling one or more of an application, a function and a service." The term itself – "enablement signal" - merely reiterates its function of "enabling one or more of an application, a function and service." Consequently, without the context of the shared specification, the term would be understood by those skilled in the art as nothing more than a meaningless nonce word.

59. The shared specification explains exactly what can be an enablement signal and how it is generated. The shared specification details the generation of an enablement signal with respect to Fig. 14 and 15 (reproduced below).

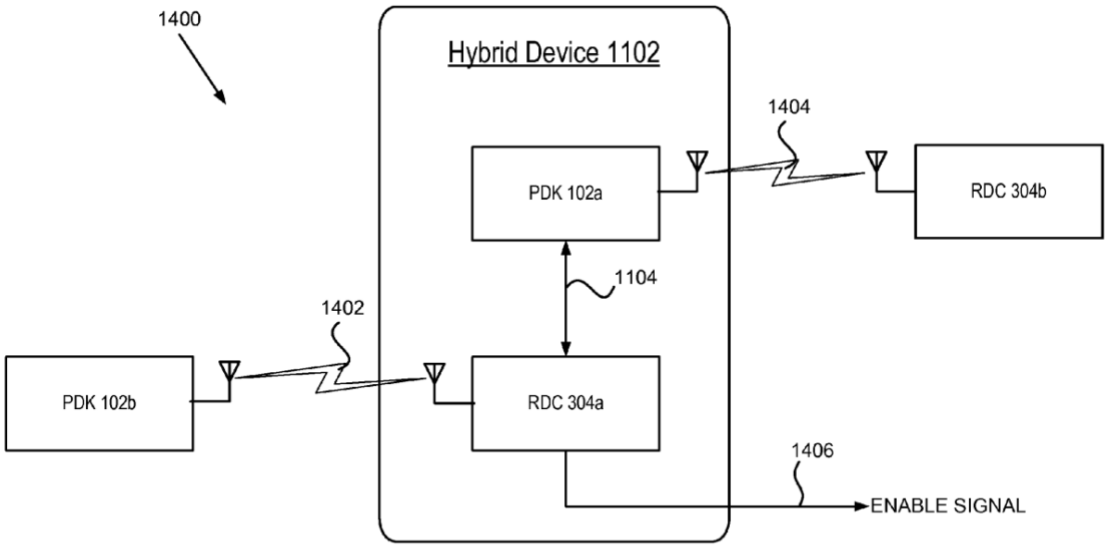


FIG. 14

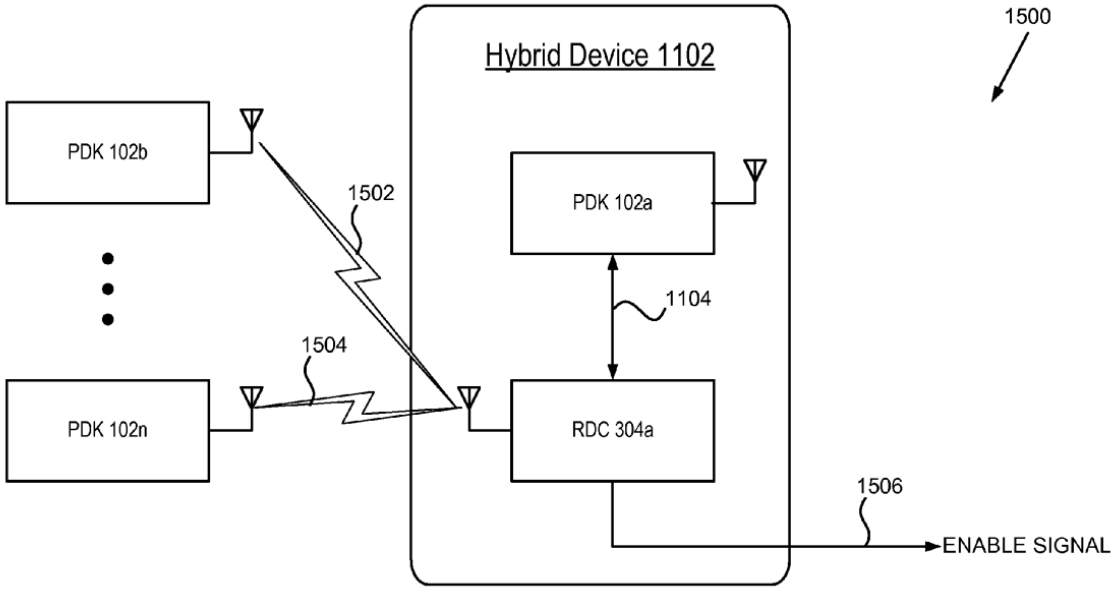


FIG. 15

60. As the specification explains, a link between a RDC and PDK is required to

generate an enablement signal on a signal line between an RDC and a device. For instance, with respect to Fig 14, the specification states, "***only when the hybrid device 1102 has multiple links 1402, 1404*** will the hybrid device 1102 ***generate an authorization or enable signal*** on signal line 1406." 289 Patent, 17:47-50; 960 Patent, 17:54-57. In Fig. 14, links 1402, 1404 are between PDKs 102b, 102a and RDCs 304a, 304b, respectively. "If either the RDC 304b or PDK102b is not present, the hybrid device 1102 does not allow operation of the personal computer." 289 Patent, 17:64-66; 960 Patent, 18:4-6. Fig 15 shows another embodiment requiring the same. "For the system 1500, only when multiple PDK links 1502,1504 to the hybrid device 1102 exist, will an authorization/enablement signal be generated on signal line 1506." 289 Patent, 18:4-6; 960 Patent, 18:11-13. Generating an enablement signal, therefore, depends upon the operation and interaction of a PDK and RDC.

61. A similar description is provided with respect to the cell phone 1202 including the hybrid device 1102, depicted in Figure 12 (reproduced below). As shown in Figure 12, cell phone 1202 has the "conventional SIM card [is] replaced with the hybrid device 1102 that provide[d] the RDC functionality." 289 Patent, 15:6-8; 960 Patent, 15:14-16. "The SIM content (Cell phone account, contact information, and credit card information) that is normally stored in the cell phone 1202 is instead stored in the PDK 102b carried by the user." 289 Patent, 15:11-14; 960 Patent, 15:19-22. "[T]he cell phone 1202 is rendered useless (except 911) if the PDK 102b is out of range of the RDC 304a of the hybrid device 1102." 289 Patent, 15:22-24; 960 Patent, 15:30-32. Accordingly, enabling cell phone 1202 also requires the operation and interaction of a PDK and RDC

62. The shared specification states that "In a minimal embodiment, the PDK 102a includes an antenna and a transceiver for communicating with a RDC (not shown) and a controller

and memory for storing information particular to a user." 289 Patent, 14:20-23; 960 Patent, 14:28-31. A PDK is thus defined in the shared specification as nothing more than a general purpose computer capable of communication. The only structures are controller (i.e., processor) and memory, which form nothing more than generic computer, and an antenna and transceiver, which add nothing more than Bluetooth, Wi-Fi, or the like. Thus, a PDK is defined in the shared specification as a generic computer with Bluetooth or Wi-Fi, such as a standard laptop, desktop, or smart phone.

63. Furthermore, as noted above, an RDC is just a wireless interface that can decrypt received data. But Bluetooth, Wi-Fi, and most other communication protocols utilize some form of data encryption to protect data in transit. Accordingly, an RDC is nothing more than the generic capacity to receive information present on any computer equipped with a wireless antenna for Wi-Fi or Bluetooth.

64. As both a PDK and RDC are defined in the shared specification as nothing more than generic computers, absent an algorithm or some other software, the claims would have no ability to "enable one or more of an application, a function and a service." An algorithm executed by the controller of the PDK is detailed in the shared specification as "control logic 250." The shared specification summarizes the operation of the algorithm as "external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding ***access key 118***." 289 Patent, 6:57-60; 960 Patent, 6:64-67. The specification then goes onto to describe the algorithm, stating that "[t]he wireless ***application provides*** a service block select 226 and ***a service block access key*** 118 in order to ***store, retrieve and/or modify data*** in a service block 112." 289 Patent, 6:63-65; 960 Patent, 7:3-5. "In an alternate method, the service block 112 may be selected based on the service block access key 118, eliminating the need

for a separate select signal 226." 289 Patent, 7:4-6; 960 Patent, 7:11-13. The detailed function of the "access key" is consistent with its plain and ordinary meaning. "Access" means "[t]o store data on and retrieve data from a disk or other peripheral device." The algorithm thus describes exchanging an access key provided by an application to retrieve, store and/or modify data. Absent this algorithm, the RDC and PDK would not be able to "enable one or more of an application, a function and a service" and the claims would lose all connection to the shared specification and be meaningless.

VIII. CONCLUSION

65. The structures recited for performing the function of "enabling one or more of application, a function and service" recited in claims 1 and 14 of the 289 Patent and claims 1 and 14 of the 960 Patent are not used in common parlance or by persons of skill in the pertinent art to designate structure or a class of structures recognized for performing the function. Rather, the structure "local, secured information stored by the integrated, secure memory," recited it claims 1 of the 289 Patent and claim 1 of the 960, is nothing more than a computer readable media providing the general and generic ability of general-purpose computers to securely store information within tamper-proof memory. Likewise, the "integrated wireless communication interface communicating wirelessly with the at least one external device within a proximity zone," recited in claim 1 of the 960 Patent, is nothing more the general ability of general-purpose computers to receive data using standards protocols such a Bluetooth, Wi-Fi, and the like. Similarly, the "integrated RDC communicating wirelessly with the at least one external device within the proximity zone," recited in claim 1 of the 289 Patent, is nothing more than general ability of general-purpose computers to decode encrypted data received via Bluetooth, Wi-Fi, and similar connection. Finally, the "enablement signal," recited in claim 14 of the 289 Patent and claim 14 of the 960 Patent, is a completely meaningless nonce defined only by the intended action to be

performed. Absent an algorithm, therefore, claim 1 of the 289 Patent and claim 1 of the 960 Patent would be meaningless.

66. An algorithm defining "local, secured information" and implemented as control logic 250 is defined in the shared specification. The operation of this algorithm "generates an enablement enabling one or more of an application, a function and service," as shown with numerous examples in the specification. Accordingly, a person of ordinary skilled in the art reading the claims in the context of the specification, would understand the structure for "enabling one or more of an application, a function or a service" and for "generating an enablement signal" is the algorithm implemented as control logic 250 and defines "local, secured information."

67. I, Markus Jakobsson, do hereby declare and state, 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, under Section 1001 of Title 18 of the United States Code.

Dated: October 15, 2024

Markus Jakobsson, PhD

Appendix A

CV and Research Statement

Markus Jakobsson
www.linkedin.com/in/markusjakobsson
www.markus-jakobsson.com

1 At a Glance

- **Focus.** *Identification of security problems, trends and solution along four axes* – computational, structural, physical *and* social*; quantitative and qualitative fraud analysis; development of disruptive security technologies.*
- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Science, University of California at San Diego, 1994); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1993).
- **Large research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); PayPal (Principal Scientist of Consumer Security, Director, 2010-2013); Qualcomm (Senior Director, 2013-2015); Agari (Chief Scientist, 2016–2018); Amber Solutions Inc (Chief of Security and Data Analytics, 2018 – 2019); ByteDance (Principal Scientist, 2020-2021)
- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2016).
- **Entrepreneurial activity.** *ZapFraud* (Anti-scam technology; CTO and founder, 2012-current); *RavenWhite Security* (Authentication solutions; CTO and founder, 2005-); *RightQuestion* (Consulting; Founder, 2007-current); *FatSkunk* (Malware detection; CTO and founder, 2009-2013 – FatSkunk was acquired by Qualcomm); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2013); *CellFony* (Mobile security; Member of technical advisory board, 2009-2013); *PopGiro* (User Reputation; Member of technical advisory board, 2012-2013); *MobiSocial* (Social networking, Member of technical advisory board, 2013); *Cequence Security* (Anti-fraud, Member of technical advisory board, 2013–current)
- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2011); *Boku* (2009-2010); *Western Union* (2009-2010).

Patent Owner Exhibit 2014, Page 31 of 50

- **Intellectual Property, Testifying Expert Witness.** *Inventor of 100+ patents; expert witness in 25+ patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale; Hunton & Williams; Quinn Emanuel Urquhart & Sullivan; Freed & Weiss; Berry & Domer; Fish & Richardson; DLA Piper; Cipher Law Group; Keker & Van Nest). Details and references upon request.

- **Publications**. Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crimeware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *Towards Trustworthy Elections: New Directions in Electronic Voting* (Springer Verlag, 2010); *Mobile Authentication: Problems and Solutions*)Springer Verlag, 2012); *The Death of the Internet* (Wiley, 2012); *Understanding Social Engineering* (Springer Verlag, 2016); *Security, Privacy and User Interaction* (Springer Verlag, 2020); *100+ peer-reviewed publications*

2 At a Glance

Ten years before Bitcoin was created, I formalized the notion of Proof of Work and described its use for mining of crypto payments. I later developed energy-efficient alternatives to this paradigm, and showed how to enable mining on mobile devices, which is not possible for Bitcoin. I am the founder of the academic discipline of phishing and have developed techniques to predict fraud trends years before they emerge, enabling countermeasures to be developed before they are needed. I developed the notion of implicit authentication, which is now ubiquitous; I also founded a company that developed the first retroactive virus detection technology, with guarantees of detection; the company was acquired by Qualcomm in 2013. I have worked as chief scientist and similar positions in startups as well as industry behemoths, such as PayPal. I have several hundred patents to my name and am a prominent security researcher with hundreds of peer reviewed publications and an array of textbooks. My 1997 PhD thesis, from University of California at San Diego, was on distributed electronic payment systems with revocable privacy.

3 Work History (Highlights)

1. **Member of Technical Staff, Bell Labs (1997-2001).** Markus was part of the security research group at Bell Labs. He formalized the notion of *proof of work*, later an integral part of BitCoin.

2. **Principal Scientist, RSA Labs (2001-2005).** Markus posited that phishing would become a mainstream problem, and developed ethical techniques for identifying likely trends based on human subject experiments.

3. **Associate Professor, Indiana University (2005-2008).** Markus was hired to lead the newly formed security group at Indiana University, and

created a research group comprising approximately 10 professors and 30 students, studying social engineering and fraud.

4. **Principal Scientist, Xerox PARC (2008-2010).** Markus was hired to lead the research efforts of the Xerox PARC security group, and developed the notion of *implicit authentication*, a technology that is now ubiquitous.

5. **Principal Scientist, PayPal (2010-2013).** Markus did research on security and user interfaces, and developed techniques to reduce the losses associated with *liar buyer fraud*.

6. **Senior Director, Qualcomm (2013-2016).** Qualcomm acquires FatSkunk, a company founded by Markus. At FatSkunk, Markus developed *retroactive* malware detection with provable security guarantees. A simplified version of this is now deployed with almost all Qualcomm chipsets.

7. **Chief Scientist, Agari (2016-2018).** Markus developed a technique to acquire fraudster intelligence by compromising scammer email accounts – *while staying within the law* – resulting in the extradition of several African scam lords to the U.S.

8. **Chief of Security and Data Analytics, Amber Solutions (2018-2020).** Markus developed usable configuration methods supporting improved security and privacy for IoT installations.

9. **Chief Scientist, ByteDance (2020-2021).** Markus oversaw the establishment of a research group and a research agenda at ByteDance, and contributed to their intellectual property and product security.

10. **Chief Scientist, Artema LABS (2021-).** Managing the research, product strategy, and patent strategy for Artema LABS, a Los Angeles based startup in the Crypto/NFT sector.

4 Publication List

Books (1-8); book chapters, journals, conference publications and other scientific publications (9-147), issued /published U.S. patents (148-234). For an updated list, and for international patents, please see `www.markus-jakobsson.com/publications` and appropriate patent search engines.

References

[1] M. Jakobsson, *Security, Privacy and User Interaction*, ISBN 978-3-030-43753-4, 110 pages, 2020.

[2] M. Jakobsson, *Understanding Social Engineering Based Scams*, ISBN 978-1-4939-6457-4, 130 pages, Springer, 2016.

[3] M. Jakobsson, *Mobile Authentication: Problems and Solutions*, ISBN 1461448778, 125 pages, Springer, 2013.

[4] M. Jakobsson, (editor) *The Death of the Internet*, ASIN B009CN2JVE, 359 pages, IEEE Computer Society Press, 2012.

[5] D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. Ryan, J. Benaloh, and M. Kutylowski, (editors), *Towards Trustworthy Elections: New Directions in Electronic Voting*, 411 pages, (Vol. 6000), Springer, 2010.

[6] M. Jakobsson and Z. Ramzan (editors), *Crimeware: Trends in Attacks and Countermeasures*, ISBN 0321501950, Hardcover, 582 pages, Symantec Press / Addison Wesley, 2008.

[7] M. Jakobsson and S. A. Myers (editors), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, ISBN 0-471-78245-9, Hardcover, 739 pages, Wiley, 2006.

[8] M. Jakobsson, M. Yung, J. Zhou, *Applied Cryptography and Network Security: Second International Conference , Yellow Mountain, China, 2004*, 511 pages, Lecture Notes in Computer Science (Book 3089), 2004.

[9] M. Jakobsson, "Permissions and Privacy," in IEEE Security & Privacy, vol. 18, no. 2, pp. 46-55, March-April 2020

[10] M. Jakobsson, "The Rising Threat of Launchpad Attacks," in IEEE Security & Privacy, vol. 17, no. 5, pp. 68-72, Sept.-Oct. 2019

[11] J Koven, C Felix, H Siadati, M Jakobsson, E Bertini, "Lessons learned developing a visual analytics solution for investigative analysis of scamming activities," IEEE transactions on visualization and computer graphics 25 (1), 225-234

[12] M Jakobsson, "Two-factor inauthentication?the rise in SMS phishing attacks" Computer Fraud & Security 2018 (6), 6-8

[13] M. Dhiman, M. Jakobsson, T.-F. Yen, "Breaking and fixing content-based filtering," 2017 APWG Symposium on Electronic Crime Research (eCrime), 52-56

[14] M. Jakobsson, "Addressing sophisticated email attacks," 2017 International Conference on Financial Cryptography and Data Security, 310-317

[15] M. Jakobsson, "User trust assessment: a new approach to combat deception," Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 2016, pages 73-78

[16] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, "Mind your SMSes: Mitigating social engineering in second factor authentication," Computers and Security, 2016

Patent Owner Exhibit 2014, Page 34 of 50

[17] M. Jakobsson, W. Leddy, "Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters," IEEE Spectrum 53 (5), 2016, 40-55

[18] N. Sae-Bae, M. Jakobsson, *Hand Authentication on Multi-Touch Tablets*, HotMobile 2014

[19] Y. Park, J. Jones, D. McCoy, E. Shi, M. Jakobsson, *Scambaiter: Understanding Targeted Nigerian Scams on Craigslist*, NDSS 2014

[20] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, and P. van Oorschot, "The future of authentication," Security & Privacy, IEEE, 10(1), 22-27, 2012.

[21] M. Jakobsson, and H. Siadati, *Improved Visual Preference Authentication: Socio-Technical Aspects in Security and Trust*, (STAST), 2012 Workshop on IEEE, 27–34, 2012.

[22] M. Jakobsson, R. I. Chow, and J. Molina, "Authentication-Are We Doing Well Enough?[Guest Editors' Introduction]" Security & Privacy, IEEE, 10(1), 19-21, 2012.

[23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," Information Security, 99-113, Springer Berlin Heidelberg, 2011.

[24] M. Jakobsson and K. Johansson, "Practical and Secure Software-Based Attestation," Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 1–9, 2011.

[25] A. Juels, D. Catalano, and M.Jakobsson, *Coercion-resistant electronic elections: Towards Trustworthy Elections*, 37–63, Springer Berlin Heidelberg, 2010.

[26] M. Jakobsson and F. Menczer, "Web Forms and Untraceable DDoS Attacks," in Network Security, Huang, S., MacCallum, D., and Du, D. Z., Eds.,77–95, Springer, 2010.

[27] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the Clouds: A Framework and its Application to Mobile Users," 2010.

[28] X. Wang, P. Golle, M. Jakobsson, and A. Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur., 13(2), 1-24, 2010.

[29] X. Wang, P. Golle, M. Jakobsson, A.Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur. 13(2): (2010)

Patent Owner Exhibit 2014, Page 35 of 50

[30] M. Jakobsson, and C. Soghoian, "Social Engineering in Phishing," Information Assurance, Security and Privacy Services, 4, 2009.

[31] M. Jakobsson, C. Soghoian and S. Stamm, "Phishing," Handbook of Financial Cryptography (CRC press, 2008)

[32] M. Jakobsson and A. Tsow, "Identity Theft," In John R. Vacca, Editor, "Computer And Information Security Handbook" (Morgan Kaufmann, 2008)

[33] S. Srikwan and M. Jakobsson, "Using Cartoons to Teach Internet Security," Cryptologia, vol. 32, no. 2, 2008

[34] M. Jakobsson, N. Johnson and P. Finn, "Why and How to Perform Fraud Experiments," IEEE Security and Privacy, March/April 2008 (Vol. 6, No. 2) pp. 66-68

[35] M. Jakobsson and S. Myers, "Delayed Password Disclosure," International Journal of Applied Cryptography, 2008, pp. 47-59.

[36] M. Jakobsson and S. Stamm, "Web Camouflage: Protecting Your Clients from Browser Sniffing Attacks," IEEE Security & Privacy Magazine. November/December 2007

[37] P. Finn and M. Jakobsson, "Designing and Conducting Phishing Experiments," IEEE Technology and Society Magazine, Special Issue on Usability and Security

[38] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer. "Social Phishing," The Communications of the ACM, October 2007

[39] A. Tsow, M. Jakobsson, L. Yang and S. Wetzel, "Warkitting: the Drive-by Subversion of Wireless Home Routers," Anti-Phishing and Online Fraud, Part II Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006

[40] M. Gandhi, M. Jakobsson and J. Ratkiewicz, "Badvertisements: Stealthy Click-Fraud with Unwitting Accessories," Anti-Phishing and Online Fraud, Part I Journal of Digital Forensic Practice, Volume 1, Special Issue 2, November 2006

[41] N. Ben Salem, J.-P. Hubaux and M. Jakobsson. "Reputation-based Wi-Fi Deployment," Mobile Computing and Communications Review, Volume 9, Number 3 (Best papers of WMASH 2004)

[42] N. Ben Salem, J. P. Hubaux, and M. Jakobsson. "Node Cooperation in Hybrid Ad hoc Networks," IEEE Transactions on Mobile Computing, Vol. 5, No. 4, April 2006.

[43] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," Journal of Cryptology, 2005

Patent Owner Exhibit 2014, Page 36 of 50

[44] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. "How To Turn Loaded Dice Into Fair Coins." IEEE Transactions on Information Theory, vol. 46(3). May 2000. pp. 911–921.

[45] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," Journal of Computer Networks, vol. 31, issue 11–16, Elsevier North-Holland, Inc., 1999. pp. 1101–1109.

[46] M. Jakobsson, "Cryptographic Protocols," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[47] M. Jakobsson, "Cryptographic Privacy Protection Techniques," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[48] M. Jakobsson, E. Shi, P. Golle, R. Chow, "Implicit authentication for mobile devices," 4th USENIX Workshop on Hot Topics in Security (HotSec '09); 2009 August 11; Montreal, Canada.

[49] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); 2009 November 13; Chicago, IL. NY: ACM; 2009; pp. 85–90.

[50] M. Jakobsson, H. Siadati, M. Dhiman, "Liar Buyer Fraud, and How to Curb It," NDSS, 2015

[51] M. Jakobsson, T.-F. Yen, "How Vulnerable Are We To Scams?," BlackHat, 2015

[52] M. Jakobsson, "How to Wear Your Password," BlackHat, 2014

[53] M. Jakobsson and G. Stewart, "Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines," in BlackHat, 2013.

[54] M. Jakobsson, and H. Siadati,"SpoofKiller: You Can Teach People How to Pay, but Not How to Pay Attention" in Socio-Technical Aspects in Security and Trust (STAST), 2012 Workshop on, 3-10, 2012.

[55] M. Jakobsson, and M. Dhiman,"The benefits of understanding passwords," in Proceedings of the 7th USENIX conference on Hot Topics in Security, Berkeley, CA, USA, 2012.

[56] M. Jakobsson, and S. Taveau, "The Case for Replacing Passwords with Biometrics," Mobile Security Technologies, 2012.

[57] M. Jakobsson and D. Liu, "Bootstrapping mobile PINs using passwords," W2SP, 2011.

Patent Owner Exhibit 2014, Page 37 of 50

[58] M. Jakobsson and R. Akavipat, "Rethinking passwords to adapt to constrained keyboards," 2011.

[59] Y. Niu, E. Shi, R. Chow, P. Golle, and M. Jakobsson, "One Experience Collecting Sensitive Mobile Data," In USER Workshop of SOUPS, 2010.

[60] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit Authentication through Learning User Behavior," 2010.

[61] M. Jakobsson and K. Johansson, Assured Detection of Malware With Applications to Mobile Platforms, 2010.

[62] M. Jakobsson and K. Johansson, "Retroactive Detection of Malware With Applications to Mobile Platforms," in HotSec 2010, Washington, DC, 2010.

[63] M. Jakobsson, A Central Nervous System for Automatically Detecting Malware, 2009.

[64] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, and J. Staddon, "Controlling data in the cloud: outsourcing computation without outsourcing control," ACM workshop on Cloud computing security (CCSW), 2009.

[65] M. Jakobsson and A. Juels, "Server-Side Detection of Malware Infection," in New Security Paradigms Workshop (NSPW), Oxford, UK, 2009.

[66] M. Jakobsson, "Captcha-free throttling," Proceedings of the 2nd ACM workshop on Security and artificial intelligence, 15–22, 2009.

[67] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," Proceedings of the 4th USENIX conference on Hot topics in security, 9–9, 2009.

[68] C. Soghoian, O. Friedrichs and M. Jakobsson, "The Threat of Political Phishing," International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)

[69] R. Chow, P. Golle, M. Jakobsson, L. Wang and X. Wang, "Making CAPTCHAs Clickable," In proc. of HotMobile 2008.

[70] M. Jakobsson, A. Juels, and J. Ratkiewicz, "Privacy-Preserving History Mining for Web Browsers," Web 2.0 Security and Privacy, 2008.

[71] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang, "Love and Authentication," (Notes) ACM Computer/Human Interaction Conference (CHI), 2008. Also see `www.I-forgot-my-password.com`

[72] M. Jakobsson and S. Myers, "Delayed Password Disclosure," Proceedings of the 2007 ACM workshop on Digital Identity Management

[73] M. Jakobsson, S. Stamm, Z. Ramzan, "JavaScript Breaks Free," W2SP '07

Patent Owner Exhibit 2014, Page 38 of 50

[74] A. Juels, S. Stamm, M. Jakobsson, "Combatting Click Fraud via Premium Clicks," USENIX Security 2007

[75] R. Chow, P. Golle, M. Jakobsson, X. Wang, "Clickable CAPTCHAs," Ad-Fraud '07 Workshop; 2007 September 14; Stanford, CA, USA

[76] S. Stamm, Z. Ramzan, and M. Jakobsson, "Drive-by Pharming," In Proceedings of Information and Communications Security, 9th International Conference, ICICS 2007

[77] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, "What Instills Trust? A Qualitative Study of Phishing," USEC '07.

[78] R. Akavipat, V. Anandpara, A. Dingman, C. Liu, D. Liu, K. Pongsanon, H. Roinestad and M. Jakobsson, "Phishing IQ Tests Measure Fear, not Ability," USEC '07.

[79] M. Jakobsson, "The Human Factor in Phishing," American Conference Institute's Forum on Privacy & Security of Consumer Information, 2007

[80] S. Srikwan, M. Jakobsson, A. Albrecht and M. Dalkilic, "Trust Establishment in Data Sharing: An Incentive Model for Biodiversity Information Systems," TrustCol 2006

[81] J.Y. Choi, P. Golle, M. Jakobsson, "Tamper-Evident Digital Signatures: Protecting Certification Authorities Against Malware," DACS '06

[82] L. Yang, M. Jakobsson, S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," SECURECOMM '06

[83] P. Golle, X. Wang, M. Jakobsson, A. Tsow, "Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks." IEEE S&P '06

[84] M. Jakobsson, A. Juels, T. Jagatic, "Cache Cookies for Browser Authentication (Extended Abstract)," IEEE S&P '06

[85] M. Jakobsson and J. Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features.", WWW '06

[86] M. Jakobsson and S. Stamm. "Invasive Browser Sniffing and Countermeasures," WWW '06

[87] J.Y. Choi, P. Golle and M. Jakobsson. "Auditable Privacy: On Tamper-Evident Mix Networks," Financial Crypto '06

[88] A. Juels, D. Catalano and M. Jakobsson. "Coercion-Resistant Electronic Elections," WPES '05

[89] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," ACNS '05, 2005.

[90] M. Jakobsson and L. Yang. "Quantifying Security in Hybrid Cellular Networks," ACNS '05, 2005

[91] Y.-C. Hu, M. Jakobsson, and A. Perrig. "Efficient Constructions for One-way Hash Chains," ACNS '05, 2005

[92] M. Jakobsson. "Modeling and Preventing Phishing Attacks," Phishing Panel in Financial Cryptography '05. 2005, abstract in proceedings.

[93] N. Ben Salem, J.-P. Hubaux, and M. Jakobsson. "Reputation-based Wi-Fi Deployment Protocols and Security Analysis," In WMASH '04. ACM Press, 2004. pp. 29–40.

[94] M. Jakobsson and S. Wetzel. "Efficient Attribute Authentication with Applications to Ad Hoc Networks," In VANET '04. ACM Press, 2004. pp. 38–46.

[95] M. Jakobsson, X. Wang, and S. Wetzel. "Stealth Attacks in Vehicular Technologies," Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004 Fall (VTC-Fall 2004). IEEE, 2004.

[96] A. Ambainis, H. Lipmaa, and M. Jakobsson. "Cryptographic Randomized Response Technique," In PKC '04. LNCS 2947. Springer-Verlag, 2004. pp. 425–438.

[97] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. "Universal Re-encryption for Mixnets," In CT-RSA '04. LNCS 2964. Springer-Verlag, 2004. pp. 163–178.

[98] P. Golle and M. Jakobsson. "Reusable Anonymous Return Channels," In WPES '03. ACM Press, 2003. pp. 94–100.

[99] M. Jakobsson, S. Wetzel, B. Yener. "Stealth Attacks on Ad-Hoc Wireless Networks," In IEEE VTC '03, 2003.

[100] N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks," In ACM MobiHoc '03. ACM Press, 2003. pp. 13–24.

[101] M. Jakobsson, J.-P.Hubaux and L. Buttyan. "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks," In FC '03. LNCS 2742. Springer-Verlag, 2003. pp. 15–33.

[102] M. Jakobsson, T. Leighton, S. Micali and M. Szydlo. "Fractal Merkle Tree Representation and Traversal," In RSA-CT '03 2003.

[103] A. Boldyreva and M Jakobsson. "Theft protected proprietary certificates," In DRM '02. LNCS 2696, 2002. pp. 208–220.

Patent Owner Exhibit 2014, Page 40 of 50

[104] P. Golle, S. Zhong, M. Jakobsson, A. Juels, and D. Boneh. "Optimistic Mixing for Exit-Polls," In Asiacrypt '02. LNCS 2501. Springer-Verlag, 2002. pp. 451–465.

[105] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," In CRYPTO '02. LNCS 2442. Springer-Verlag, 2002. pp. 385–400.

[106] M. Jakobsson. "Fractal Hash Sequence Representation and Traversal," In Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT '02). 2002. pp. 437–444.

[107] M. Jakobsson, A. Juels, and R. Rivest. "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking," In Proceedings of the 11th USENIX Security Symposium. USENIX Association, 2002. pp. 339–353.

[108] D. Coppersmith and M. Jakobsson. "Almost Optimal Hash Sequence Traversal," In Financial Crypto '02. 2002.

[109] M. Jakobsson. "Financial Instruments in Recommendation Mechanisms," In Financial Crypto '02. 2002.

[110] J. Garay, and M. Jakobsson. "Timed Release of Standard Digital Signatures," In Financial Crypto '02. 2002.

[111] F. Menczer, N. Street, N. Vishwakarma, A. Monge, and M. Jakobsson. "Intellishopper: A Proactive, Personal, Private Shopping Assistant," In AAMAS '02. ACM Press, 2002. pp. 1001–1008.

[112] M. Jakobsson, A. Juels, and P. Nguyen. "Proprietary Certificates," In CT-RSA '02. LNCS 2271. Springer-Verlag, 2002. pp. 164–181.

[113] M. Jakobsson and A. Juels. "An Optimally Robust Hybrid Mix Network," In PODC '01. ACM Press. 2001. pp. 284–292.

[114] M. Jakobsson and M. Reiter. "Discouraging Software Piracy Using Software Aging," In DRM '01. LNCS 2320. Springer-Verlag, 2002. pp. 1–12.

[115] M. Jakobsson and S. Wetzel. "Security Weaknesses in Bluetooth," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 176–191.

[116] M. Jakobsson and D. Pointcheval. "Mutual Authentication for Low-Power Mobile Devices," In Financial Crypto '01. LNCS 2339. Springer-Verlag, 2001. pp. 178–195.

[117] M. Jakobsson, D. Pointcheval, and A. Young. "Secure Mobile Gambling," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 110–125.

[118] M. Jakobsson and S.Wetzel. "Secure Server-Aided Signature Generation," In PKC '01. LNCS 1992. Springer-Verlag, 2001. pp. 383–401.

Patent Owner Exhibit 2014, Page 41 of 50

[119] M. Jakobsson and A. Juels. "Addition of ElGamal Plaintexts," In T. Okamoto, ed., ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 346–358.

[120] M. Jakobsson, and A. Juels. "Mix and Match: Secure Function Evaluation via Ciphertexts," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 162–177.

[121] R. Arlein, B. Jai, M. Jakobsson, F. Monrose, and M. Reiter. "Privacy-Preserving Global Customization," In ACM E-Commerce '00. ACM Press, 2000. pp. 176–184.

[122] C.-P. Schnorr and M. Jakobsson. "Security of Signed ElGamal Encryption," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 73–89.

[123] P. Bohannon, M. Jakobsson, and S. Srikwan. "Cryptographic Approaches to Privacy in Forensic DNA Databases," In Public Key Cryptography '00. LNCS 1751. Springer-Verlag, 2000, pp. 373–390.

[124] J. Garay, M. Jakobsson, and P. MacKenzie. "Abuse-free Optimistic Contract Signing," In CRYPTO '99. LNCS 1666. Springer-Verlag, 1999. pp. 449–466.

[125] M. Jakobsson. "Flash Mixing," In PODC '99. ACM Press, 1999. pp. 83–89.

[126] G. Di Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. "How To Forget a Secret," In STACS '99. LNCS 1563. Springer-Verlag, 1999. pp. 500–509.

[127] M. Jakobsson, D. M'Raihi, Y. Tsiounis, and M. Yung. "Electronic Payments: Where Do We Go from Here?," In CQRE (Secure) '99. LNCS 1740. Springer-Verlag, 1999. pp. 43–63.

[128] C.P. Schnorr and M. Jakobsson. "Security Of Discrete Log Cryptosystems in the Random Oracle + Generic Model," In Conference on The Mathematics of Public-Key Cryptography. 1999.

[129] M. Jakobsson and A. Juels "Proofs of Work and Breadpudding Protocols," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 252 – 272.

[130] M. Jakobsson and C-P Schnorr. "Efficient Oblivious Proofs of Correct Exponentiation," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 71–86.

[131] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," In World Wide Web '99

Patent Owner Exhibit 2014, Page 42 of 50

[132] M. Jakobsson, J.P. Stern, and M. Yung. "Scramble All, Encrypt Small," In Fast Software Encryption '99. LNCS 1636. Springer-Verlag, 1999. pp. 95–111.

[133] M. Jakobsson and J. Mueller. "Improved Magic Ink Signatures Using Hints," In Financial Cryptography '99. LNCS 1648. Springer-Verlag, 1999. pp. 253–268.

[134] M. Jakobsson. "Mini-Cash: A Minimalistic Approach to E-Commerce," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 122–135.

[135] M. Jakobsson. "On Quorum Controlled Asymmetric Proxy Re-encryption," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 112–121.

[136] M. Jakobsson and A. Juels. "X-Cash: Executable Digital Cash," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 16–27.

[137] M. Jakobsson and D. M'Raihi. "Mix-based Electronic Payments," In Proceedings of the Selected Areas in Cryptography. LNCS 1556. Springer-Verlag, 1998. pp. 157173.

[138] M. Jakobsson, E. Shriver, B. Hillyer, and A. Juels. "A Practical Secure Physical Random Bit Generator," In CCS '98: Proceedings of the 5th ACM conference on Computer and communications security. ACM Press, 1998. pp. 103–111.

[139] M. Jakobsson. "A Practical Mix," In Advances in Cryptology – EuroCrypt '98. LNCS 1403. Springer-Verlag, 1998. pp. 448–461.

[140] M. Jakobsson and M. Yung. "On Assurance Structures for WWW Commerce," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 141–157.

[141] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. "Curbing Junk E-Mail via Secure Classification," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 198–213.

[142] M. Jakobsson and M. Yung. "Distributed 'Magic Ink' Signatures," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 450–464.

[143] M. Jakobsson and M. Yung. "Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System," In Financial Cryptography '97. LNCS 1318. Springer-Verlag, 1997. pp. 217–238.

[144] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. "Proactive public-key and signature schemes," In Proceedings of the 4th Annual Conference on Computer Communications Security. ACM Press, 1997. pp. 100–110.

Patent Owner Exhibit 2014, Page 43 of 50

[145] M. Bellare, M. Jakobsson, and M. Yung. "Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 280–305.

[146] M. Jakobsson and M. Yung. "Proving Without Knowing," In Crypto '96. LNCS 1109. Springer-Verlag, 1996. pp. 186–200.

[147] M. Jakobsson, K. Sako, and R. Impagliazzo. "Designated Verifier Proofs and Their Applications," In Advances in Cryptology – EuroCrypt '96. LNCS 1070. Springer-Verlag, 1996. pp. 143–154.

[148] M. Jakobsson and M. Yung. "Revokable and Versatile Electronic Money," In CCS '96: Proceedings of the 3rd ACM conference on Computer and communications security. ACM Press, 1996. pp. 76–87.

[149] M. Jakobsson. "Ripping Coins for a Fair Exchange," In Advances in Cryptology – EuroCrypt '95. LNCS 921. Springer-Verlag, 1995. pp. 220–230.

[150] M. Jakobsson. "Blackmailing using Undeniable Signatures," In Advances in Cryptology EuroCrypt '94. LNCS 950. Springer-Verlag, 1994. pp. 425–427.

[151] M. Jakobsson. "Reducing costs in identification protocols," Crypto '92, 1992.

[152] M. Jakobsson. "Machine-Generated Music with Themes," In International Conference on Artificial Neural Networks '92. Vol 2. Amsterdam: Elsevier, 1992. pp. 1645–1646

[153] M. Jakobsson, "Social Engineering 2.0: What's Next," McAfee Security Journal, Fall 2008

[154] M. Jakobsson and S. Myers, "Delayed Password Disclosure," ACM SIGACT News archive, Volume 38, Issue 3 (September 2007), pp. 56 - 75

[155] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," CryptoBytes, 2007.

[156] M. Jakobsson, A. Juels, J. Ratkiewicz, "Remote-Harm Detection," Beta-version available at `rhd.ravenwhitedevelopment.com/`

[157] S. Stamm, M. Jakobsson, "Social Malware," Experimental results available at `www.indiana.edu/ phishing/verybigad/`

[158] M. Jakobsson. "Privacy vs. Authenticity," Ph.D. Thesis, University of California at San Diego, 1997

[159] Markus Jakobsson, Automatic PIN creation using passwords, US20130125214 A1, 2012.

Patent Owner Exhibit 2014, Page 44 of 50

[160] Markus Jakobsson, Systems and methods for creating a user credential and authentication using the created user credential, US 20130111571 A1, 2012.

[161] Markus Jakobsson, Password check by decomposing password, US 20120284783 A1, 2012.

[162] Markus Jakobsson, William Leddy, System and methods for protecting users from malicious content, US 20120192277 A1, 2011.

[163] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8370935 B1, 2011.

[164] Markus Jakobsson, Methods and Apparatus for Efficient Computation of One-Way Chains in Cryptographic Applications, US20120303969 A1, 2011.

[165] Markus Jakobsson, Automatic PIN creation using password, US 20120110634 A1, 2011.

[166] Markus Jakobsson, Jim Roy Palmer, Gustavo Maldonado, Interactive CAPTCHA, US20130007875 A1, 2011.

[167] Markus Jakobsson, System access determination based on classification of stimuli, US 20110314559 A1, 2011.

[168] Markus Jakobsson, System access determination based on classification of stimuli, WO 2011159356 A1, 2011.

[169] Markus Jakobsson, Method, medium, and system for reducing fraud by increasing guilt during a purchase transaction, US8458041 B1, 2011.

[170] Markus Jakobsson, Visualization of Access Information, US 20120233314 A1, 2011.

[171] Markus Jakobsson, Richard Chow,Runting Shi, Implicit authentication, US20120137340 A1, 2010.

[172] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, EP2467793 A1, 2010.

[173] Markus Jakobsson, Event log authentication using secure components, US 20110314297 A1, 2010.

[174] Markus Jakobsson, Philippe J.P. Golle, Risk-based alerts, US 20110314426 A1, 2010.

[175] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041178 A1, 2010.

[176] M. Jakobsson, A. Juels, J. Kaliski Jr, S. Burton and others, Identity authentication system and method, US Patent 7,502,933, 2009.

[177] Markus Jakobsson, Method and system for facilitating throttling of interpolation-based authentication, US8219810 B2, 2009.

[178] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8375442 B2, 2009.

[179] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041180 A1, 2009.

[180] Markus Jakobsson, Pattern-based application classification, US 20110055925 A1, 2009.

[181] Markus Jakobsson, Method and apparatus for detecting cyber threats, US8286225 B2, 2009.

[182] Markus Jakobsson, Method and apparatus for detecting cyber threats, US20110035784 A1, 2009.

[183] Markus Jakobsson, CAPTCHA-free throttling, US8312073 B2, 2009.

[184] Markus Jakobsson, Captcha-free throttling, US 20110035505 A1, 2009.

[185] Markus Jakobsson, Christopher Soghoian, Method and apparatus for throttling access using small payments, US 20100153275 A1, 2008.

[186] Markus Jakobsson, Christopher Soghoian, Method and apparatus for mutual authentication using small payments, US 20100153274 A1, 2008.

[187] Philippe J.P. Golle, Markus Jakobsson,Richard Chow, Resetting a forgotten password using the password itself as authentication, US 20100125906 A1, 2008.

[188] Philippe J. P. Golle, Markus Jakobsson,Richard Chow, Authenticating users with memorable personal questions, US8161534 B2, 2008.

[189] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Authentication based on user behavior, US20100122329 A1, 2008.

[190] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Enterprise password reset, US 20100122340 A1, 2008.

[191] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US8086866 B2, 2008.

[192] Richard Chow, Philippe J. P. Golle, Markus Jakobsson, Selectable captchas, US8307407 B2, 2008.

[193] Markus Jakobsson, Ari Juels, Sidney Louis Stamm, Method and apparatus for combatting click fraud, US 20080162227 A1, 2007.

[194] Jakobsson, Method and apparatus for evaluating actions performed on a client device, US 20080037791 A1, 2007.

[195] Jakobsson, Ari Juels, Method and apparatus for storing information in a browser storage area of a client device, US 20070106748 A1, 2006.

[196] Markus Jakobsson, Steven Andrew Myers, Anti-phising logon authentication object oriented system and method, WO 2006062838 A1, 2005.

[197] Jakobsson, Jean-Pierre Hubaux,Levente Buttyan, Micro-payment scheme encouraging collaboration in multi-hop cellular networks, US 20050165696 A1, 2004.

[198] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , System and method providing disconnected authentication, WO2005029746 A3, 2004.

[199] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane Rice, Ronald Rivest, Less , System and method providing disconnected authentication, US 20050166263 A1, 2004.

[200] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , Systeme et procede d'authentification deconnectee, WO 2005029746 A2, 2004.

[201] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Identity authentication system and method, WO2004051585 A3, 2003.

[202] Markus Jakobsson, Ari Juels, Burton S. Kaliski, Jr., Identity authentication system and method, US 7502933 B2, 2003.

[203] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Systeme et procede de validation d'identite, WO 2004051585 A2, 2003.

[204] Markus Jakobsson, Burton S. Kaliski, Jr., Method and apparatus for graph-based partition of cryptographic functionality, US7730518 B2, 2003.

[205] Markus Jakobsson, Phong Q. Nguyen, Methods and apparatus for private certificates in public key cryptography, US7404078 B2, 2002.

[206] Jakobsson, Philip MacKenzie, Thomas Shrimpton, Method and apparatus for performing multi-server threshold password-authenticated key exchange, US20030221102 A1, 2002.

[207] Markus Jakobsson, Philip D MacKenzie, Method and apparatus for distributing shares of a password for use in multi-server password authentication, US 7073068 B2, 2002.

[208] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, EP 1389376 A1 (text from WO2002084944A1), 2002.

[209] Markus Jakobsson, Adam Lucas Young, Method and apparatus for identification tagging documents in a computer system, US 7356845 B2, 2002.

[210] Juan A. Garay, Markus Jakobsson, Methods and apparatus for computationally-efficient generation of secure digital signatures, US 7366911 B2, 2001.

[211] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US 7404080 B2, 2001.

[212] Markus Jakobsson, Susanne Gudrun Wetzel, Securing the identity of a bluetooth master device (bd addr) against eavesdropping by preventing the association of a detected channel access code (cac) with the identity of a particular bluetooth device, WO2002019641 A3, 2001.

[213] Markus Jakobsson, Susanne Gudrun Wetzel, Procede et appareil permettant d'assurer la securite d'utilisateurs de dispositifs a capacites bluetooth, WO 2002019641 A2, 2001.

[214] Robert M. Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose, Michael Kendrick Reiter, Less , Methods and apparatus for providing privacy-preserving global customization, US 7107269 B2, 2001.

[215] Markus Jakobsson, Susanne Gudrun Wetzel, Secure distributed computation in cryptographic applications, US6950937 B2, 2001.

[216] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of short range wireless enable devices, US6981157 B2, 2001.

[217] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of bluetooth TM-enabled devices, US 6574455 B2, 2001.

[218] Garay; Juan A. (West New York, NJ), Jakobsson; M. (Hoboken, NJ), Kristol; David M. (Summit, NJ), Mizikovsky; Semyon B.(Morganville, NJ), Cryptographic key processing and storage , 7023998, 2001.

[219] Markus Jakobsson, Method, apparatus, and article of manufacture for generating secure recommendations from market-based financial instrument prices, US 6970839 B2, 2001.

[220] Markus Jakobsson, Encryption method and apparatus with escrow guarantees, US7035403 B2, 2001.

[221] Jakobsson, Call originator access control through user-specified pricing mechanism in a communication network, US20020099670 A1, 2001.

[222] Markus Jakobsson, Claus Peter Schnorr, Tagged private information retrieval, US7013295 B2, 2000.

[223] Markus Jakobsson, Secure enclosure for key exchange, US 7065655 B1, 2000.

[224] Markus Jakobsson, Michael Kendrick Reiter, Software aging method and apparatus for discouraging software piracy, US 7003110 B1, 2000.

[225] Markus Jakobsson, Probabilistic theft deterrence, US6501380 B1, 2000.

[226] Markus Jakobsson, Michael Kendrick Reiter, Abraham Silberschatz, Anonymous and secure electronic commerce, EP 1150227 A1, 2000.

[227] Markus Jakobsson, Ari Juels, Proofs of work and bread pudding protocols, US 7356696 B1, 2000.

[228] Markus Jakobsson, Joy Colette Mueller, Methods of protecting against spam electronic mail, US7644274 B1, 2000.

[229] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, EP1043862 B1, 2000.

[230] Markus Jakobsson, Ari Juels, Mix and match: a new approach to secure multiparty computation, US6772339 B1, 2000.

[231] Markus Jakobsson, Ari Juels, Mixing in small batches, US6813354 B1, 2000.

[232] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, US 6901145 B1, 36566

[233] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US6931126 B1, 2000.

[234] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US 6931126 B1, 2000.

[235] Markus Jakobsson, Flash mixing apparatus and method, US 6598163 B1, 1999.

[236] Markus Jakobsson, Minimalistic electronic commerce system, US 6529884 B1, 1999.

[237] Markus Jakobsson, Method and system for providing translation certificates, US 6687822 B1, 1999.

[238] Markus Jakobsson, Verification of correct exponentiation or other operations in cryptographic applications, US6978372 B1, 1999.

[239] Markus Jakobsson, Non malleable encryption apparatus and method, US 6507656 B1, 1999.

[240] Markus Jakobsson, Method and system for quorum controlled asymmetric proxy encryption, US 6587946 B1, 1998.

[241] Markus Jakobsson, Practical mix-based election scheme, US 6317833 B1, 1998.

[242] Markus Jakobsson, Ari Juels, Method and apparatus for extracting unbiased random bits from a potentially biased source of randomness, US 6393447 B1, 1998.

[243] Markus Jakobsson, Ari Juels, Executable digital cash for electronic commerce, US6157920 A, 1998.

[244] Bruce Kenneth Hillyer, Markus Jakobsson, Elizabeth Shriver, Storage device random bit generator, US 6317499 B1, 1998.

[245] Markus Jakobsson, Method and apparatus for encrypting, decrypting, and providing privacy for data values, US 6049613 A, 1998.

Patent Owner Exhibit 2014, Page 50 of 50