

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON
WIRELESS, AND NOKIA OF AMERICA CORPORATION,
Petitioners,

v.

RIGHTQUESTION, LLC,
Patent Owner.

U.S. Patent No. 11,856,132
Issue Date: December 26, 2023

Title: VALIDATING AUTOMATIC NUMBER IDENTIFICATION DATA

Inter Partes Review No.: IPR2025-00361

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 11,856,132
UNDER 35 U.S.C. §§311-319 and 37 C.F.R. §§42.1-.80, 42.100-.107**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450

Table of Contents

PETITIONER’S EXHIBIT LIST.....7

Claim Element Table9

I. Introduction.....1

II. Overview.....1

III. Grounds for Standing.....2

IV. Reasons for the Requested Relief.....2

V. Background.....3

 A. The ‘132 Patent’s Summary3

 B. Prosecution History3

 C. Claim Construction4

 D. The Challenged Claims’ Priority4

 E. Person of Ordinary Skill in the Art4

 F. State of the Art5

VI. Identification of challenges6

 A. Challenged Claims6

 B. Statutory Grounds for Challenges6

 1. Ground 16

 2. Ground 26

VII. Identification of How the Challenged Claims Are Unpatentable6

 A. Ground 1: Claims 1-19 are Obvious over Har combined with Miller6

 1. Har.....6

2.	Miller.....	9
3.	The Proposed Combination of Har and Miller.	14
4.	Motivation to Combine the Teachings of Har and Miller	21
5.	Detailed Application of Har/Miller.....	25
a.	Claim 1.....	25
i.	A method, comprising:.....	25
ii.	receiving information pertaining to a call initiated by a caller device, wherein the information pertaining to the call comprises data related to (1) a phone number associated with a callee device, (2) device information associated with the caller device, and (3) a cryptographic element associated with the caller device;.....	25
iii.	performing a security determination based at least in part on the cryptographic element associated with the caller device comprised in the received information pertaining to the call; and	42
iv.	based at least in part on a result of the security determination performed based at least in part on the cryptographic element associated with the caller device, transmitting, using a cellular network, a notification directed to the callee device.....	48
a.	Claim 2.....	50
b.	Claim 3.....	52
c.	Claim 4.....	52
d.	Claim 5.....	55
e.	Claim 6.....	56

f.	Claim 7.....	57
g.	Claim 8.....	58
a.	Claim 9.....	59
b.	Claim 10.....	60
c.	Claim 11.....	63
d.	Claim 12.....	65
e.	Claim 13.....	68
f.	Claim 14.....	69
g.	Claim 15.....	70
h.	Claim 16.....	72
i.	Claim 17.....	72
j.	Claim 18.....	72
k.	Claim 19.....	72
B.	Ground 2: Claims 2 and 9 are Obvious over Ground 1 in further view of French.....	73
1.	French.....	73
2.	Detailed Application of Ground 2	73
a.	Claim 2.....	73
	The method of claim 1,	74
b.	Claim 9.....	75
	The method of claim 1	75
VIII.	The Board Should Not exercise its discretion to deny institution Under <i>Fintiv</i>	75
IX.	Mandatory Notices under 37 C.F.R. §42.8.....	78

A. Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1).....78

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)79

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)80

D. Service Information Under 37 C.F.R. § 42.8(b)(4).....81

X. CONCLUSION.....81

CERTIFICATION OF SERVICE ON PATENT OWNER.....82

CERTIFICATE OF COMPLIANCE.....84

Table Of Authorities

Cases

<i>Dish Network v. Broadband iTV</i> , IPR2020-01280, Paper 17 (PTAB Feb. 4, 2021)	77
<i>HP Inc. v. Slingshot Printing LLC</i> , IPR2020-01084, Paper 13 (Jan. 14, 2021).....	78
<i>PEAG LLC v. Varta Microbattery GMBH</i> , IPR2020-01214, Paper 8 (Jan. 6, 2021)	77
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (June 16, 2020)	76
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (Dec. 1, 2020)	76

PETITIONER’S EXHIBIT LIST

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 11,856,132 (“132 Patent”)
1002	File History for U.S. Patent No. 11,856,132
1003	Expert Declaration of Patrick McDaniel, Ph.D.
1004	U.S. Patent Publication No. 2012/0144198 (“Har”)
1005	Intentionally Omitted
1006	Intentionally Omitted
1007	AT&T Infringement Contentions Cover Pleading, <i>RightQuestion, LLC v. AT&T Corp., et al.</i> , No. 2:24-cv-00094-JRG (E.D. Tex.) Served: May 14, 2024.
1008	Second Amended Docket Control Order in <i>RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.</i> , No. 2:24-cv-00091 (E.D. Tex., October 20, 2024) (Lead Case)
1009	Dave Otway and Owen Rees. 1987. Efficient and timely mutual authentication. <i>SIGOPS Oper. Syst. Rev.</i> 21, 1 (Jan. 1987), 8–10. https://doi.org/10.1145/24592.24594
1010	Simpson, E., Schaumont, P. (2006). Offline Hardware/Software Authentication for Reconfigurable Platforms. In: Goubin, L., Matsui, M. (eds) <i>Cryptographic Hardware and Embedded Systems - CHES 2006</i> . CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_25 (“Simpson”)
1011	Loh Chin Choong Desmond, Cho Chia Yuan, Tan Chung Pheng, and Ri Seng Lee. 2008. Identifying unique devices through wireless fingerprinting. In <i>Proceedings of the first ACM conference on Wireless network security (WiSec '08)</i> . Association for Computing Machinery, New York, NY, USA, 46–55. https://doi.org/10.1145/1352533.1352542
1012	Ke Gao, C. Corbett and R. Beyah, "A passive approach to wireless device fingerprinting," <i>2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)</i> , Chicago, IL, 2010, pp. 383-392, doi: 10.1109/DSN.2010.5544294.

<i>Exhibit #</i>	<i>Description</i>
1013	Martins, Rui & Augusto, Alexandre & Correia, Manuel Eduardo. (2013). A Potpourri of Authentication mechanisms - The mobile device way.
1014	Abu-Hakima, Suhayya, Mansour Toloo and Tony White. “A Multi-Agent Systems Approach for Fraud Detection in Personal Communication Systems.” (2002).
1015	Hossain, A.K.M. Mahtab & Jin, Yunye & Soh, Wee-Seng & Van, Hien. (2013). SSD: A Robust RF Location Fingerprint Addressing Mobile Devices' Heterogeneity. Mobile Computing, IEEE Transactions on. 12. 65-77. 10.1109/TMC.2011.243.
1016	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – Proposed Standard (May, 2008)
1017	Burnett, S. and Paine, S. (2001) RSA Security’s Official Guide to Cryptography. McGraw-Hill
1018	Boris Danev (2011) Physical-Layer Identification of Wireless Devices [Doctoral dissertation, ETH Zurich]. ETH Zurich Library Collection. https://www.research-collection.ethz.ch/handle/20.500.11850/72822
1019	Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. ACM Comput. Surv. 45, 1, Article 6 (November 2012). https://doi.org/10.1145/2379776.2379782
1020	U.S. Pat. No. 9,129,130 (Filed: August 30, 2013; Priority: August 31, 2012)
1021	U.S. Patent Publication No. 2012/0131354 (“French”)
1022	U.S. Patent Publication No. 2012/0201381 (“Miller”)
1023	Joint Claim Construction Statement, RightQuestion, LLC v. AT&T Corp., et al., No. 2:24-cv-00094-JRG (E.D. Tex.)

Claim Element Table

Element	Claim Language
1.i	1. A method, comprising:
1.ii	receiving information pertaining to a call initiated by a caller device, wherein the information pertaining to the call comprises data related to (1) a phone number associated with a callee device, (2) device information associated with the caller device, and (3) a cryptographic element associated with the caller device;
1.iii	performing a security determination based at least in part on the cryptographic element associated with the caller device comprised in the received information pertaining to the call; and
1.iv	based at least in part on a result of the security determination performed based at least in part on the cryptographic element associated with the caller device, transmitting, using a cellular network, a notification directed to the callee device.
2	2. The method of claim 1, wherein the security determination is based at least in part on a policy.
3	3. The method of claim 1, wherein the device information associated with the caller device comprises a unique identifier.
4	4. The method of claim 1, wherein the device information associated with the caller device comprises Automated Number Identification (ANI) information.
5	5. The method of claim 1, wherein the security determination is based at least in part on a validation of the information pertaining to the call.
6	6. The method of claim 1, further comprising storing, in a data store, at least one record including contents associated with the caller device.
7	7. The method of claim 1, further comprising storing, in a data store, at least one certificate used to validate the call.

8	8. The method of claim 1, wherein the call is validated at least in part by using at least one of a secret key or a public key.
9	9. The method of claim 1, wherein the security determination is based at least in part on execution of a rule.
10	10. The method of claim 1, wherein the security determination is based at least in part on a timestamp associated with the call.
11	11. The method of claim 10, further comprising detecting a replay attack based at least in part on the timestamp.
12	12. The method of claim 1, wherein the result of the security determination comprises a score indicating a validity of a phone number associated with the caller device.
13	13. The method of claim 1, wherein the security determination is risk-based.
14	14. The method of claim 1, wherein the device information associated with the caller device is not conveyed to a relying party.
15	15. The method of claim 1, wherein the device information associated with the caller device comprises at least one of a unique software identifier, a semi-unique software identifier, an embedded hardware identifier, or a user-added hardware identifier.
16	16. The method of claim 1, wherein the result of the security determination is transmitted to a relying party.
17	17. The method of claim 1, wherein transmitting the notification using the cellular network comprises conveying an assurance to the callee device or conveying a failure to confirm the call.
18	18. The method of claim 1, wherein transmitting the notification using the cellular network comprises conveying caller identification information to the callee device.
19	19. The method of claim 1, wherein transmitting the notification using the cellular network causes a visual indication of the result of the security determination to be displayed on the callee device.

I. INTRODUCTION

AT&T Services Inc., Cellco Partnership D/B/A Verizon Wireless, and Nokia of America Corporation, (collectively, “Petitioners”) hereby petition for an *inter partes* review (“IPR”) of Claims 1-19 (the “Challenged Claims”) of U.S. Patent No. 11,856,132 (the “’132 patent”; EX-1001) *See* 35 U.S.C. § 311, 37 C.F.R. § 42.1. Petitioners respectfully request that the Board institute an *inter partes* review of the ’132 Patent, pursuant to 37 C.F.R. § 42.108, because this Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail.

II. OVERVIEW

The Challenged Claims are directed to receiving device information and other data during a phone call to verify the caller identification information. This comparison is used to perform a security determination related to the communication. Ex-1001, 2:46-62. The Challenged Claims’ allowance was based solely on inclusion of a “cryptographic element associated with the caller device” limitation. Section V.B, *infra*. Ex-1003, ¶25.

As detailed below, Har teaches a system for authenticating a “caller” which teaches, or renders obvious, the Challenged Claims – including the allegedly novel use of a “cryptographic element”. A person of ordinary skill in the art (“POSA”) also would be motivated to combine Har with Miller, which provides additional and

complimentary disclose regarding the authentication of a calling device and device-specific authentication. As detailed below, Miller heavily overlaps the (later) '132 patent and provides extensive details about device-specific authentication. Ex-1003, ¶26

The Challenged Claims thus recite nothing more than a combination of prior art elements, each used for its normal and intended purpose, that were well-known obvious modifications to a POSA. Ex-1003, ¶27.

III. GROUNDS FOR STANDING

Petitioners certify that the '132 Patent is available for IPR and Petitioners are not barred or estopped from requesting this review. 37 C.F.R. §42.104(a). This Petition is being filed less than one year after the date on which Petitioners (or a privy of Petitioners) were served with a Complaint alleging infringement of the '132 Patent. This Petition is filed under 37 C.F.R. §42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in this Petition and the Declaration of Petitioners' Expert, Dr. Patrick McDaniel (EX-1003), the methods claimed in the '132 Patent were obvious in view of the prior art to a POSA at the time of the invention.

V. BACKGROUND

A. The '132 Patent's Summary

The '132 Patent describes “techniques for ascertaining the identity of a device initiating communications” to detect “potential attempts at spoofing of caller ID or automatic caller identification (ANI) data.” Ex-1001, 2:46-50; Ex-1003, ¶28.

To address caller identification spoofing, the '132 Patent describes a verification process that stores device information based on unique hardware and/or software details. Ex-1001, 9:20-57. When the caller or callee needs to verify the other party's identity, that information, plus other information related to a party of the communication, such as public and secret keys, can be shared. Ex-1001, 3:13-22, 4:42-49, 7:43-53, 13:1-5, 15:28-61. Based on a comparison between the stored and shared information, a security determination can be made to include “blocking access, requesting additional authentication factors, permitting access, etc.” Ex-1001, 9:55-57; Ex-1003, ¶¶29-30.

B. Prosecution History

Application 17/228,566, which became the '132 Patent, was filed on April 12, 2021, with one claim. Subsequently added claims 2-17 were substantively rejected as obvious. Ex-1002, 232-244. Independent Claim 2 was amended following a non-final rejection. Ex-1002, 276 (adding score limitations). However, that amendment was withdrawn following a final action for being obvious. Ex-1002, 288-301 (removed score limitations). Ex-1002, 346.

A notice of allowance was filed. Ex-1002, 391. Applicants filed an additional RCE (Ex-1002, 405-409) after the notice of allowance (Ex-1002, 421) which amended independent claim 2 and dependent claim 16, and added claims 18-21. Then, the '132 Patent issued. (Ex-1002, 468-469).

C. Claim Construction

Petitioners propose that each claim term be given its plain and ordinary meaning, and that the prior art herein meets the claims under any reasonable construction.

In the related litigations, Petitioners assert that the “performing a security determination” element is subject to Section 112(f) and is indefinite. Ex-1023. Recognizing that indefiniteness cannot be raised in IPR proceedings, Petitioners assert that this term encompasses performing a validation / authentication using information related to a communication and/or devices and entities related to the communication. Ex-1001, 15:21-16:23; 16:58-17:37.

D. The Challenged Claims’ Priority

Petitioners herein rely on prior art as of the November 7, 2013 date (“Priority Date”) alleged by the Patent Owner. Ex. 1007, VI.

E. Person of Ordinary Skill in the Art

A POSA would have had at least a Bachelor’s degree in computer science, electrical engineering or a related technical field, and at least two years of professional experience, or an equivalent advanced education, in the field in security

of cellular/telephony networks and mobile systems. Additional work experience in relevant industries could compensate for less education or education in a different field, and vice versa. EX-1003, ¶¶34-37.

F. State of the Art

The '132 Patent was allowed based on the addition of “cryptographic element” limitations to well-known call verification and authentication techniques. However, the '132 Patent admits that secret and public keys were prior art. *See* Ex-1001, 12:37-58 (“a method such as Diffie-Hellman key exchange or RSA key transport can be used . . .”). A POSA would have understood that Diffie-Hellman key exchange methods (*i.e.*, using public and secret keys) was widely adopted and well-known since its inception in the mid-1970s. Ex-1017, 93-94. The algorithm based on Diffie-Hellman key exchange was published in 1978 and was named “RSA.” *Id.* Ex-1003, ¶¶38-41.

Symmetric keys, where one algorithm is used to encrypt and decrypt, were also widely known. Ex-1007, 23. *Id.* Ex-1003, ¶42. Using verification/certificate authorities to manage the keys was also well known to a POSA. Ex-1007, 171-207; Ex-1003, ¶43.

Finally, verifying the identity of an individual by comparing device related information was also well-known. Ex-1018, Abstract, Chapter 3 (Device Identification Background), Figure 3.1; Ex-1019, 6:2-6:3; Ex-1003, ¶44.

VI. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-19 are challenged herein.

B. Statutory Grounds for Challenges

Ground	Claim(s)	Basis	Reference
1	1-19	§103	Har combined with Miller
2	2, 9	§103	Har combined with Miller and French

1. Ground 1

Har (Ex-1004) published June 7, 2012. Miller (Ex-1022) published August 9, 2012. Both are prior art under at least 35 U.S.C. AIA § 102(a)(1).

2. Ground 2

U.S. Pat. Publ. No. 12/0131354 (“French”) (Ex-1021) published May 24, 2012, and is prior art under at least 35 U.S.C. AIA 102(a)(1).

* * *

The references herein were not cited during prosecution of the ’132 Patent or its parent applications.

VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-19 are Obvious over Har combined with Miller

1. Har

Har teaches a call authentication system using a data channel and an authentication server to “authenticate the identity of one or more parties to a call

where at least one of the parties to the call is using a mobile device.” Ex-1004, Abstract. Har’s “authentication server and authentication methodology [that] can be used in a mobile network environment to authenticate a first user to a second user by authenticating a message sent by the first user to the authentication server.” Ex-1004, [0002]. “The message can include the identity of the first user and other information” and “[e]ither the first user or the second user can request authentication of the first user to the second user.” *Id.* Notably, Har’s authentication request sent to the authentication server “can be encrypted and/or signed and sent over a data channel.” *Id.* “In response to successful validation by the authentication server, the authentication server can send an authentication indication to the device of the user receiving the authentication results” which “can display identification information and other (optional) data associated with the first user.” *Id.* Ex-1003, ¶47.

Har’s Fig. 1 illustrates authentication in a mobile environment. Ex-1004, [0006], [0022]. As shown in Fig. 1, “a first user can be a caller such as caller 114 using a caller mobile device.” Har’s “[c]aller 114 (e.g. a service provider) can authenticate his identity to callee 116 (e.g. a customer or potential customer) by sending an authentication request to a third party trusted server (e.g., authentication server 102).” Ex-1004, [0023]. “The authentication request can include information identifying the caller 114, information identifying the callee 116, any other information that caller 114 would like callee 116 to have and/or any

other information that caller 114 specifies.” *Id.* “An authentication server such as authentication server 102 can receive the authentication request, can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message.” Ex-1004, [0026]. Notably, “[t]he message can include information associated with the first user, as registered in the server's database, and any other data sent in the authentication request.” Ex-1004, [0035]; Ex-1003, ¶48.

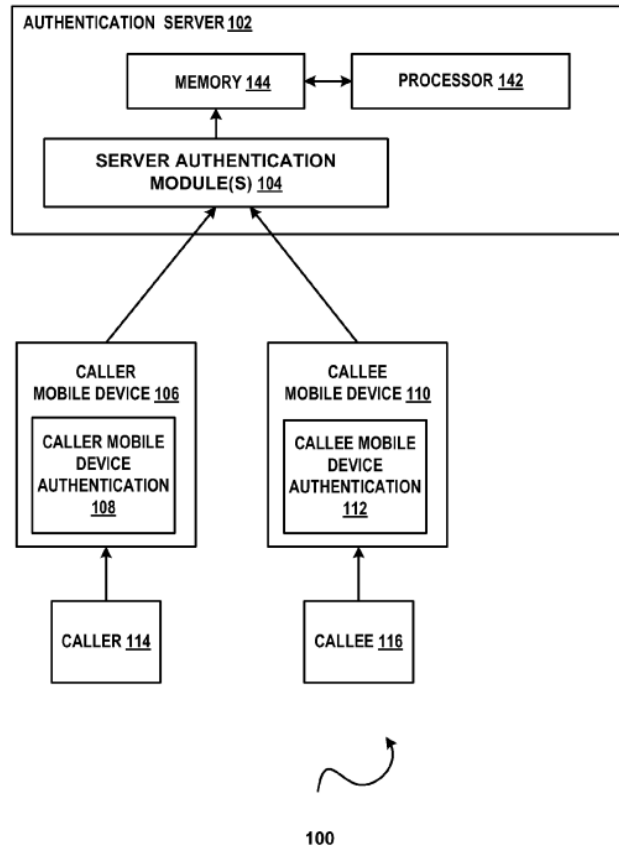


FIG. 1

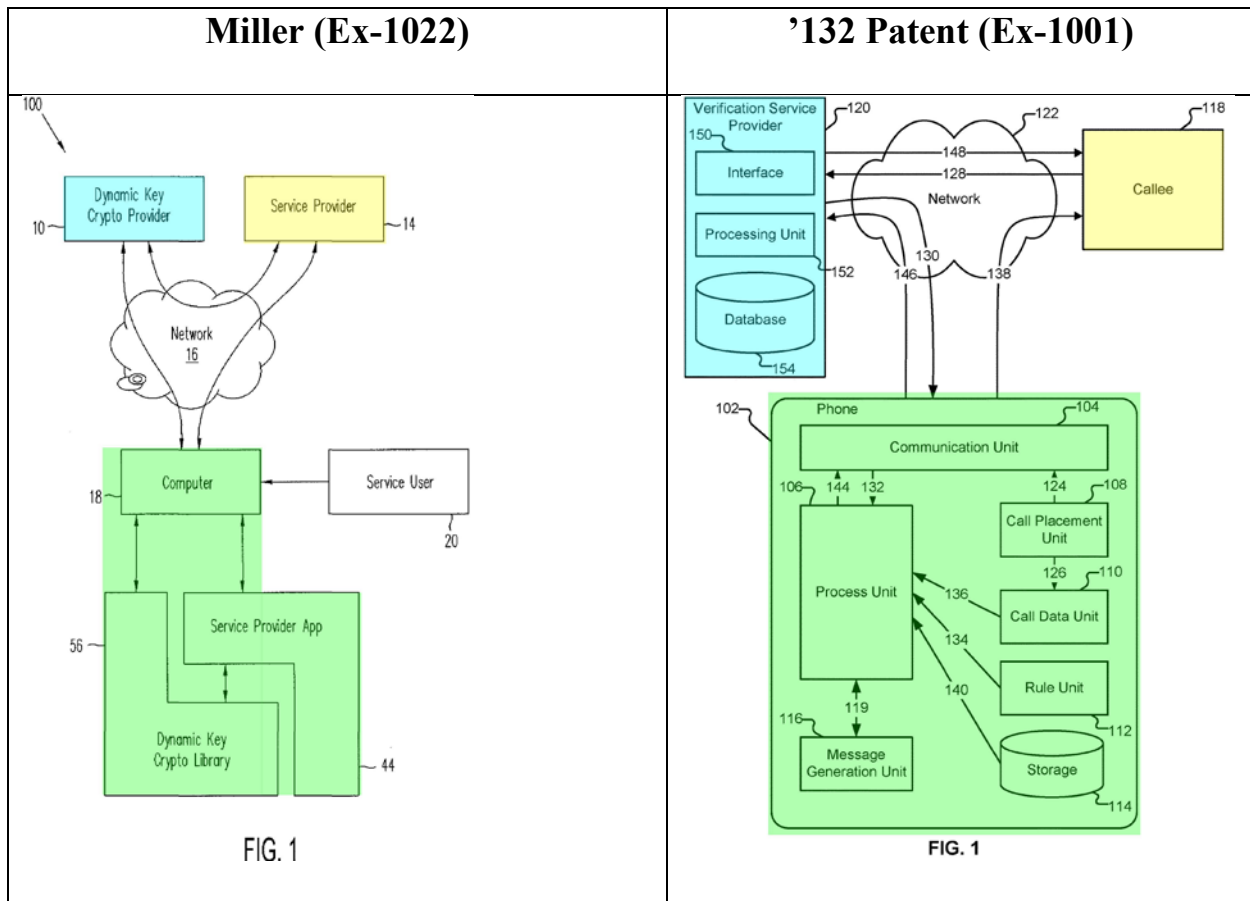
Har – Fig. 1

Har's "authentication server may have a data store of user information that includes the mobile telephone numbers of users, usernames, passwords, PIN codes, the name, address and public keys for users, credentialing information, identification information and so on." Ex-1004, [0018]. More specifically, Har specifically teaches that the system "supports authentication of mobile devices." Ex-1004, [0044]; Ex-1003, ¶49.

2. Miller

Miller describes a system for authorizing / verifying a device involved in a communication that heavily overlaps with the (later) '132 patent system. For such verification, Miller "uniquely identif[ies] the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device." Ex-1022, Abstract; Ex-1003, ¶50.

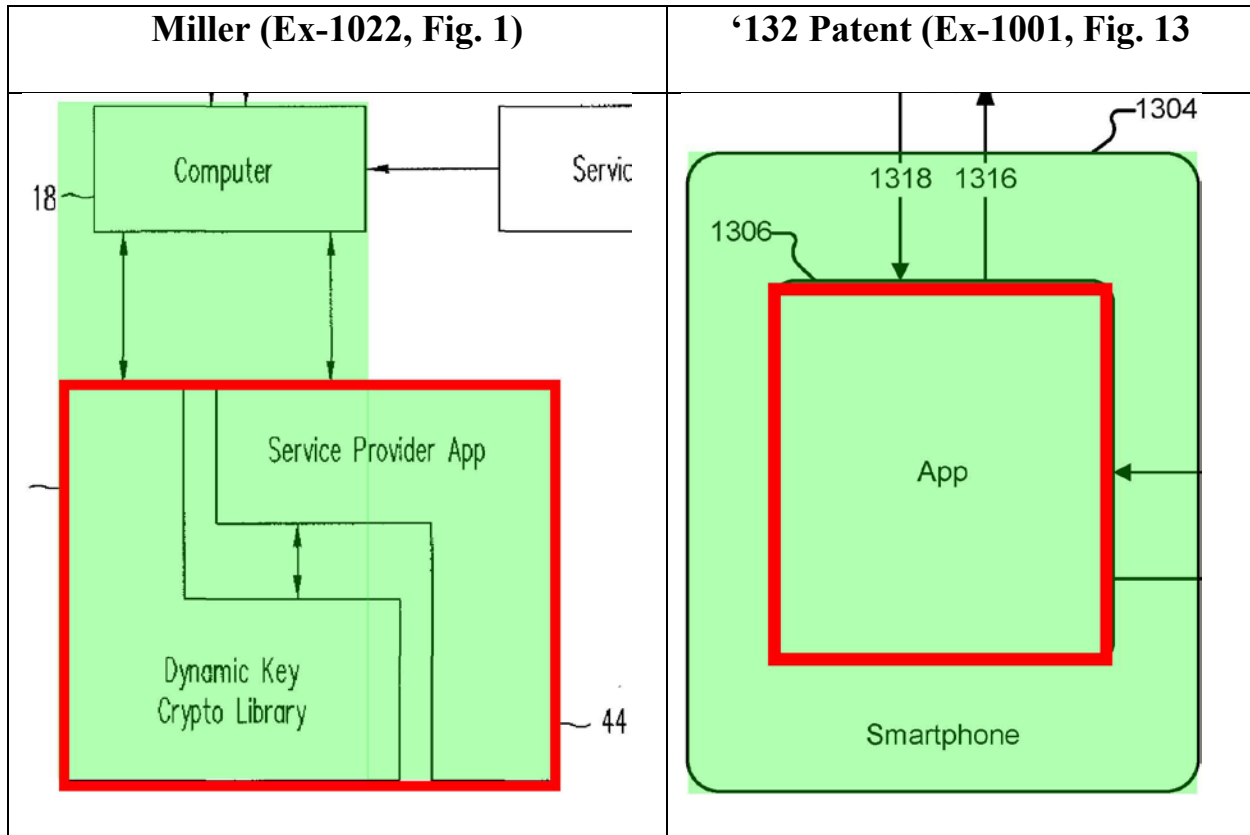
The '132 patent adopted (and claimed) an architecture and processes largely matching Miller's disclosure. For example, Figures 1 from each of Miller and the '132 patent shows the matching relevant components in the communication.



Miller and the '132 patent each teach communication between a first device (green) and a second device (yellow) for which the “first device” is authorized / verified by a verification provider (blue) which Miller calls a “dynamic key crypto provider” (herein, “DKCP”) and the '132 patent calls a “verification service provider” (herein, “VSP”). Ex-1003, ¶51.

Miller and the '132 patent describe the same types of “devices” in the communication. Compare Ex-1022, [0048] and Ex-1001, 12:26-31. Ex-1003, ¶52.

Miller and the '132 patent both teach that an “app” may be used on the device to facilitate verification.

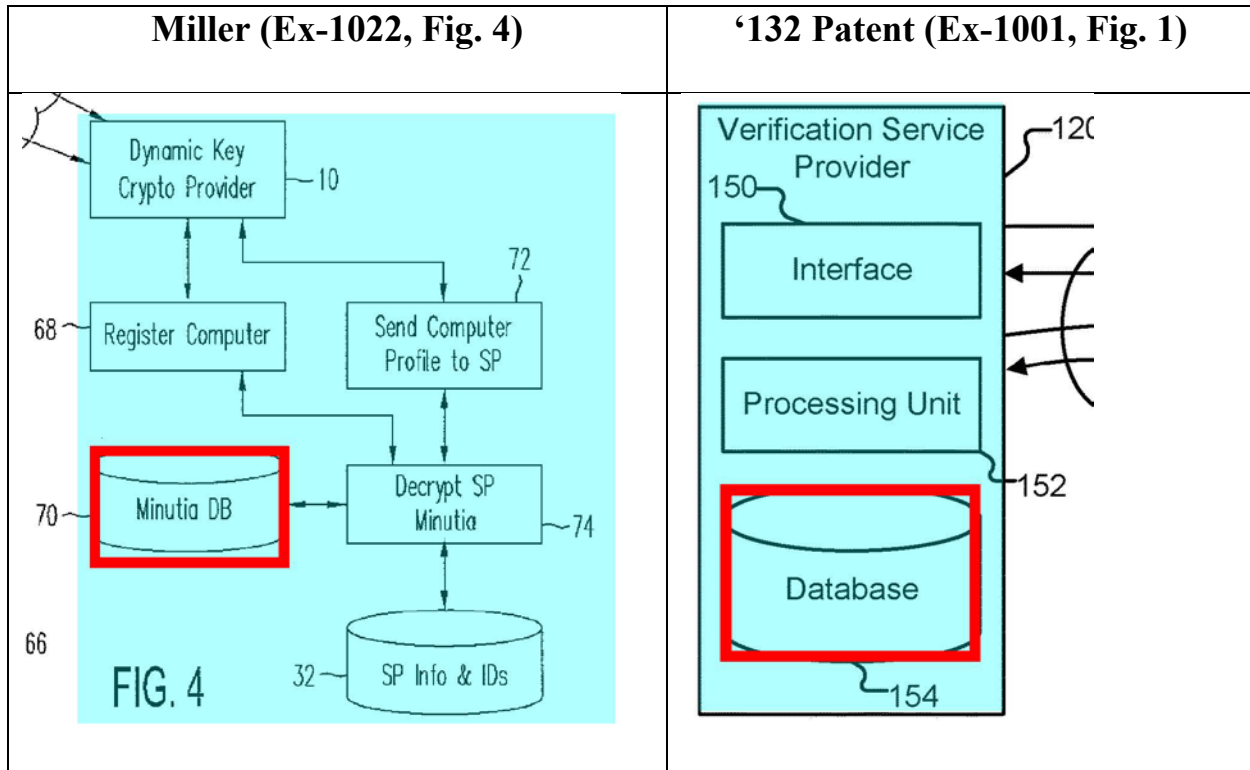


Compare Ex-1022, [0048], Ex-1001, 5:60-63; Ex-1003, ¶53.

Miller's DKCP and the '132 patent VSP are both implemented as computer servers using the typical server hardware such as processors, memories and software. Ex-1022, [0177-0179]; Ex-1001, 4:5-22; Ex-1003, ¶54.

Miller teaches the same functional steps that the '132 patent later regurgitated. First, both Miller and the '132 patent register devices with the DKCP/VSP using unique device identifiers – which Miller calls “computer minutia” or “computer fingerprints” and the '132 calls a “device fingerprint.” Ex-1003, ¶55.

Second, both Miller's DKCP and the '132 patent VSP store the enrolled device information (fingerprint/minutia) in databases for later usage.



Compare Ex-1022, [0092], Ex-1001, 3:65-67, Ex-1003, ¶56.

Third, both Miller's DKCP and the '132 patent VSP receive a device information (minutia) from the device during authentication.

seeking authentication. *Compare* Ex-1022, [0066], Ex-1001, 9:24-26. Ex-1003, ¶58.

Fifth, both Miller's DKCP and the '132 patent VSP teach calculating a "score" based upon the device's information and other factors to help determine authenticity. *Compare* Ex-1022, [0105], Ex-1001, 9:39-45. Ex-1003, ¶59.

Sixth, both Miller's DKCP and the '132 patent VSP select actions, such as blocking (denying) communication, allowing communication, or seeking further information, such as PIN's or passwords from the users. *Compare* Ex-1022, [0112-0116], Ex-1001, 9:55-59; Ex-1003, ¶60.

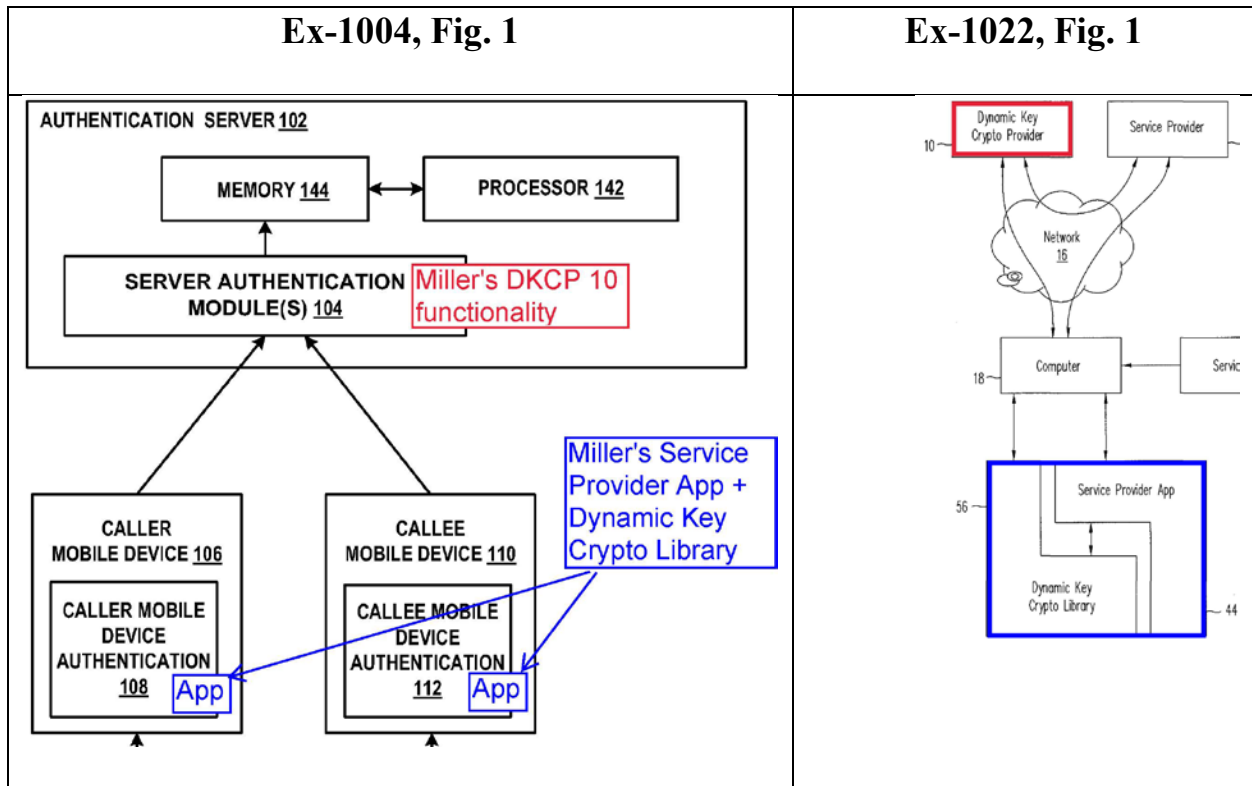
Simply put, Miller discloses the same architecture and functionality that the '132 patent subsequently disclosed and claimed. Ex-1003, ¶61.

3. The Proposed Combination of Har and Miller.

As noted in the Introduction, when read reasonably, Har teaches or renders obvious the methods claimed in the '132 patent. However, if Patent Owner argues that Har teaches only using information related to the person using a device and does not teach / suggest authentication of the device itself, then Miller provides explicit details of device-based authentication, including cryptographic elements specifically associated with the device (and not the person using the device). Ex-1003, ¶62.

The proposed combination augments Har's existing authentication system to include the functionality of Miller's authentication system specific to device authentication. Ex-1003, ¶63.

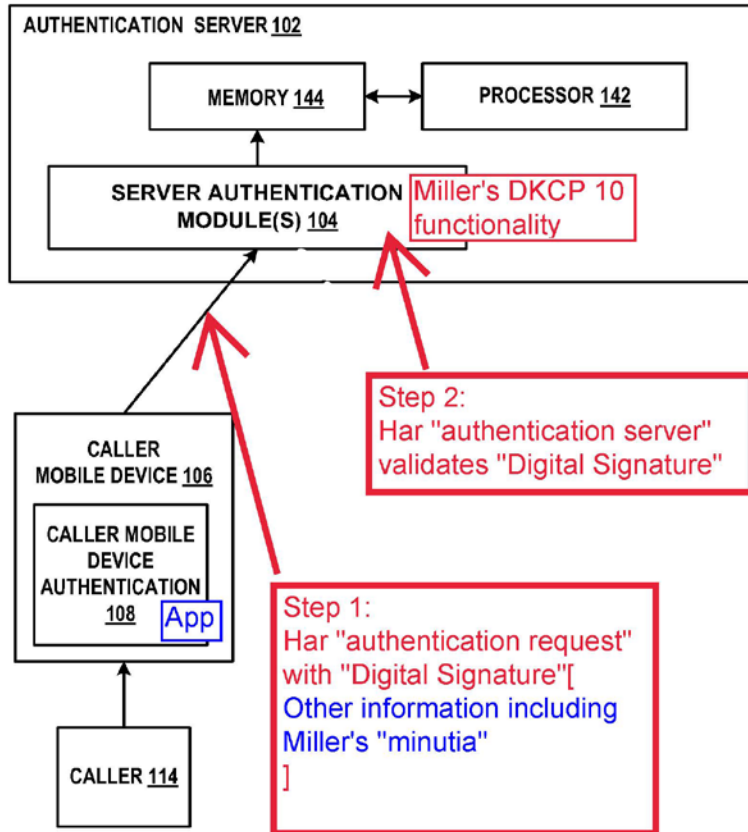
As shown below, this augmentation includes (1) incorporating aspects of Miller's DKCP server 10 functionality into Har's "authentication server 102" and (2) incorporating Miller's DKCP client app functionality ("service provider app 44" and "dynamic key crypto library 56" which may be combined into one program as per Ex-1022, [0072], [0048]) into Har's "Mobile Device Authentication Modules" 108 and 112. Ex-1003, ¶64.



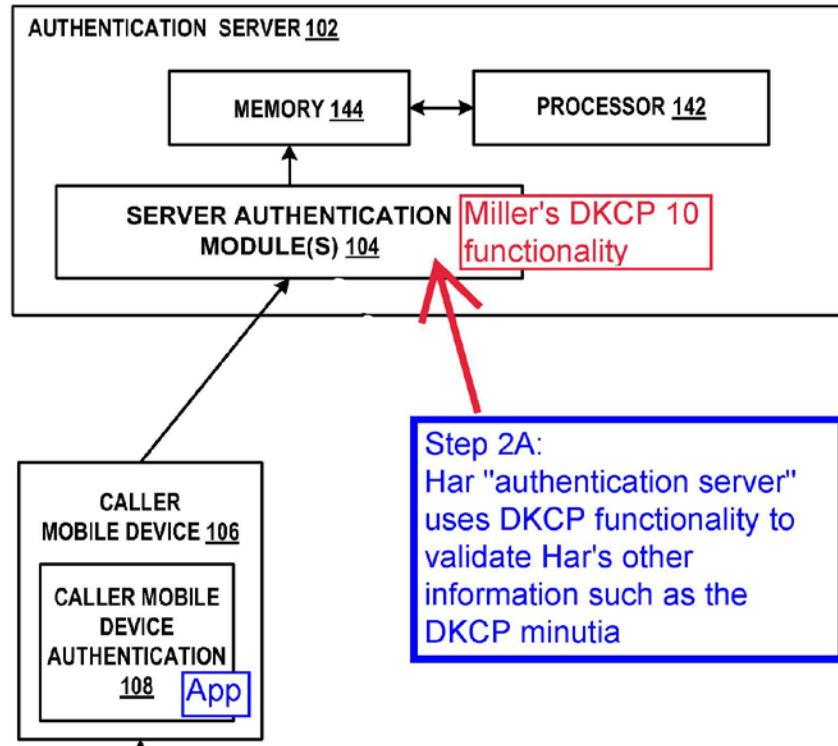
The Har/Miller System uses Har’s basic authentication flow augmented by Miller’s DKCP functionality. *E.g.*, Ex-1004, Fig. 2; elements 1.ii-1.iv *infra*. Ex-1003, ¶65.

Step 1 (adopted directly from Har): The caller sends an “authentication request [of] a message encrypted using the server's public key ... and signed using the private key ...” Ex-1004, [0016]. The “authentication request [] includes” other forms of “identification information associated with the authentication request sender” or “information volunteered by the authentication request sending” or “desired by the requesting user.” Ex-1004, [0016]; Ex-1003, ¶66.

In the Har/Miller System, the authentication request identification information includes “minutia” that Miller’s DKCP system uses for device-based authentication. *See* Section VII.A.2 (*supra*), elements 1.ii, 1.iii (*infra*). Ex-1003, ¶67.



Step 2 (adopted directly from Har): Har's authentication server attempts to validate / authenticate the request using the encrypted wrapper and the keys for the devices. Ex-1004, [0026-0032]; Ex-1003, ¶68.



Ex-1004, Fig. 1.

Step 2A (adopted directly from Har, as modified by Miller): This step checks if the request's content matches the authentication server's data store.

Moreover, authentication server 102 can verify that information included in the transmission sent by the sender agrees with information for the sender stored in a data store associated with the authentication server 102. If decryption is successful and the digital signature of the sender of the message is verified, and the information included in the transmission by the sender agrees with information stored in the data store of the authentication server 102...

Ex-1004, [0026]. Ex-1003, ¶69.

The emphasized sections above reflect Miller's augmented functionality included into Har. Miller's authentication request sends device "minutia" to the DKCP server to be used for authentication. Miller's DKCP authentication process

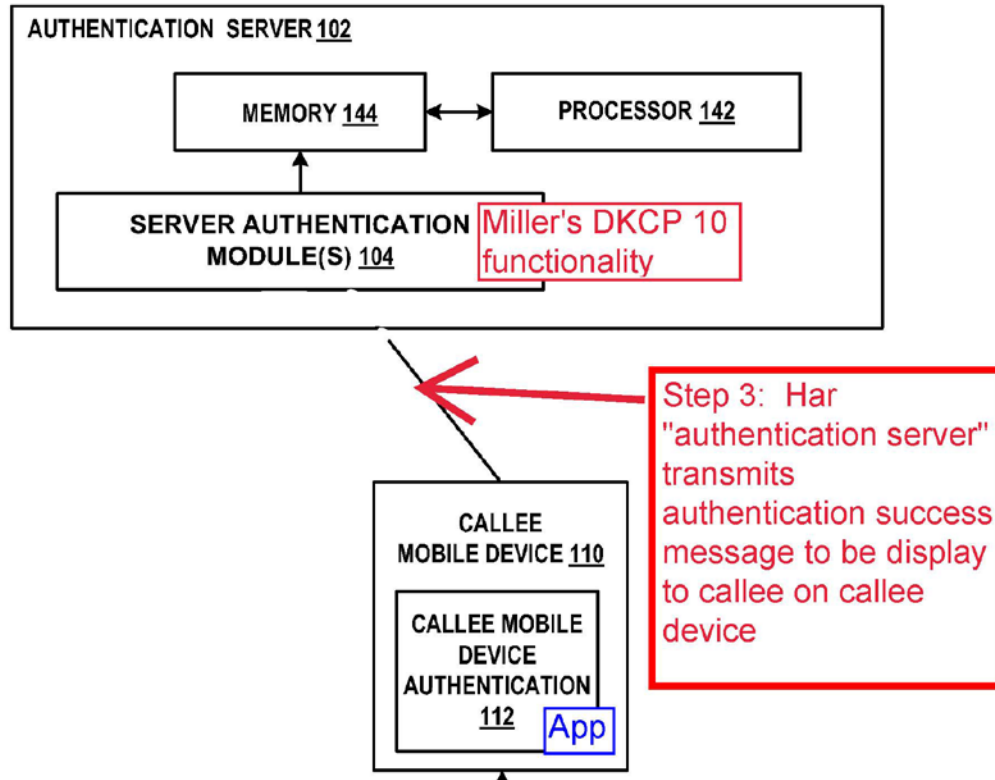
includes an optional iterative challenge / response sequence with the requesting / caller device to refine and improve the authentication process. See Section VII.A.2 (*supra*), elements 1.ii, 1.iii (*infra*). Ex-1003, ¶70.

Har's system includes a bi-directional "data channel" between the authentication server and mobile devices. Ex-1004, [0002-0003], [0031]. Har uses the "data channels" for the server, challenging the device for more authentication information and receiving a response with such authentication information. Har's users can be "prompted for credentials including but not limited to a password or personal identification number (PIN) code and/or other information." Ex-1004, [0019]. "The credentialing information can be verified against information stored at the authentication server for the user." Ex-1004, [0019]; *see also* Ex-1004, [0029]. Thus, Miller's challenge / response interactions merely use an existing Har data channel for its normal and intended usage. Ex-1003, ¶71.

In the Har/Miller System, Har's "mobile device's" (106/108) are "smart phones" that both Har and Miller each identify. Ex-1004, [0001], [0045]; Ex-1022, [0048]. Ex-1003, ¶72

Step 3 (adopted directly from Har): After the authentication server makes a final security determination (based upon steps 2 and 2A above), Har's authentication server may send the authentication information to the callee's device

for display to the callee (e.g., if authentication succeeds). See element 1.iv (*infra*); Ex-1004, [0028-0032].



Ex-1004, Fig. 1. Ex-1003, ¶73.

Separately, the Har/Miller System uses Miller’s registration procedures (which is consistent with the Har disclosure) to store information about the users / devices in Har’s authentication server. See Section VII.A.2 (*supra*), elements 1.ii, 1.iii (*infra*); Ex-1004, [0035] (“information associated with the first user, as registered in the server’s database...”). Ex-1003, ¶74.

Thus, the proposed Har/Miller System is merely Har’s system with Miller’s device-based authentication that bolsters Har’s teaching of comparing information

in the authentication request against information in the authentication server's data store for matches. Ex-1003, ¶75.

4. Motivation to Combine the Teachings of Har and Miller

A POSA would have been motivated to combine Har with Miller to arrive at the Har/Miller System with a reasonable expectation of success. Ex-1003, ¶76.

The references themselves include motivations to combine. Har's authentication server performs a two-step authentication check (steps 2 and 2A above). Har emphasizes Step 2 (checking the digital certificate surrounding the authentication request). While Har teaches checking the authentication request's contents, Har does not detail how request's content is matched to the authentication server's data store (step 2A above). Miller provides additional details, and additional security, to implement Har's step 2A. Ex-1003, ¶77.

Miller itself provides a motivation to augment Har for multiple reasons. First, a POSA would recognize that Miller's system provides significantly "increased security" and authentication for the reasons stated in Miller. Ex-1022, [0031-0033]. For example, Miller's system describes using a broad array of device "minutia" which can be formed into different "subsets" for authentication. Ex-1022, [0031-0033]. By enhancing the authentication process and offering different forms of authentication bases (minutia), the Har/Miller System better effectuates Har's basic goal that the "authentication server can vouch for the identity of the [first/second]

user, the message integrity and the message privacy.” Ex-1004, [0002-0003]. Har identifies, and seeks to address, the problem of “security” when interacting with “service providers.” Ex-1004, [0011-0013]. Miller’s enhanced authentication provides “increased security” ([0031]) or “unprecedented security” ([0028]) by using “dynamic” key information and by using the device-based unique identifiers (in various subsets) as increased protection against “spoofing” attacks when interacting with service providers. Ex-1022, [0028], [0011], [0033], [0041], [0045]. Ex-1003, ¶78.

Miller details existing authentication systems including systems using “cryptographic keys” such as “symmetric, public or private” keys as are described in Miller. Ex-1022, [0006-0011]. Miller’s “dynamic” system improves existing “static” key systems. Ex-1022, [0031-0033]. Miller describes an embodiment where the keys used to sign “digital certificates” (such as those described in Har) can be based upon Miller’s dynamic key system for improved security. Ex-1022, [0133], [0047]; Ex-1003, ¶79.

Thus, a POSA would have been motivated to augment Har’s authentication functionality with Miller’s DKCP functionality to improve security and better vouch for the calls and interactions with service providers as described in Har. Ex-1003, ¶80.

Furthermore, by using Har’s existing digital signature authentication wrapped around Miller’s enhanced device-based authentication, a POSA would recognize benefits in improved system performance. For example, Har’s system utilized existing, known techniques for the digital signatures. Thus, the initial security determination (Step 2 above) can use known, existing technologies and algorithms for an initial check that can be performed efficiently and quickly. If the authentication using digital certificates fails using Har’s “older” technology, then time and effort can be saved by not performing Miller’s detailed additional authentication (Har’s Step 2A above). This allows for efficiency through “quick fails” and requires only the more detailed processing (Step 2A) if the initial authentication (Step 2 using digital certificates) is successful. A POSA would recognize this as a performance benefit that retains the augmented security provided by Miller. Ex-1003, ¶81.

A POSA would be confident of the combination’s success as it is a software solution that uses known techniques – rules and logical arrangement of rules, and well-known cryptographic techniques – all for their intended purpose – implementing objectives of verifying a caller. Ex-1003, ¶82.

Har and Miller are also analogous art to each other, and to the claimed invention, being in the same field of authentication of communications and using information about the call, caller, and caller’s device, to make a security

determination about the treatment of a calls. Moreover, Miller provides details absent from Har regarding Har’s system “that supports authentication of mobile devices.” Ex-1004, [0044]. Both Miller and Har are directed to the same problem as the ’132 Patent – “[d]etermining the trustworthiness of information used to identify entities involved in communications” so the communication is not “spoofed by unscrupulous entities.” Ex-1001, 1:27-31. *E.g.*, Ex-1004, [0002] (“authentication server can vouch for the identification of the first user, the message integrity and the message privacy.”); Ex-1022, [0041] (DKCP “increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer”). Ex-1003, ¶83.

Augmenting Har’s *authentication* system to include Miller’s DKCP authentication would be within a POSA’s skill. Call authentication systems were well known in the art and combining the teachings of Har and Miller would involve routine skill to a POSA with a reasonable expectation of success. As detailed above, Har and Miller describe the same type of fundamental components (e.g., servers for authentication and smartphones for devices being authenticated). Moreover, Har and Miller include bi-directional communication between the server and devices – including for the purpose of requesting and receiving additional authentication information. Thus, the basic architectures and data flows within Har and Miller are compatible and bolster a POSA’s expectation of success. Ex-1003, ¶84.

5. Detailed Application of Har/Miller

a. Claim 1

Claim 1 recites a simple process: (1) receiving certain information about a call; (2) performing a “security determination” using part of that information; and (3) transmitting a “notification” to the callee based on the security determination.

The Har/Miller System teaches this process. Ex-1003, ¶85.

i. A method, comprising:

Har and Miller disclose the claimed method. Ex-1004, [0007], [0033], Claims 8-13. Ex-1022, Figs. 1-9. Ex-1003, ¶86.

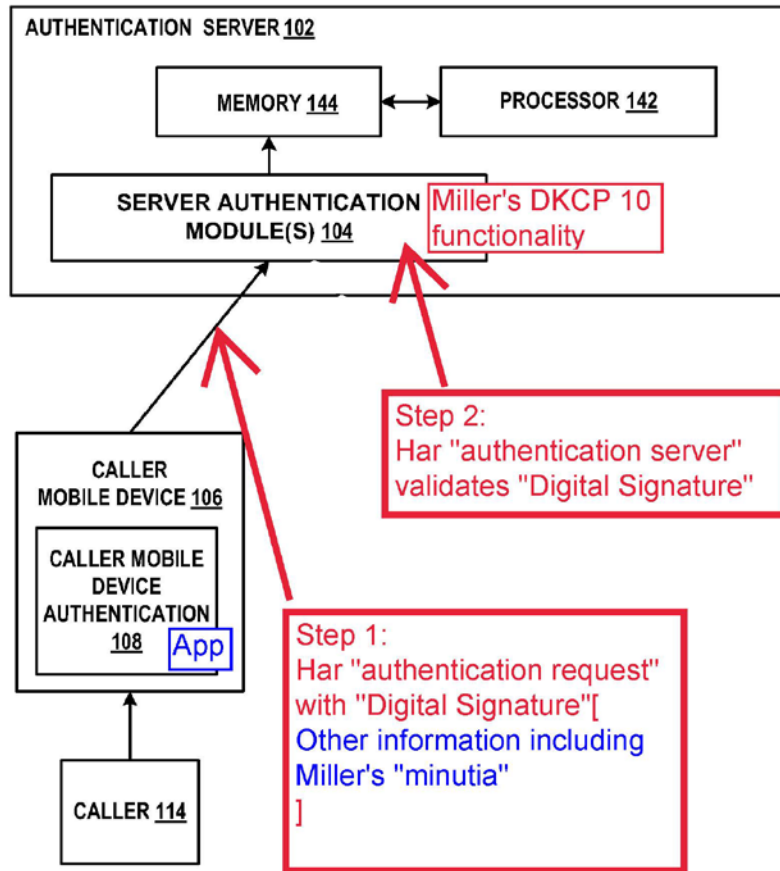
- ii. receiving information pertaining to a call initiated by a caller device, wherein the information pertaining to the call comprises data related to (1) a phone number associated with a callee device, (2) device information associated with the caller device, and (3) a cryptographic element associated with the caller device;

This element describes receiving three pieces of “information.” Only the “cryptographic element” is referenced later in claim 1. Ex-1003, ¶87.

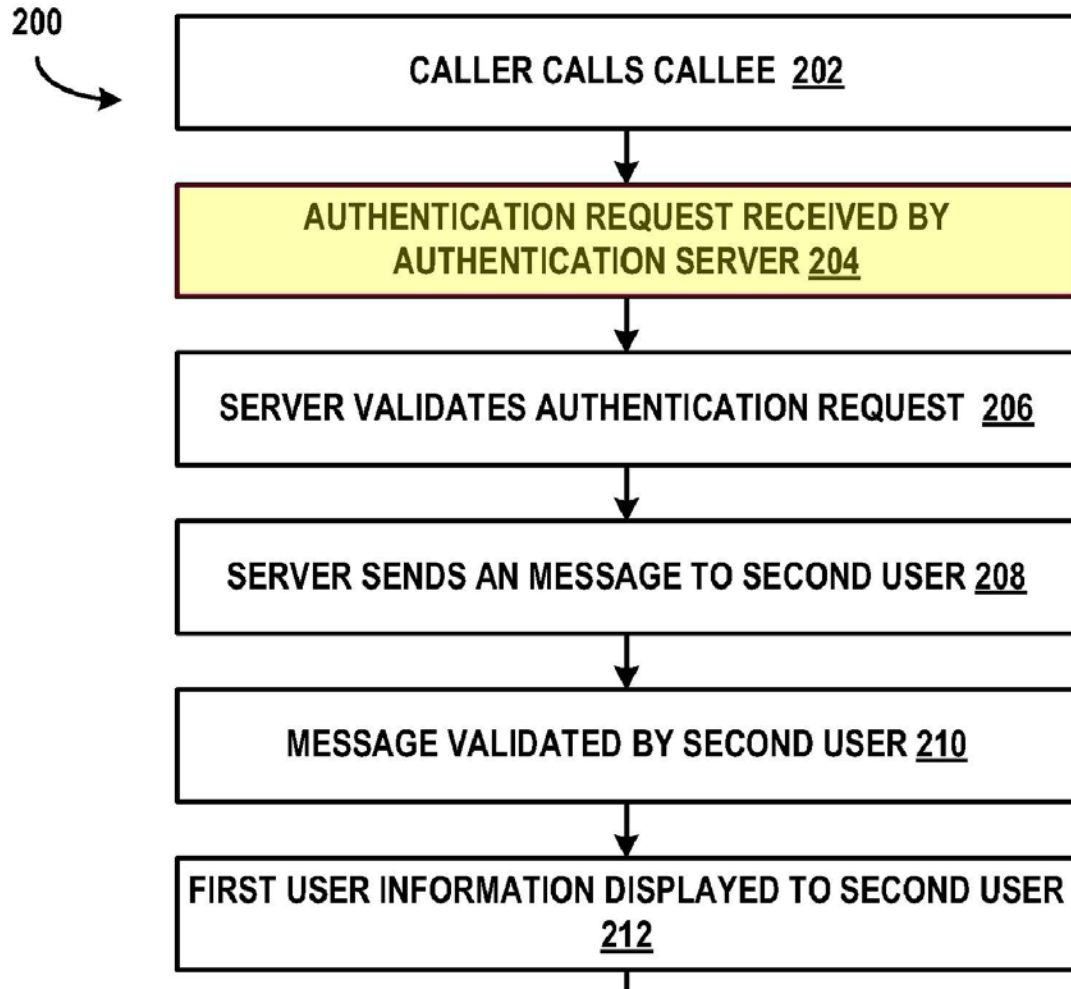
- (a) The Har/Miller Authentication Server Receives Information from the Caller Device

Har’s “authentication server” as supplemented by Miller’s DKCP functionality, discloses this element. One “receive” occurs when Har’s

“authentication server” *receives* an “authentication request” from the “caller mobile device” as depicted in Step 1 below.



Ex-1004, Fig. 1, [0016]. Similarly, Har’s Fig. 2 shows this “receive” action.



Ex.-1004, Fig. 2, [0016]. Ex-1003, ¶88.

The “receiving” can also include the information received in the “challenge” and “response” that may (optionally) occur after the initial “authentication request.” As detailed below and in Sections VI.A.2, VI.A.3 (incorporated herein), Miller’s DKCP (as adopted by Har) includes both an initial transmission of authentication information in the “authentication request” and then a subsequent “challenge” and “response” from the calling device to the authentication server. Ex-1003, ¶89.

This “receiving” element does not recite that all “information” is necessarily received in the same communication. Indeed, the ’132 patent teaches the type of “challenge” system that Miller teaches. Specifically, the ’132 patent includes a multi-step authentication procedure with: (1) a first communication received by the authentication server seeking authentication; and (2) the server “requesting additional authentication factors” from the calling device and (3) the calling device sending “additional authentication factors” to the server. Ex-1001, 9:26-57, 13:22-32; 10:9-24. Furthermore, in the ’132 patent (as in Miller and Har), the authentication server receives information during registration. Ex-1001, Figs. 3A/3B, 9:20-57, 13:13-33, 14:52-15:20; Ex-1022, Fig. 4, [0085-0094] (Miller’s registration process). Ex-1003, ¶90.

Thus, in the Har/Miller System (like the ’132 patent), “receiving information” can occur in multiple steps and different forms of communication, if needed. Each “*data related to*” category below is “information pertaining to a call” because each example identifies information used in the calling and authentication process. The “*pertaining to a call*” does not require the information to necessarily be within the same calling structure (or even time frame). Ex-1003, ¶91.

- (b) The Har/Miller Authentication Server Receives the Three Types of Claimed Information.

This element recites receiving “*data related to (1) a phone number associated with a callee device, (2) device information associated with the caller device, and (3) a cryptographic element associated with the caller device.*” Har’s authentication request includes information that suggests, or renders obvious, all three claimed “*data related to...*” categories:

The authentication request can include information identifying the caller 114, information identifying the callee 116, any other information that caller 114 would like callee 116 to have and/or any other information that caller 114 specifies... The request can be signed using the caller's private key and encrypted using the server's public key or other encryption/decryption methodologies can be used.

Ex-1004, [0023]; *see also* Ex-1004, [0016]. Furthermore, if PO argues that Har does not disclose these categories by itself, Miller’s DKCP functionality fills any minimal gaps. Ex-1003, ¶92.

“Data related to (1) a phone number associated with a callee device.”

The Har/Miller authentication server receives “*data related to ... a phone number associated with a callee device*” in multiple ways. As quoted above, Har’s “request” includes “information identifying the callee.” Furthermore, Har’s authentication server “receives” data for its information store:

The authentication server may have a data store of user information that includes the mobile telephone numbers of users, ..., credentialing information, identification information and so on.

Ex-1004, [0018]. This disclosure shows two forms of “*receiving ... data related to ... a phone number associated with the calling device.*” First, because Har’s

authentication request included “information identifying the callee” (Ex-1004, [0023]) it would be, at a minimum, obvious that such “information identifying the callee” discloses callee’s phone number. Har teaches that “user information ... includes the mobile telephone number of users.” Thus, the “information” in Har’s request is at least “*data related to ... a phone number associated with a callee device.*” It is also obvious that the “authentication request” would include the phone number so that the authentication server could identify the callee device and communicate with it. Furthermore, it is also obvious, and well-known, that information related to a call includes the recipient’s phone number. Finally, the claim only requires “*data related to... a phone number.*” The “information identifying the callee” teaches or renders obvious such “*data related to*” because the callee is contacted and identified by using the phone number. Ex-1003, ¶93.

Second, Har’s authentication server “can look up the mobile telephone number of the second user in its data store.” Ex-1004, [0027]; [0018]. To “look up” this number in a “data store,” it is at least obvious that the authentication server “received” the callee user’s phone number previously – such as through a registration process. Ex-1004, [0035] (“information associated with the first user, as registered in the server's database”). Ex-1003, ¶94. Har teaches receiving a PIN/password (or “credentials”) from the callee device for authentication sent in a

message digitally signed by the callee – which both also meets this element. Ex-1004, [0019], [0025], [0029].

Furthermore, Miller’s DKCP functionality includes the functionality to receive, store and utilize “*data related to ... a phone number*”. The “collection of minutia” includes “phone numbers.” Ex-1022, [0051]; *see also* Ex-1022, [0067] (a “validate response ... can employ multiple methods of collecting ... a smartphone’s phone number” or a “phone number” in the “returned minutia.”); [0052], [0056] (“(e.g., frequently called phone numbers)”). Thus, Miller’s DKCP receives, stores and utilizes the phone numbers of registered users (including callees) during authentication. Ex-1022, [0085-0094] (registration); Ex-1003, ¶95.

Miller’s DKCP communicates with the callee device (*e.g.*, Miller’s “service provider”). Ex-1022, Figs. 1, 4, [0085-0089]. In the context of Har focused on mobile phones, it would be at least obvious that the authentication server implementing Miller’s DKCP would have received the phone number of the recipient device (callee) to successfully communicate with the recipient device. Ex-1003, ¶96.

Thus, it would be at least obvious that the Har/Miller authentication server would receive “*data related to ... a phone number associated with a callee device.*” Ex-1003, ¶97.

“Data related to ... (2) device information associated with the caller device.”

The Har/Miller authentication server would receive “*data related to ... device information associated with the caller device*” in multiple fashions. Har focuses on information primarily related to the user and the phone number. However, Har also suggests using additional identification information for authentication. Miller’s DKCP provides explicit details regarding the receipt and usage of “*data related to ...device information associated with the caller device.*” Ex-1003, ¶98.

Har contemplates device information for authentication. “FIG. 4 illustrates an example of a system 400 that supports authentication of mobile devices.” Ex-1004, [0044]. Har’s authentication “server 408 may act as an authentication server to authenticate mobile devices...” Ex-1004, [0044]. Har repeatedly teaches usage of “identification information” for authentication including the “identification information” stored in the server. Ex-1004, [0018]; see also Ex-1004, [0016], [0027], [0034], [0035]. To “authenticate mobile devices,” it would be obvious for Har’s system to use device “identification information.” Ex-1003, ¶99. Furthermore, Har describes using a PIN/password challenge for the caller device as part of the authentication which also provides this element. Ex-1004, [0017].

If PO argues that Har’s “identification information” does not disclose “*data related to ... device information...*,” then Miller discloses many forms of such data from the initiating device (computer 18). Ex-1003, ¶100.

Miller creates a unique device identifier using sets of “computer minutia” to uniquely identify computers 18 (*data related to ...device information associated with the caller device*).

[S]ystem 200 may collect and catalog a number of minutiae values of computer 18 and service user 20 that may be useful for identifying the computer 18 and service user 20 in the sense that computer minutia 64 and secrets and biometric minutia 26 can be used by the dynamic key crypto provider 10 to form dynamic keys unique to each and every distinct computer 18 and service user 20.... The unique identification of a computer 18 may be processed by system 100, ...

Ex-1022, [0050]. Miller’s device information matches the ’132 patent device information. Ex-1001, 9:30-37. Ex-1003, ¶101.

Miller’s “computer minutia” includes different permutations of “hardware,” “firmware” and “software” minutia. Ex-1022, [0057-0061]; Figs. 2A-2B. These “minutia may include which firmware and software codes are installed on the computing device and ... what particular version or release date of firmware or software are installed” – matching the ’132 patent’s identification of a device information as including “installed applications, system or application software versions.” Ex-1022, [0031], Ex-1001, 9:34-37; *see also* Ex-1022, [0052-0056] (identifying various computer minutia). Miller identifies device settings and device-specific identifiers used for the computer minutia. Ex-1022, [0031]. Ex-1003, ¶102.

Miller also teaches a “hash” of combination of minutia which is “often referred to as a computer fingerprint.” Ex-1022, [0011], [0038-0039], [0051],

[0094], [0132-0133], [0142-0143]. Miller describes “millions of different possible combinations of minutia DB 70 and the related practically infinite range of minutia values in the anticipated minutia DB 98” such that “each single computer 18 can be uniquely identified by matching its unique computer minutia 64...” Ex-1022, [0056]. This also discloses the claimed “*data related to ... device information associated with the caller device.*” Ex-1003, ¶103.

Miller “registration” describes “enrollment” used in the ’132 patent. The ’132 patent enrolls the device with the VSP to store the unique device identifier at both the VSP and “locally on the smartphone device.” Ex-1001, Fig. 9, 17:38-18:40; 19:9-33. Miller’s “registration” also stores the device information on the authentication server (DKCP) and locally on the device. Ex-1022, [0085], Fig. 4; Ex-1003, ¶104.

The computer minutia are received by the DKCP and stored in “Minutia DB 70” for verification:

By performing a transmit minutia to DKCP 62 process, various values of computer minutia 64 ...may be sent along with their minutia descriptor to the dynamic key crypto provider 10 which [] may record the computer minutia 64 and secrets and biometric minutia 26 into a minutia DB 70.

Ex-1022, [0092]; [0055-0058] (describing subsequent usage), [0037]. This matches Har’s authentication server having a “data store.” Ex-1004, [0018]; Ex-1003, ¶105.

Regardless of whether Miller's minutia is used (or stored) in the unhashed or hashed form or whether the cryptographic function is applied, these aggregations of computer minutia are *data related to ... device information associated with the caller device*. Ex-1022, Abstract; [0029], [0050], [0055-0056]. Ex-1003, ¶106.

Miller's hashed (and cryptographic) device information corresponds to the '132 patent. For example, the "hashed" version is a combination of different minutia. Ex-1022, [0064]. This matches the '132 disclosure of a "device 'fingerprint' created from a combination of" criteria. Ex-1001, 9:34-37; Ex-1003, ¶107.

In authenticating the device, Miller's DKCP receives device information from computer 18. Ex-1022, [0048-0049], [0026]. For example, computer 18 sends a "challenge response" containing "computer minutia" (*device information*) back to the DKCP. Ex-1022, Abstract, [0065], [0013-0016], [0039], [0080], [0091]. Figures 2A/2B below show Miller's challenge / response sequence.

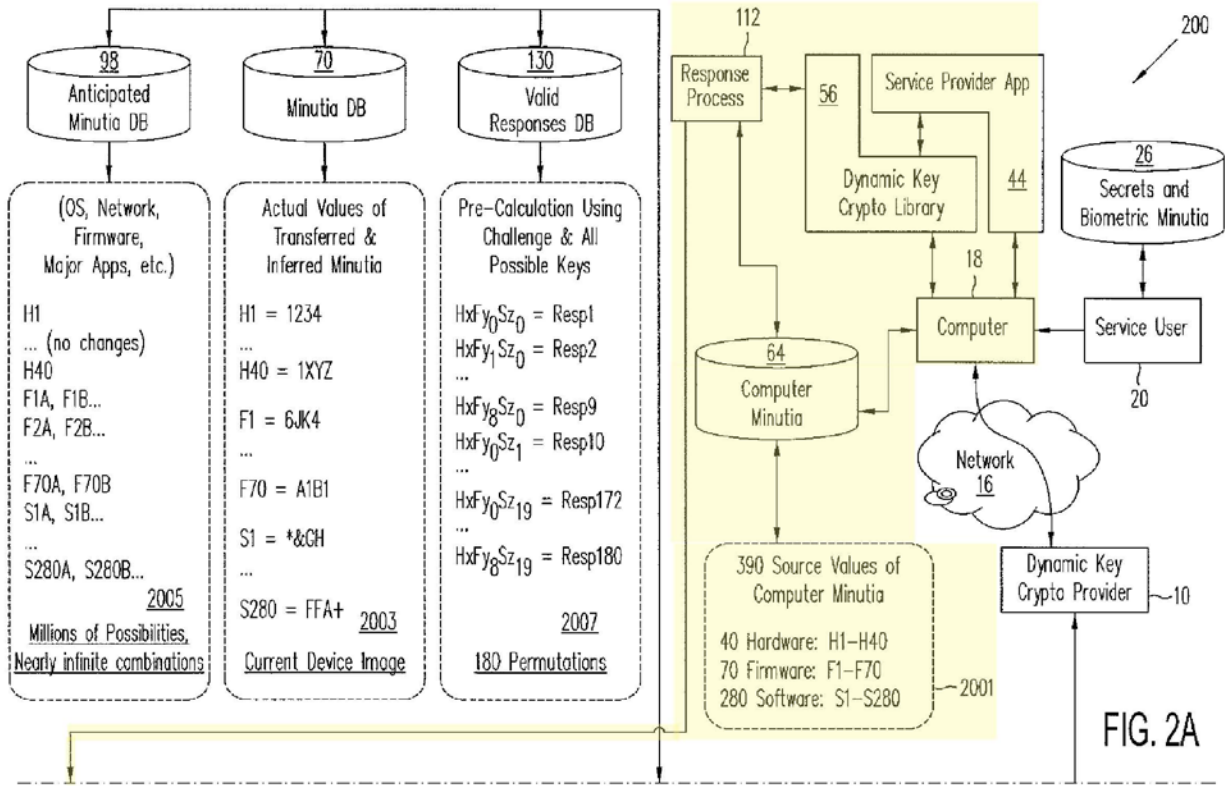


FIG. 2A

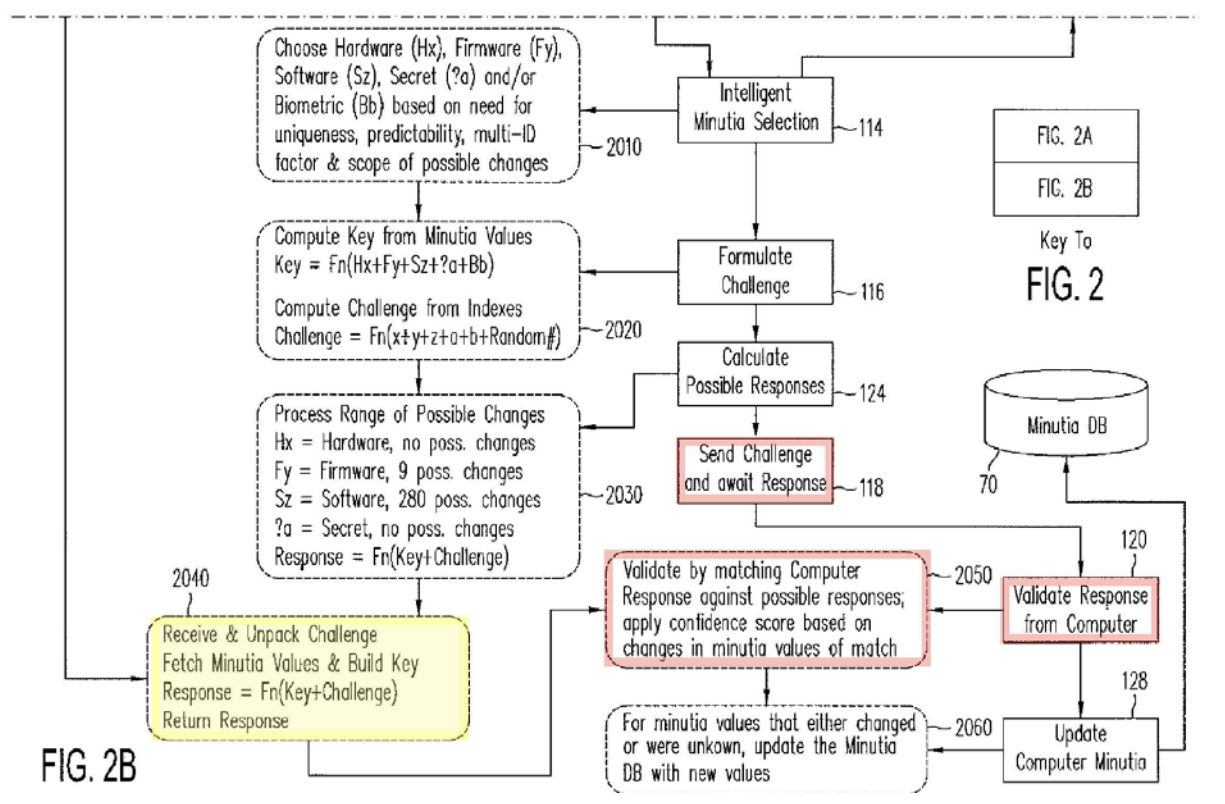


FIG. 2B

Ex-1022, Figs. 2A-2B. "Computer 18" components and algorithm are highlighted

in yellow. “[R]esponse process 112” uses information from the “computer minutia” database to “return response” as highlighted in box 2040. Ex-1022, [0064-0065]. The DKCP uses that “response” for validation as highlighted by boxes 118, 120, 2050. Ex-1022, [0065-0070]; Ex-1003, ¶108.

Thus, in combination, the Har/Miller authentication server “receives” many forms of “*data related to... device information associated with a caller device*” including the specific types of “*device information*” taught in the ’132 patent. Ex-1001, 9:30-37. Ex-1003, ¶109.

“Data related to ... (3) a cryptographic element associated with the caller device.”

The ’132 specification does not use “cryptographic.” However, the ’132 specification includes an embodiment with “certificates” and “public keys” for security determinations. See Ex-1001, 7:33-47; claim 7. Thus, a POSA would understand that “cryptographic element” encompasses techniques using certificates and public keys because they are examples of elements used for cryptographic purposes. Ex-1003, ¶110.

The Har/Miller combination teaches this element. First, as in the ’132 patent, Har teaches using a “digital signature” with a “digital certificate” and keys (including public/private keys) for authentication (“*cryptographic element*”).

The authentication request can be a message encrypted using the server's public key (also called the server's public certificate) and signed using the private key (also called the private certificate) of the first user (the user for whom authentication has been requested), using PKI

authentication methodology (asymmetric key encryption/decryption).

....

Ex-1004, [0015-0016]; see also Ex-1022, [0023] (“request can be signed using the caller's private key.”); [0002] (listing request information). Har teaches using both the digital signature for the communication and the information within the communication for verification.

An authentication server such as authentication server 102 can receive the authentication request, can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message.

Ex-1004, [0026]. Ex-1003, ¶111.

The “caller’s private key” (used to encrypt the digital signature / communication), teaches or renders obvious, that Har’s authentication request digital signature is “*data related to ... a cryptographic element associated with the calling device.*” The “digital signature” is itself a cryptographic element because it relies upon encryption / decryption for usage. Moreover, the digital signature is “*data related to*” both the “server’s public [and private] key” and the “key of the user sending the message” (both private and public) (which are themselves “*cryptographic elements*”) because all these keys must be used to successful encrypt/sign, and then decrypt/verify, the signature. Ex-1004, [0015-0016], [0026]. Moreover, the caller’s private key is associated with the mobile device because it is stored on the mobile device and used by the mobile device to “sign” the certificate.

Similarly, the digital certificate teaches or renders obvious “*data related to*” and “*associated with the device*”, because it is signed by the key of the caller, it is created by the device based upon the key(s) stored in the device memory, and it is used/transmitted by the device for the purpose of authentication the device (or its user using the device). Thus, Har itself discloses, or renders obvious, that Har’s authentication server receives “*data related to ... a cryptographic element associated with the device.*” Ex-1003, ¶112.

If PO argues that Har only discloses the “caller’s” keys, and that “caller” refers to the user/person not the “caller device” as claimed, the Board should reject such arguments. Ex-1003, ¶113.

Har teaches, or at a minimum, renders obvious that the “private key” is “*data related to*” and “*associated with the caller device.*” For example, Har teaches that for “authentication of mobile devices ... [t]he server 408 may act as an authentication server to authenticate mobile devices as described herein” which is a teaching or suggestion that the authentication pertains to devices (not people). Similarly, Har teaches using the “server’s public key” and “server’s private key” to encrypt/sign messages. Ex-1004, [0016], [0018]. Thus, Har at least renders obvious that such private keys are associated with devices because the “server” is a device, not a person. Ex-1003, ¶114.

Given that Har recites authentication of “mobile devices” and teaches keys associated with devices, it would be an obvious variation to use the private key associated with the caller device to digitally sign the communication from the caller device to the authentication server. Such a usage would effectuate the goals of both Har and Miller to ensure correct authentication. Moreover, both Har and Miller provide storage on the caller device and authentication server of device-specific information used for authentication, such as the keys. Ex-1003, ¶115.

Thus, the Har/Miller combination teaches, or renders obvious, that the authentication server would receive “*information pertaining to a call ...comprises data related to . . . cryptographic element associated with the caller device*”). Ex-1003, ¶116.

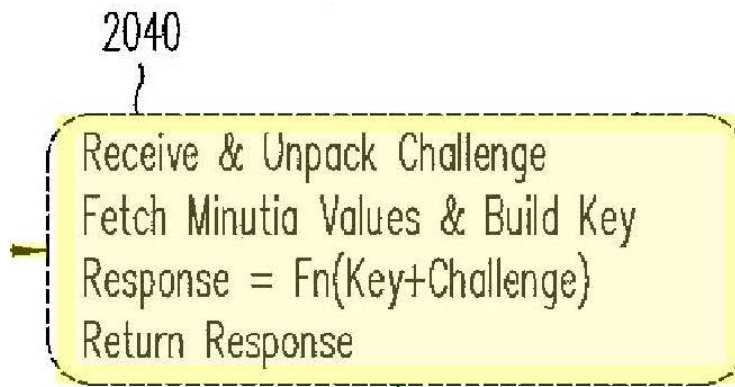
Second, even if PO argues that Har does not disclose this element, Miller unequivocally discloses a cryptographic element (a “key”) that is specifically based on the “minutia” specific to the device and used to identify the specific device. As detailed above, Miller includes an embodiment in which a cryptographic function can be applied to the sets of computer minutia used for identification / verification (at both the device and DKCP). Ex-1022, [0063-0065]. Miller references such encrypted versions as a “key” or “identifier key.” Ex-1022, [0063-0070], [0090]. Ex-1003, ¶117.

The “response” received by Miller’s DKCP includes “*data related to ... a cryptographic element associated with the caller device*” in the form of this key.

Miller describes how the key is computed using a “cryptographic function:”

The particular computer 18 being challenged may form a response to the challenge by applying a mathematical or cryptographic function “Fn”, which should be the same as that used at step 2020 or step 2030, to the key+challenge as shown in FIG. 2. The computer 18 being challenged may then communicate the response to return it directly to the dynamic key crypto provider

Ex-1022, [0065]. This “key” is received by Miller’s DKCP in the “response.” [0065-0070]. Element 2040 depicts creating the response received by the DKCP:



Ex-1022, Fig. 2B; see also elements 2030, 2050. Ex-1003, ¶118.

Furthermore, the ’132 patent discloses an embodiment describing a “cryptographic element” similar to Miller’s cryptographic function:

[T]he response ... information includes computed values that are computed, for example, using keys or codes that are known only to the device and verification provider.

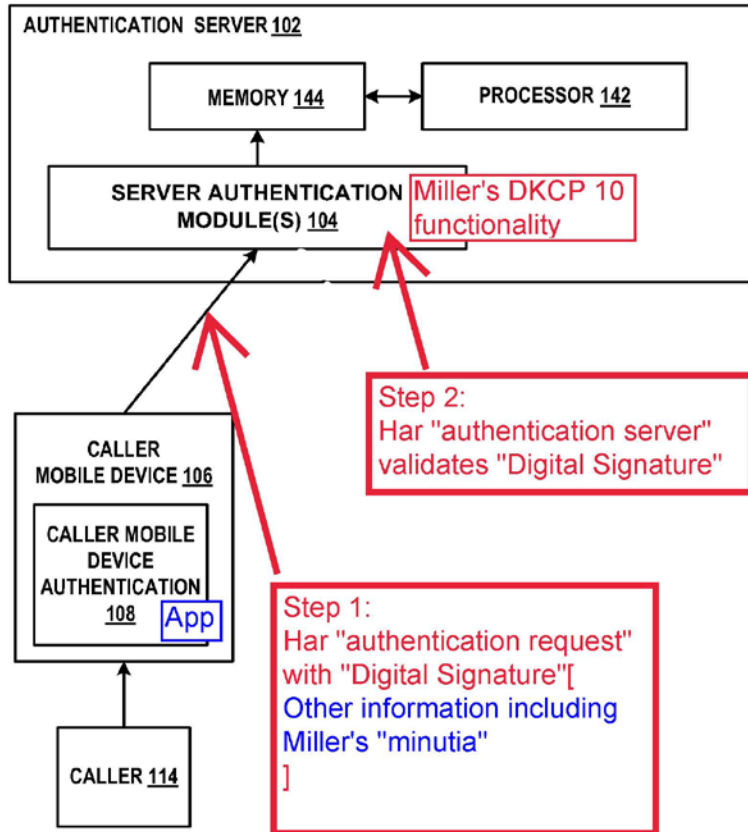
Ex-1001, 15:66-16:7. The “computed values ... using keys or codes...” corresponds to Miller’s cryptographic function applied to device information being exchanged between computer 18 and the DKCP. Ex-1003, ¶119.

Thus, the Har/Miller System discloses this element. Ex-1003, ¶120.

- iii. performing a security determination based at least in part on the cryptographic element associated with the caller device comprised in the received information pertaining to the call; and

This element uses the “cryptographic element” recited in element 1.ii for “*performing a security determination...*” The Har/Miller authentication server performs such a security determination in at least two ways. Ex-1003, ¶121.

First, as detailed in element 1.ii, Har discloses, or renders obvious, the claimed “*a security determination based at least in part on the cryptographic element associated with the caller device.*” See “Step 2” in Section VII.A.3 (incorporated herein):



Ex-1004, Fig. 1. Ex-1003, ¶122.

Har’s authentication request is “signed” with a digital certificate based on a key and that it was at least obvious that Har’s signature is “associated with the caller device.” Element 1.ii, *supra* (citing Ex-1004, [0015-0018], [0023], [0026]). Ex-1003, ¶123.

Har teaches that its authentication is based, in part, on the ability to successfully decrypt the device signature. Ex-1004, [0017], [0021], [0026]; Ex-1003, ¶124.

Har’s authentication server using the digital certificate to determine successful or unsuccessful authentication teaches the claimed “*security determination*” when

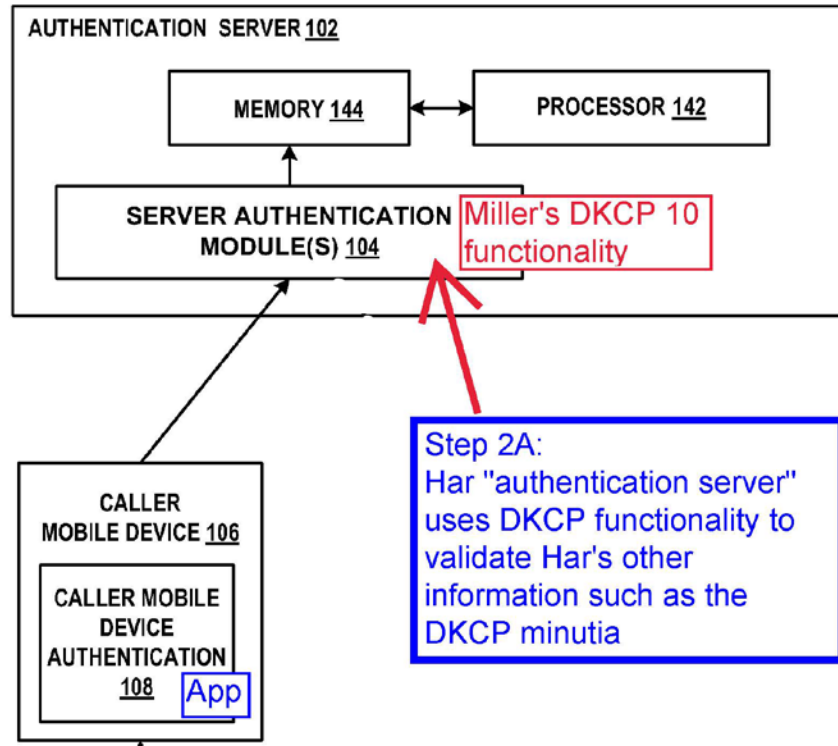
the digital certificate is associated with the calling device (as detailed above and in element 1.ii) because, as taught in Har, the digital certificate uses cryptography to attempt to decrypt the authentication request and bases its authentication results on the success of that cryptography usage. Ex-1003, ¶125.

Finally, Har teaches that both the digital certificate authentication and authentication using the information within the request may be used as a security determination.

An authentication server such as authentication server 102 can receive the authentication request, can decrypt the encrypted request using the server's public key and the digital signature can be verified using the public key of the user sending the message. ... If the decryption fails, the authentication of the sender's transmission (and thus authentication of the identity of the sender) fails. If the digital signature cannot be verified, the authentication of the sender's transmission fails. Moreover, authentication server 102 can verify that information included in the transmission sent by the sender agrees with information for the sender stored in a data store associated with the authentication server 102. If decryption is successful and the digital signature of the sender of the message is verified, and the information included in the transmission by the sender agrees with information stored in the data store of the authentication server 102, the transmission (the identity) of the sender is authenticated.

Ex-1004, [0026]. This teaches two separate claimed “*security determinations*” by the authentication server: (1) the certificate-based determination; and (2) the “information included in the transmission sent by the sender” (corresponding to Miller’s cryptographic key below). Ex-1003, ¶126.

Second, if PO argues that Har does not disclose this element, Miller’s DKCP uses the “key” received from the initiating device (computer 18) to authenticate the device. This was explained as “Step 2A” in Section VII.A.3 (incorporated herein).



Ex-1004, Fig. 1; Ex-1003, ¶127.

Miller’s DKCP matches the minutia received from computer 18 (either in the initial communication or in the “challenge response”) against the registered minutia stored in the DKCP database. Miller’s Fig. 2B shows this “matching” (element 2050) performed with “Validate Response from Computer” (element 120):

Using Miller's cryptographic function response from computer 18, "for example, as seen at step 2007, if the actual response matches the 172nd possible response 'Resp172' or permutation, then the actual device values must match those of Hx, the first possibility for Fy (e.g., Fy0), and the twentieth possibility for Sz (e.g., Sz19)." Ex-1022, [0066]. "If a match is found, the subset of minutiae used in the challenge may be regarded as being known or authenticated." Ex-1022, [0066]; Ex-1003, ¶128.

By attempting to match any one or more of the Hx/Fy/Sz triplet as subject to Millers "cryptographic function," Miller discloses a "*security determination [is] performed based at least in part on the cryptographic element associated with the caller device.*" This element is met both because the information received for the call is subject to a cryptographic function and because Miller's DKCP can store the registered information (for performing the match) in its "pre-processed" form by calculating all the available encrypted responses that can be received. Ex-1022, [0013-0016], [0064-0070], claims 1, 12. Ex-1003, ¶129.

Miller also describes a "scoring" based on the (encrypted) information received from the calling device that teaches, or renders obvious this claim element. Ex-1022, [0040], [0073], [0100], [0102-0120]; Fig. 6. After calculating a score, "the resulting score is compared against the initial threshold defined by the service provider" "to determine if a possible response and corresponding score are equal to

or above the threshold using information from the valid responses 130 database.”
Ex-1022, [0111], [0113]; Ex-1003, ¶130.

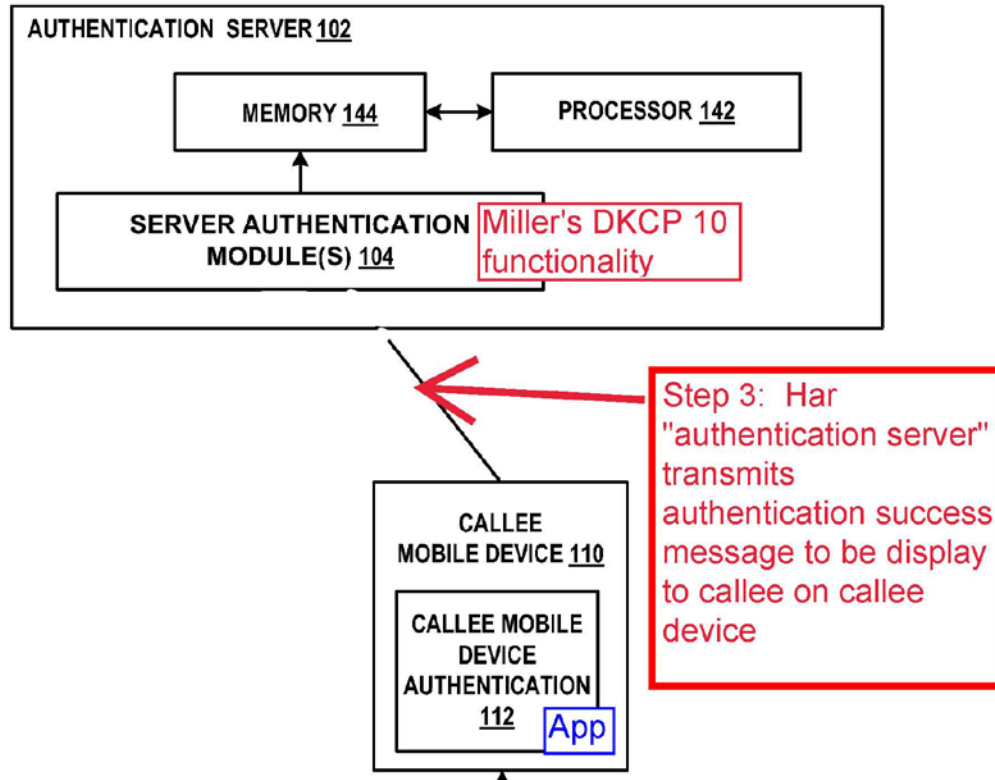
Miller’s “scoring” teaches, or renders obvious, the claimed “*security determination...*” To calculate the scores, Miller compares (matches) the received minutia to verify the device. Ex-1022, [0105], [0064]. Thus, the process of “comput[ing]” Miller’s score teaches or renders obvious, the claimed security determine because it “determin[es] whether the obtained information ... matches at least a portion of” Miller’s store computer information which may be in encrypted form. Miller’s “scoring” matches the ’132 patent using “scoring” for a security determination. Ex-1001, 10:61-64, 9:38-10:24, 12:14-27; Ex-1003, ¶131.

Thus, Miller’s DKCP processing discloses the claimed “*security determination...*” through its “matching” and through its “scoring” system. Thus, the Har/Miller combination discloses this element. Ex-1003, ¶¶132-133.

- iv. based at least in part on a result of the security determination performed based at least in part on the cryptographic element associated with the caller device, transmitting, using a cellular network, a notification directed to the callee device.

The Har/Miller authentication server transmits notifications directed to the callee devices. Har/Miller each teach: (1) transmitting notifications based on the

security determination results from 1.iii; and (2) using a cellular network. This notification was explained in Section VII.A.3 as “Step 3” (incorporated herein):



Ex-1004, Fig. 1; Ex-1003, ¶134.

Har’s server transmits an “authentication indication” (*notification*) that includes caller identification to be displayed on the callee’s device:

In response to successful validation ... the authentication server can send an authentication indication to the device of the user receiving the authentication results. The receiving user's device can display identification information and other (optional) data associated with the first user.

Ex-1004, [0002]. See Ex-1004, [0017-0018], [0026-0027], [0030-0035] (same); Ex-1003, ¶135.

Miller also discloses that a notification. *E.g.*, Ex-1022, [0111], [0068], [0117] (each sending either the score or failure to the call recipient). Ex-1003, ¶136.

Har uses cellular networks for inter-device communications. Ex-1004, [0033] (“mobile network environment”), [0045] (“cellular telephone”); [0046] (“communication via a cellular telephone”); [0012]; [0034]. A POSA would recognize that an “SMS” or “MMS” connection using Har’s “mobile devices” teaches or renders obvious a cellular network because those messaging platforms are typically associated with cellular networks. Miller also may use cellular networks for inter-device communications. Ex-1022, Figs. 1-9; [0097]. Ex-1003, ¶137.

Thus, the Har/Miller authentication server transmits a notification to the callee device based on its authentication results (as described in Har) using a cellular network. Ex-1003, ¶138.

a. Claim 2

The method of claim 1, wherein the security determination is based at least in part on a policy.

Har and Miller teach, or render obvious, such a policy-based determination. The ‘132 patent has sparse recitation of “policy” and references “custom verification processing and policies” and “the relying party incorporates the score into a risk-based decision system to be used in conjunction with other variables... such as ... service policies” for security determinations. Ex-1001, 9:6-8, 9:48-54. In this

context, a POSA would understand a “policy” to encompass selecting criteria for the security determination differentially. Ex-1003, ¶139.

Miller teaches, or renders obvious, such “policies” by “us[ing] intelligent minutia selection 114 to select a combination of minutia from the total set of minutia” which “may employ a number of considerations” for “a particular computer...” Ex-1022, [0057], [0060]; Ex-1003, ¶140.

Miller’s “intelligent” selection allows for differentiated levels of security based on criteria “for the particular computer.” Ex-1022, [0057-0060]. The “intelligent” selection also allows for differentially selecting the criteria (subset of minutia) for each individual device / user to be authenticated. Furthermore, such “intelligent” selection allows for user-specific efforts to increase the “scoring” for particular thresholds that are set for each user and service. Ex-1022, [0040] (“intelligently chosen ... [to] yield[] a higher confidence score...”). Miller’s DKCP authenticates by “tying the minutiae to an online service provider account identifier” during registration. Ex-1022, [0037], [0088], [0092], [0156-0159]. Ex-1003, ¶141.

Thus, while Miller does not use the word “policy,” it would be an obvious variation to implement Miller’s intelligent minutia selection through “policies.” Such “policies” are merely a re-formulation (or renaming) of Miller’s processing which differentiates the security determinations for different devices based upon different minutia. Ex-1003, ¶142.

Har similarly suggests such differentiation for basing security determinations on different criteria for different rules. As detailed in 1.ii and 1.iii, Har's caller may include "other information" in the authentication request, which is then matched against "information for the sender stored in a data store." Ex-1004, [0016], [0026]. It would be, at most, an obvious and well-known implementation to assess this user-specific "other information" using policies. Ex-1003, ¶143.

b. Claim 3

The method of claim 1, wherein the device information associated with the caller device comprises a unique identifier.

Har teaches, or renders obvious, using a unique device identifier including the information stored in its data store. *See* element 1.ii, Ex-1004, [0018]. Furthermore, as detailed in element 1.ii, Miller teaches, or renders obvious, using a unique device identifier. *E.g.*, Ex-1022, [0011], [0026], [0029], [0050], [0055-0056]. Ex-1003, ¶144.

c. Claim 4

The method of claim 1, wherein the device information associated with the caller device comprises Automated Number Identification (ANI) information.

The Har/Miller authentication system teaches, or renders obvious, this element. As detailed in element 1.ii (incorporated herein), the Har/Miller authentication system uses a wide swath of device information. Ex-1003, ¶145.

The '132 patent provides information on what it asserts to be “Automated Number Identification (ANI)”¹ information.

When contacting callee 118, automatic number identification (ANI) data, such as caller id, for the calling device 102 is presented to the callee.

Ex-1001, 3:1-3. The '132 patent identifies the “caller id” / ANI information as the information that is presented to the recipient to identify the caller. Ex-1001, 4:35-38, 12:4-8. Beyond these examples of usage, the '132 patent does not contribute any teaching regarding ANI and appears to rely upon the knowledge of a POSA to fill in any gaps in the disclosure. Ex-1003, ¶146.

Har, alone or in combination with Miller, discloses this limitation. Har repeatedly teaches that the “identity of the caller” is presented to the callee. Ex-1004, [0028] (“display the sender’s identification information...”), [0035] (“identification information associated with the first user can be displayed to the second user along with any additional data indicated in the authentication request”), Abstract (“display identification information and other (optional) data associated with the” caller). Moreover, Har teaches that a wide variety of information is included in the authentication request as detailed in element 1.ii. E.g., Ex-1004,

¹ The '132 patent references “ANI” as both “automatic” and “automated” number information but appears to intend that these terms are the same. *Compare* Ex-1001, 1:30-31 (“automated”) with 2:49-50, 3:1-2 (both “automatic”).

[0034] (“authentication request can include identification information associated with the sender of the authentication request.”), [0016]. Har’s data store includes “mobile telephone numbers of users, usernames, passwords, PIN codes, the name, address and public keys for users, credentialing information, identification information and so on.” Ex-1004, [0018]. Moreover, as detailed in element 1.ii, Miller’s “minutia” transmitted for authentication includes the “phone number” and “any piece of information that can be definitively associated with the computer and its user...” Ex-1022, [0030]; Ex-1003, ¶147.

Furthermore, consistent with the ‘132 specification, a POSA would have understood that automatic number identification (ANI) is technology was widely used long prior to the ‘132 patent and may be used in call centers and telecommunications equipment to automatically identify and capture the telephone number of a caller. A POSA would have also understood that ANI information is transmitted for every call, based on various telecommunications standards. *E.g.* North American Number Plan Administration, 2003. Ex-1003, ¶148.

Thus, the Har/Miller authentication system discloses, or renders obvious the use of ANI data. First, the ‘132 patent relies upon the knowledge of a POSA for understanding of ANI information – knowledge that is also used by a POSA in an obviousness analysis. Second, Har/Miller discloses a wide swath of information identifying the calling device – including the phone number that a POSA would

understand is encompassed by ANI in light of the ‘132 disclosure. Third, both Har and Miller render the use of device identity information, like phone numbers (or any other form of identification information) to aid in call authentication. Ex-1003, ¶149

The inclusion in the Har/Miller request (as detailed in 1.ii) of the claimed ANI information would thus have been disclosed by, or obvious over, Har/Miller and of routine skill to a POSA. Ex-1003, ¶150.

d. Claim 5

The method of claim 1, wherein the security determination is based at least in part on a validation of the information pertaining to the call.

This element adds little to claim 1 which recites “*information pertaining to [the/a] call*” comprises three categories of “*data related to...*” Also, the claim 1 “*security determination*” is “*based at least in part on the cryptographic element*” (the third category of “*data related to*”). Thus, this claim adds only a “validation” aspect. Ex-1003, ¶151.

As detailed in elements 1.ii-1.iv, the security determinations in Har and Miller perform “validation” of the information. For Har’s digital signature (referenced in 1.ii-1.iv), Har characterizes the results as a “validation.” Ex-1004, [0034] (Based on the digital signature, the authentication server “can validate or invalidate the” request), Abstract (“validation ...”), [0002] (“successful validation ...r”), [0019] (“authentication server can decrypt and/or validate the digital signature” to

determine “validation”), [0028], [0032], [0035]. Moreover, a POSA would understand Har’s digital signature evaluation to teach, or render obvious, “validation” of that signature. Ex-1003, ¶152.

Similarly, Miller’s cryptography function (described in 1.iii and incorporated here) is a “*validation*” of the information within the “key” transmitted to the DKCP. Miller repeatedly uses “validation” (or forms of “valid”). Ex-1022, [0030], [0050] (“validation sequences”), [0057] (“rapidly validated”), [0065-0070] (“validate response from computer 120 process” leads to “validation”), [0091-0092], [0011-0018], [0022], Figs. 2A/2B, 6A/6B. Ex-1003, ¶153.

Thus, the Har/Miller authentication server performs the claimed “validation” as detailed herein and in 1.iii. Ex-1003, ¶154.

e. Claim 6

The method of claim 1, further comprising storing, in a data store, at least one record including contents associated with the caller device.

Har and Miller each include the claimed data store. Ex-1004, [0018] (describing Har’s server “data store”); [0027]; [0047] (each device includes a data store with its own information in “memory 312”). Ex-1003, ¶155.

Miller details two different databases that each store “*at least one record including contents associated with the caller device*” – one on the device, and one on the server. E.g., Ex-1022, Figs. 2A, 4 (element 64 “computer minutia”), [0052]

(“computer minutia 64 can represent a set of 390 distinct minutiae values that may be chosen for collecting and cataloging from the computer 18”); Figs. 2A, 4 (element 70 “minutia DB”), [0092], [0053], [0056-0058]. Ex-1003, ¶156.

Thus, the Har/Miller system discloses this claim. Ex-1003, ¶157.

f. Claim 7

The method of claim 1, further comprising storing, in a data store, at least one certificate used to validate the call.

Har discloses the “storing ... at least one certificate” by using the digital signature used to validate the authenticate request as detailed in 1.ii and 1.iii.

The authentication request can be a message encrypted using the server's public key (also called the server's public certificate) and signed using the private key (also called the private certificate) of the first user (the user for whom authentication has been requested)

Ex-1004, [0016]. Similarly, the authentication server uses “the server's private key and/or encrypted with the receiving user's public key” as part validation. Ex-1004, [0018] Thus, it would be at least obvious that Har’s authentication server stored the various certificates (the server’s public/private certificates / keys and the public / private certificates / keys of each user) to be able to use those for authentication. Har’s “data store of user information [] includes ... public keys for users, credentialing information, identification information....” Ex-1004, [0018]. Thus, the Har/Miller authentication server stores the claimed certificate. Ex-1003, ¶158.

Har's description matches the sole usage of "certificate" in the '132 patent. Ex-1001, 7:34-35 ("data stored along with the verification process contains certificates used to verify such phone numbers"). Ex-1003, ¶159

Moreover, Miller's DKCP stores and uses certificates. For example, as detailed in 1.ii, 1.iii, Miller's DKCP stores the pre-processed results for which the cryptography has been applied and describes these as "keys." See 1.ii, 1.iii; Ex-1022, [0050], [0053], [0064-0070], [0090], [0074], [0006], [0029], [0032], [0008]. Ex-1003, ¶160.

g. Claim 8

The method of claim 1, wherein the call is validated at least in part by using at least one of a secret key or a public key.

Har, alone or in view of Miller, renders this claim obvious. As detailed in 1.ii, 1.iii, claim 7, Har discloses the use of secret or public keys in, for example, the digital certificate validation. *See e.g.*, Ex-1004, Abstract, [0016] ("The authentication request can be a message encrypted using the server's public key (also called the server's public certificate) and signed using the private key (also called the private certificate) of the first user (the user for whom authentication has been requested), using PKI authentication methodology (asymmetric key encryption/decryption)."). Ex-1003, ¶161.

Miller’s description of the “cryptographic function” used for validation matches the ‘132 patent’s description of a “secret key.” Ex-1001, 12:45-56. In Miller, the purpose of the “dynamic key” is that it is a secret key that is generated dynamically by the cryptographic functions on the device and server. Ex-1022, [0064-0070]. Miller identifies many “encryption algorithms” including “RSA” that can be used for the cryptographic function that generates the dynamic keys. Ex-1022, [0074], [0006]. Miller’s dynamic secret keys are an improvement over the known static secret keys. Ex-1022, [0011], [0028-0032]. Thus, Miller teaches the usage of “secret keys” that can be stored (and/or computed) only by the device and the DKCP server based on the cryptographic functions. Ex-1003, ¶162.

a. Claim 9

The method of claim 1, wherein the security determination is based at least in part on execution of a rule.

Har and Miller teach, or render obvious, the use of a “rule.”² A POSA would understand a rule to encompass a condition associated with an action performed based upon evaluation of the condition. Har and Miller each teach such rules (without using the word “rule.”). Ex-1003, ¶163

As detailed in 1.iii, Har teaches a rule in evaluation of its two conditions and the subsequent actions. *E.g.*, Ex-1004, [0026] (“If decryption is successful and the

² The ‘132 patent uses “rule” in two short passages. Ex-1001, 3:28-35, 7:61.

digital signature of the sender of the message is verified, and the information included in the transmission by the sender agrees with information stored in the data store of the authentication server 102, the transmission (the identity) of the sender is authenticated.”). This defines conditions and the resulting action based on those conditions. Such disclosure teaches, or renders obvious “execution of a rule.” Ex-1003, ¶164.

Similarly, Miller’s security determinations, including scoring, teach or render obvious the “execution of a rule” because it is based upon specification of conditions associated with actions performed based on the conditions. For example, Miller’s “service provider” identifies “thresholds” for validation. Ex-1022, [0111-0120]. “If the computed score \geq threshold” then certain actions result. Ex-1022, [0111-0120]. Miller “matches” minutia as part of its security determination. Ex-1022, [0065-0066]. “If a match is found, the subset of minutiae used in the challenge may be regarded as being known or authenticated.” Ex-1022, [0066]. Thus, Miller’s security determinations teach, or render obvious, “execution of a rule.” Ex-1003, ¶165.

b. Claim 10

The method of claim 1, wherein the security determination is based at least in part on a timestamp associated with the call.

Har in view of Miller renders this claim obvious. Miller teaches that an evaluation of time information can be used in its security determination. For example, in Miller's security determination (as detailed in 1.iii):

[a]nother **scoring input** can be the time since a particular minutia value was last validated in a challenge and response exchange with the computer 18.

Ex-1022, [0109]. Miller's usage of the timestamp as a "scoring" input matches the '132 patent:

the message sent to the verification service includes a timestamp, which can be used to prevent a replay attack. For example, the **timestamp can be used by the verification service to score the validity of the communication**, where an old or aged timestamp may be indicative of an attack.

Ex-1001, 8:58-63. Ex-1003, ¶166.

In Miller, to be able to use (or calculate) the "time since a particular minutia value" in a request was last validated, it would be obvious (at a minimum) that the DKCP would beneficially know the current timestamp of the request that is presently being scored. At a minimum, this "time since..." language renders obvious the use of a timestamp of the current communication being scored because a timestamp provides one input (the current time) to be compared against another input (the previous time the minutia was validated) for evaluating the "time since" aspect. Consistent with this evaluation, Miller describes how the other input (the minutia validation time) is collected and stored for usage. For example, Miller

teaches that the “current device image” (used for the security determination / validation) is associated with collecting information “at a particular time or within some pre-defined time frame” and used for verification. Ex-1022, [0055-0056], claim 29. Miller identifies “time and time zone” as minutia used for verification. Ex-1022, [0067]. Miller uses these time-based verifications to prevent attacks that “intercept” and seek to use later “fraudulent responses” based on the interception. Ex-1022, [0029], [0067], [0041], [0135]. Ex-1003, ¶167.

Miller also describes an additional authentication process in which a user may be prompted for a “PIN” as part of Miller’s validation / security determination process for the DKCP system. Ex-1022, Fig. 7, [0121-0133]. As part of that “PIN” entry, there is a determination of the “time since last successful PIN entry.” Ex-1022, [0129]. Using this “time since” also requires usage of the current request timestamp to be able to perform the comparison (for the same reason as detailed in the paragraph above). Ex-1003, ¶168.

Miller also describes a “heartbeat” process using a timestamp associated with the call for a security determination and that a response must be provided “within a timeframe” or otherwise the service is deleted. Ex-1022, [0150-0151]. To determine that the response message was “within a timeframe,” it would be (at a minimum) obvious that the response included a timestamp to use as one of the inputs to this determination. Ex-1003, ¶169.

Furthermore, Miller describes its system as providing a “digital signature.” Ex-1022, [0132-0133]. Using this “digital signature” aspect of Miller’s DKCP system, “the dynamic crypto key can bind the instrument, place, time and person to a particular message.” Ex-1022, [0133]. This teaches, or renders obvious, that the “key” generated by the computer 18 includes a timestamp associated with the communication and is used for the security determination (as detailed in 1.iii). Finally, Miller notes that it was already known in the art to perform verification / identification through “analysis of time (both in clock and network latency).” Ex-1022, [0011]. Ex-1003, ¶170.

Moreover, Har’s usage of public/private keys (certificates) as detailed in 1.ii and 1.iii also renders obvious the use of a timestamp as detailed in this claim. A POSA would understand that such public / private keys typically have an expiration time associated with the key. It would be obvious that the evaluation of such keys would include a comparison of the current communication’s timestamp against the expiration time of the key used for the authentication. Ex-1003, ¶171.

c. Claim 11

The method of claim 10, further comprising detecting a replay attack based at least in part on the timestamp.

Har in view of Miller renders this claim obvious. A POSA would understand a “replay attack” to encompass intercepting and counterfeiting the validation by re-

using old data to “replay” a prior validation. Using a “timestamp” to prevent a “replay attack” was well-known in the art. Ex-1020, 16:48-56 (“The timestamp is used to employ a simple logic operation protecting against a replay attack...”). Ex-1003, ¶172.

Miller specifically addresses the “replay attack” by using the time of the request (timestamp) as a “scoring input” for validity – which, as detailed in claim 10, is exactly the only “security determination” described in the ‘132 patent for “replay attacks.” Ex-1001, 8:58-63. Moreover, Miller specifically uses different minutia (including time-based minutia) to prevent attacks based upon such “intercepting” of messages and attempted re-use. Ex-1022, [0041] (Miller “increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer.”); [0029] (Miller’s validation system addresses attempts “[t]o counterfeit a dynamic key crypto-identified computer” which “intercept” messages by detecting “fraudulent response[s].”). Moreover, one method in Miller to prevent such “intercept[ion]” and “fraudulent responses” is to “force the user to enter the user's standard PIN into the computer” which, as detailed for claim 10, specifically uses a time-based assessment. Ex-1022, [0029]; Ex-1003, ¶173.

Thus, Miller identifies the underlying issues for a replay attack (interception and subsequent fraudulent usage) and describes using the time of the responses for a security determination to detect (and thwart) such replay attacks. Ex-1003, ¶174.

Furthermore, a POSA would understand that Miller’s “heartbeat” process (described in claim 10) is a well-known method for detecting “replay attacks.” “if the heartbeat and chatter 194 process does not perform a valid challenge and response cycle within a timeframe defined by service provider” (indicating a possible replay attack scenario), then the service may be deleted to prevent unauthorized usages. Ex-1022, [0151], [0135]. Ex-1003, ¶175.

d. Claim 12

The method of claim 1, wherein the result of the security determination comprises a score indicating a validity of a phone number associated with the caller device.

The Har/Miller authentication server operation renders obvious this claim. “[A] score indicating a validity of a phone number...” encompasses using various information about the call/communication and the related devices to calculate the score. Ex-1001, 9:20-57; Ex-1003, ¶176.

As detailed in 1.iii, Miller’s DKCP scoring system uses various minutia to determine the validity / authentication. In the context of the Har/Miller System, this authentication is performed for the “authentication request” associated with the call using the caller’s identification to “vouch for” the caller. Ex-1004, [0002]. This

teaches, or renders obvious, that the score relates to the validity of the caller's phone number because, at a minimum, the caller's device phone number is one form of identification. Ex-1004, [0018]. It is also obvious that, when authenticating a voice phone call (as in Har), the authentication encompasses indicating the validity of the phone number of devices engaged in that call. Ex-1003, ¶176.

Moreover, as detailed in 1.ii, Miller's DKCP discloses that the phone number of the calling device can be one "minutia" used for the DKCP scoring system. Moreover, as detailed in 1.ii and 1.iii, Har collects and uses the caller's identification, including the mobile phone number, as part of its authentication. Ex-1003, ¶176.

Thus, in the context of the Har/Miller authentication server, because the focus of that system is security verification within the context of telephone calls (as detailed in element 1.ii), it would be obvious to use the phone number associated with the caller device as one minutia within Miller's scoring system and/or that the phone number itself is considered as being "valid" based upon the information (including minutia) assessed to authenticate the communication. Ex-1003, ¶176. Miller uses "at least one type of minutia" in its authentication system. Ex-1022, [0014-0016], claims 13, 24. Moreover, Miller describes an iterative process in which there can be sequences of challenges and responses in an effort to increase the score based on various additional minutia. Ex-1022, [0067], [0104], [0113-0120],

[0045]. “Different minutia can be intelligently chosen for the challenge to achieve a response that yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation.” Ex-1022, [0040]; Ex-1003, ¶177.

Thus, in one exemplary usage of Har/Miller, the scoring would assess the phone number minutia either as part of the initial scoring or as part of subsequent attempts to increase the score to reflect the validity of the phone number (“particular minutia isolation” as quoted above). This scoring could, if needed, be supplemented by the further challenge/response sequence on other minutia (or combinations of minutia) including possibly the caller device’s phone number. Ex-1003, ¶178.

As detailed in 1.iii, the ’132 patent description of its “scoring” system used an approach very similar to Miller’s in which: (1) different criteria could be combined for the score; and (2) the authentication server could send further requests for additional information to the calling device in an attempt to raise the score. Ex-1001, 9:37-10:24. Ex-1003, ¶179.

Thus, given the overlap between Miller’s scoring determination and the (much later) ’132 patent’s scoring system, and the context in which the Har/Miller system is proposed, the Har/Miller scoring system at a minimum renders obvious that the calculated score “*indicat[e]s* a validity of a phone number associated with the caller device.” Ex-1003, ¶180.

e. Claim 13

The method of claim 1, wherein the security determination is risk-based.

Har in view of Miller renders this claim obvious for the same reasons as elements 1(iii), 5, and 12. The '132 patent sparsely references "risk-based" in only two passages. Ex-1001, 2:62, 9:48-57; Ex-1003, ¶181.

Miller's purpose of authentication is to address "risk of particular actions." Ex-1022, [0011], *see also* Ex-1022, [0005], [0009]. Miller's recipient device uses a "SP risk process" which "compares the score against its own risk tables." Ex-1003, ¶182.

Miller's scoring system is based upon "confidence" levels based on "thresholds." Ex-1022, [0040] ("scoring the confidence of a valid response based on the minutia used"), [0030] ("complex confidence scoring"); [0067], [0100-0106]. Moreover, Miller's dynamic and iterative challenge response system allows for evaluation of different criteria to improve those confidence levels. Ex-1022, [0111-0119]. Ex-1003, ¶183.

Given that Har and Miller seek to reduce the risk improper communications by authenticating the caller and/or caller device, the security determinations referenced herein, with their variable confidence scoring applied against variable thresholds in an iterative process either disclose or render obvious, the claimed "risk-based" security determination. Ex-1003, ¶184.

f. Claim 14

The method of claim 1, wherein the device information associated with the caller device is not conveyed to a relying party.

The '132 patent's "relying party" includes a "callee." Ex-1001, 2:59-62, 4:45-49. Moreover, the '132 specification and claims distinguish between a "callee" (apparently a person or entity) and a "callee device" (the recipient device). Ex-1001, 2:66-3:1 ("contact callee 118 (e.g., a bank)), ("presented to the callee"), 12:16 ("callee's device"), 10:53, 14:51, claims 1, 17-19 (all "callee device"). Thus, this claim encompasses not conveying caller device information to a "callee" which encompasses not conveying such information to the entity or the callee device. Ex-1003, ¶185

Har teaches both not conveying to the callee "person" and callee "device." Har's authentication server can send authentication indications to the callee device, and optionally display additional information to the callee. Ex-1004, Abstract, [0002] ("In response to successful validation by the authentication server, the authentication server can send an authentication indication to the device of the user receiving the authentication results. The receiving user's device can display identification information and other (optional) data associated with the first user"), [0002]. Because Har's display teaches that only the "authentication information" is displayed to the user and the other data is "optional," Har discloses or renders

obvious that the “device identification” is not conveyed to the person. Har’s disclosure does not mandate that such device information be conveyed and thus encompasses not conveying the device information. Moreover, Har consistently notes that that Har’s called device “can display” information to the callee (person). Ex-1004, [0028], [0032], [0035]. The use of “can” denotes an optional display and encompasses not displaying (conveying) such information to the user. Ex-1003, ¶186.

Furthermore, Har does not mandate that “device information” be conveyed to the callee’s device – which also meets this claim. Har merely “can send an authentication indication” to the callee device. Ex-1004, Abstract, [0002], [0015], [0027]. The repeated use of “can” does not require the additional information transmitted to the callee device must include the device identification. Ex-1003, ¶187.

Finally, Har teaches a “successful” and a “failure” security determination outcome. When authentication (security determination) fails, Har does not transmit the device information to the callee device. Ex-1004, [0028-0032]. This also meets this claim. Ex-1003, ¶188.

g. Claim 15

The method of claim 1, wherein the device information associated with the caller device comprises at least one of a unique software identifier, a semi-unique software identifier, an

embedded hardware identifier, or a user-added hardware identifier.

The Har/Miller authentication system renders this claim obvious for the same reasons as 1.ii, 1.iii and 3. The '132 patent references these claim terms in passing. Ex-1001, 9:30-37; Ex-1003, ¶189.

Har's "system ... supports authentication of mobile devices." Ex-1004, [0044]. As detailed in 1.ii, 1.iii and 3, Miller's DKCP receives a wide variety of computer minutia (both in registration and for authentication sequences) including (1) "a circuit manufacturer's ID number which may be readable from a circuit chip element of the computing device" or "memory reads, ...clock and other counters, and date" (*embedded hardware identifier*); (2) "which firmware and software codes are installed on the computing device and characteristics such as what particular version or release date of firmware or software are installed on the computing device" or "name of the firmware vendor, version number, revision number, revision date, ..., and operating system [and] ... application name, ... software release number" (*unique [or] semi-unique software identifier*). Ex-1022, [0031], [0052]. Miller's "[h]ardware minutia values typically cannot change without changing a physical component of the computer" which teaches or renders obvious the "embedded hardware identifier." Ex-1022, [0052]; Ex-1003, ¶190.

Thus, at a minimum, the Har/Miller authentication server discloses or renders obvious this claim. Ex-1003, ¶191.

h. Claim 16

The method of claim 1, wherein the result of the security determination is transmitted to a relying party.

The Har/Miller authentication system discloses or renders obvious this claim for the reasons detailed in 1(iv) and 14. Ex-1003, ¶192.

i. Claim 17

The method of claim 1, wherein transmitting the notification using the cellular network comprises conveying an assurance to the callee device or conveying a failure to confirm the call.

The Har/Miller authentication system discloses or renders obvious this claim for the reasons detailed in 1(iv) and 14. Ex-1003, ¶193.

j. Claim 18

The method of claim 1, wherein transmitting the notification using the cellular network comprises conveying caller identification information to the callee device.

The Har/Miller authentication system discloses or renders obvious this claim for the reasons detailed in 1(iv) and 14. Ex-1003, ¶194.

k. Claim 19

The method of claim 1, wherein transmitting the notification using the cellular network causes a visual indication of the result of the security determination to be displayed on the callee device.

The Har/Miller authentication system discloses or renders obvious this claim for the reasons detailed in 1(iv) and 14. Har's callee device displays the

“authentication information” after a successful authentication. Ex-1004, Abstract, [0002], [0028-0035], claims 8-10; Ex-1003, ¶195.

B. Ground 2: Claims 2 and 9 are Obvious over Ground 1 in further view of French.

Claims 2 and 9 recite merely the well-known implementation of computer operations being specified by a “policy” or “rule.” As detailed in Ground 1, Miller and Har implement both “policies” and “rules” without using those terminologies. Ex-1003, ¶196.

If PO argues that the specific name of a “policy” or “rule” is required for these claims, French uses the term “policy” and “rule” to describe its intelligent authentication processing specific to particular requests. Ex-1003, ¶197.

1. French

French teaches encryption algorithms for device authentication implemented using the well-known constructs of “policies” and “rules.” Ex-1021, Abstract, [0121-0130]. French teaches an “encryption server” that evaluates a “request” and “then processes the request(s) by determining the appropriate encryption policy.” Ex-1021, [0056]; Ex-1003, ¶198.

2. Detailed Application of Ground 2

a. Claim 2

The method of claim 1,

French uses “policy” to describe its security determination. French uses a particular, selected “encryption policy” for authentication requests. Ex-1021, Abstraction, [0015-0016]. French selects a particular “key” based upon policies. Ex-1021, [0045-0056], [0329-0369]; Ex-1003, ¶199.

As detailed for Ground 1, Miller uses “intelligent” selection of minutia and uses encryption algorithms applied to those minutia to generate device-specific “keys” for authentication. Element 1.ii, 1.iii (citing, e.g., Ex-1022, [0063-0070]). It would be an obvious implementation of Miller to use the term “encryption policy” to characterize this processing. Similarly, as detailed in 1.ii and 1.iii, Har’s authentication server performs encryption/decryption of the authentication request and may use different algorithms. Ex-1003, ¶200

Moreover, a POSA would have a motivation to combine Miller (and/or Har) and French’s terminology with a reasonable expectation of success. French’s system uses a “cryptographic server for processing the requests and determining, for each request, an encryption policy to be applied.” Miller’s DKCP is such a server which receives requests for authentication and selects particular minutia and encryption algorithms to generate an encryption key for that request. Har’s authentication server is similarly characterized as “third party trusted server” which validates based upon encryption techniques. French supplies the implementation of Miller and Har

using the nomenclature of “policies” (which the ‘132 patent does not define and sparsely references). Ex-1003, ¶201.

b. Claim 9

The method of claim 1

As detailed in Ground 1, Har and Miller both perform security determinations based upon execution of a rule. If PO argues that there must be specific reference to the term “rule,” then French supplies it. French characterizes its authentication processing as “permission rules” and “format rules” to specify how permissions and formats for encryption are defined. Ex-1021, [0121-0134]. Both Miller and Har (as detailed in 1.ii and 1.iii) specify permissions and formats for their encryption processing. Thus, French merely confirms that a POSA would understand that the processing in Miller and Har corresponds to the name of a “rule.” Ex-1003, ¶202.

VIII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER *FINTIV*

In *Apple Inc. v. Fintiv, Inc.*, the Board set forth six non-dispositive factors to guide whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued interim procedure regarding application of the *Fintiv* factors (Interim Guidance) stating that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* [] when a petition presents compelling evidence of unpatentability.” USPTO Memorandum, Interim Procedure for Discretionary

Denials in AIA PostGrant Proceedings with Parallel District Court Litigation (June 21, 2022), at 9.

Here, the Petition is particularly strong and presents compelling evidence of the Challenged Claims' unpatentability. Specifically, the Petition explains how the prior art renders the Challenged Claims obvious – including by explicit teaching of the elements that purported to provide novelty during prosecution. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable. Thus, under the Interim Guidance, the Board should not deny institution.

Likewise, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) (precedential as to § II.A) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed in the District Court Litigation (§VIII.B). *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the earliest scheduled trial date has been set for October 20, 2025. Further, a Final Written Decision in this matter is expected in or around July, 2026. Because much can change in trial schedules, the current trial date does not

support denial. *Dish Network v. Broadband iTV*, IPR2020-01280, Paper 17 at 16 (PTAB Feb. 4, 2021).

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties will not begin claim construction briefing until February 28, 2025. EX-1008, at 6. The *Markman* hearing is not until April 30, 2025. EX-1008, at 6. Fact discovery closes in May 9, 2025, and expert discovery closes in July 3, 2025. EX-1008, at 5; see *PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021).

Under factor 4, there will not be any overlap in the issues raised in the IPR and in the co-pending litigation. If the Board institutes IPR, Petitioners stipulate to not raising in the Related litigations any grounds that use the same combination of references herein. Furthermore, although Petitioners challenge here all claims asserted in the co-pending litigation, PO has asserted 70 claims from 3 patents in Related Litigations (Ex-1016 at 3) – an amount that far exceeds the number of claims that the district court will allow at trial. See <https://txed.uscourts.gov/?q=model-order-focusing-patent-claims-and-prior-art-reduce-costs>. Given that the PO will likely be limited to only five claims from the '132 Patent (at most), it is highly unlikely the district court addresses all Challenged Claims.

Under factor 5, while Petitioners are defendants in District Court, nothing within *Fintiv* suggests that the same parties between the proceedings weighs in favor

of discretionary denial. *See HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 at 9 (Jan. 14, 2021).

Under factor 6, other circumstances weigh in favor of institution. The Petition demonstrates compelling merits of invalidity. Miller teaches the same architecture and the same functionality to achieve the same result of device verification as claimed in the '132 Patent. As discussed *supra*, the Examiner found most features in the prior art, but did not consider the prior art identified herein, which discloses or suggests precisely what the Examiner found lacking in the prior art. The Examiner would not have allowed the application over the prior art relied upon herein.

When viewed holistically, the timing of the present Petition is reasonable, there has been relatively limited investment in the EDTX litigation, and there is likely to be minimal overlap between the present IPR and the parallel litigation. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

IX. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioners are AT&T Services Inc., Cellco Partnership D/B/A Verizon Wireless, and Nokia Of America Corporation and are the real parties-in-interest. Furthermore, Petitioners identify Microsoft Corporation, AT&T Mobility II LLC,

AT&T Enterprises, LLC f/k/a AT&T Corp., AT&T Mobility LLC, Verizon Business Network Services LLC f/k/a Verizon Business Network Services, Inc., TracFone Wireless, Inc. and Verizon Corporate Services Group Inc. as a real-party-in-interest.

Out of an abundance of caution, Petitioners identify all current defendants in the below identified cases as potential real parties in interest only for the purpose of this proceeding and only to the extent that Patent Owner contends that these separate legal entities should be named real parties in interest in this IPR. Petitioners do so to avoid the potential expenditure of resources to resolve such a challenge. Petitioners also acknowledge that each petitioner has a number of affiliates. No unnamed entity is funding, controlling, or otherwise has an opportunity to control or direct this Petition or Petitioners' participation in any resulting IPR. Petitioners are also not aware of any affiliate that would be barred from filing this Petition under 35 U.S.C. § 315(e)

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '132 Patent is asserted against Petitioners in *RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.*, No. 2:24-cv-00091 (E.D. Tex.) filed February 9, 2024 and *RightQuestion, LLC v. AT&T Inc. et al.*, 2:24-cv-00094 (E.D. Tex.) filed February 12, 2024.

To Petitioners’ knowledge, as of the date of this filing, the ’132 Patent was not involved in any additional cases that may be affected by a decision in this proceeding.

Concurrent with this Petition, Petitioners also file Petitions for Inter Partes Review of U.S. Patents 10,674,009 and 11,005,989 which are related to the ’132 Patent and have substantial overlap in the claim language. See IPR2025-00360; IPR2025-00362.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

LEAD COUNSEL	BACK-UP COUNSEL
Patrick D. McPherson, USPTO Reg. No. 46,255 DUANE MORRIS LLP 901 New York Avenue N.W., Suite 700 East Washington, DC 20001 P: (202) 776-7800 F: (202) 776-7801 PDMcPherson@duanemorris.com	Glenn D. Richeson Reg. No. 73,780 GDRicheson@duanemorris.com DUANE MORRIS LLP 1075 Peachtree Street NE, Suite 1700 Atlanta, GA 30309-3929 P: (404) 253-6998 F: (404) 759-2703
	Brian H. Pandya Reg. No. 60,991 BHPandya@duanemorris.com DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20004 P: (202) 776-7807 F: (202) 776-7801
	Kevin Anderson Reg. No. 43,471 KPAnderson@duanemorris.com

	DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20004 P: (202) 776-5213 F: (202) 776-7801
--	---

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Service via hand-delivery may be made at the postal mailing address of either lead or back-up counsel. Petitioners consent to service by e-mail at the addresses listed above.

X. CONCLUSION

Petitioners request the Board institute IPR and cancel all Challenged Claims.

Respectfully submitted,

/Kevin P. Anderson/

Kevin P. Anderson, USPTO Reg. No. 43,471
kpanderson@duanemorris.com

ATTORNEY FOR PETITIONERS

February 7, 2025

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the 7th of February, 2025, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 11,856,132 and all supporting exhibits were served by electronic means by agreement with Patent Owner to:

34060 - MICHAEL N. HAYNES
P.O. Box 460
RUCKERSVILLE, VA 22968
UNITED STATES

Service copies are also being sent via email to litigation counsel of record:

Robert F. Kramer
CA Bar No. 181706 (Admitted E.D. Texas)
rkramer@krameralberti.com
David Alberti
CA Bar No. 220265 (Admitted E.D. Texas)
dalberti@krameralberti.com
Sal Lim
CA Bar No. 211836 (Admitted E.D. Texas)
slim@krameralberti.com
Russell S. Tonkovich
CA Bar No. 233280 (Admitted E.D. Texas)
rtonkovich@krameralberti.com
Robert Mattson (pro hac vice)
Virginia Bar No. 43568
rmattson@krameralberti.com
Michele Woodruff Lyons
CA Bar No. 234891 (pro hac vice)
mlyons@krameralberti.com
Jeremiah A. Armstrong
CA Bar No. 253705 (pro hac vice)
jarmstrong@krameralberti.com
KRAMER ALBERTI LIM
& TONKOVICH LLP
577 Airport Blvd., Suite 250

Burlingame, CA 94010
Telephone: (650) 825-4300
Facsimile: (650) 460-8443

Nicole Glauser
Texas State Bar No. 24050694
nglauser@krameralberti.com
KRAMER ALBERTI LIM
& TONKOVICH LLP
500 W 2nd Street, Suite 1900
Austin, Texas 78701
Telephone: (737) 256-7784
Facsimile: (650) 460-8443

Andrea Fair
andrea@wsfirm.com
Ward, Smith & Hill, PLLC
1507 Bill Owens Parkway
Longview, TX 75604
(903) 757-6400
(903) 757-2323

/Kevin P. Anderson/
Kevin P. Anderson, Reg. No. 43,471
901 New York Avenue, N.W.
Suite 700 East
Washington, D.C. 20001
P: (202) 776-7800
F: (202) 776-7801
kpanderson@duanemorris.com

ATTORNEY FOR PETITIONERS

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 13,852 words as calculated by the “Word Count” feature of Microsoft Word 2010, the word processing program used to create it.

Dated: February 7, 2025

By: Kevin P. Anderson
Kevin P. Anderson
Reg. No. 43,471
Duane Morris LLP
901 New York Avenue, N.W.,
Suite 700 East
Washington D.C., 20001
P: (202) 776-7800
F: (202) 776-7801
kpanderson@duanemorris.com