

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner.

Case No. IPR2026-00099
Patent No. 8,116,749

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 et seq**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	STANDING CERTIFICATION.....	4
III.	UNPATENTABILITY GROUNDS.....	4
IV.	'749 PATENT.....	6
	A. Background.....	6
	B. Prosecution History	8
	C. PTAB History.....	8
	D. POSITA	9
V.	CLAIM INTERPRETATION	9
	A. Non-limiting Statements of Purpose	10
	B. Contingent Limitations.....	11
VI.	GROUND 1: BUCUK ANTICIPATES AND/OR RENDERS OBVIOUS CLAIMS 1-3, 13, AND 17-20.....	11
	A. Bucuk.....	11
	B. Anticipation and Obviousness.....	13
	C. Claim Mappings	15
	1. Claim 1	15
	a. [1.PRE] “A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:”.....	15
	b. [1.A.I] “at the first wireless device, providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices,”	17
	c. [1.A.II] “wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and”.....	19

d.	[1.A.III] “wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;”	20
e.	[1.B.I] “at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server,”	21
f.	[1.B.II] “within a specific application on the second wireless device,”	22
g.	[1.B.III] “providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information,”	23
h.	[1.C] “at the first wireless device, collecting said modified identification information.”	24
2.	Claim 2: “[Claim 1] wherein the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.”	25
3.	Claim 3: “[Claim 1] wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”	26
a.	Interpretation	26
b.	Mapping	27
4.	Claim 13: “[Claim 1] wherein the user or entity identification information is changed to protect the privacy of the identity of the a [<i>sic</i>] user or entity associated with the second wireless device.”	28
a.	Interpretation	28
b.	Mapping	28
5.	Claim 17: “[Claim 1] wherein the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device.”	29

6. Claim 18: “[Claim 1] wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”	29
a. Interpretation	29
b. Mapping	30
7. Claim 19: “[Claim 17] wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.”	30
a. Interpretation	30
b. Mapping	30
8. Claim 20: “[Claim 17] wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”	31
a. Interpretation	31
b. Mapping	31
VII. GROUND 2: BUCUK IN VIEW OF NORDMAN RENDERS	
OBVIOUS CLAIMS 1-3, 7-9, 13, 15, AND 17-26	32
A. Bucuk	32
B. Nordman	33
C. Motivation to Combine	34
D. Claim Mappings	37
1. Claim 1	37
a. [1.PRE]	37
b. [1.A.I]	38
c. [1.A.II]	39
d. [1.A.III]	40
e. [1.B.I]	40
f. [1.B.II]	41

g.	[1.B.III]	41
h.	[1.C]	42
2.	Claim 2	42
3.	Claim 3	43
a.	Interpretation	43
b.	Mapping	44
4.	Claim 7	45
a.	[7.PRE] “A server for exchanging information between one or more applications executing on at least two wireless devices, the server comprising:”	45
b.	[7.A.I] “a receiver, for receiving initial identification information having been collected by a first wireless device from a second wireless device via a, first, direct, short range local wireless link between the first and second wireless devices,”	46
c.	[7.A.II] “wherein the initial identification information is associated at the server with an identity of a user or entity associated with the second wireless device, and”	46
d.	[7.A.III] “wherein the initial identification information is received by the server from the first wireless device over a second wireless link distinct from the first wireless link; and”	46
e.	[7.B.I] “a transmitter for, upon an occurrence of a predetermined event coordinated with the second wireless device,”	47
f.	[7.B.II] “sending a message to the second wireless device to change the identification information within a specific application on the second wireless device and”	47
g.	[7.B.III] “for subsequently providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, and”	48
h.	[7.B.IV] “such that the modified identification information is associated at the server with said identity of a user or entity associated with the second device.”	48

5. Claim 8: “[Claim 7] wherein the predetermined event is one or more of: an elapsed time; and/or a number of uses of the identifier; and/or a step in a process.”	48
6. Claim 9: “[Claim 7] wherein the change of user or entity identification information is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”	49
7. Claim 13	49
a. Interpretation	49
b. Mapping	49
8. Claim 15: “[Claim 7] wherein the user or entity identification information is changed to protect the privacy of the identity of a user or entity associated with the second wireless device.”	49
9. Claim 17	49
10. Claim 18	51
a. Interpretation	51
b. Mapping	51
11. Claim 19	52
a. Interpretation	52
b. Mapping	52
12. Claim 20	55
a. Interpretation	55
b. Mapping	55
13. Claims 21/26: “The [method of claim 1][server of claim 7] wherein upon the [occurrence] of the predetermined event, [the server] further [notifies][notifying] the second wireless device of the modified identification information via a wireless configuration message or an instruction to change communication state.”	57
14. Claim 22: “[Claim 7] wherein the central server further receives modified identification information, as collected by the first wireless device from the second wireless device.”	58

15. Claim 23: “[Claim 7] wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”	58
16. Claim 24: “[Claim 23] wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.”	58
17. Claim 25: “[Claim 7] wherein the modified identification information is used by the central server to verify legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”	58
VIII. GROUND 3: BUCUK IN VIEW OF NORDMAN AND KALLIO RENDERS OBVIOUS CLAIMS 4-6 AND 10-12.....	58
A. Kallio and Motivation to Combine.....	58
B. Claim Mappings	61
1. Claim 4: “[Claim 1] further comprising: at said second wireless device, receiving a user or entity identifier from a central server, the user or entity identifier taken from a pool of identifiers determined by the central server.”	61
a. Interpretation.....	61
b. Mapping	62
2. Claims 5/11: “The [method of claim 1][server of claim 7] further comprising: [using] an identity manager [within a server][,] to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link [to said second wireless device;][,] and wherein the user [or entity] identifiers are changed over time.”	63
3. Claims 6/12: “The [method of claim 5][server of claim 11] wherein [at least one of] the user or entity identifiers are associated with a device identifier by the identity manager, [and the device identifier is associated with one or more of the initial identification information or modified identification information,] and [wherein] the device identifier is [selected from] one [or more] of: a media access control (MAC) [device]	

[address][addresses] of a short range wireless network adapter; a SSID in an IEEE-802.11 network beacon; a BSSID of an IEEE802.11 network adapter; a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message; a device name in a Bluetooth name response packet; or one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.”.....	64
4. Claim 10: “[Claim 7] further comprising: a receiver, for receiving a user or entity identifier from a central server, the identifier taken from a pool of identifiers determined by the central server.”.....	66
IX. GROUND 4: BUCUK IN VIEW OF NORDMAN AND PERTTILA RENDERS OBVIOUS CLAIMS 14 AND 16	68
A. Interpretation	68
B. Perttola and Motivation to Combine	68
C. Claim Mappings	70
1. Claims 14/16: “The method of [claim 1][claim 7] wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.”.....	70
X. SECONDARY CONSIDERATIONS	72
XI. CONCLUSION.....	73
XII. APPENDIX A: U.S. PATENT NO. 8,116,749 CLAIM LISTING	74

TABLE OF AUTHORITIES

CASES

<i>Apple Inc. v. FastVDO LLC</i> , IPR2016-01203, Paper 39 (Dec. 11, 2017)	27
<i>Bos. Sci. Scimed, Inc. v. Cordis Corp.</i> , 554 F.3d 982 (Fed. Cir. 2009)	15
<i>Ex parte Schulhauser</i> , Appeal 2013-007847 (PTAB April 28, 2016).....	11
<i>Google Inc. v. Spring Ventures Ltd.</i> , IPR2017-01653, Paper 68 (Jan. 15, 2019)	27
<i>K/S HIMPP v. III Holdings 4, LLC</i> , IPR2017-00782, Paper 8 (Jul. 27, 2017)	27
<i>KSR Int’l v. Teleflex</i> , 550 U.S. 398 (2007)	36, 61, 70
<i>Minton v. Nat’l Ass’n of Securities Dealers, Inc.</i> , 336 F.3d 1373 (Fed. Cir. 2003)	11
<i>Net MoneyIN, Inc. v. VeriSign, Inc.</i> , 545 F.3d 1359 (Fed. Cir. 2008)	13
<i>Purdue Pharma L.P. v. Epic Pharma, LLC</i> , 811 F.3d 1345 (Fed. Cir. 2016)	14

OTHER AUTHORITIES

MPEP §2111.04.I.....	11
MPEP §2111.04.II.....	11
MPEP §2144.04.V	45

EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent No. 8,116,749
1002	Prosecution History of U.S. Patent No. 8,116,749
1003	Declaration of Mark R. Lanning
1004	Curriculum Vitae of Mark R. Lanning
1005-1009	[RESERVED]
1010	U.S. Patent Application Publication No. 2002/0131445
1011	U.S. Patent Application Publication No. 2002/0174364 (“Nordman”)
1012	U.S. Patent Application Publication No. 2005/0164717
1013	U.S. Patent Application Publication No. 2006/0165100
1014	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00903, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 8, 2020)
1015	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00903, Paper 31 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1016	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00904, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 8, 2020)
1017	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00904, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1018	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00931, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)
1019	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00931, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1020	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00932, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)
1021	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00932, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1022	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00933, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 15, 2020)
1023	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00933, Paper 30 (Final Written Decision) (P.T.A.B Nov. 8, 2021)
1024	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00934, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 27, 2020)
1025	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00934, Paper 31 (Final Written Decision) (P.T.A.B Nov. 30, 2021)

Exhibit	Description
1026	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00977, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B May 27, 2020)
1027	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00977, Paper 31 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1028	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B. June 1, 2020)
1029	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 10 (Decision Denying Institution) (P.T.A.B. Dec. 4, 2020)
1030	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00979, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B. June 1, 2020)
1031	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00979, Paper 33 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1032	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00980, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B June 1, 2020)
1033	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00980, Paper 32 (Final Written Decision) (P.T.A.B Nov. 30, 2021)
1034	<i>Target Corporation v. Proxicom Wireless, LLC</i> , Nos. 2022-1282, 2022-1283, 2022-1338, 2022-1339, 2023 U.S. App. LEXIS 24861 (Fed. Cir. Sep. 20, 2023) (nonprecedential)
1035-1036	[RESERVED]
1037	U.S. Patent Application Publication No. 2004/0243519 (“Perttila”)
1038-1046	[RESERVED]
1047	U.S. Patent Application Publication No. 2003/0224756 (“Kallio”)
1048	<i>Secure Communication Technologies LLC v. Google LLC</i> , 1:25-cv-01207, Dkt. 11-7 (W.D. Tex. Sep 8, 2025) (Amended Complaint, Exhibit 7)
1049	<i>Proxicom Wireless, LLC v. Macy's, Inc.</i> , 6:18-cv-00064, Dkt. 49 (M.D. Fla. Aug. 10, 2018) (Joint Claim Construction Statement)
1050	<i>Proxicom Wireless, LLC v. Macy's, Inc.</i> , 6:18-cv-00064, Dkt. 94 (M.D. Fla. Feb. 12, 2019) (Order in re Claim Constructions)
1051	U.S. Patent Application Publication No. 2010/0274859 (“Bucuk”)
1052	U.S. Patent Application Publication No. 2009/0028082
1053	U.S. Patent No. 9,305,119
1054	U.S. Patent Application Publication No. 2005/0204309

MANDATORY NOTICES

A. Real Party-In-Interest

Petitioner Google LLC¹ is a real party-in-interest to this proceeding under 37 C.F.R. §42.8(b)(1).

B. Related Matters

A decision in this proceeding could affect or be affected by the following.

1. United States Patent & Trademark Office

U.S. Patent No. 8,116,749 issued from application no. 12/364,938, filed 2009-02-03, and claims priority to the following applications:

Application No.	Filing Date
61/095,359	2008-09-09
61/095,001	2008-09-08

No patent applications claim priority to U.S. Patent No. 8,116,749 and application no. 12/364,938.

Petitioner recently filed petitions for *inter partes* review of U.S. Patent Nos. 11,687,971 (application 17/942,197; IPR2025-01183), 11,443,344 (application 17/366,826; IPR2025-01182), 11,344,918 (application 15/271,410; IPR2025-

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

01181), and 11,995,685 (18/204,528; IPR2026-00098)—patents which claim priority to the same provisional applications—and recommends assigning this case to the same panel.

2. United States District Court

a. Western District of Texas

Secure Communication Technologies, LLC. v. Google LLC, No. 1:25-cv-01207 (W.D. Tex.), filed 2025-08-04. U.S. Patent No. 8,116,749 was added to this district court case in an amended complaint filed 2025-09-08.

C. Counsel and Service Information - §§42.8(b)(3) and (4)

Lead Counsel	Scott A. McKeown, Reg. No. 42,866
Backup Counsel	Libbie A. DiMarco (<i>pro hac vice</i> forthcoming) Victor Cheung, Reg. No. 66,229
Service Information	<p><u>E-mail</u>: SMcKeown-PTAB@wolfgreenfield.com Elizabeth.DiMarco@WolfGreenfield.com VCheung-PTAB@wolfgreenfield.com</p> <p><u>Post and hand delivery</u>: WOLF, GREENFIELD & SACKS, P.C. 600 Atlantic Avenue Boston, MA 02210-2206</p> <p><u>Telephone</u>: 617-646-8000 <u>Facsimile</u>: 617-646-8646</p>

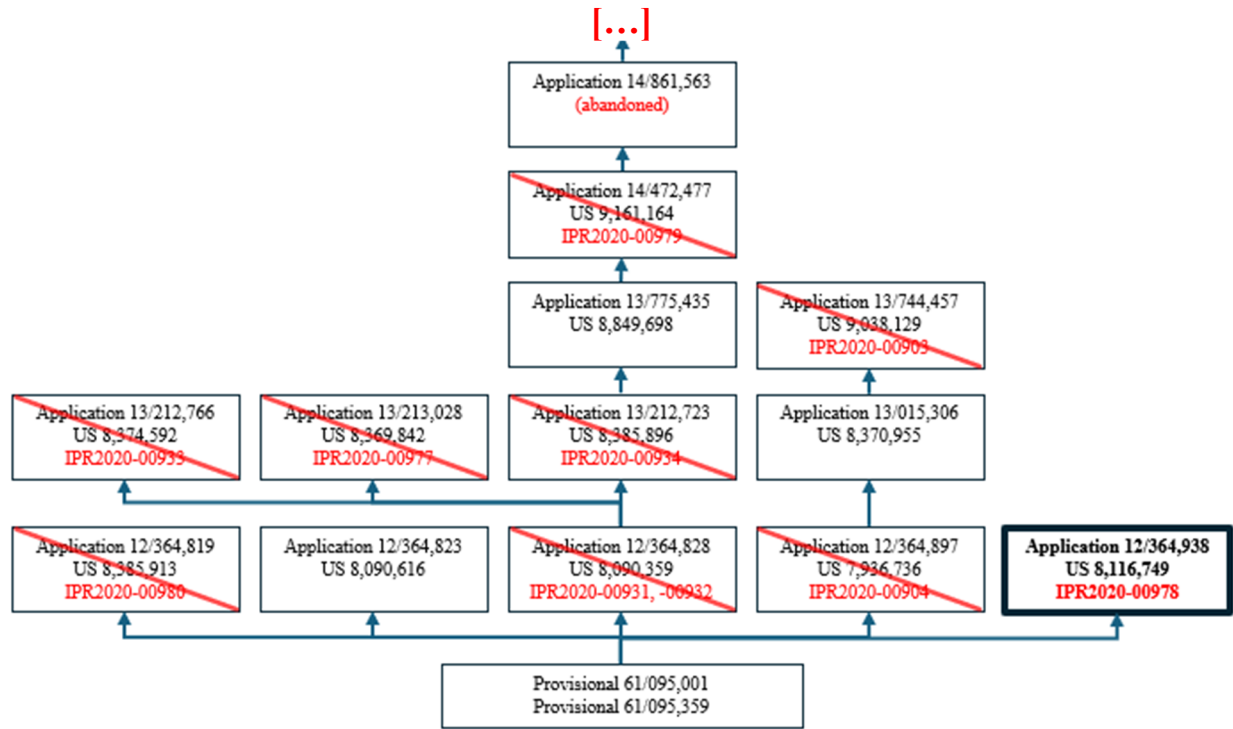
A power of attorney is submitted with the Petition. Counsel for Petitioner consents to service of all documents via electronic mail.

Petitioner requests *inter partes* review (IPR) and cancellation of claims 1-26 (“Challenged Claims”) of U.S. Patent No. 8,116,749 (EX1001, the “’749”).

I. INTRODUCTION

The ’749 is directed to a mobile communication architecture for “facilitating the exchange of information” between two wireless devices, each device employing short-range communication (*e.g.*, Bluetooth) and long-range communication (*e.g.*, cellular) wireless capabilities. EX1001, 2:8-4:57. A first device may detect an identifier transmitted from a second device in short-range proximity and send information identifying the second device to a server via long-range communications. EX1001, 2:55-3:11, 7:16-25, 7:48-58. Based on policy information stored at the server, the server may alert the first device to the second device’s presence with, *e.g.*, the second device’s contact information. EX1001, 3:12-18, 7:64-8:4, 8:31-49, 8:50-64.

This architecture of exchanging information between nearby devices and servers was claimed in other patents within the ’749’s family (none are direct continuations but claim priority to the same provisional applications) and previously cancelled by the PTAB as known in the art (*see* diagram below; all previous IPRs were requested by an unrelated third party).



IPR was also previously requested for the '749 by a different petitioner, but trial was not instituted because of petitioner-specific presentation deficiencies in its chosen art, which are not relevant to the new prior art and grounds at issue here. For example, the Board faulted that petitioner for failing to address the claimed “predetermined event” with respect to its prior art, Mgrdechian. EX1029, 15. The Board further found that the petitioner did not “support adequately” that Mgrdechian’s “dynamic or pseudo-random” IDs met limitations requiring IDs to change. EX1029, 16. Finally, the Board faulted the petitioner for failing to establish a motivation to combine Mgrdechian and its other prior art, Kulakowski. EX1029, 19-20. These deficiencies in the other petitioner’s presentation are not representative of the state of the art prior to the '749—predetermined events and

changing identifiers were well known and in no way innovative concepts in wireless systems.

A predetermined event that triggers another function amounts to little more than *cause and effect*, and the practice of changing identifiers was well-known as a basic privacy/security measure. Bucuk is shown below to **anticipate** the method claims of the '749, illustrating an embodiment that discloses the same predetermined events and changing identifiers as claimed. Other embodiments render the same concepts obvious in view of Nordman (EX1011), which describes several types of predetermined events for changing identifiers (*e.g.*, based on time, use, and location). The fact that the previous petitioner did not identify these known features expressly described in their chosen prior art—different from Bucuk and Nordman cited in this petition—does not establish the patentability of the '749 claims. The state of the prior art, as reflected in the other patent family IPR trials after denial of the prior '749 IPR petition, have led to the cancellation of similar broad device-server information exchange architectures. The '749 claims should follow suit and be similarly cancelled.

Ground 1 explains how Bucuk (EX1051) anticipates method claims 1-3, 13, and 17-20 using a short-range/long-range architecture, including modifying identifiers based on predetermined events.

Ground 2 explains how Bucuk in view of Nordman (EX1011) renders obvious method and server claims 1-3, 7-9, 13, 15, and 17-26 using a short-range/long-range architecture, including modifying identifiers based on predetermined events such as elapsed times.

Ground 3 explains how Kallio (EX1047) further renders obvious dependent claims 4-6 and 10-12 reciting server-specific features, such as a pool of identifiers.

Ground 4 explains how Perttila (EX1037) further renders obvious dependent claims 14 and 16 reciting intended results of systems that use identifiers.

Accordingly, Petitioner requests that the Board institute IPR and cancel the Challenged Claims.

II. STANDING CERTIFICATION

Petitioner certifies that the '749 is available for IPR and that Petitioner is neither barred nor estopped from requesting IPR of the Challenged Claims. 37 C.F.R. §42.104(a).

III. UNPATENTABILITY GROUNDS

The Challenged Claims are unpatentable as follows:

Ground	References	Claims	Pre-AIA Basis
1	Bucuk	1-3, 13, 17-20	§102/103
2	Bucuk in view of Nordman	1-3, 7-9, 13, 15, 17-26	§103
3	Bucuk in view of Nordman and Kallio	4-6, 10-12	
4	Bucuk in view of Nordman and Perttila	14, 16	

The '749's earliest possible effective filing date is 2008-09-08. EX1001, code (60). Each relied-upon reference is pre-AIA §102(b) and/or (e) prior art even under the earliest 2008 filing date.

Name	Filing Date	Issue/Publication Date
Bucuk (EX1051)	2008-05-23 (PCT)	2010-10-28
Nordman (EX1011)	2001-05-21	2002-11-21
Kallio (EX1047)	2002-05-30	2003-12-04
Perttila (EX1037)	2003-06-02	2004-12-02

The Declaration of Mark R. Lanning (EX1003, ¶¶1-230; "Lanning") describes the prior art's scope and content at the time of the '749.

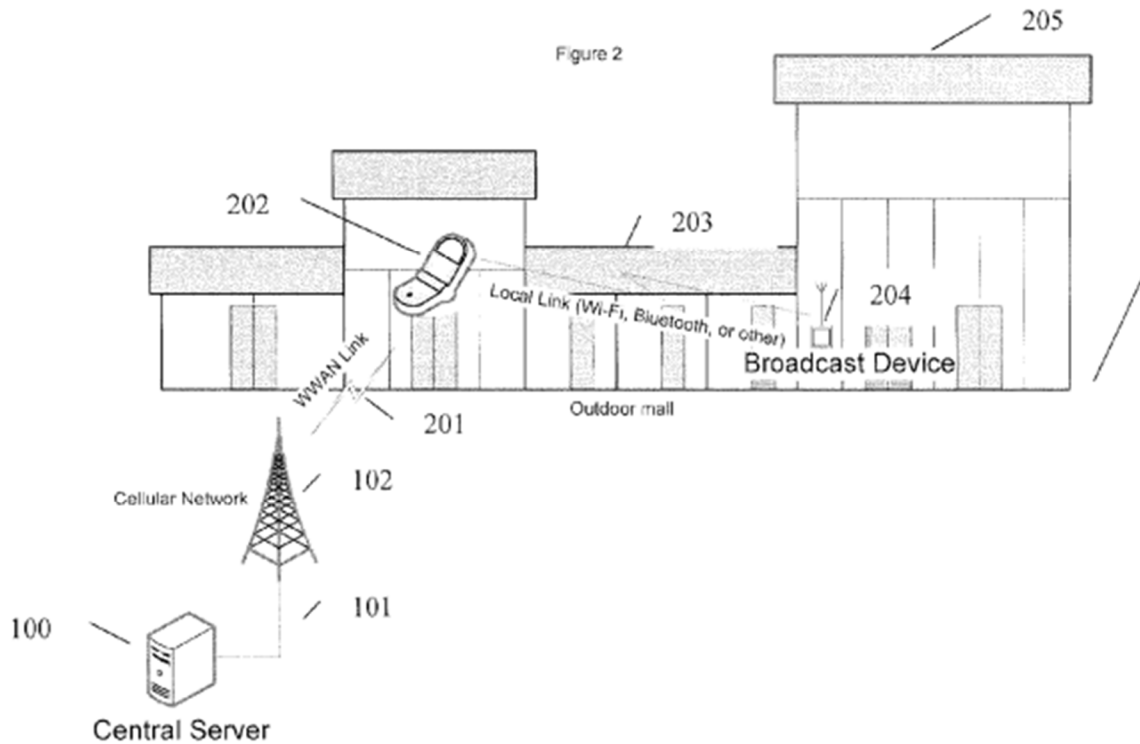
IV. '749 PATENT²

A. Background

The '749 is directed to the exchange of information between two wireless devices using short-range communications (*e.g.*, Bluetooth/Wi-Fi), with the aid of a remote server using long-range communications (*e.g.*, cellular). EX1001, 2:8-4:57.

Fig. 2 (below) shows one implementation with devices 202 and 204 in short-range communication, and device 202 and server 100 in long-range communication. EX1001, 7:16-25.

² Unless otherwise noted, all emphasis in the Petition (including figure annotations) is added.



Device 204 is a device associated with a museum exhibit that “transmits identifying information [to device 202] using short range wireless link 203,” which device 202 “passes... to the central server 100,” and the server 100 recognizes the identifying information as being associated with device 204. EX1001, 7:20-37. The server uses stored account settings or policy information to determine “what information and under which situations information may be disclosed to another device or user” to facilitate further short-range communications. EX1001, 4:28-45, 8:50-64, 15:33-43.

A server may assign device identifiers to devices, and assignment may occur, *e.g.*, at regular intervals or random time periods. EX1001, 16:58-17:17.

Lanning, ¶¶39-43.

B. Prosecution History

The Examiner's first actions rejected claims over prior art Birch (US 7,213,742), Fraser (US 6,629,149), and Ramer (US 2008/0214166). EX1002, 91-98, 145-157.

Applicant submitted significant amendments to the claims—adding or redefining wireless devices, identification information, wireless links, and specific information communicated with servers. EX1002, 182-193. The Examiner allowed some claims but rejected others that Applicant promptly cancelled. EX1002, 210-219, 239-246.

The Examiner issued a Notice of Allowance and identified, as reasons for allowance, limitations directed to a first device providing a server with initial identification information and modified identification over a second wireless link, the identification information having been provided by a second device over a first short-range wireless link. EX1002, 267-268. Lanning, ¶¶44-47.

C. PTAB History

The '749 was previously the subject of a petition for IPR, by an unrelated party sued years prior, in IPR2020-00978 (EX1028), which relied on prior art Mgrdechian (US 7,545,784) and Kulakowski (WO 2007/084973) that is entirely different from the art presented here. EX1028, 12. That IPR was not instituted

because of weaknesses the PTAB identified in that petition's prior art. *See* §I. Lanning, ¶¶48-50.

D. POSITA

On 2008-09-08, a person having ordinary skill in the art ("POSITA") would have had a Bachelor's degree in electrical or computer engineering, or a related field, with approximately 3-5 years of experience in wireless communications.³ A higher level of education may substitute for less experience. Lanning, ¶¶52-54.

V. CLAIM INTERPRETATION

Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. §282(b), in accordance with the ordinary and customary meaning as understood by a POSITA and the patent's prosecution history. 37 C.F.R. §42.100(b). In addition to the below remarks regarding the interpretation of intended results and contingent processes, which are nevertheless anticipated and/or rendered obvious by the prior art as discussed below, other minor issues in claims 3-4 and 16 are discussed in their respective mappings. §VI.C.3-4, §VII.D.3, §VIII.B.1, §IX.C.1. No other constructions are required at this time because the claims are unpatentable under any reasonable construction as detailed below.

³ This same level was adopted in prior proceedings in the '749 family and is now fixed by operation of estoppel. EX1019, 8-9.

A. Non-limiting Statements of Purpose

Claims 13-14, 16, 19-20, and 24-25 each include language reciting an intended purpose that carries no patentable weight. For example:

- Claim 13: identification information is changed “to protect the privacy of the identity of the a [*sic*] user or entity.”
- Claims 14 and 16: identification information is changed “to provide for a confirmation of the identification information...” or “provide a validation of the legitimacy of” devices and applications.
- Claims 19 and 24: identification information is used “to verify the legitimacy, identity or authenticity” of the first device.
- Claims 20 and 25: identification information is used “to verify the legitimacy, validity, or authenticity of a transaction.”

None of these claim limitations recite steps or appropriately claimed functionality, nor do they articulate any particular manner by which the claimed identification information is changed or utilized to achieve the results of protecting privacy, providing a confirmation/validation, and/or verifying legitimacy/identity/authenticity. Instead, the limitations are merely expressions of the intended results or goals of using the claimed methods or servers, and therefore, these claim limitations are not given any patentable weight. MPEP

§2111.04.I (citing *Minton v. Nat'l Ass'n of Securities Dealers, Inc.*, 336 F.3d 1373, 1381 (Fed. Cir. 2003)).

B. Contingent Limitations

Claims 18 and 23 recite that “if” initial identification information is “re-sent to the central server following said pre-determined event,” a certain result will occur. Because the condition of re-sending the initial information is not required to be performed (*i.e.*, is contingent), the result that follows is not required. As such, this limitation carries no patentable weight. MPEP §2111.04.II; *Ex parte Schulhauser*, Appeal 2013-007847, 8-10 (PTAB April 28, 2016) (“If the condition for performing a contingent step is not satisfied, the performance recited by the step need not be carried out...”).

VI. GROUND 1: BUCUK ANTICIPATES AND/OR RENDERS OBVIOUS CLAIMS 1-3, 13, AND 17-20

A. Bucuk

Bucuk is directed to a system for establishing links between users and devices, through transmission identifiers sent using short-range communications between devices and long-range communications to a server, to facilitate access to data, devices, services, and the like. Bucuk, Abstract, [0001], [0007]-[0011].

An exemplary system including a user device 172 (*e.g.*, a mobile phone), a device 170 to be accessed (*e.g.*, a car), and an authentication server 174 is shown in Fig. 1c (below). Bucuk, [0153]-[0177].

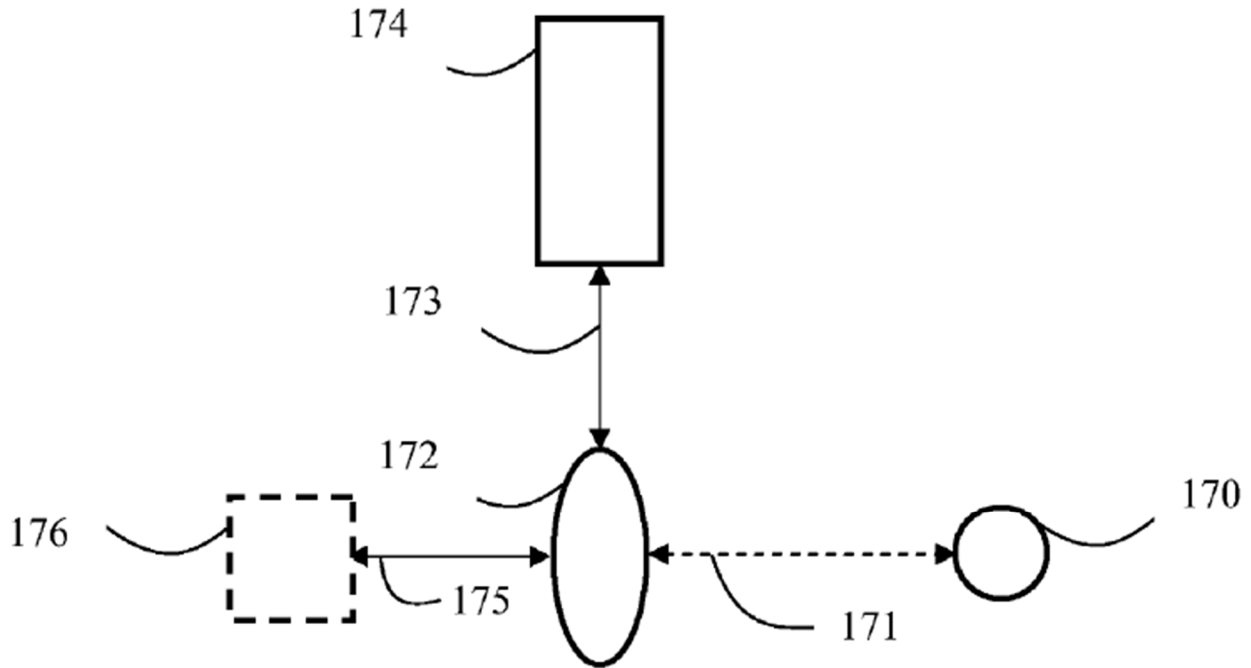


Figure 1c

In this example, phone 172 and car 170 each search for nearby devices and read each other's Bluetooth name. Car 170 reads phone 172's name as "John@1c1c.5c5c" and remains locked (as the phone does not presently have valid unlocking information). Bucuk, [0166]. Phone 172 reads car 170's name as "Car15#2c2c.8c8c" and provides, to authentication server 174, car 170's information (*e.g.*, extracted IP address "2c2c" and device ID "8c8c") as well as information about itself (*e.g.*, IP address "1c1c" and device ID "5c5c"). Bucuk, [0166]-[0167].

The server recognizes an authorized link between the user of device 172 and the entity in control of device 170, and subsequently issues an unlocking key ("1f1f") to phone 172 to unlock car 170. Bucuk, [0164], [0168]-[0169]. Phone 172

changes its own Bluetooth name to incorporate the received number (*e.g.*, to “John@1c1c.1f1f”), which unlocks car 170 when read by car 170. Bucuk, [0169].

Car 170 then changes its identifying information according to a pre-arranged scheme, “effectively guaranteeing only one device ID (unlocking key) at the time can unlock device (170).” Bucuk, [0170]-[0171]. Lanning, ¶¶61-66.

B. Anticipation and Obviousness

Bucuk anticipates claims of the '749. The mappings below primarily rely on the embodiment shown in Fig. 1c of Bucuk with additional details explained in other sections of Bucuk, *e.g.*, from Bucuk’s description of Fig. 1a and other disclosures. A POSITA would have recognized that these additional details and features are necessarily present in the embodiment of Fig. 1c, and thus anticipatory, and are not merely obvious modifications. Lanning, ¶67.

To the extent PO argues that Bucuk does not expressly disclose a single “embodiment” anticipating claims of the '749 because, *e.g.*, Bucuk’s Figs. 1a-1d are each described as “another” embodiment and allegedly distinct, that is incorrect because Bucuk’s “embodiments” are not wholly separate systems to be considered in isolation. *See Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1368-71 (Fed. Cir. 2008) (reference showing limitations arranged or combined in the same way as recited in the claims is anticipatory). For example, Bucuk references the “system mentioned in FIG. 1” or “described in FIG. 1” despite there being no figure “1,”

implying that, despite the variations between Figs. 1a-1d, Figs. 1a-1d are directly related and anticipatory. Bucuk, [0181], [0183]. See *Purdue Pharma L.P. v. Epic Pharma, LLC*, 811 F.3d 1345, 1358-59 (Fed. Cir. 2016) (combination of disclosures in a prior art reference found to anticipate where disclosures were directly related). Indeed, Figs. 1a-1d vary in their broad configurations (*e.g.*, what types of servers are included, what devices have internet access) and not the underlying technologies that are intrinsic to the devices and connections themselves (*e.g.*, the technologies used for the short-range and long-range communications common to each figure). Lanning, ¶68.

For example, the description of Fig. 1c explains that “software” is used to change a device’s Bluetooth name (Bucuk, [0169]), but does not *explicitly* state that “software” is also used to exchange information between devices in short-range proximity (as may be required for [1.PRE]’s recitation of an “exchange of information between one or more applications”). However, a POSITA would have recognized that the devices of Fig. 1c are configured similarly to the devices of Fig. 1a, wherein installed software is executed to exchange identifying information (Bucuk, [0118], [0147]). Therefore, Bucuk’s disclosures are anticipatory. Lanning, ¶69.

Nevertheless, out of an abundance of caution, Bucuk is presented as rendering obvious the same claims under §103. It would have been obvious to a

POSITA to combine these well-known features from, *e.g.*, Figures 1a-d, because Bucuk teaches that “[a]spects of any of the examples... may be combined with aspects of any of the other examples described to form further examples” (Bucuk, [0073], [0310]) and, at the very least, features of Bucuk’s embodiments are all directed to closely related variations of wireless devices in short-range proximity and remote servers. *See Bos. Sci. Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009) (finding claimed invention obvious in view of closely related embodiments within a single prior art reference). Lanning, ¶70.

C. Claim Mappings

1. Claim 1

- a. **[1.PRE] “A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:”**

To the extent this preamble is limiting, Bucuk discloses *a method for exchange of information (e.g., exchanging identification information) between one or more applications executing (e.g., between software executing on devices communicating via Bluetooth) on at least a first wireless device (e.g., phone 172) and a second wireless device (e.g., car 170)*. Lanning, ¶72.

Bucuk discloses devices 170 and 172, shown in Fig. 1c (below), that exchange identification information, such as Bluetooth names and unique IDs (hereinafter “UIDs”), via short-range wireless communications. Bucuk, [0157],

[0162]-[0163], [0166], [0169]; *see also* [0100]-[0108] (examples of UIDs exchanged in short-range communications include device names, device addresses, phone numbers, numbers, strings, and algorithmically changing IDs). Device 172 (a *first wireless device*) and device 170 (a *second wireless device*) are, *e.g.*, a mobile phone 172 and a car 170, respectively. Bucuk, [0153]. Lanning, ¶73.

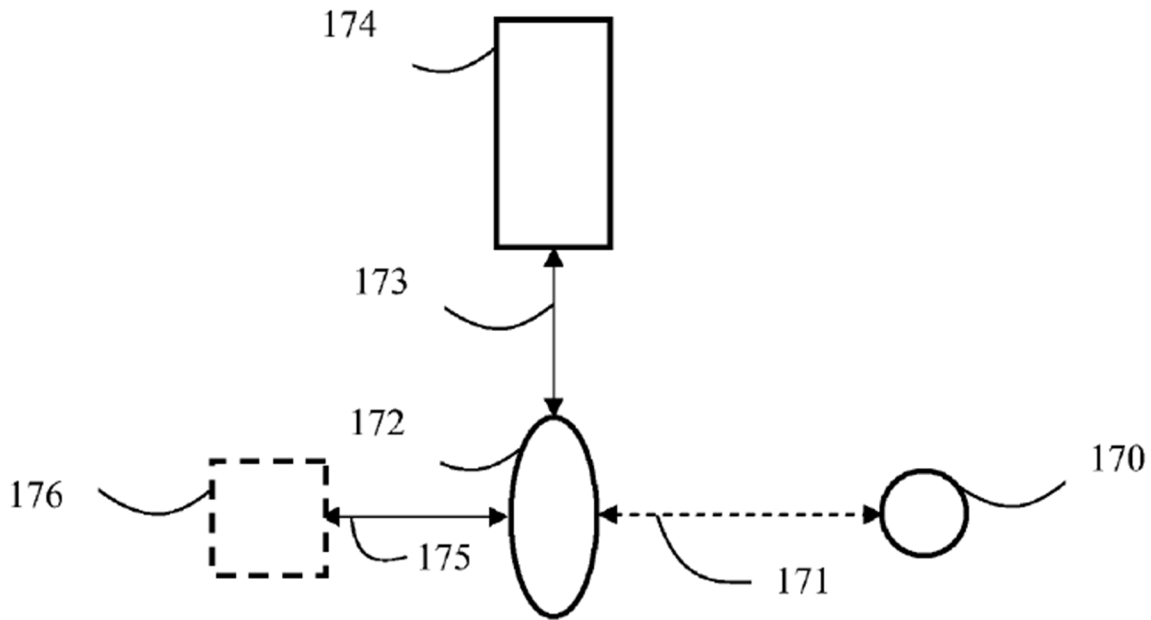


Figure 1c

Bucuk further discloses that phone 172 and car 170 (the respective *first* and *second devices*) perform disclosed methods by executing installed software *applications*. Bucuk, [0071]-[0072] and [0305]-[0307] (stored software executed by a processor), [0333] (mobile devices and other computing devices with short-range communication capabilities install “software drivers and applications... necessary for functioning”). *See also* Bucuk, [0089], [0118], [0147], [0169]

(describing examples of executing installed software to perform functions).

Lanning, ¶74.

- b. **[1.A.I] “at the first wireless device, providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices,”**

Bucuk discloses *at the first wireless device, providing initial identification information to a central server (e.g., phone 172 provides car 170’s IP address and Device ID to server 174), said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices (e.g., phone 172 received car 170’s IP address and Device ID via short-range communications)*. Lanning, ¶75.

Bucuk discloses that phone 172 searches for and reads the Bluetooth names of nearby devices, discovering car 170’s Bluetooth name “Car15#2c2c.8c8c.” Bucuk, [0166]. Phone 172 receives car 170’s Bluetooth name via Bluetooth, which provides a *short range local wireless link between the second and first devices*, as shown in Fig. 1c (below). Bucuk, [0157], [0163]; *see also* EX1001, 6:37-42 (short-range wireless “link” “only used for... detection..., or to advertise a device’s presence”). Lanning, ¶76.

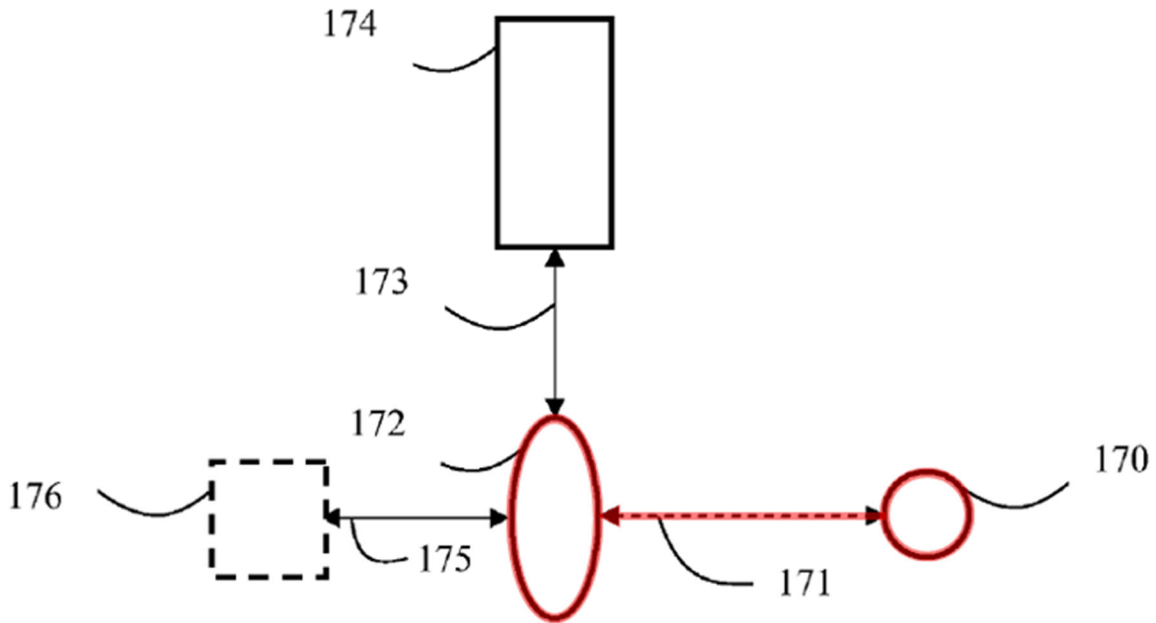


Figure 1c

From car 170’s Bluetooth name, phone 172 extracts car 170’s *initial identification information*—car 170’s IP address and Device ID information—and provides that *initial identification information* to server 174. Bucuk, [0167]; Fig. 1c (below). That is, phone 172 extracts “2c2c” and “8c8c” from car 170’s Bluetooth name “Car15#2c2c.8c8c” and sends it to server 174. *See also* Bucuk, [0165] (describing the IP address and Device ID parts of the Bluetooth name). Lanning, ¶77.

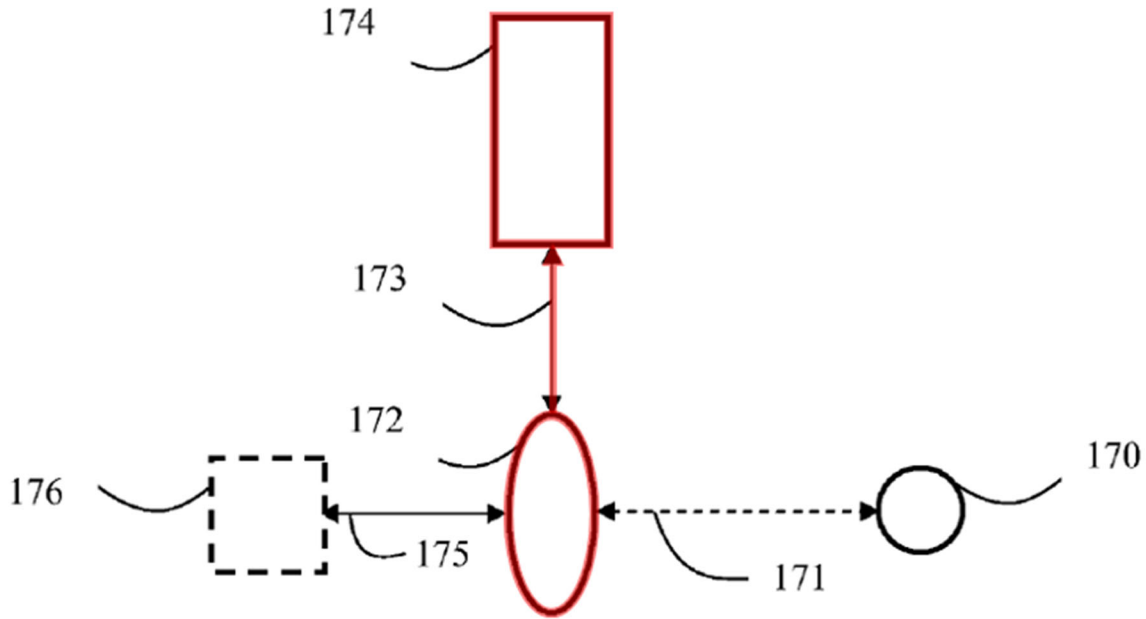


Figure 1c

- c. [1.A.II] “wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and”

Bucuk discloses that *the initial identification information (e.g., car 170’s IP address and Device ID, which are UID information) is associated at the central server with an identity of a user or entity associated with the second wireless device (e.g., at server 174, car 170’s UID information resolves to a user and Entity ID of the car 170)*. Lanning, ¶78.

Car 170 initializes itself with a unique Entity ID (*identity of a user or entity associated with the second wireless device*) at server 174. Bucuk, [0155].

Therefore, because car 170’s IP address and Device ID information (*the initial identification information*) are UID information that, “for a particular server or

database,” “directly or indirectly identify an Entity (which could be a User..., an object...),” Bucuk discloses that *the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device*. Bucuk, [0324] (also disclosing that a “[UID]... such as Device ID... will resolve [to the] Unique Entity ID and/or identify an Entity, for example through prior registration or login information”). Lanning, ¶79.

d. [1.A.III] “wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;”

Bucuk discloses that *the initial identification information is provided to the central server, by the first wireless device, over a second wireless link (e.g., phone 172 provides car 170’s IP address and Device ID to server 174 over the Internet)*. Lanning, ¶80.

Bucuk discloses that phone 172 provides the initial identification information to server 174. *See [1.A.I]. Communications between phone 172 and server 174 are over the Internet*. Bucuk, [0165], [0167] (car 170 “has no internet connection available..., so [phone 172] will use its own connection to contact the authentication server (174)”). Bucuk explains that Internet connections between mobile devices and servers (*e.g., between phone 172 and server 174*) include wireless links, *e.g., GSM, GPRS, and UMTS*, and are separate from the mobile device’s short-range radio connections. Bucuk, [0089], [0333]. Lanning, ¶81.

e. [1.B.I] “at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server,”

Bucuk discloses that, *at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server (e.g., each time server 174 issues an unlocking key, car 170’s identification information is changed according to a scheme coordinated with server 174), car 170 performs additional actions (e.g., see [1.B.III]-[1.C]).* Lanning, ¶82.

Bucuk discloses that after server 174 authorizes phone 172 to access car 170 by providing phone 172 with the unique number or unlocking key programmed into car 170 (e.g., server 174 provides “1f1f” to phone 172 to unlock car 170 once) (Bucuk, [0167]-[0169]), car 170 will “change Bluetooth® name according to a *pre-arranged scheme* (established at initialisation)..., effectively guaranteeing only one device ID (unlocking key) at the time can unlock [car 170].” Bucuk, [0170] (emphasis added). Thus, car 170 will change its Device ID from “8c8c” to the next device ID (unlocking key) that will be recognized by server 174 as valid the next time phone 172 and car 170 perform the same steps for unlocking the car (i.e., the next time phone 172 provides car 170’s Device ID to server 174 and receives an unlocking key in return). Bucuk, [0170] (repeating the disclosed cycle for further security). Lanning, ¶83.

Bucuk explains that the above system uses a “‘static’ list of unlocking numbers” and associated Device IDs (unlocking keys) that are known to the server and pre-programmed to the device (car 170). Bucuk, [0171]-[0172]; *see also* [0157] and [0168] (the unlocking keys are programmed into car 170 during initialization or registration with the server). That is, car 170 has initialized itself with the server and so “codes... change in a sequence which is known to the authentication server,” thus triggering a *predetermined event coordinated with said central server* each time car 170’s Device ID is used and then changed for the next cycle. Bucuk, [0160]. Lanning, ¶84.

f. [1.B.II] “within a specific application on the second wireless device,”

Bucuk discloses that car 170’s functions (including those claimed in [1.B]-[1.C]) are performed *within a specific application on the second wireless device* (e.g., within installed software). *See* [1.PRE]; Bucuk, [0071]-[0072], [0305]-[0307], [0333] (functions are performed by executing software applications); *see also* [0147], [0155], [0157], [0168], [0170] (devices/car 170 initialised by installing software and registering with the server). Lanning, ¶85.

g. [1.B.III] “providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information,”

Bucuk discloses *providing modified identification information* (e.g., providing a changed Bluetooth name with a changed Device ID) *over the first, direct, short range local wireless link* (e.g., over the short-range link) *in place of the initial identification information* (e.g., rather than providing the initial Bluetooth name that was already used to unlock car 170). Lanning, ¶86.

Bucuk discloses that after car 170 provides its *initial identification information* to phone 172 over the short-range link (*see* [1.A.I]) and phone 172 unlocks car 170 with an unlocking key received from server 174, car 170 changes its Bluetooth name with a new Device ID, thus creating *modified identification information*. *See* [1.B.I]; Bucuk, [0170]. As previously discussed for [1.B.I], car 170’s Device ID is “change[d]... according to a pre-arranged scheme” and “in a sequence... known to the authentication server,” “guaranteeing [that] only one device ID (unlocking key) at the time can unlock [car 170].” Bucuk, [0157], [0160], [0168], [0170]-[0171]. Accordingly, car 170’s Device ID is changed

according to a sequence of Device IDs and will not use the initial (or previous) Device ID in subsequent exchanges of identification information.⁴ Lanning, ¶87.

“[C]ycles of exchanging unique Device IDs” are “repeated” (Bucuk, [0170]), and so the next time phone 172 wants access to car 170, car 170 will provide its *modified* Bluetooth name (with changed Device ID) *over the first, direct, short range local wireless link* (e.g., over the short-range link when “new values are [passed] to the authentication server”) *in place of its initial* Bluetooth name (with initial Device ID). Bucuk, [0160], [0170]. Lanning, ¶88.

h. [1.C] “at the first wireless device, collecting said modified identification information.”

Bucuk discloses, *at the first wireless device, collecting said modified identification information* (e.g., phone 172 receives the modified Bluetooth name). Lanning, ¶90.

⁴ Even if the initial Device ID and changed Device ID use the same value (a low but non-zero probability if the sequence was generated randomly), phone 170 still goes through the process of changing its Device ID and creating *modified identification information*. Bucuk, [0170]. In most cases, the changed Device ID would be expected to have a different value. Bucuk, [0171]-[0173] (describing a list of 100,000 Device IDs/unlocking keys). Lanning, ¶89.

Bucuk discloses that “cycles of exchanging unique Device IDs” are “repeated” (Bucuk, [0170]), which includes search for and receiving Bluetooth names of nearby devices (Bucuk, [0166]). Thus, phone 172 will collect car 170’s modified Bluetooth name the next time it searches for devices (*e.g.*, the next time the user of phone 172 wants access to car 170). Bucuk, [0166], [0170]. Lanning, ¶91.

2. Claim 2: “[Claim 1] wherein the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.”

Bucuk discloses that *the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.* Lanning, ¶92.

As discussed for [1.A.I], [1.A.III], and [1.B.I], car 170 changes its Bluetooth name (which includes its Device ID) each time car 170’s Device ID is used by phone 172 to contact server 174 and server 174 issues an unlocking key. Bucuk, [0160], [0167]-[0170]. Lanning, ¶93.

The *predetermined event* of issuing an unlocking key based on car 170’s Device ID is *a number of uses of the identifier* because a single successful use of car 170’s Device ID that results in issuing an unlocking key causes car 170 to change its Bluetooth name. The *predetermined event* is also *a step in a process* because the step of car 170’s changing its Bluetooth name is only performed when

the step of issuing an unlocking key is performed first, as discussed above, and both steps together are part of an overall process. Lanning, ¶94.

3. **Claim 3: “[Claim 1] wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”**

- a. **Interpretation⁵**

Claim 3 references claim 1’s alleged “step of changing the user or entity identification information....” Claim 1 fails to provide proper antecedent basis for this term. Claim 1 requires “providing modified identification information” but does not describe when or how that identification information is modified or “chang[ed]” (if at all). Additionally, while PO previously agreed to construe claim 1’s “modified identification information” as “changed identification information” (EX1049, 2; EX1050, 13) that construction did not introduce a “changing” step. For the purposes of this Petition, and consistent with the ’749 disclosure (*see, e.g.*,

⁵ The claims are interpreted to at least cover the specification embodiment, which is met by the art, since indefinite challenges in IPR are not considered. 35 U.S.C. § 311(b) (“The scope of inter partes review is limited to a ground raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications.”).

'749 claim 7 referencing the second wireless device changing identification information), Petitioner interprets this limitation as a typographical error introducing “a step of changing,” which is an obvious step related to “providing modified identification information” (as in [1.B.III]), and which is taught by the prior art (*see* [1.B.I] (changing identification information)). *See K/S HIMPP v. III Holdings 4, LLC*, IPR2017-00782, Paper 8, 24-25 (Jul. 27, 2017), *Google Inc. v. Spring Ventures Ltd.*, IPR2017-01653, Paper 68, 37 n.7 (Jan. 15, 2019), and *Apple Inc. v. FastVDO LLC*, IPR2016-01203, Paper 39, 9-10 (Dec. 11, 2017) (interpreting claims with indisputable corrections; correcting typos).

b. Mapping

Bucuk discloses that *changing is effected by a rule-based generation local to the application*. For example, the change is carried out by car 170's *local application* (e.g., installed software, *see* [1.B.II]) that follows a “pre-arranged scheme” set at initialisation, such that the next Bluetooth name used for identification information is the next in a “sequence” “pre-programmed” in car 170 and coordinated with server 174. Bucuk, [0160], [0170]-[0171]. Each subsequent Bluetooth name generated is therefore based on a *rule* of taking the next identification information in a sequence. Lanning, ¶¶95-96.

4. **Claim 13: “[Claim 1] wherein the user or entity identification information is changed to protect the privacy of the identity of the a [sic] user or entity associated with the second wireless device.”**

- a. **Interpretation**

Claim 13 is directed to an intended result that carries no patentable weight.

See §V.A. Claim 13 is nevertheless anticipated by the prior art.

- b. **Mapping**

Bucuk discloses that both car 170’s and phone 172’s identification information are changed once for every iteration of the unlocking process. Bucuk, [0169]-[0170]. A POSITA would have recognized that changing identification information such that each identifier can only be used once before being changed *protects the privacy of the identity of the user or entity associated with the second wireless device (e.g., protects the privacy of user(s) unlocking their car; Bucuk, [0153])*. For example, if car 170’s identification information did not change over time, an observer would be able to see car 170’s same identification information broadcast over time and correlate it with the identity of nearby persons (*e.g., the user(s) unlocking the car time after time*) and devices (*e.g., the user(s)’s devices used to unlock the car*). Lanning, ¶97.

5. **Claim 17: “[Claim 1] wherein the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device.”**

Bucuk discloses that *the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device (e.g., phone 172 provides car 170’s modified Bluetooth name to server 174 to unlock car 170 at a subsequent time)*. Lanning, ¶98.

Bucuk discloses the process of phone 172 unlocking car 170 once, as discussed for [1.A.I]-[1.B.I], is a “cycle[] of exchanging unique Device IDs [that] could be repeated.” Bucuk, [0170]. Thus, after phone 172 collects car 170’s modified identification information (*see* [1.C]), it will provide the modified identification information to server 174 to unlock car 170 a subsequent time. Lanning, ¶99.

6. **Claim 18: “[Claim 1] wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”**

- a. **Interpretation**

Claim 18 is directed to a contingent limitation that carries no patentable weight. *See* §V.B. Claim 18 is nevertheless anticipated by the prior art.

b. Mapping

Bucuk discloses that car 170's Device ID is used to verify a link to phone 172 at server 174 for unlocking car 170. Bucuk, [0166]-[0169]; *see* [1.A.I]-[1.B.I]. The Device ID that represents car 170 is changed after every use (Bucuk, [0169]-[0170]) and is a "single use code" that changes in a sequence. Bucuk, [0160]. Accordingly, if car 170's initial identification information were re-sent to server 174 after being used to unlock car 170, server 174 will no longer recognize it as valid identification information for unlocking car 170 and will not provide an unlocking code to phone 172, therefore *processing it in a manner different from which it was processed prior to said pre-determined event*. Bucuk, [0170] ("only one device ID (unlocking key) at the time can unlock [car 170]"). Lanning, ¶100.

7. **Claim 19: "[Claim 17] wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device."**

a. Interpretation

Claim 19 is directed to an intended result that carries no patentable weight. *See* §V.A. Claim 19 is nevertheless anticipated by the prior art.

b. Mapping

Bucuk discloses that authentication server 174 uses the Device IDs (both initial and modified) to determine whether phone 172 and its user are associated with the car 170 in server 174's database, wherein an authorized link between the

two results in granting an unlocking key to unlock car 170. *See* [1.B.I]-[1.B.III]; Bucuk, [0164], [0167]-[0168]. In this way, Bucuk discloses that *the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device (e.g., authentication server 174 uses the changed Device ID to verify phone 172's legitimacy and identity as an entity authorized to unlock car 170)*. Lanning, ¶101.

- 8. Claim 20: “[Claim 17] wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”**

a. Interpretation

Claim 20 is directed to an intended result that carries no patentable weight. *See* §V.A. Claim 20 is nevertheless anticipated by the prior art.

b. Mapping

Bucuk discloses that *the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction (e.g., authentication server 174 uses the changed Device ID to verify the legitimacy and validity of phone 172's request to unlock car 170) associated with one or (a) the first wireless device or (b) a user or entity associated with the first wireless device (e.g., the request is initiated by phone 172 and its associated)*. *See* discussion of claim 19; Bucuk, [0153] (user of phone 172 requests access from car 170), [0166]-[0169]. The user's request to unlock the car is a *transaction*

associated with phone 172 (used to communicate with the car 170 and server 174) and its user. Lanning, ¶102.

VII. GROUND 2: BUCUK IN VIEW OF NORDMAN RENDERS OBVIOUS CLAIMS 1-3, 7-9, 13, 15, AND 17-26

A. Bucuk

Ground 1 introduced Bucuk above and described Bucuk’s Fig. 1c as an exemplary embodiment with two devices (phone and car) communicating in short-range proximity and with only one of the two devices (the phone) having a connection to an authentication server.

Bucuk describes other variations of systems with devices in short-range communication, including, *e.g.*, systems with devices registered to, and communicating with, the same authentication server. Bucuk, [0188]. In such systems, one device or both devices in short-range communication may provide the other’s identification information to the server to gain access to desired information and objects. Bucuk, [0188].

Bucuk also describes that identification information (or UIDs) take many forms, *e.g.*, device names and addresses, numbers/strings, changing numbers/strings that are periodically generated according to an algorithm, etc. Bucuk, [0100]-[0108], [0259], [0324]-[0325]. UIDs are generated “by the system on the server... side” and “periodically changed and updated to the mobile phone

device... and all authentication servers... to provide greater privacy.” Bucuk, [0108], [0259], [0325]. Lanning, ¶¶104-105.

B. Nordman

Nordman is directed to a method for protecting the privacy of a Bluetooth device by preventing the correlation of a user’s identity, routes, and activities with their device’s address through use of a pseudonym address instead of a device’s real Bluetooth device address (BD_ADDR). Nordman, Abstract, [0005]-[0006], [0051], [0095].

Furthermore, a device’s pseudonym address is changed periodically to further enhance privacy because “[t]he anonymity of the user would otherwise be undermined if the same pseudonym address were to be used indefinitely.” Nordman, [0010]. Nordman therefore illustrates several options for changing addresses based on elapsed time, use counts, connections made, location information, and others. Nordman, [0010]-[0011], [0043]-[0051].

The generation of addresses is accomplished by, *e.g.*, randomizing parts of a real address, selecting an address from previously computed values, and/or downloading addresses from a server. Nordman, [0057]-[0066], [0073], [0094]. Lanning, ¶¶106-109.

C. Motivation to Combine

The '749 is in the field of wireless communications—claiming to improve secure communications using wireless service identifiers, safety and privacy with locally stored policies, and facilitating the exchange of information between two entities associated with two wireless devices. *See* EX1001, 2:34-54 (also describing concerns of fraud, identity discovery and/or spoofing, personal safety and privacy). Lanning, ¶111.

Bucuk and Nordman are each analogous to the '749, as they are in the same field of wireless communications and/or reasonably pertinent to the objectives identified above. Bucuk, [0001], [0019] (establishing relationships between devices in short-range communication, aided by a server), [0160], [0172], [0325]-[0326] (describing features that enhance privacy and security); Nordman, Abstract, [0004]-[0005], [0013], [0095]-[0096] (protecting the privacy of a user's identity, routes, and activities that could be tracked through wireless technologies). Lanning, ¶112.

Bucuk teaches that embodiments of “system could be designed so that the unique number... is periodically changed and updated to the mobile phone device... and all authentication servers... to provide greater privacy to the user of the system from malicious monitoring of the [UID].” Bucuk, [0325]; *see also* [0108], [0259] (UIDs “generated by the system” are generated “on the server”);

[0100]-[0107] (exemplary UIDs include BD_ADDRs and changing numbers). In embodiments implementing changes, Bucuk describes that periodic changes occur when UIDs can be “used only once” and/or are “time expiring.” Bucuk, [0161]-[0162], [0172]-[0173], [0259]. Lanning, ¶113.

To the extent PO argues that embodiments of Bucuk relied upon in Ground 2 (such as in [0188] and [0325]) do not explicitly describe detailed mechanisms for changing a device’s identification information in accordance with a “predetermined event”—as required by claims 1 and 7, such as an “elapsed time” as described in claims 2 and 8—Bucuk nonetheless leaves it to the POSITA methods for implementing and triggering “periodically chang[ing]” of UIDs, a concept that is taught by Nordman. Lanning, ¶114.

Like Bucuk, Nordman explains that a device (and its user) using the same identifier over time is susceptible to tracking, which may be “exploited... by market researchers, and possibly by more sinister observers, ...compromising the user’s privacy and... safety.” Nordman, [0004]. Lanning, ¶115. Nordman thus teaches program conditions and functions to prevent tracking by periodically changing identifiers based upon, *e.g.*, time, use counts, connections made, and/or locations. Nordman, [0010]-[0011], [0043]-[0051], [0060]-[0085]. It would have been obvious to a POSITA to modify Bucuk’s servers to generate periodically changing UIDs based on Nordman’s teachings of predetermined events such as an

elapsed time. Modifications to processes for periodically changing UIDs according to Nordman's described system design options would have been accomplished through coding techniques known to a POSITA, such as by modifying the software applications executed for server functions. Bucuk, [0335]-[0338]. Lanning, ¶116.

This modification would have been further obvious as it is the application of a known technique (Nordman's variations of periodically changing identifiers) to a known device ready for improvement (Bucuk's server that periodically change device identifiers) to yield predictable results (periodically changing those identifiers based on different events such as time and use counts). *KSR Int'l v. Teleflex*, 550 U.S. 398, 417-418 (2007). Lanning, ¶117.

A POSITA would have also had a reasonable expectation of success in modifying Bucuk with the teachings of Nordman. For example, Nordman teaches how to implement steps for monitoring events, such as elapsed times and identifier use, utilizing counters and conditional logic. Nordman, [0059]-[0085]. A POSITA would have required no more than ordinary software coding skills to modify and/or add to Bucuk's software applications so that they monitor and act on the various conditions for periodically changing UIDs, as known in the art. Lanning, ¶118.

D. Claim Mappings⁶

1. Claim 1

a. [1.PRE]

To the extent this preamble is limiting, Bucuk discloses *a method for exchange of information (e.g., exchanging identification information and other data) between one or more applications executing on at least a first wireless device and a second wireless device (e.g., between software executing on devices communicating via short-range communications)*. Lanning, ¶119.

Bucuk that “two devices” (*i.e., a first wireless device and a second wireless device*) “exchange their [UIDs] via a short range communication connection between the two devices.” Bucuk, [0188]. An authentication server may authorize a link/bond between the first and second device that grants the devices access to information, data, services, resources, etc. associated with the other device. Bucuk, [0188], [0191], [0329], [0332]; *see also* [0042], claims 23 and 28 (example sending a data object from the first device to a linked second device), [0184]-[0185] (example of bonding between two devices that permits each device to

⁶ Text for claims 1-3, 13, and 17-20, which are discussed in both Ground 1 and Ground 2, are produced in §VI.C above (Ground 1) and in §XII below (Appendix A).

access selected data of the other). These are *exchanges of information*. Lanning, ¶120.

Bucuk further discloses that devices in its system perform disclosed methods by executing installed software applications. Bucuk, [0333]; *see also* Bucuk, [0071]-[0072], [0089], [0118], [0147], and [0305]-[0307] (describing executing stored software to perform functions). Lanning, ¶121.

b. [1.A.I]

Bucuk discloses *at the first wireless device, providing initial identification information to a central server (e.g., the first device sends the second device's UID to an authentication server), said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices (e.g., the first device received the second device's UID via short-range communications)*. Lanning, ¶122.

As discussed for [1.PRE]⁷, Bucuk discloses that the two devices “exchange their [UIDs] via a short range communication connection between the two

⁷ In these sections discussing grounds 2-4 (§§VII-IX), references to discussions of other claims and limitations are in reference to the discussions in the obvious

devices.” Bucuk, [0188]. Examples of short-range communications include Bluetooth, Wifi, NFC, etc. Bucuk, [0009], [0312]-[0315]. Lanning, ¶123.

After the exchange, “[a]t least one device... sends the other device’s [UID] to the authentication server...,” thus *providing initial identification information to a central server*. Bucuk, [0188]. Lanning, ¶124.

c. [1.A.II]

Bucuk discloses that *the initial identification information (e.g., the second device’s UID) is associated at the central server with an identity of a user or entity associated with the second wireless device (e.g., the server associates the second device’s UID with a user and Unique Entity ID of the device)*. Lanning, ¶125.

A UID, such as the second device’s UID (*the initial identification information*), is information that, “for a particular server or database,” “directly or indirectly identify an Entity (which could be a User..., an object...)” Bucuk, [0324]. Therefore, because the second device is registered with the authentication server (Bucuk, [0188]) and the second device’s UID information “will resolve [to identify a] Unique Entity ID and/or identify an Entity, for example through prior registration or login information” (Bucuk, [0324]), the second device’s UID is

grounds (§§VII-IX) and not to discussions in anticipation ground 1 (§VI), unless otherwise noted.

associated at the central server with an identity of a user or entity associated with the second wireless device. Lanning, ¶126.

d. [1.A.III]

Bucuk discloses that *the initial identification information is provided to the central server, by the first wireless device, over a second wireless link (e.g., the first device provides the second device's UID to the authentication server over a long-range communication connection).* Lanning, ¶127.

Bucuk discloses that the first device “sends the [second] device's [UID] to the authentication server via its own long range communication connection,” which is different from the short-range connection between the two devices. Bucuk, [0188]. Examples of long-range communications include internet connections and GSM, GPRS, and UMTS cellular connections. Bucuk, [0002], [0135], [0333]. Lanning, ¶128.

e. [1.B.I]

Bucuk-Nordman teaches performing additional actions (*e.g., see [1.B.III]-[1.C]*) *at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server (e.g., at the second device, on the occurrence of a periodic changing of the second device's UID).* Lanning, ¶129.

Bucuk teaches that the second device's UID is “periodically changed” (Bucuk, [0325]) upon the *occurrence of a predetermined event, e.g., using known*

criteria such as an identifier's expiration and/or one-time use (Bucuk, [0161]-[0162], [0172]-[0173], [0259]), which Nordman teaches in detail (Nordman, [0010]-[0011], [0043]-[0051], [0060]-[0085]). *See* §VII.C and discussion of claim 2. Lanning, ¶130.

Bucuk further teaches that changed UIDs are “updated to the mobile phone device... and all authentication servers.” Bucuk, [0325]. Therefore, the *predetermined event* that causes the second device's UID to be changed is *coordinated with said central server*. Lanning, ¶131.

f. [1.B.II]

Bucuk discloses that the second device's functions (including those claimed in [1.B]-[1.C]) are performed *within a specific application on the second wireless device* (e.g., within installed software). *See* [1.PRE]. Lanning, ¶132.

g. [1.B.III]

Bucuk discloses *providing modified identification information* (e.g., providing the second device's changed UID) *over the first, direct, short range local wireless link* (e.g., over the short-range communication link between the first and second device) *in place of the initial identification information* (e.g., rather than providing the UID that existed before the change). Lanning, ¶133.

Bucuk discloses that when the first and second device “come into close proximity, they exchange their [UIDs] via a short range communication connection

between the two devices.” Bucuk, [0188]; *see* [1.A.I]. Bucuk further discloses that the system process of exchanging UIDs to access services and objects is “repeated” between devices. Bucuk, [0123], [0129], [0170], [0296]; *see also* [0208]-[0209] (example where nearby devices “constantly” transmit/receive identification information to unlock a door and where authorizations change over time). Accordingly, after the second device changes its UID (*see* [1.B.I]), subsequent exchanges of UIDs will include *providing modified identification information in place of the initial identification information* to the first device. Lanning, ¶134.

h. [1.C]

Bucuk discloses, *at the first wireless device, collecting said modified identification information (e.g., first device receives the modified UID)*. *See* [1.B.III]. Lanning, ¶135.

2. Claim 2

Bucuk-Nordman teaches that *the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process*. Lanning, ¶136.

Bucuk-Nordman teaches the occurrence of the predetermined event for changing identifiers (or UIDs), *e.g., a predetermined time or use count*. *See* [1.B.I]. Another example of a predetermined event is a location change. Nordman, [0010], [0029]-[0051], [0054], claims 13-18. Lanning, ¶137.

For example, the identifier changes after a “predetermined time or count,” which changes identifiers after a certain amount of time elapses. Nordman, Fig. 3 (steps 304 and 320-332), [0048], [0060]-[0070]. A change based on a predetermined time/count is therefore based on *an elapsed time*. Lanning, ¶138.

In another example, the identifier changes after “inquiries/connections,” which changes identifiers after every connection—*e.g.*, if an inquiry is received but no connection is made, or if a connection is terminated. Nordman, Fig. 3 (steps 304, 306-318), [0049], [0071]-[0085]. A change based on a number of inquiries/connections is therefore based on *a number of uses of the identifier*. Lanning, ¶139.

In another example, the identifier changes after a location change, which follows steps to change an identifier after determining that a device changes physical location by a predetermined distance (*e.g.*, 10m). Nordman, Fig. 3 (steps 304, 306-318), [0050], [0071]-[0085]. A change based on a location change is therefore based on a *step in a process*. Lanning, ¶140.

3. Claim 3

a. Interpretation

See §VI.C.3.a (interpreting this limitation as including “a step of changing” instead of “the step of changing”).

b. Mapping

Bucuk as modified by Nordman teaches that *changing identification information may be downloaded from the server directly*. For example, Bucuk describes that the changed UID is generated by the system (*e.g.*, the server; Bucuk, [0108], [0259]) and “updated to the mobile phone device” (Bucuk, [0325]), which a POSITA would have recognized as obviously including a download from the server (which generated the UID) to the second device (which is updated with the generated UID). *See also* Bucuk, [0115], [0328] (UIDs are transferred through SMS, MMS, email, WAP push, etc.); Nordman, [0094] (known technique of a server computing an identifier that is “downloaded” to a wireless device). Lanning, ¶¶141-142.

To the extent PO argues that Bucuk does not describe that the server generating the changed UID is the authentication server, it would have been obvious to a POSITA to utilize one or many servers to carry out system functionality in Bucuk-Nordman, choosing a balance between costs (*e.g.*, constructing and maintaining multiple servers compared to a single server) and benefits, such as distributing loads (*e.g.*, providing multiple servers in different locations to address regional communication latency, multiple servers to increase processing capacity, scaling, etc.) and providing failure redundancies. The integration, division, and/or distribution of functions in one or more “server” units

would have been no more than an obvious design choice for a POSITA. MPEP §2144.04.V.B-C. Lanning, ¶143.

4. Claim 7

- a. [7.PRE] “A server for exchanging information between one or more applications executing on at least two wireless devices, the server comprising:”**

To the extent this preamble is limiting, Bucuk discloses *a server for exchanging information (e.g., a server generates Unique UIDs for devices that are exchanged to authorize further exchanges of information) between one or more applications executing on at least two wireless devices (e.g., between software executing on devices communicating via short-range communications)*. Lanning, ¶144.

As discussed for [1.PRE], Bucuk discloses a system including a first device executing software, a second device executing software, and an authentication server that facilitates exchanges of information between the two devices by authorizing links/bonds between them. Lanning, ¶145.

Additionally, as discussed for [1.A.I], [1.B.I], and claim 3, Bucuk-Nordman teaches that the server provides the periodically changed UIDs that are exchanged between the devices. Accordingly, the server further facilitates the exchange of identification information between the devices. Lanning, ¶146.

- b. **[7.A.I] “a receiver, for receiving initial identification information having been collected by a first wireless device from a second wireless device via a, first, direct, short range local wireless link between the first and second wireless devices,”**

Bucuk discloses the server function of *receiving initial identification information...* for the same reasons discussed for [1.A.I]. Lanning, ¶147.

Furthermore, the server receives the initial identification information over a long-range communication connection such as the Internet (*see* [1.A.III]), and Bucuk discloses that the server includes a *receiver* such as “a network card or modem” for communications over the Internet. Bucuk, [0336]. Lanning, ¶148.

- c. **[7.A.II] “wherein the initial identification information is associated at the server with an identity of a user or entity associated with the second wireless device, and”**

See [1.A.II]. Lanning, ¶149.

- d. **[7.A.III] “wherein the initial identification information is received by the server from the first wireless device over a second wireless link distinct from the first wireless link; and”**

See [1.A.III].

Furthermore, the second wireless link (*e.g.*, cellular or Internet connection; *see* [1.A.III]) is *distinct* from the first wireless link (*e.g.*, Bluetooth; *see* [1.A.I]) because, *e.g.*, they are separate and different links used to connect different devices (*e.g.*, server and first device versus first and second device) using different

communications standards (e.g., cellular GSM versus Bluetooth). Lanning, ¶¶150-151.

- e. **[7.B.I] “a transmitter for, upon an occurrence of a predetermined event coordinated with the second wireless device,”**

See [1.B.I].

Bucuk further discloses the server including *a transmitter* (e.g. network card or modem) for the same reasons it includes a receiver—to communicate information with wireless devices over the long-range communication connection (*see* [7.PRE]-[7.A.I]). Lanning, ¶¶152-153.

- f. **[7.B.II] “sending a message to the second wireless device to change the identification information within a specific application on the second wireless device and”**

Bucuk-Nordman teaches the transmitter *sending a message to the second wireless device to change the identification information* (e.g., updating the second device to change UID) *within a specific application on the second wireless device* (e.g., UIDs are used within the second device’s installed software). Lanning, ¶154.

Bucuk-Nordman teaches changing the second device’s UID from an initial UID to a modified UID. *See* [1.B.I]-[1.B.III]. Bucuk further teaches that UIDs are generated by the system on the server and “updated to the mobile phone device” (*i.e.*, the second device) through, e.g., a download from the server to the second device using a known technology such as SMS, MMS, email, WAP push, etc.

Bucuk, [0115], [0328]; *see* discussion of claim 3. A POSITA would have recognized that a UID update using one of these types of communications would have included a *message* that causes the second device *to change its identification information*. Lanning, ¶155.

Furthermore, Bucuk's second device uses the modified UID in at least its exchange of information with the first device. *See* [1.B.III]. Because the second device executes a software application to perform that function and other functions related to UIDs (*see* [1.PRE]), *the identification information is changed within a specific application on the second wireless device*. Lanning, ¶156.

- g. [7.B.III] “for subsequently providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, and”**

See [1.B.III]. Lanning, ¶157.

- h. [7.B.IV] “such that the modified identification information is associated at the server with said identity of a user or entity associated with the second device.”**

See [1.B.IV]. Lanning, ¶158.

- 5. Claim 8: “[Claim 7] wherein the predetermined event is one or more of: an elapsed time; and/or a number of uses of the identifier; and/or a step in a process.”**

See claim 2. Lanning, ¶159.

6. **Claim 9:** “[Claim 7] wherein the change of user or entity identification information is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”

See claim 3. Lanning, ¶160.

7. **Claim 13**

- a. **Interpretation**

Claim 13 is directed to an intended result that carries no patentable weight.

See §V.A. Claim 13 is nevertheless obvious over the prior art.

- b. **Mapping**

Bucuk discloses that periodically changing a UID “provide[s] greater privacy to the user of the system from malicious monitoring of the [UID].” Bucuk, [0325]. Since UIDs identify associated users and devices, changing the second device’s UID *protects the privacy of the identity of the user or entity associated with the second device*. Lanning, ¶161.

8. **Claim 15:** “[Claim 7] wherein the user or entity identification information is changed to protect the privacy of the identity of a user or entity associated with the second wireless device.”

See claim 13. Lanning, ¶162.

9. **Claim 17**

Bucuk-Nordman teaches that *the first wireless device further performs the step of providing modified identification information to said central server, as*

collected by the first wireless device from the second wireless device (e.g., the first device receives the changed UID from the second device and provides it to the authentication server). Lanning, ¶163.

Bucuk discloses that the system's process of exchanging UIDs is repeated, such that the devices exchange initial UIDs (as in [1.A.I]) and, later, modified UIDs (as in [1.C]). Thus, following the same process for the initial UID, the first device will provide the modified UID, received from the second device, to the authentication server (as similarly discussed for [1.A.I]). Lanning, ¶164.

For example, as applied to an embodiment in which an automatic door (a first device) receives a mobile phone's (a second device's) UIDs to unlock the door, the door will provide the phone's received UID to the authorization server even after changing/modifying. That is because the modified UID will appear to the door as a "new" UID (having been changed) and/or the modified UID is not recognized as an authorized UID after the user loses access (e.g., no longer an employee of a company, based on non-payment of fees), each situation requiring verification with the server. Bucuk, [0208]-[0209]. Lanning, ¶165.

10. Claim 18

a. Interpretation

Claims 18 and 23 (further below) are directed to contingent limitations that carry no patentable weight. *See* §V.B. Claims 18 and 23 are nevertheless obvious over the prior art.

b. Mapping

Bucuk as modified by Nordman teaches that the second device's initial identification information is changed to the modified identification information after the predetermined event, and this change is synchronized across devices and servers. *See* [1.B.I]; Bucuk, [0325] (changing UID to protect user privacy). Accordingly, because the second device and its user are no longer associated with the initial UID after the predetermined event, *if* the initial UID were to be *re-sent* to the authentication server, the *initial identification information* will be *processed* by the authentication server *in a manner* (*e.g.*, not identifying an entity associated with the second device) *different from which it was processed prior to said predetermined event* (*e.g.*, prior to the predetermined event, the initial UID would have identified an entity associated with the second device). Bucuk, [0324]. Lanning, ¶166.

11. Claim 19

a. Interpretation

Claims 19 and 24 (further below) are directed to an intended result that carries no patentable weight. *See* §V.A. Claims 19 and 24 are nevertheless obvious over the prior art.

b. Mapping

Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, *e.g.*, to “verify an identity or authenticity of an entity.” Bucuk, [0191], [0330]. Discussed below, Bucuk describes different applications of its system that render claim 19 obvious. Lanning, ¶167.

i. First example (Police ID)

In one example, the first device and the second device are the mobile phone devices of a resident and a police officer, respectively, and the officer wants to “verify the identity of [the] mobile phone device user.” Bucuk, [0228]. Through bonding (which includes exchanging UIDs and the modified UID as discussed above), aided by the common police authentication server, the officer is able to see details about the identity of the resident and verify the resident’s identity. Bucuk, [0228]-[0229]. Lanning, ¶168.

Accordingly, *the modified identification information (e.g., the officer device's modified UID) is used by the central server (e.g., by bonding the officer device's modified UID with the resident device's UID at an authentication server) to verify the legitimacy, identity or authenticity of the first wireless device (e.g., bonding of the UIDs is part of a process to verify the identity or authenticity of the resident)*. Lanning, ¶169.

Additionally, while the “entity” being verified in this example is the user/resident, Bucuk teaches that “entity” also refers to devices. Bucuk, [0320]. Accordingly, it would have been obvious to a POSITA that this exemplary use not only verifies the identity and authenticity of the user (the resident) but may also be used to verify the user/resident's mobile device that exchanges UIDs (*i.e., verifying the first wireless device*). Lanning, ¶170.

ii. Second example (Web Access)

In another example, the first device and the second device are a desktop computer and a mobile phone device, respectively, and the user of the mobile phone device wants to log into the desktop computer (*e.g., to access a secure bank website*). Bucuk, [0231]-[0234]. The mobile phone device collects the UID of the desktop computer of interest and sends that information to its authentication server. Bucuk, [0233]. The desktop computer similarly collects the Bluetooth names and UIDs of devices in its proximity, including the mobile phone device, and sends that

information to a bank authentication server. Bucuk, [0234]. The bank authentication server uses the UIDs “to positively identify [the] mobile phone device[] as being in close proximity of the desktop[] and having [the particular UID].” Bucuk, [0234]. Lanning, ¶171.

Accordingly, *the modified identification information (e.g., the mobile phone’s modified UID) is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device (e.g., used by the bank authentication server to verify that the desktop computer is identified as legitimately in proximity of the mobile phone).* Lanning, ¶172.

Additionally, while this example makes use of one other server in addition to the bank authentication server (*see* [0233]-[0234], in addition to bank authentication server 314, describing an authentication server 316 associated with the mobile phone), Bucuk makes clear that the server configurations in various embodiments and systems are obvious design choices for a POSITA. Bucuk, [0025] (servers associated with devices are the same), [0126] (“server” as software on shared hardware), [0251]-[0252] (same server for multiple devices and services). Accordingly, to the extent PO argues that this Web Access example is deficient because it includes two servers, it would have been obvious to a POSITA to consolidate those functions as an obvious design choice to, *e.g.*, minimize the amount of hardware required. Lanning, ¶173.

12. Claim 20

a. Interpretation

Claims 20 and 25 (further below) are directed to an intended result that carries no patentable weight. *See* §V.A. Claims 20 and 25 are nevertheless obvious over the prior art.

b. Mapping

Bucuk as modified by Nordman teaches that *the modified identification information (e.g., the second device's modified UID) is used by the central server to verify the legitimacy, validity, or authenticity of a transaction (e.g., the authentication server receives the modified UID to verify the legitimacy and validity of a money transfer request) associated with one or (a) the first wireless device or (b) a user or entity associated with the first wireless device (e.g., the money transfer is from the second device and user to a first device and user).* Lanning, ¶174.

Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, *e.g.*, to trigger an event or action, execute code, perform a business process, verify an identity or authenticity of an entity, etc. Bucuk, [0191], [0330]. Lanning, ¶175.

For example, the first device and second device are devices of users that exchange UIDs to conduct a currency transfer (a *transaction*)—*e.g.*, corresponding to a “newspaper[] seller” collecting money from a “newspaper reader.” Bucuk, [0222]-[0224]. The first device collects the modified UID information from the second device and transmits that information to a bank authentication server, which looks up the “respective [UIDs] collected during the bonding procedure” to authorize a “one off money transfer.” Bucuk, [0224]; *see also* [0223] (devices “enable currency transfer” by first making themselves available for bonding at the authentication server), [0225] (both devices deal with the bank authentication server). Lanning, ¶176.

Accordingly, because the requested money transfer is only authorized by the authentication server if the two devices made themselves available for bonding, which the server determines by looking up received UIDs as discussed above, the authentication server uses UIDs (including the modified UID) *to verify the legitimacy or validity of a transaction* as being authorized between two *devices* and *users* that have made themselves available for bonding and currency transfer. Lanning, ¶177.

- 13. Claims 21/26: “The [method of claim 1][server of claim 7] wherein upon the [occurrence] of the predetermined event, [the server] further [notifies][notifying] the second wireless device of the modified identification information via a wireless configuration message or an instruction to change communication state.”**

Bucuk-Nordman teaches that *upon the occurrence of the predetermined event (e.g., after the predetermined time), further notifying the second wireless device of the modified identification information via a wireless configuration message (e.g., the server transmits a message to the second device to change its UID)*. Lanning, ¶¶178, 185.

Bucuk-Nordman teaches using a predetermined event, such as an elapsed time or use count, as a basis for changing the second device’s UID, which is generated at the server and updated to the second device. *See* §VII.C and discussions of claims 1-3. The server updates the second device with a message (e.g., SMS, MMS, email, WAP push) that causes the second device to change its UID. *See* [7.B.II]. Lanning, ¶179.

A POSITA would have recognized that the message to the second device that causes the second device to thereafter use the modified UID is a *wireless configuration message* because it is a message that the second device receives and recognizes as containing data that alters the second device’s wireless behavior—*i.e.*, by providing the modified UID in subsequent transmissions instead of the initial UID. Lanning, ¶180.

14. **Claim 22:** “[Claim 7] wherein the central server further receives modified identification information, as collected by the first wireless device from the second wireless device.”

See claim 17. Lanning, ¶181.

15. **Claim 23:** “[Claim 7] wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”

See claim 18. Lanning, ¶182.

16. **Claim 24:** “[Claim 23] wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.”

See claim 19. Lanning, ¶183.

17. **Claim 25:** “[Claim 7] wherein the modified identification information is used by the central server to verify legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”

See claim 20. Lanning, ¶184.

VIII. GROUND 3: BUCUK IN VIEW OF NORDMAN AND KALLIO RENDERS OBVIOUS CLAIMS 4-6 AND 10-12

A. Kallio and Motivation to Combine

Bucuk-Nordman teaches a system including devices that exchange identifiers (UIDs) and an authentication server that facilitates further communication between those devices based on their UIDs. Bucuk-Nordman

further teaches enhancing privacy and safety by periodically changing device UIDs. *See* §VII.A-C above. Lanning, ¶189.

To the extent PO argues that Bucuk-Nordman does not describe server functions in detail, such as taking an identifier from a pool of identifiers (as in claims 4, 10) or using an identity manager within a server to assign identifiers (claims 5-6, 11-12), those server functions would have been obvious to a POSITA, as taught by Kallio. Lanning, ¶190.

Kallio (EX1047), is in the same field of endeavor as the '749 Patent. Kallio, [0001]-[0003], [0011]-[0017] (facilitating access to services from, *e.g.*, a Bluetooth base station with managing servers), [0024] (communicating device and service identifiers)). Kallio teaches that a wireless device or terminal identifying itself to a server may use an identifier such as a Bluetooth device address or a randomly generated “48-bit address similar in form to a Bluetooth hardware address, but whose composition [bears] no relation to any identifier corresponding to [the] terminal.” Kallio, [0020], [0024]-[0026]. The 48-bit addresses may be generated according to rules or constraints (*e.g.*, ensuring uniqueness among devices, having values in certain ranges, etc.) and/or in particular ways (*e.g.*, generated one by one or assigned from a bank of addresses). Kallio, [0024]-[0027]. Lanning, ¶¶187-188.

It would have been obvious to modify Bucuk’s server to generate the periodically changing UIDs with enhancements taught by Kallio. Bucuk teaches

that UIDs take the form of names, addresses, numbers, strings, codes, etc. Bucuk, [0100]-[0108], [0324]-[0325]. Nordman and Kallio both express concern over the possibility of generating duplicate identifiers that may conflict with the existing identifiers of nearby wireless devices. Nordman, [0012], [0066], [0076] (performing extra steps to generate an address “because of other duplicate addresses in the vicinity”); Kallio, [0024]-[0025] (“constraint that no other terminal be currently assigned the particular address”), [0026] (“constraint that a created address not be identical to an actual and/or existing Bluetooth hardware address, MAC address or other identifier”). Kallio addresses this concern by, *e.g.*, generating a “bank” (or *pool*) of identifiers from which a server assigns identifiers. Kallio, [0026]. Thus, by implementing a centralized source to assign identifiers from a pool (*e.g.*, functioning as an *identity manager*), the server advantageously avoids extraneous processing and ensures that no two devices use the same identifier. These modifications would have been accomplished through coding techniques known to a POSITA, such as by modifying the server software for generating UIDs. Bucuk, [0335]-[0338] (servers include installed “software drivers and applications” for functionality); Kallio, [0039]-[0043]. Lanning, ¶191.

Accordingly, a POSITA would have combined the teachings of Bucuk-Nordman-Kallio to arrive at wireless devices that periodically change their UIDs by receiving modified UIDs selected by a server from a pool of identifiers. This

modification would have been further obvious as an application of a known technique (Kallio's assignment of identifiers from a pool) to a known device ready for improvement (Bucuk-Nordman's server generates identifiers) to obtain predictable results (assigning non-duplicative identifiers to devices from a centralized server) to ensure duplicate addresses are avoided. *KSR*, 550 at 417-418. Lanning, ¶192.

A POSITA would have also had a reasonable expectation of success in modifying server functions to generate/assign addresses and coordinate the same with participating devices. For example, the generation of a "bank" of identifiers would have required no more than ordinary software coding skills to modify and/or add to the server software so that it generates, stores, selects, and communicates those values, as known in the art. Lanning, ¶193.

B. Claim Mappings

- 1. Claim 4: "[Claim 1] further comprising: at said second wireless device, receiving a user or entity identifier from a central server, the user or entity identifier taken from a pool of identifiers determined by the central server."**

a. Interpretation

It is unclear whether claim 4's "a central server" is a new recitation of a central server or references the central server of claim 1. Nevertheless, it would have been obvious to a POSITA to utilize one or many servers to carry out system functionality in Bucuk-Nordman-Kallio such that the integration, division, and/or

distribution of functions in one or more “server” units would have been no more than an obvious design choice for a POSITA. *See* §VII.D.3.b (discussion of claim 3). Lanning, ¶194.

b. Mapping

Bucuk-Nordman-Kallio teaches, *at said second wireless device, receiving a user or entity identifier from a central server (e.g., the second devices receives a modified UID from a server), the user or entity identifier taken from a pool of identifiers determined by the central server (e.g., the modified UID is selected from a bank of identifiers at the server)*. Lanning, ¶195.

As discussed above (§VIII.A), a POSITA would have been motivated to use a central server to distribute to devices UIDs (identifying users and devices; Bucuk, [0324]), thereby avoiding duplicate values across a plurality of devices. Lanning, ¶196.

For example, Kallio describes a server assigning identifiers by generating a “bank” of acceptable identifiers (*i.e., a pool of identifiers*) and randomly selecting an identifier from that bank for assignment, thereby, ensuring that the identifier is not identical to an actual and/or existing identifier. Kallio, [0024]-[0026]. Lanning, ¶197.

2. **Claims 5/11: “The [method of claim 1][server of claim 7] further comprising: [using] an identity manager [within a server][,] to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link [to said second wireless device;][,] and wherein the user [or entity] identifiers are changed over time.”**

Bucuk-Nordman-Kallio teaches *using an identity manager within a server to assign user or entity identifiers to devices* (e.g., a server assigns identifiers to devices using software applications) *by sending the same over a WWAN cellular data link to said second wireless device* (e.g., server-device communications are over cellular links); *and wherein the user or entity identifiers are changed over time* (e.g., see claims [1.B.I] and 2). Lanning, ¶¶198, 209.

As similarly discussed for claim 4, it would have been obvious to use a server to assign identifiers, selected from a pool of identifiers, to devices for use as UIDs, as taught by Kallio. Kallio teaches that the server executes “software modules” to implement that functionality. Kallio, [0039]-[0043]; *see also* Bucuk, [0335]-[0338] (servers include “software drivers and applications”). The ’749 does not describe *identity manager* as necessarily requiring any particular structure—“identity manager” is the descriptive name for a functional block or application agent of the server. EX1001, Fig. 13, 16:58-17:1. Bucuk’s and Kallio’s server software applications and modules performing the same claimed functions are at least equivalent to the claimed *identity manager*. Lanning, ¶199.

As discussed for [1.A.III], the server and devices communicate via long-range communications, *e.g.*, GSM, GPRS, or UMTS cellular connections—*i.e.*, *WWAN cellular data links*. Bucuk, [0002], [0135], [0333]. Lanning, ¶200.

Further discussed above, UIDs identifying users and devices are “periodically changed” upon the occurrence of a predetermined event, such as an elapsed time, and are therefore *changed over time*. See §VII.C, discussion of [1.B.I] and claim 2. Lanning, ¶201.

3. **Claims 6/12: “The [method of claim 5][server of claim 11] wherein [at least one of] the user or entity identifiers are associated with a device identifier by the identity manager, [and the device identifier is associated with one or more of the initial identification information or modified identification information,] and [wherein] the device identifier is [selected from] one [or more] of: a media access control (MAC) [device] [address][addresses] of a short range wireless network adapter; a SSID in an IEEE-802.11 network beacon; a BSSID of an IEEE802.11 network adapter; a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message; a device name in a Bluetooth name response packet; or one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.”**

Bucuk-Nordman-Kallio teaches that *at least one of the user or entity identifiers (e.g., one of the generated UIDs) are associated with a device identifier by the identity manager (e.g., the modified UID is associated with an Entity ID at the server), and the device identifier is associated with one or more of the initial identification information or modified identification information (e.g., the Entity*

ID is associated with the initial UID prior to the predetermined event and with the modified UID after the predetermined event). Lanning, ¶202, 210.

Bucuk teaches that the server, which includes the *identity manager* (i.e., server software applications performing functions related to identification information; see discussion of claim 5), manages a database of user account information that associates various information about a user (e.g., names, addresses, UIDs, etc.) to a unique “Entity ID.” Bucuk, [0109], [0155], [0254], [0320]. The Entity ID is different from the UID (though optionally the same), and in use, the UID identifies an entity user and/or device by resolving to its Entity ID at the server. Bucuk, [0324]; see [1.A.II]; see also Bucuk, [0160] (“code[s] which represent the same user/device/entity change[] whilst still representing the same user/device/entity”). Lanning, ¶203.

The Entity ID associated with the second device is, therefore, a *device identifier associated with the second device’s initial identification information* (second device’s initial UID) and *modified identification information* (second device’s modified UID) because the second device’s UID, whether it is the pre- or post-predetermined event UID, is configured to resolve to the Entity ID.

Additionally, because the value of the second device’s modified identification information is taken from an assigned *user or entity identifier* generated by the server (see discussion of claim 5), the Entity ID associated with the modified

identification information is also *associated with at least one of the user or entity identifiers*. Lanning, ¶204.

Furthermore, Bucuk discloses that *the device identifier is one or more of: a media access control (MAC) device address of a short range wireless network adapter; a BSSID of an IEEE802.11 network adapter; [and] a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message*. Like the UID, the Entity ID may comprise, *e.g.*, a Bluetooth *BD_ADDR*, WiFi *BSSID*, or network card *MAC address*. Bucuk, [0090], [0100]-[0103] (describing values used for unique identifiers), [0259] (*BD_ADDR*, *BSSID*, and other identification codes used for Unique Entity IDs). Lanning, ¶205.

4. **Claim 10: “[Claim 7] further comprising: a receiver, for receiving a user or entity identifier from a central server, the identifier taken from a pool of identifiers determined by the central server.”**

See [7.A.I] (server includes a receiver) and claim 4 (second device receives an identifier, from a pool of identifiers, from a central server). Additionally, Bucuk discloses that the second device includes “a long range radio transmitter and receiver” (*a receiver*) for communicating in GSM, GPRS, or UMTS systems and for *receiving a user or entity identifier* from the server. Bucuk, [0333]; *see* discussion of claim 5. Lanning, ¶206.

To the extent PO argues that claim 10 requires “the server of claim 7” to receive a user or entity identifier from another different server—*a central server*

that is not *the server*—a POSITA would have recognized the use of multiple servers to be an obvious variation of Bucuk-Nordman-Kallio. As discussed for claim 4, it would have been obvious to a POSITA to configure servers and server functions in one server or a plurality of servers—combining, separating, and/or distributing functions as desired. Thus, where Kallio teaches that the server is “present[ed]... with a bank of acceptable anonymity addresses” (Kallio, [0026]) but does not explain in further detail the origin of the bank of addresses (*e.g.*, generated locally or remotely), it would have been an obvious design choice to include a separate central server for generating addresses. For example, Kallio describes that, in some embodiments, different servers serve different terminals, requiring servers to share lists of assigned addresses to avoid duplicate assignments. Kallio, [0025]; *see also* Bucuk, [0325] (periodically changing UID and updating to “all authentication servers”). Using a central server (*i.e.*, consolidating servers’ address generation functions) would have limited the risk of those double assignments and avoided the need for additional communications for verification. Lanning, ¶207.

Accordingly, it would have been further obvious to modify Bucuk-Nordman-Kallio to use a central server to generate banks of keys for the server. Lanning, ¶208.

IX. GROUND 4: BUCUK IN VIEW OF NORDMAN AND PERTTILA RENDERS OBVIOUS CLAIMS 14 AND 16

A. Interpretation

Claims 14 and 16 are directed to an intended result that carries no patentable weight. *See* §V.A. Claims 14 and 16 are nevertheless obvious over the prior art.

B. Perttala and Motivation to Combine

Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, *e.g.*, to share data, trigger an event or action, execute code, perform a business process, verify an identity or authenticity of an entity, etc. Bucuk, [0191], [0330]. Applications of Bucuk's system of establishing relationships using identifiers and short-range communications are numerous. Bucuk, Abstract, [0180]. Lanning, ¶214.

Perttala is in the same field of wireless communications and reasonably pertinent to objectives of facilitating the exchange of information and validating commercial transactions. EX1001, 1:58-2:7; Perttala, Abstract, [0001], [0006]-[0008], [0016], [0026], [0042]-[0043].⁸ Lanning, ¶213.

⁸ Related patents' claims were previously found unpatentable over Perttala.

Arguments that Perttala is not analogous or does not teach features already decided

Perttola teaches a method for wirelessly providing users access to services and products in a secure way through electronic coupon redemptions. Perttola, Abstract, [0008]. For example, a user's Bluetooth device detects a Bluetooth beacon inside a store, notifies a server with its ID information and beacon information, and in return receives an electronic coupon for redemption. Perttola, [0011], [0028], [0031], [0037]-[0039]; EX1019, 13-14; EX1034, 6-7. The coupon may be a ticket to purchase or receive a "merchant offering," redeemed electronically by transferring and validating coupon information using ID information at the server. Perttola, [0005], [0031], [0041]-[0042], claims 17, 26. Through validation, used/expired coupons may be rejected, providing merchants control over offerings. Perttola, [0042]-[0043]; *see also* [0006] (describing coupons with time/location limitations). Lanning, ¶215.

A POSITA applying Bucuk's system for a "business process" (Bucuk, [0191], [0330]) would have been motivated to look towards known e-commerce solutions for implementation, and it would have been obvious to modify Bucuk-Nordman's server to alert devices (*e.g.*, the first device) of nearby offerings (*e.g.*, from the second device) with coupon data linked and redeemable with device IDs

by the PTAB/CAFC are estopped. EX1018-EX1023 (IPR petitions, FWDs), EX1034 (CAFC opinion).

(e.g., UUIDs). Perttila’s teachings advantageously “ensure that the user has rights” to offerings—permitting merchants to control their offerings. Perttila, [0005]-[0015], [0043]. Lanning, ¶216.

Moreover, the modification would have been no more than the application of a known technique (Perttila’s proximity-based coupons) to a known device ready for improvement (Bucuk-Nordman’s proximity-aware system that identifies nearby contacts and facilitates associations and links/bonds) to yield predictable results (controlling access to resources) with a reasonable expectation of success (techniques for transferring and analyzing data were within the skill of a POSITA). *KSR*, 550 at 417-418. Lanning, ¶217.

C. Claim Mappings

1. **Claims 14/16: “The method of [claim 1][claim 7⁹] wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.”**

Bucuk-Nordman-Perttila teaches that *the user or entity identification information is changed* (e.g., the second device’s initial UID to the modified UID) *to... provide a validation of the legitimacy of one or both of the first or the second*

⁹ Claim 16 recites the “method of claim 7” but should properly recite the “server of claim 7” instead.

wireless devices and respective applications (e.g., the authentication server uses the changing UIDs to validate the legitimacy of the first and second devices and their applications). Lanning, ¶¶218, 222.

As discussed (§IX.B), Bucuk-Nordman-Perttila teaches the server using UIDs for coupon distribution and redemption. For example, a device (a terminal; e.g., the first device) provides a server with its ID information (e.g., the first device's UID) and merchant ID information (a merchant ID code from a "tag" or beacon; e.g., the second device's modified UID) and receives coupon information in response. Perttila, [0037]-[0039]. To redeem the coupon at a later time, the first device provides information to the server, which attempts to validate the coupon by checking its database for device ID information (e.g., the first device's UID) and merchant ID information ("tag" information; e.g., the second Device's modified UID) to see if the coupon is valid. Perttila, [0041]-[0042]. Lanning, ¶219.

Because the second device's identification information (UID) changes periodically, the server will therefore verify that the first device is in possession of, and attempting to redeem, a current and valid coupon. For example, Perttila teaches that ID codes identify coupon types, which are useful for identifying coupons with "expiration periods restrictions." Perttila, [0029]; *see also* Bucuk, [0161]-[0162], [0173] (validity of codes and IDs configured to expire). Thus, the second device may have had an initial UID associated with a coupon expiring in a

first time period, and a modified UID associated with a coupon valid in a subsequent second time period. If the first device provides the second device's initial UID in the second time period (*i.e.*, after it expired), the server will not *validate the legitimacy of the first device* (*i.e.*, not a legitimate coupon holder). On the other hand, if the first device provides the second device's modified UID in the second time period (*i.e.*, valid and not expired; after changing), the server will *validate the legitimacy of the first device* (*i.e.*, as a legitimate coupon holder) and the *legitimacy of the second device* (*i.e.*, as a distributor of legitimate unexpired coupons). Lanning, ¶220.

Additionally, because devices execute respective applications to perform functions in the system of Bucuk-Nordman-Kallio-Perttola (*see* [1.B.II]), the transmission, reception, and verification of data from those applications as being valid (*e.g.*, determined to have transmitted valid coupons) also *validates the legitimacy* of those *respective applications*. Devices executing respective applications will only produce the right information (*e.g.*, UIDs) and communicate to the right devices and servers if they are executing legitimate applications for the communications system. Lanning, ¶221.

X. SECONDARY CONSIDERATIONS

Secondary considerations are irrelevant to the anticipation of claims in Ground 1.

Petitioner is unaware of any secondary considerations relevant to the obviousness of claims in Grounds 2-4, let alone any arguments that could overcome the strong showing of obviousness above and have a sufficient nexus to the Challenged Claims. The prior art demonstrates that any purported solutions to problems or unexpected results in the '749 were already well known. To the extent PO asserts secondary considerations in its responses, Petitioner reserves the right to address such evidence. Lanning, ¶¶223-224.

XI. CONCLUSION

The Board should institute review and cancel the Challenged Claims.

Respectfully submitted,

Dated: January 9, 2026 By: /Scott A. McKeown/
Scott A. McKeown, Reg. No. 42,866
WOLF, GREENFIELD & SACKS, P.C.

XII. APPENDIX A: U.S. PATENT NO. 8,116,749 CLAIM LISTING

Claim 1
[1.PRE] A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:
[1.A] [1.A.I] at the first wireless device, providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices, [1.A.II] wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and [1.A.III] wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;
[1.B] [1.B.I] at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server, [1.B.II] within a specific application on the second wireless device, [1.B.III] providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, [1.B.IV] such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device; and
[1.C] at the first wireless device, collecting said modified identification information.
Claim 2
The method of claim 1 wherein the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.
Claim 3
The method of claim 1 wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.
Claim 4
The method of claim 1 further comprising:

at said second wireless device, receiving a user or entity identifier from a central server, the user or entity identifier taken from a pool of identifiers determined by the central server.

Claim 5

The method of claim 1 further comprising:
using an identity manager within a server to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link to said second wireless device; and
wherein the user or entity identifiers are changed over time.

Claim 6

The method of claim 5 wherein at least one of the user or entity identifiers are associated with a device identifier by the identity manager, and the device identifier is associated with one or more of the initial identification information or modified identification information, and wherein the device identifier is one or more of:
a media access control (MAC) device address of a short range wireless network adapter;
a SSID in an IEEE-802.11 network beacon;
a BSSID of an IEEE802.11 network adapter;
a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message;
a device name in a Bluetooth name response packet; or
one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.

Claim 7

[7.PRE] A server for exchanging information between one or more applications executing on at least two wireless devices, the server comprising:

[7.A] [7.A.I] a receiver, for receiving initial identification information having been collected by a first wireless device from a second wireless device via a, first, direct, short range local wireless link between the first and second wireless devices, [7.A.II] wherein the initial identification information is associated at the server with an identity of a user or entity associated with the second wireless device, and [7.A.III] wherein the initial identification information is received by the server from the first wireless device over a second wireless link distinct from the first wireless link; and

[7.B] [7.B.I] a transmitter for, upon an occurrence of a predetermined event coordinated with the second wireless device, [7.B.II] sending a message to the second wireless device to change the identification information within a specific application on the second wireless device and [7.B.III] for subsequently

providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, and [7.B.IV] such that the modified identification information is associated at the server with said identity of a user or entity associated with the second device.

Claim 8

The server of claim 7 wherein the predetermined event is one or more of:
an elapsed time; and/or
a number of uses of the identifier; and/or
a step in a process.

Claim 9

The server of claim 7 wherein the change of user or entity identification information is further:
effected by a rule-based generation local to the application,
downloaded from the server directly, or
synchronized such that it is coordinated with predetermined receiving and transmitting times.

Claim 10

The server of claim 7 further comprising:
a receiver, for receiving a user or entity identifier from a central server, the identifier taken from a pool of identifiers determined by the central server.

Claim 11

The server of claim 7 further comprising:
an identity manager, to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link, and wherein the user identifiers are changed over time.

Claim 12

The server of claim 11 wherein the user or entity identifiers are associated with a device identifier by the identity manager, and the device identifier is selected from one of:
a media access control (MAC) addresses of a short range wireless network adapter;
a SSID in an IEEE-802.11 network beacon;
a BSSID of an IEEE802.11 network adapter;
a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message;
a device name in a Bluetooth name response packet; or
one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.

Claim 13

The method of claim 1 wherein the user or entity identification information is changed to protect the privacy of the identity of the a user or entity associated with the second wireless device.
Claim 14
The method of claim 1 wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.
Claim 15
The method of claim 7 wherein the user or entity identification information is changed to protect the privacy of the identity of a user or entity associated with the second wireless device.
Claim 16
The method of claim 7 wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.
Claim 17
The method of claim 1 wherein the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device.
Claim 18
The method of claim 1 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.
Claim 19
The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.
Claim 20
The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.
Claim 21
The method of claim 1 wherein upon the occurrence of the predetermined event, further notifying the second wireless device of the modified identification

information via a wireless configuration message or an instruction to change communication state.

Claim 22

The server of claim 7 wherein the central server further receives modified identification information, as collected by the first wireless device from the second wireless device.

Claim 23

The server of claim 7 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.

Claim 24

The server of claim 23 wherein the modified identification information is used by the central server to verify legitimacy, identity or authenticity of the first wireless device.

Claim 25

The server of claim 7 wherein the modified identification information is used by the central server to verify legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.

Claim 26

The server of claim 7 wherein upon the occurrence of the predetermined event, the server further notifies the second wireless device of the modified identification information via a wireless configuration message or an instruction to change communication state.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. §42.6(E)(4)

I certify that on January 9, 2026, a copy of the foregoing document, including any exhibits or appendices filed therewith, is being served via *Overnight FedEx* at the following correspondence address of record for the patent:

VLP Law Group LLP
555 Bryant Street
Suite 820
Palo Alto, CA 94301

A courtesy copy was also sent via electronic mail to Patent Owner's counsel of record in IPR2025-01183 at the following addresses:

Brent Bumgardner	brent@nelbum.com
Charles Austin Ginnings	austin@nelbum.com
Christopher G. Granaghan	chris@nelbum.com
Timothy E. Grochocinski	tim@nelbum.com
Taryn N. Trusty	taryn@nelbum.com

Date: January 9, 2026

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned certifies that the foregoing Petition for *Inter Partes* Review contains 13,992 words excluding a table of contents, a table of authorities, Mandatory Notices under §42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: January 9, 2026

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.