

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.

Petitioners

v.

SURECELL TRANSACTIONS LLC,
Patent Owner

Case No. IPR2026-00506
U.S. Patent No. 7,924,156

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 7,924,156**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. REQUIREMENTS UNDER 37 C.F.R. §42.104.....	1
A. GROUNDS FOR STANDING	1
B. IDENTIFICATION OF CHALLENGE AND STATEMENT OF PRECISE RELIEF REQUESTED	1
III. '156 PATENT.....	2
A. SPECIFICATION	2
B. FILE HISTORY	3
IV. LEVEL OF ORDINARY SKILL IN THE ART.....	3
V. CLAIM CONSTRUCTION	3
A. TERMS CONSTRUED IN <i>MYNETTE</i>	4
B. “MECHANICAL SWITCH”	5
VI. SUMMARY OF PRIOR ART.....	6
A. <i>WATERS</i> (EX1024)	6
B. <i>DUA</i> (EX1023).....	7
C. <i>PONT</i> (EX1026).....	8
D. <i>SELKER</i> (EX1027).....	11
VII. INVALIDITY	12
A. GROUND 1A: <i>WATERS</i>	12
i. Independent Claim 1	13
ii. Independent Claim 11	20
iii. Independent Claim 14	20
iv. Independent Claim 20	22
v. Independent Claim 29	24
vi. Independent Claim 51	25
vii. Independent Claim 53	25
viii. Independent Claim 54	26
ix. Independent Claim 57	26

x.	Independent Claim 60	27
xi.	Dependent Claims	28
B.	GROUND 1B: <i>WATERS WITH PONT</i>	33
i.	Motivation to Combine	33
ii.	“State Memory” Claims: 1, 4, 6-7, 11, 14, 20, 23-24, 29, 51-54, 57, 60.....	37
iii.	Claims 2-3, 5, 8-10, 12-13, 15-19, 21-22, 25-28, 30-33, 55-56, 58-59	38
C.	GROUND 1C: <i>WATERS WITH SELKER</i>	38
i.	Motivation to Combine	39
ii.	Independent Claim 39	42
iii.	Dependent Claims	43
D.	GROUND 2A: <i>DUA</i>	44
i.	Independent Claim 1	44
ii.	Independent Claim 14	51
iii.	Independent Claim 20	53
iv.	Independent Claim 29	56
v.	Independent Claim 34	57
vi.	Independent Claim 44	58
vii.	Independent Claim 51	60
viii.	Independent Claim 53	60
ix.	Independent Claim 54	61
x.	Independent Claim 57	61
xi.	Dependent Claims	62
E.	GROUND 2B: <i>DUA WITH PONT</i>	68
i.	Motivation to Combine	68
ii.	“State Memory” Claims: 1, 4, 6-7, 14, 20, 23-24, 29, 34, 44, 47, 51-54, 57	71
iii.	Claims 2-3, 5, 8-10, 15-19, 21-22, 25-28, 30-33, 35-38, 45-46, 48-50, 55-56, 58-59.....	72
F.	GROUND 2C: <i>DUA WITH SELKER</i>	72

i.	Motivation to Combine	72
ii.	Independent Claim 39	75
iii.	Dependent Claims	76
VIII.	SECONDARY CONSIDERATIONS	77
IX.	CONCLUSION	77

PETITIONERS' EXHIBIT LIST¹

Exhibit	Description of Documents
EX1001	U.S. Patent No. 7,924,156
EX1002-1006	RESERVED
EX1007	Prosecution History of U.S. Patent No. 7,924,156
EX1008-1012	RESERVED
EX1013	Declaration of Sayfe Kiaei in support of petition for <i>inter partes</i> review of U.S. Patent No. 7,924,156
EX1014	RESERVED
EX1015	Sony, Near Field Communication Technology jointly developed by Sony and Philips approved as ISO/IEC International Standard, https://www.sony.com/en/SonyInfo/News/Press/200312/03-059E/ (Dec. 8, 2003)
EX1016	RFID Journal, Nokia Unveils RFID Phone Reader, https://www.rfidjournal.com/news/nokia-unveils-rfid-phone-reader/78579/ (Mar. 17, 2004)
EX1017	EuroTechnology, ApplePay vs Osaifu-Keitai - CNBC Interview, https://www.eurotechnology.com/2014/09/18/applepay-vs-osaifu-keitai-cnbc/ (Sept. 18, 2014)
EX1018	IEEE Spectrum, Here Comes The Wallet Phone, https://spectrum.ieee.org/here-comes-the-wallet-phone (Nov. 1, 2005)
EX1019	Declaration of Sylvia D. Hall-Ellis, Ph.D. in support of authenticity and public availability of documents for <i>inter partes</i> review of U.S. Patent No. 7,924,156
EX1020	<i>SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-00106, Dkt. 9 (E.D. Tex. Feb. 26, 2026) (“Amended Complaint”)

¹ Unless otherwise indicated, U.S. patents are cited by column:line, U.S. patent application publications, complaints, and declarations by paragraph number, patent figures by figure number, and all other materials by Bates number.

EX1021	SureCell’s Infringement Contentions, <i>SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.</i> , No. 2:26-cv-00106 (E.D. Tex. Feb. 26, 2026)
EX1022	Claim Construction Order, <i>Mynette Techs., Inc. and Steven M. Colby v. The United States and Unisys Corp.</i> , No. 16-1647 (COFC Aug. 17, 2018)
EX1023	U.S. Patent Publication No. 2006/0165060 (“ <i>Dua</i> ”), published July 27, 2006 (filed Jan. 21, 2005)
EX1024	U.S. Patent Publication No. 2009/0215385 (“ <i>Waters</i> ”), published August 27, 2009 (PCT filed Feb. 15, 2005)
EX1025	RESERVED
EX1026	Pont, <i>Embedded C</i> (2002)
EX1027	U.S. Patent Publication No. 2003/0132301 (“ <i>Selker</i> ”), published July 17, 2003
EX1028	U.S. Army, <i>Engineering Design Handbook: Timing Systems and Components</i> (Dec. 31, 1975)
EX1029	Finkenzeller, <i>RFID Handbook</i> , 2d ed. (2003)
EX1030	Koslowski, <i>Global Migration Perspectives</i> (Oct. 2004)
EX1031-1033	RESERVED
EX1034	CV of Sayfe Kiaei
EX1035	Petitioners’ Stipulation

MANDATORY NOTICES UNDER 37 C.F.R. §42.8(A)(1)

Real Parties in Interest: The real parties in interest are Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc., Petitioners.

Related Matters: U.S. Patent No. 7,924,156 (“156 patent”) is currently asserted by Patent Owner (“PO”) against Petitioners in the case styled: *SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-00106 (E.D. Tex.), which was originally filed on February 26, 2026.

Lead Counsel and Back-Up Counsel: Petitioners designate lead and back-up counsel as noted below. Powers of Attorney are filed concurrently herewith under 37 C.F.R. §42.10(b).

LEAD COUNSEL	BACK-UP COUNSEL
Eliot D. Williams, Reg. No. 50,822 Baker Botts L.L.P. 700 K Street, N.W. Washington, D.C. 20001-5692 Phone: 202.639.1334 Fax: 202.639.7890 eliot.williams@bakerbotts.com	Neil Sirota, Reg. No. 38,306 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2548 Fax: 212.259.2548 neil.sirota@bakerbotts.com Megan LaDriere White, Reg. No. 75,995 Baker Botts L.L.P. 2001 Ross Avenue Suite 900 Dallas, Texas 75201-2980 Phone: 214.953.6948 megan.white@bakerbotts.com

LEAD COUNSEL	BACK-UP COUNSEL
	Eric Faragi, Reg. No. 51,259 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2591 eric.faragi@bakerbotts.com Benjamin Rosen, Reg. No. 84,598 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2691 benjamin.rosen@bakerbotts.com Coleman Strine, Reg. No. 79,981 Baker Botts L.L.P. 30 Rockefeller Plaza, Ste 4340 New York, NY 10112-4498 Phone: 212.408.2595 coleman.strine@bakerbotts.com

Service Information: Correspondence to lead and back-up counsel can be provided at the postal and electronic addresses above. Petitioners also consent to service by electronic mail at DLSamsungvSureCell_IPRs@bakerbotts.com.

CLAIMS LISTING

Claim 1:

1[pre]	A RFID tag comprising:
1[a]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal; and
1[b]	integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna,
1[c]	an output configured to provide the second RF signal to the antenna for transmission,
1[d]	a state memory configured to store an ON/OFF state including two or more ON states of the RFID tag;
1[e]	a key memory configured for storing a key for changing the ON/OFF state stored in the state memory, and
1[f]	a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison,
1[g]	the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory.

Claim 2:

2	The RFID tag of claim 1, wherein the ON/OFF state of the RFID tag is OFF by default and temporally ON.
---	--

Claim 3:

3	The RFID tag of claim 1, wherein the ON/OFF state of the RFID tag is stored in static memory.
---	---

Claim 4:

4	The RFID tag of claim 1, wherein the determination is responsive to which of the alternative ON states are stored in the state memory.
---	--

Claim 5:

5	The RFID tag of claim 1, wherein the RFID tag is disposed within a passport.
---	--

Claim 6:

6	The RFID tag of claim 1, where in the state memory is configured to store in the alternative, an OFF state, a first ON state and a second ON state.
---	---

Claim 7:

7	The RFID tag of claim 1, where in the state memory is configured to store a first value indicating an ON/OFF state and a second value indicating one of at least two alternative ON states.
---	---

Claim 8:

8	The RFID tag of claim 1, wherein the RFID tag is disposed within a cellular telephone.
---	--

Claim 9:

9	The RFID tag of claim 1, wherein the RFID tag is disposed within a passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
---	--

Claim 10:

10	The RFID tag of claim 1, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	---

Claim 11:

11[pre]	A RFID tag comprising:
11[a]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal; and
11[b]	integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna,
11[c]	an output configured to provide the second RF signal to the antenna for transmission,

11[d]	a state memory configured to store an ON/OFF state of the RFID tag,
11[e]	a key memory configured for storing a key for changing the ON/OFF state stored in the state memory, and
11[f]	a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison,
11[g]	the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory,
11[h]	wherein the state memory or switch logic are shared by two or more RFID tags.

Claim 12:

12	The RFID tag of claim 11, wherein the antenna is shared by several RFID tags.
----	---

Claim 13:

13	The RFID tag of claim 11, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 14:

14[pre]	A RFID tag comprising:
14[a]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal; and
14[b]	integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna,
14[c]	an output configured to provide the second RF signal to the antenna for transmission,
14[d]	a state memory configured to store an ON/OFF state of the RFID tag, the ON/OFF state being responsive to timing using a resistor-capacitor circuit;
14[e]	a key memory configured for storing a key for changing the ON/OFF state stored in the state memory, and

14[f]	a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison,
14[g]	the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory.

Claim 15:

15	The RFID tag of claim 14, wherein the ON/OFF state of the RFID tag is OFF by default and temporally ON.
----	---

Claim 16:

16	The RFID tag of claim 14, wherein the ON/OFF state of the RFID tag is stored in static memory.
----	--

Claim 17:

17	The RFID tag of claim 14, wherein the RFID tag is not remotely detectable using an RF signal when the ON/OFF state is OFF.
----	--

Claim 18:

18	The RFID tag of claim 14, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 19:

19	The RFID tag of claim 14, wherein the RFID tag is disposed within a passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
----	---

Claim 20:

20[pre]	A RFID tag comprising:
20[a]	a mechanical switch configured for selecting between two or more ON states of the RFID tag;
20[b]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal; and

20[c]	integrated circuitry including an input configured to receive data from the antenna,
20[d]	an output configured to provide the second RF signal to the antenna for transmission,
20[e]	a state memory configured to store a state of the RFID tag, and
20[f]	a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch.

Claim 21:

21	The RFID tag of claim 20, wherein the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power.
----	--

Claim 22:

22	The RFID tag of claim 20, wherein the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch.
----	---

Claim 23:

23	The RFID tag of claim 20, wherein the mechanical switch must be activated and the state stored in the state memory must be an ON state before the second RF signal is transmitted.
----	--

Claim 24:

24	The RFID tag of claim 20, further including a key memory configured for storing a key for changing the state stored in the state memory, the switch logic being further configured to read the key from the key memory, to compare the received data with the read key, and to change the state stored in the state memory responsive to the comparison between the received data with the read key.
----	--

Claim 25:

25	The RFID tag of claim 20, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 26:

26	The RFID tag of claim 20, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 27:

27	The RFID tag of claim 20, wherein the RFID tag is disposed within a passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
----	---

Claim 28:

28	The RFID tag of claim 20, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	--

Claim 29:

29[pre]	A RFID tag comprising:
29[a]	a mechanical switch configured to set a state of the RFID tag stored in a state memory;
29[b]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal;
29[c]	integrated circuitry including an input configured to receive data from the antenna,
29[d]	an output configured to provide the second RF signal to the antenna for transmission,
29[e]	the state memory configured to store the state of the RFID tag, and
29[f]	a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch.

Claim 30:

30	The RFID tag of claim 29, wherein the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power.
----	--

Claim 31:

31	The RFID tag of claim 29, wherein the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch.
----	---

Claim 32:

32	The RFID tag of claim 29, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 33:

33	The RFID tag of claim 29, wherein the RFID tag is disposed within passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
----	---

Claim 34:

34[pre]	A RFID tag comprising:
34[a]	a mechanical switch;
34[b]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal; and
34[c]	integrated circuitry including an input configured to receive data from the antenna,
34[d]	an output configured to provide the second RF signal to the antenna for transmission,
34[e]	a state memory configured to store a state of the RFID tag, and
34[f]	a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch,
34[g]	the state logic being further configured to store a plurality of alternative ON states,
34[h]	the mechanical switch being configured for switching the RFID tag from an OFF state to one of the plurality of alternative ON states.

Claim 35:

35	The RFID tag of claim 34, wherein the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power.
----	--

Claim 36:

36	The RFID tag of claim 34, wherein the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch.
----	---

Claim 37:

37	The RFID tag of claim 34, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 38:

38	The RFID tag of claim 34, wherein the RFID tag is disposed within a passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
----	---

Claim 39:

39[pre]	A RFID tag comprising:
39[a]	a mechanical switch responsive to a state of a mechanical security device;
39[b]	an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal; and
39[c]	integrated circuitry including an input configured to receive data from the antenna,
39[d]	an output configured to provide the second RF signal to the antenna for transmission,
39[e]	a state memory configured to store a state of the RFID tag, and
39[f]	a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch.

Claim 40:

40	The RFID tag of claim 39, wherein the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch.
----	---

Claim 41:

41	The RFID tag of claim 39, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 42:

42	The RFID tag of claim 39, wherein the RFID tag is disposed within passport, identity card, driver's license, immigration document, student
----	--

	identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document.
--	--

Claim 43:

43	The RFID tag of claim 39, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	--

Claim 44:

44[pre]	A method of changing a state of an RFID Tag, the method comprising:
44[a]	receiving energy sufficient to power the RFID Tag through an RF antenna included in the RFID tag;
44[b]	receiving first data through the RF antenna;
44[c]	reading a key from a key memory;
44[d]	using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy;
44[e]	determining a state of a mechanical switch in the RFID tag; and
44[f]	writing data to state memory responsive to the comparison only if the mechanical switch is activated, the data written to the state memory being configured to change the RFID tag from a first state to a second state.

Claim 45:

45	The method of claim 44, wherein the first state is a state in which the RFID tag will not transmit an RF signal.
----	--

Claim 46:

46	The method of claim 44, wherein using an integrated circuit to compare the first data received through the RF antenna with the key is only performed if the state of the mechanical switch is ON.
----	---

Claim 47:

47	The method of claim 44, wherein the state memory is non-volatile memory.
----	--

Claim 48:

48	The method of claim 44, further including automatically returning to the OFF state.
----	---

Claim 49:

49	The method of claim 44, further sending a response signal using the RF antenna if the second state is an ON state.
----	--

Claim 50:

50	The method of claim 44, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	--

Claim 51:

51[pre]	A method of changing a state of an RFID Tag, the method comprising:
51[a]	receiving energy sufficient to power the RFID Tag through an RF antenna included in the RFID tag;
51[b]	receiving first data through the RF antenna;
51[c]	reading a key from a key memory;
51[d]	using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy; and
51[e]	writing data to state memory responsive to the comparison, the data written to the state memory being configured to change the RFID tag from a first state to a second state,
51[f]	wherein the first state and the second state are alternative ON states.

Claim 52:

52	The method of claim 51, wherein the state memory is non-volatile memory.
----	--

Claim 53:

53[pre]	A method of changing a state of an RFID Tag, the method comprising:
53[a]	receiving energy sufficient to power the RFID Tag through an RF antenna included in the RFID tag;
53[b]	receiving first data through the RF antenna;
53[c]	reading a key from a key memory;

53[d]	using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy;
53[e]	writing data to state memory responsive to the comparison, the data written to the state memory being configured to change the RFID tag from a first state to a second state; and
53[f]	providing an RF response, a content of data in the RF response being responsive to the comparison.

Claim 54:

54[pre]	A method comprising:
54[a]	receiving a first signal at an RFID Tag through an RF antenna included in the RFID tag;
54[b]	reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state; and
54[c]	sending a response signal using the RF antenna if the state is the first ON state or the second ON state, the response signal being a response to the first signal,
54[d]	wherein contents of the response signal are responsive to whether the state is the first ON state or the second ON state.

Claim 55:

55	The method of claim 54, wherein the RFID tag is disposed within a cellular phone.
----	---

Claim 56:

56	The RFID tag of claim 54, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	--

Claim 57:

57[pre]	A method comprising:
57[a]	receiving a first signal at an RFID Tag through an RF antenna included in the RFID tag;
57[b]	reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state; and

57[c]	sending a response signal using the RF antenna if the state is the first ON state or the second ON state, the response signal being a response to the first signal,
57[d]	wherein sending the response signal is responsive to a mechanical switch.

Claim 58:

58	The RFID tag of claim 57, wherein the RFID tag is disposed within a cellular telephone.
----	---

Claim 59:

59	The RFID tag of claim 57, wherein the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard.
----	--

Claim 60:

60[pre]	A method comprising:
60[a]	receiving a first signal at an RFID Tag through an RF antenna included in the RFID tag;
60[b]	reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state;
60[c]	sending a response signal using the RF antenna if the state is the first ON state or the second ON state, the response signal being a response to the first signal; and
60[d]	changing the state in the state memory responsive to an RF signal.

I. INTRODUCTION

The Office materially erred in granting U.S. Patent No. 7,924,156 (“the ’156 Patent”). As Petitioners will address in detail in their brief regarding the discretionary institution factors, the Examiner overlooked the obviousness of the claimed limitations, and the search was insufficient to locate highly relevant references. Grounds 1A-2C disclose or render obvious every claimed element of the ’156 Patent.

II. REQUIREMENTS UNDER 37 C.F.R. §42.104

A. GROUNDS FOR STANDING

Petitioners certify under 37 C.F.R. §42.104(a) that the ’156 Patent is eligible for IPR and that Petitioners are not barred or estopped from requesting IPR on Grounds 1A-2C.

B. IDENTIFICATION OF CHALLENGE AND STATEMENT OF PRECISE RELIEF REQUESTED

This IPR, supported by the declaration of Dr. Sayfe Kiaei (EX1013), asserts the following grounds of unpatentability:

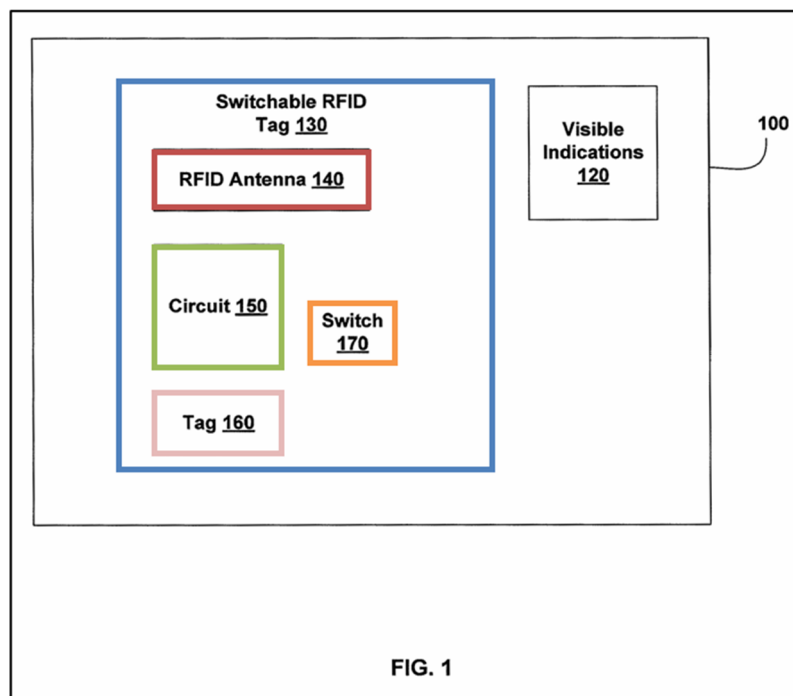
Ground 1A	<i>Waters</i> renders obvious claims 1-33 and 51-60
Ground 1B	<i>Waters</i> with <i>Pont</i> renders obvious claims 1-33 and 51-60
Ground 1C	<i>Waters</i> with <i>Selker</i> renders obvious claims 39-43
Ground 2A	<i>Dua</i> renders obvious claims 1-10, 14-38, and 44-59
Ground 2B	<i>Dua</i> with <i>Pont</i> renders obvious claims 1-10, 14-38, and 44-59
Ground 2C	<i>Dua</i> with <i>Selker</i> renders obvious claims 39-43

III. '156 PATENT

A. SPECIFICATION

The '156 Patent is titled “Electronically Switchable RFID Tags,” and generally relates to an RFID tag which can operate in a plurality of states, including an OFF state and one or more ON states. EX1001, Cover, 3:15-28, claims 1-60, FIG.

1. In some embodiments, an RFID tag 130 can include switch 170, which selects a state. *Id.* Tag 160 controls RFID communication, responsive to the state. *Id.*, 8:65-9:15. Circuit 150 conveys signals between tag 160 and RFID antenna 140. *Id.*, 7:62-8:3.



EX1001, FIG. 1.²

² All colored text/annotations in figures and emphasis in quotes are added unless noted.

B. FILE HISTORY

The '156 Patent, filed July 19, 2006 (Application No. 11/458,620), purports on its face to claim priority to a provisional application filed May 6, 2005. EX1001, Cover. The '156 Patent published May 17, 2007 and issued April 12, 2011. *Id.*

Following several Non-Final Office Actions, Applicant amended claims on July 30, 2009, March 15, 2010, September 21, 2010, and October 24, 2010. EX1007, 125-131, 78-93, 40-55, 20-35.

On December 16, 2010, the pending claims were allowed without further rejection. EX1007, 9-11.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in the Art (“POSITA”) at the time of the '156 Patent would have had either (i) a Master of Science in Electrical Engineering or an equivalent field, or (ii) a Bachelor of Science in Electrical Engineering or an equivalent field and two years of experience in the field of RFID communications. EX1013, ¶¶50-51.

V. CLAIM CONSTRUCTION

Petitioners propose that all terms be given their ordinary and customary meaning and identify the following terms for construction, in view of potential differing interpretations.

A. TERMS CONSTRUED IN *MYNETTE*

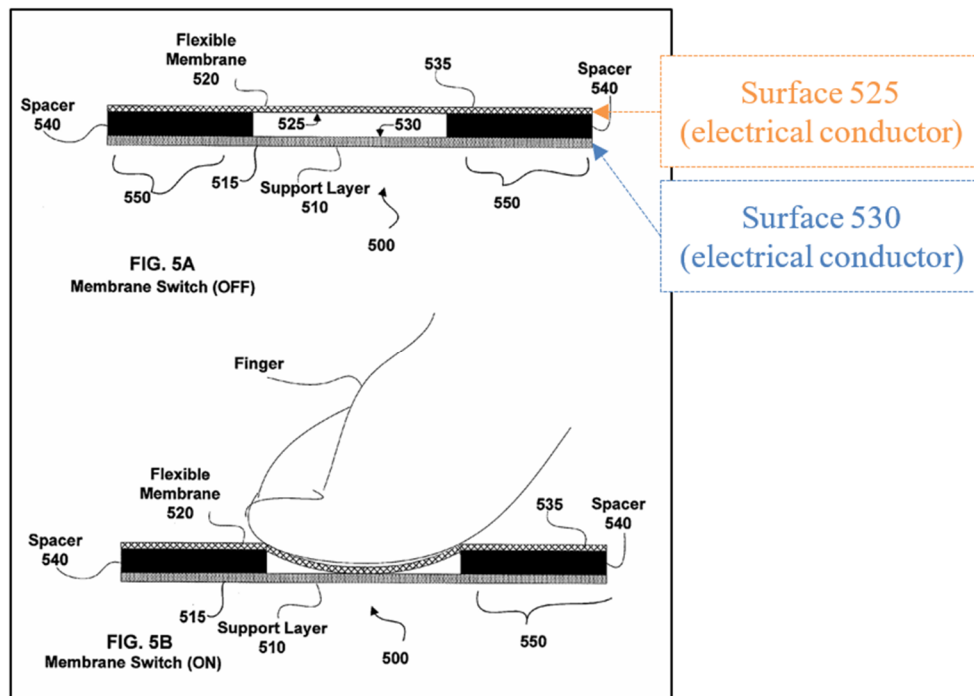
The following terms, which Petitioners identify for construction, were construed in prior litigation involving the '156 Patent:

Term	Proposed Construction
RFID tag	Radio Frequency Identification Tag
State memory	Volatile memory, non-volatile memory, FLASH, SDRAM, ROM, or DRAM which stores/holds the status of an RFID Tag
Key memory	Volatile memory, non-volatile memory, FLASH, SDRAM, ROM, or DRAM which stores/holds a key of an RFID Tag
Response	Plain and ordinary meaning
Responsive	Plain and ordinary meaning
ON/OFF state	A switchable status that includes an OFF state and at least one ON state. An OFF state is one in which data cannot be transmitted from a RFID tag; an ON state is one in which data can be transmitted from a RFID tag
Switch	A control device that makes or breaks an electrical connection in a circuit
Switch logic	Circuitry and set or sets of logic instructions directing the operation of a RFID tag
Passport	A passport booklet

EX1022, 15, 20, 41.

B. “MECHANICAL SWITCH”

Petitioners further identify the term “mechanical switch” for construction. A POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.” EX1013, ¶¶52-55. The specification describes that a mechanical switch “is optionally a sliding switch, a flip switch, a rotating switch, membrane switch, pushbutton switch, or other mechanical switch.” EX1001, 25:20-23. The specification further describes that in some embodiments, the switch “is a mechanical contact switch activated by applying pressure to an outside surface of Switchable RFID Device 2200.” *Id.*, 25:28-31. Further, the switch can be “configured to be moved between the on position and the off position, for example using a finger.” *Id.*, 26:38-40. As illustrated in Figures 5A-B (showing a membrane switch, which is a type of mechanical switch), the switch makes or breaks an electrical connection responsive to movement of the switch components. *Id.*, 25:20-23 (listing “membrane switch” among types of mechanical switches), 26:59-61 (when the membrane switch is pressed by a user, “electrical conductors on a Surface 2630 and a Surface 2625 [are brought] together” and “a switchable RFID tag is controlled, activated or deactivated”); EX1013, ¶¶52-55.



EX1001, FIGs. 5A-B.

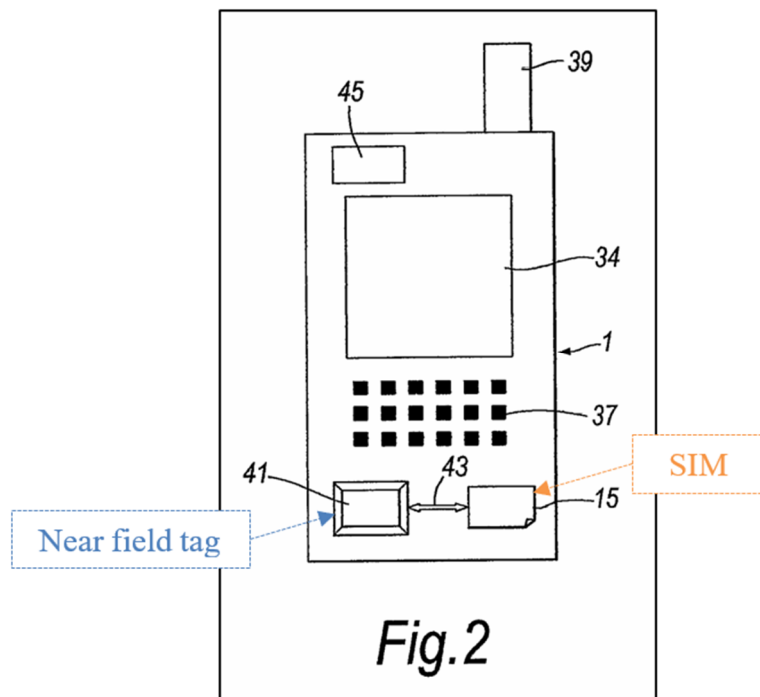
VI. SUMMARY OF PRIOR ART

Petitioners assume, without conceding, that claims 1-60 of the '156 Patent (“Challenged Claims”) are entitled to a May 6, 2005 priority date and are subject to pre-AIA provisions.

A. *WATERS* (EX1024)

US 2009/0215385 (“*Waters*”) published on August 27, 2009 and claims priority to WO 2006/087503, which was filed on February 15, 2005. WO 2006/087503 was a PCT application in Great Britain, published in English, and designated the United States. Thus, *Waters* is prior art under pre-AIA 35 U.S.C. §102(e).

Waters is titled “Improved Security for Wireless Communication” and relates to cellphones having a **SIM** that controls a **near field tag** for facilitating financial transactions. EX1024, Abstract, [0057]. *Waters* discloses pressure sensors, PINs, and biometrics to authenticate users and enable RFID communication. *Id.*, [0051]-[0054]. Additionally, the RFID tag actively jams nearby readers when not in use. *Id.*, [0055].

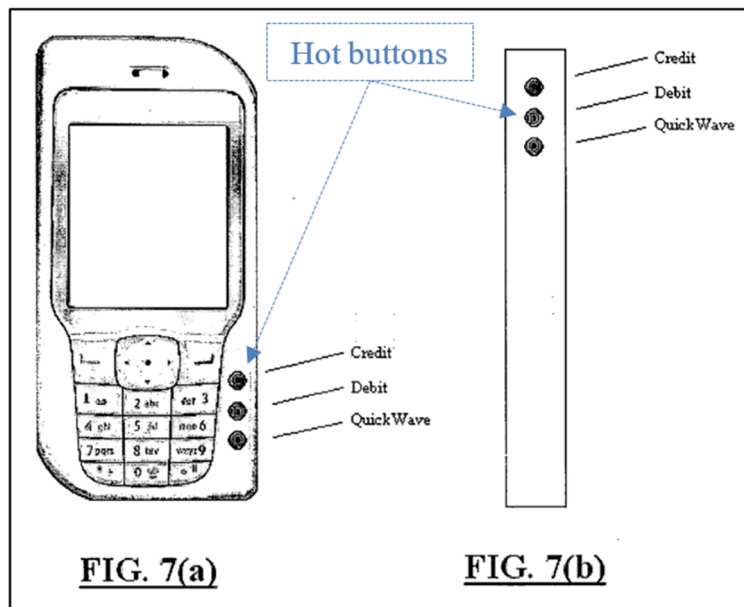


Id., FIG. 2.

B. DUA (EX1023)

US 2006/0165060 (“*Dua*”) was filed on January 21, 2005 and published on July 27, 2006. Thus, *Dua* is prior art under pre-AIA 35 U.S.C. §102(e).

Dua is titled “Method and Apparatus for Managing Credentials Through a Wireless Network.” *Dua* relates to systems and methods for conducting cellphone-based financial transactions. EX1023, [0026], [0041], [0296], FIG. 7. *Dua*’s wallet application manages user interface, storage, processing, and communication functionality for RFID transactions. *Id.*, [0288], [0309]-[0311]. Hot buttons can enable/disable RFID communication and select a transaction mode. *Id.*, [0388]-[0395].



EX1023, FIG. 7.

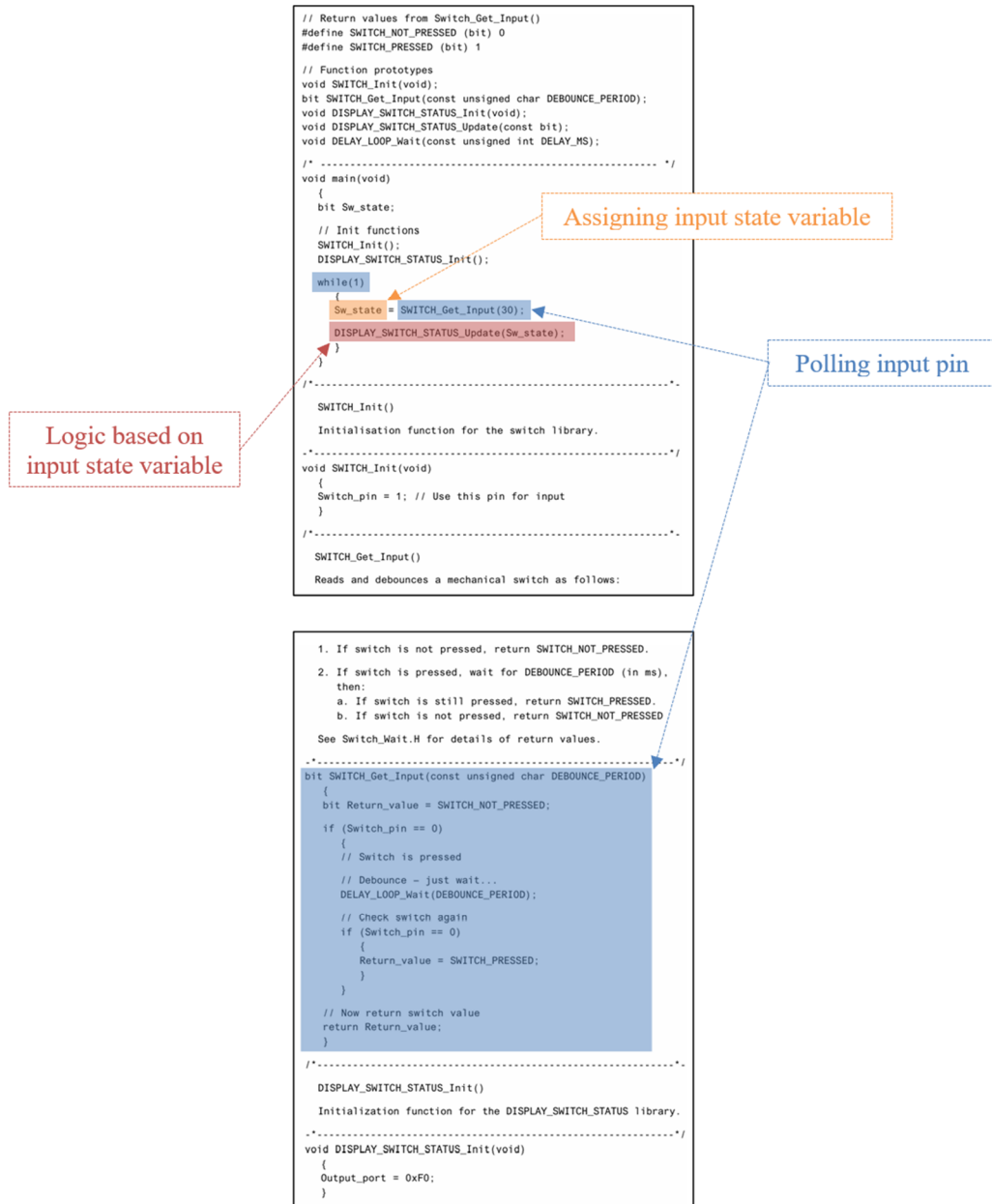
C. *PONT* (EX1026)

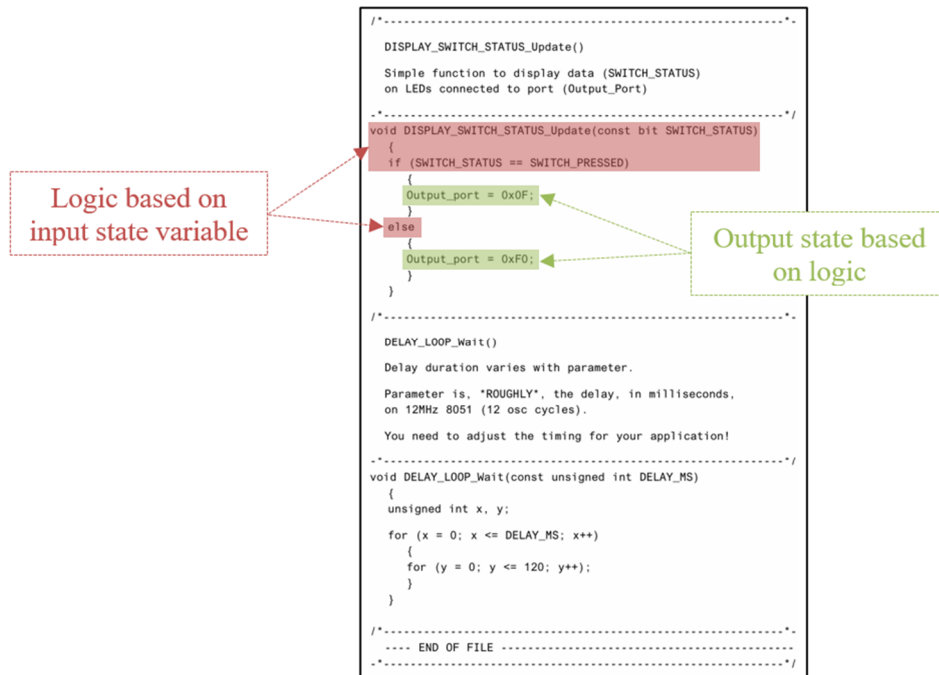
Pont is a textbook, which published in 2002. EX1019, 24. Thus, *Pont* is prior art under pre-AIA 35 U.S.C. §§102(a) and/or (b).

Pont is titled “Embedded C,” and relates to programming embedded processors using the C programming language. EX1026, xi. Such processors are used for many applications, including cellphones. *Id.*, xi, 2. *Pont* teaches a programmer to program a processor to control outputs based on inputs. *Id.*, ch. 4. Specifically, *Pont* teaches programming a processor to poll an input pin, assign the input value to an input state variable, perform logic using the input state variable, and set an output state variable based on the logic. *Id.*, 71-74.

```
/*-----*/
Switch_read.C (v1.00)
-----
A simple 'switch input' program for the 8051.
- Reads (and debounces) switch input on Pin1^0
- If switch is pressed, changes Port 3 output
/*-----*/

#include <Reg52.h>
// Connect switch to this pin
sbit Switch_pin = P1^0;
// Display switch status on this port
#define Output_port P3
```





EX1026, 71-74.

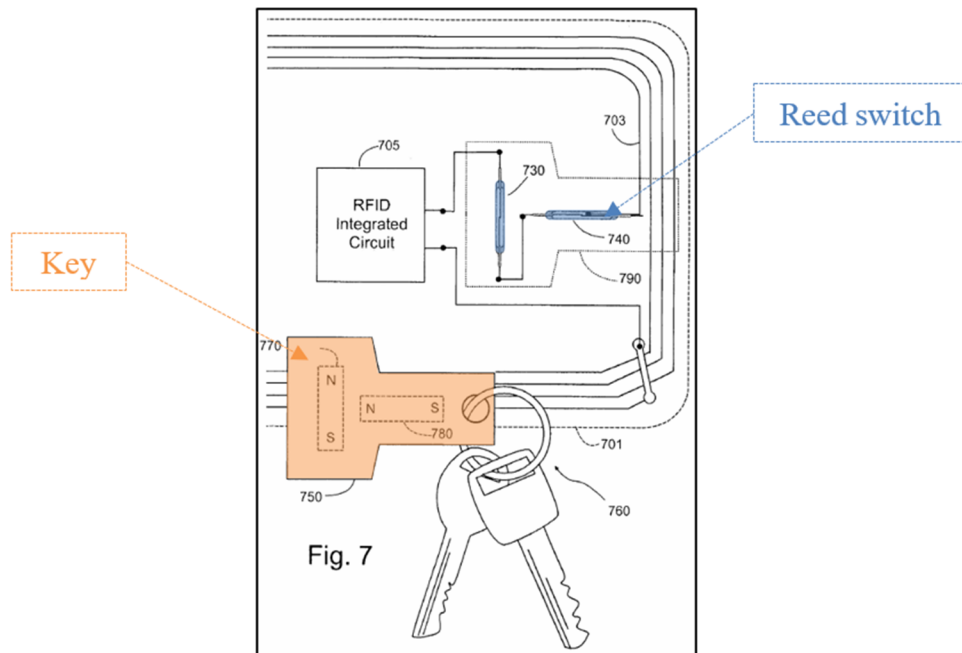
D. ***SELKER*** (EX1027)

US 2003/0132301 (“*Selker*”) was filed on December 31, 2002, and published on July 17, 2003. Thus, *Selker* is prior art under pre-AIA 35 U.S.C. §§102(a), (b), and/or (e).

Selker is titled “Manually Operated Switch for Enabling and Disabling an RFID Card,” and relates to security measures for opening and closing RFID circuits. EX1027, Abstract. Specifically, *Selker* discloses a reed switch mechanism including two perpendicular reed switches connected in series, which is implemented on an RFID device. EX1027, [0004], [0027], [0031], FIG. 7. When a key having two perpendicularly-arranged magnets is brought within close proximity to the card, and

aligned with the reed switches, the reed switches close, and the circuit is completed.

Id. This technique can be applied using “different keys, or different placements of a single key...to selectively close only certain on-card switches to provide the needed connections.” *Id.*, [0031].



Id., FIG. 7.

VII. INVALIDITY

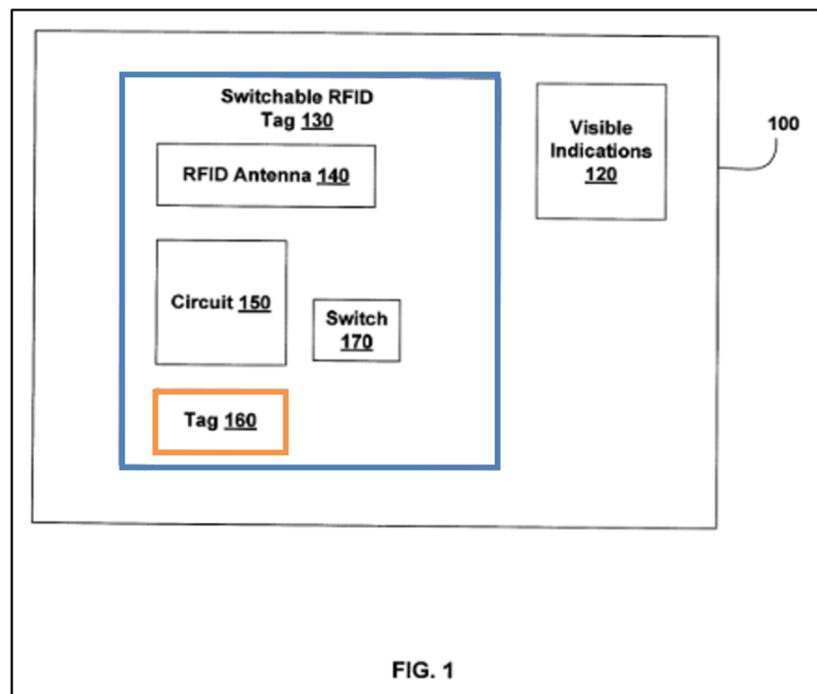
A. GROUND 1A: *WATERS*

Waters renders obvious claims 1-33 and 51-60.

i. **Independent Claim 1**

1[pre]: A RFID tag

The '156 Patent inventors use the term “RFID tag” to encompass a Radio Frequency Identification Device, which includes a “tag.” See EX1001, FIG. 1 (below); EX1013, ¶72.



Waters similarly discloses hardware/software components that enable RFID communication (RFID tag), including SIM 15. EX1024, [0034], [0037]; EX1021, 250 (similarly, in its Infringement Contentions, SureCell interprets an RFID tag as “any subset of the accused device that performs the recited functions, for example...the combination of the NFC antenna, the NFC controller, and the associated secure element and/or host card-emulation subsystem”). SIM 15 further includes near field tag 41 and control link 43. *Id.*, [0037], [0057] (“the mechanism

for activating/deactivating the tag may be incorporated directly into...SIM 15 itself. Also, the tag 41 or part of the tag 41 may be incorporated into the SIM 15.”); EX1013, ¶¶72-75. Near field tag 41 provides RFID communication functionality and SIM 15 controls tag 41 via control link 43. EX1024, [0035]-[0037].

Thus, *Waters* discloses 1[pre].

1[a]: an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal

Tag 41 includes an “inbuilt inductive antenna” (antenna), which can receive data and power from a signal emitted by an RFID reader (first RF signal) and “exchange information” with the RFID reader when in “close proximity,” including financial transaction data (second RF signal). *Id.*, [0035]; Abstract. Tag 41 can be “passive,” such that transmission of the financial transaction data (second RF signal) is powered by the energy received from the signal emitted by the RFID reader (first RF signal). *Id.*; EX1013, ¶¶76-78.

Thus, *Waters* discloses 1[a].

1[b]: integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna

Waters discloses that the device circuitry receives data and power. For example, the circuitry receives RFID data from a tag reader via the inductive antenna.

Id., [0035]. Additionally, as discussed above, the device can be “passive,” such that its circuitry receives power from the tag reader. *Id.*, [0035]; Abstract.

A POSITA would understand that an input to receive and analyze data and power necessarily flows or is a natural result of such RFID functionality, because without such an input, the device circuitry could not receive power or data from the antenna, or any other source, as described. EX1013, ¶¶79-84; EX1024, [0035] (the circuitry receives data and power from the antenna), [0051] (the circuitry also receives data from a keypad).

It would also have been obvious to a POSITA that the functionality discussed above would be implemented as integrated circuitry. EX1013, ¶¶79-84. For example, as discussed above, *Waters* describes a passive RFID device powered by a reader’s RF signal, and a POSITA would therefore understand that the device contains integrated circuitry coupled to its antenna, to obtain the received data and operating power. EX1013, ¶¶79-84. Further, such integrated circuits were commonly used in mobile phone and RFID applications to provide communications and control functionality, with increased efficiency and decreased cost, compared to other methods. *Id.*; EX1029, 292-293; EX1026, 4.

Thus, *Waters* renders obvious 1[b].

1[c]: integrated circuitry including...an output configured to provide the second RF signal to the antenna for transmission

Similar to the above, tag 41 (including SIM 15, which *Waters* explains provides “control...to the operation of” tag 41) controls the inductive antenna to “exchange information” (send/receive data) with a “tag reader when the two are brought into close proximity.” EX1024, [0035]. Such functionality includes an output to provide financial transaction data (second RF signal) to the antenna. *Id.*, Abstract, [0045].

Thus, *Waters* discloses 1[c].

1[d]: integrated circuitry including...a state memory configured to store an ON/OFF state including two or more ON states of the RFID tag

Tag 41, under control of SIM 15, can enter a jamming state (first ON state), a transaction state (second ON state), and a deactivated state (OFF state). In the jamming state (first ON state), the “device attempts to create collisions and other forms of interference,” such that other RFID tags cannot nefariously communicate with a nearby RFID reader. *Id.*, [0055]. This state corresponds to a first ON state, because the device transmits data. *See supra* §V.A (“an ON state is one in which data can be transmitted from a RFID tag”); EX1013, ¶¶88-92.

The jamming functionality is disabled when “authorized use” of the device is required. EX1024, [0055]. *Waters* discloses that a PIN can be used to authorize a user prior to a transaction. *Id.*, Abstract (“mobile terminal (1) is operable to obtain

security data from the user thereof, such as a PIN....The input device or sensor is used to confirm the identity of the user or to evaluate whether the user wishes to use the near field tag (41) to make a payment...”), [0051] (“the keypad 37 of the mobile terminal 1 is used to enter a PIN (or other secret password) to enable the near field tag 41”). Thus, a POSITA would understand that when a PIN is successfully entered by a user, the jamming functionality can be disabled and near field tag 41 can transition from the jamming state (first ON state) to a transaction state (second ON state), in which near field tag 41 can communicate with an RFID reader to facilitate a financial transaction. *Id.*, Abstract, [0045], [0051], [0055]-[0056]; EX1013, ¶¶88-92. Then, near field tag 41 can automatically enter a deactivated state (OFF state) after it has been read by an RFID reader. *Id.*, [0052]. In this state, RFID communication is disabled. *Id.*

Further, the device includes memory, and a POSITA would have understood that the current state (jamming, transaction enabled, or deactivated) would be stored in that memory, reflecting the current device state. *Id.*, [0036], [0051]. Alternatively, it would have been obvious to a POSITA that the device circuitry would store the current state (jamming, transaction, or deactivated) of near field tag 41 in memory (state memory), to enable implementation of the logic described above (transitioning from the jamming state to the transaction state responsive to a PIN, and transitioning from the transaction state to the deactivated state responsive to being read by an

RFID reader). *Id.* As described above, near field tag 41 determines state transitions based on (1) a PIN and (2) whether the tag has been read by an RFID reader. Both of these logical transitions require reading an input and applying logic based on the status thereof. A POSITA would have understood that to implement such functionality, the control software of near field tag 41 would store the current state in a variable, according to logic based on input values, such that state transitions can be implemented. EX1013, ¶¶88-92. Such techniques were well-known at the time of invention. *See* EX1026, 72 (storing switch state in a “Sw_state” variable), 74 (applying logic to “Sw_state” variable and storing output state in an “Output_port” variable). The value of the state variable would be stored in device memory (state memory), such that the software can use the state variable during operation, to control the RFID circuitry to output jamming, transaction, or no data. *See id.*, 26.

Thus, *Waters* renders obvious 1[d].

1[e]: integrated circuitry including...a key memory configured for storing a key for changing the ON/OFF state stored in the state memory

The PIN (key) may be stored in a “secure location” (key memory) of SIM 15. EX1024, [0051], [0057]. As discussed above with reference to 1[d], the PIN (key) is used to change the state stored in state memory from a jamming state (first ON state) to a transaction state (second ON state). *See supra* §VII.A.i.1[d].

Thus, *Waters* discloses 1[e].

1[f]: integrated circuitry including...a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison

As discussed above, *Waters* discloses that a PIN is used to transition from the jamming state (first ON state) to the transaction state (second ON state). Specifically, a PIN (data) is received from a keypad on the device. EX1024, [0051]. The PIN (data) is received by the device circuitry via the input, which as described above, includes the data receiving means of the device circuitry. *See supra* §VII.A.i.1[b].

Then, a stored PIN (key) is read from a secure location (key memory) of SIM 15 and compared with the entered PIN (data). *Id.* If the entered PIN (data) matches the stored PIN (key), SIM 15 controls near field tag 41 to transition from a jamming state (first ON state) to a transaction state (second ON state). *Id.*, [0051], [0057]; *see supra* §VII.A.i.1[d].

Thus, *Waters* discloses 1[f].

1[g]: the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory

As discussed above with reference to 1[d], *Waters* discloses, or otherwise renders obvious, logic to determine whether to provide financial transaction data (second RF signal) to the antenna for transmission, depending on the current state

(jamming, transaction, or deactivated) stored in state memory. *See supra* §VII.A.i.1[d].

Thus, *Waters* discloses, or otherwise renders obvious 1[g].

ii. Independent Claim 11

11[pre]-[g]

Waters discloses and/or renders obvious 11[pre]-[g] for the same reasons discussed above with respect to 1[pre]-[g]. *See supra* §VII.A.i.1[pre]-[g].

11[h]: the state memory or switch logic are shared by two or more RFID tags

One mobile terminal (e.g., a mobile telephone) can include multiple RFID tags, each of which is controlled by a shared controller implementing the logic described above (switch logic). EX1024, [0005], [0076].

Thus, *Waters* discloses 11[h].

iii. Independent Claim 14

14[pre]-[c]

Waters discloses and/or renders obvious 14[pre]-[c] for the same reasons discussed above with respect to 1[pre]-[c]. *See supra* §VII.A.i.1[pre]-[c].

14[d]: integrated circuitry including...a state memory configured to store an ON/OFF state of the RFID tag, the

ON/OFF state being responsive to timing using a resistor-capacitor circuit

Waters further renders obvious “a state memory configured to store an ON/OFF state of the RFID tag” for the same reasons discussed above with respect to 1[d]. *See supra* §VII.A.i.1[d].

Additionally, tag 41, under control of SIM 15, can include a “round trip detector,” which operates when tag 41 is in an ON state and “sends a test signal when the near field tag 41 is being read/probed and expects a response within a certain round trip delay.” EX1024, [0055]-[0056]. The detector “measures the time taken for a signal to travel from the near field tag 41 to the reader and back to the tag 41,” to determine whether the near field tag 41 is within an acceptable range of an RFID reader. *Id.* If the response signal is not received from the RFID reader after a “predetermined delay” (i.e., near field tag 41 is far from the RFID reader, which has an “RF field[] that [has] been greatly extended”), near field tag 41 enters the deactivated state (OFF state). *Id.* It would have been obvious to a POSITA that this timing functionality could be implemented using a resistor-capacitor (“RC”) circuit, as it was commonly known in the art to build timers using RC circuits. EX1013, ¶¶107-11; *see, e.g.*, EX1028, 10-1 (“RC networks are probably the most commonly used delay networks”); EX1029, 276-78 (discussing use of RC timers in RFID applications). Indeed, a POSITA implementing such predetermined-time deactivation functionality would have recognized a resistor-capacitor timing circuit

as a conventional, inexpensive, and predictable circuit for defining the duration of the temporary ON state. EX1013, ¶¶107-11.

Thus, *Waters* renders obvious 14[d].

14[e]-[g]

Waters discloses and/or renders obvious 14[e]-[g] for the same reasons discussed above with respect to 1[e]-[g]. *See supra* §VII.A.i.1[e]-[g].

iv. Independent Claim 20

20[pre]

Waters discloses 20[pre] for the same reasons discussed above with respect to 1[pre]. *See supra* §VII.A.i.1[pre].

20[a]: a mechanical switch configured for selecting between two or more ON states of the RFID tag

As discussed above with respect to 1[d], near field tag 41, which is incorporated in SIM 15, can transition between a jamming state (first ON state) and a transaction state (second ON state). *See supra* §VII.A.i.1[d]. *Waters* further discloses that a pressure sensor (mechanical switch) can trigger this transition and thus select between these states. EX1024, [0053], [0056]. Thus, the pressure sensor allows a user to select between the jamming state (first ON state) and transaction state (second ON state) by pressing and activating the pressure sensor. EX1013, ¶¶114-17. The pressure sensor discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device

circuitry, responsive to its components being pressed (moved) by a user. *Id.*; *see supra* §V.B (a POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.”). As further discussed above, when “authorized use” of the device is required (i.e., the user presses the pressure sensor), the jamming functionality is disabled and near field tag 41 enters a transaction state. *See supra* §VII.A.i.1[d]; EX1024, [0055]. Thus, a POSITA would understand that when the user “physically presses” the pressure sensor, the device selects between a jamming state (first ON state) and a transaction state (second ON state). EX1013, ¶¶114-17. Indeed, this functionality is similar to the enabling embodiment of the ’156 Patent, which includes an RFID tag that “will transmit a limited amount of data when Switch 170 is off and a less limited amount of data when Switch 170 is on.” EX1001, 8:65-9:10.

Thus, *Waters* discloses 20[a].

20[b]-[e]

Waters discloses and/or renders obvious 20[b]-[e] for the same reasons discussed above with respect to 1[a]-[d]. *See supra* §VII.A.i.1[a]-[d].

20[f]: integrated circuitry including...a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna

for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch

As discussed above with respect to 1[b], near field tag 41 receives data from an input. *See supra* §VII.A.i.1[b].

As discussed above with respect to 20[a], near field tag 41 determines whether to provide financial transaction data (second RF signal) to the antenna for transmission, based on the pressure sensor (mechanical switch). *See supra* §VII.A.iv.20[a]. Alternatively, as discussed above with respect to 1[g], it would have been obvious to a POSITA that such determination can be based on the state stored in state memory. *See supra* §VII.A.i.1[g].

Thus, *Waters* renders obvious 20[f].

v. Independent Claim 29

29[pre]

Waters discloses 29[pre] for the same reasons discussed above with respect to 1[pre]. *See supra* §VII.A.i.1[pre].

29[a]: a mechanical switch configured to set a state of the RFID tag stored in a state memory

As discussed above with reference to 20[a], *Waters* discloses a pressure sensor (mechanical switch) configured to select between a jamming state (first ON state) and a transaction state (second ON state). *See supra* §VII.A.iv.20[a]. As further discussed above, it would have been obvious to a POSITA to store the current state (set by the mechanical switch) in memory (state memory). *See supra* §VII.A.i.1[d].

Thus, *Waters* renders obvious 29[a].

29[b]-[f]

As discussed above, with reference to claim 1, *Waters* discloses and/or renders obvious 29[b]-[e]. *See supra* §VII.A.i.1[a]-[d]. As discussed above with reference to claim 20, *Waters* renders obvious 29[f]. *See supra* §VII.A.iv.20[f].

vi. Independent Claim 51

51[pre]-[f]

Waters discloses and/or renders obvious 51[pre]-[f] for the same reasons discussed above with respect to claims 1 and 20. *See supra* §§VII.A.i, VII.A.iv.

vii. Independent Claim 53

53[pre]-[e]

Waters discloses and/or renders obvious 53[pre]-[e] for the same reasons discussed above with respect to claims 1 and 20. *See supra* §§VII.A.i, VII.A.iv.

53[f]: providing an RF response, a content of data in the RF response being responsive to the comparison

As discussed above with respect to 1[d] and 1[f], near field tag 41 can emit (provide an RF response) either (1) jamming signals (first content type) in a jamming state (first ON state), or (2) transaction data (second content type) in a transaction state (second ON state), depending on whether a user is authenticated (i.e., whether an input PIN matches a stored PIN) (responsive to the comparison). *See supra* §§VII.A.i.1[d], VII.A.i.1[f].

Thus, *Waters* discloses 53[f].

viii. Independent Claim 54

54[pre]-[a]

Waters discloses 54[pre]-[a] for the same reasons discussed above with respect to claims 1 and 20. *See supra* §§VII.A.i, VII.A.iv.

54[b]

Waters renders obvious 54[b] for the same reasons discussed above with respect to 1[d] and 1[g]. *See supra* §§VII.A.i.1[d] (storing an OFF state, a first ON state, and a second ON state in state memory), VII.A.i.1[g] (reading the state from state memory to determine whether to provide a response signal).

54[c]-[d]

Waters discloses 54[c]-[d] for the same reasons discussed above with respect to 1[d] and 1[g]. *See supra* §§VII.A.i.1[d] (contents of response signal depend on whether the current state is the first ON state or the second ON state), VII.A.i.1[g] (sending response signal using antenna depending on whether the current state is the first ON state or the second ON state).

ix. Independent Claim 57

57[pre]-[a]

Waters discloses 57[pre]-[a] for the same reasons discussed above with respect to claim 1. *See supra* §VII.A.i.

57[b]-[c]

Waters discloses 57[b]-[c] for the same reasons discussed above with respect to 54[b]-[c]. *See supra* §§VII.A.viii.54[b]-[c].

57[d]

Waters discloses 57[d] for the same reasons discussed above with respect to 20[f]. *See supra* §VII.A.iv.20[f].

x. Independent Claim 60

60[pre]-[a]

Waters discloses 60[pre]-[a] for the same reasons discussed above with respect to claim 1. *See supra* §VII.A.i.

60[b]-[c]

Waters discloses 60[b]-[c] for the same reasons discussed above with respect to 54[b]-[c]. *See supra* §§VII.A.viii.54[b]-[c].

60[d]: changing the state in the state memory responsive to an RF signal

Tag 41, which is under control of the SIM 15, can be “automatically deactivat[ed] after it has been read by a reader.” EX1024, [0052]-[0054], [0074]. Accordingly, the RFID tag can transition from a transaction state (second ON state) to a deactivated state (an OFF state), responsive to an interrogation signal (RF signal) received from the RFID reader.

As discussed above with reference to 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §VII.A.i.1[d]. Thus, the current state in state memory would be changed from a transaction state (second ON state) to a deactivated state (an OFF state), responsive to an interrogation signal (RF signal) received from the RFID reader.

Thus, *Waters* renders obvious 60[d].

xi. Dependent Claims

Dependent Claims 2, 15: the ON/OFF state of the RFID tag is OFF by default and temporally ON

As discussed above with respect to 1[d], near field tag 41 can be disabled (OFF) by default and is only temporally or temporarily enabled when the user enters a PIN or presses a pressure sensor, after which it automatically returns to the disabled state (OFF state). *See supra* §VII.A.i.1[d]; EX1024, [0053]-[0054].

Thus, *Waters* discloses Claims 2 and 15.

Dependent Claims 3, 16: the ON/OFF state of the RFID tag is stored in static memory

Waters renders obvious Claims 3 and 16 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.A.i.1[d]. As discussed above, it would have been obvious to a POSITA to store the ON/OFF state of near field tag 41 as a value of a state variable. EX1013, ¶¶147-48; EX1026, 26, 47, 72-74. It also would have been obvious to a POSITA that data memory (which stores variable values) would

be implemented as static RAM, as this was a well-known practice at the time of invention. EX1013, ¶¶147-48; EX1026, 24, 26, 34, 47.

Thus, *Waters* renders obvious Claims 3 and 16.

Dependent Claim 4: the determination is responsive to which of the alternative ON states are stored in the state memory

Waters renders obvious Claim 4 for the same reasons discussed above with respect to 1[g]. *See supra* §VII.A.i.1[g].

Dependent Claim 5: the RFID tag is disposed within a passport

Waters teaches incorporating near field tag 41 into portable smart cards and credential devices used “to obtain entry to a building (for example).” EX1024, Abstract, [0002]. It would have been obvious to a POSITA to dispose such an RFID tag within a passport, as RFID-enabled passports are used to “obtain entry” and were well-known at the time of invention. EX1013, ¶¶150-51; EX1030, 4, 14.

Thus, *Waters* renders obvious Claim 5.

Dependent Claim 6: the state memory is configured to store in the alternative, an OFF state, a first ON state and a second ON state

Waters renders obvious Claim 6 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.A.i.1[d].

Dependent Claim 7: the state memory is configured to store a first value indicating an ON/OFF state and a second value indicating one of at least two alternative ON states

Waters renders obvious Claim 7 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.A.i.1[d].

Dependent Claims 8, 13, 18, 25-26, 32, 55, 58: the RFID tag is disposed within a cellular telephone

SIM 15 is incorporated within mobile terminal 1, which may be a handheld mobile telephone (cellular telephone). EX1024, [0020], [0034].

Thus, *Waters* discloses Claims 8, 13, 18, 25-26, 32, 55, and 58.

Dependent Claims 9, 19, 27, 33, & 10, 28, 56, 59

Waters explains the tag/SIM structures may be “incorporated directly into the smart card or SIM 15 itself” and used to make payments (a financial card) or to obtain entry to a building (a keycard). *Id.*, Abstract, [0002], [0045], [0057].

Thus, *Waters* discloses Claims 9, 19, 27, 33, & 10, 28, 56, and 59.

Dependent Claim 12: the antenna is shared by several RFID tags

As discussed above with respect to 11[h], *Waters* discloses that multiple near field tags may be incorporated in a single mobile terminal. *See supra* §VII.A.ii.11[h]. A POSITA would have understood that *Waters*’s multi-tag terminal would be implemented using a single, common antenna to reduce space, component count, cost, and antenna coupling problems in a compact SIM or mobile terminal. EX1013,

¶¶156-58. Such a shared antenna would route received reader signals to a selected tag circuit and transmit the selected tag's response. *Id.*

Thus, *Waters* renders obvious Claim 12.

Dependent Claim 17: the RFID tag is not remotely detectable using an RF signal when the ON/OFF state is OFF

As discussed above with respect to 1[d], near field tag 41 can enter a disabled state (OFF state). *See supra* §VII.A.i.1[d]. In this state, an RFID reader cannot obtain any information from near field tag 41, even when brought into close proximity, and thus near field tag 41 is not remotely detectable. EX1024, [0037].

Thus, *Waters* discloses Claim 17.

Dependent Claims 21, 30: the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power

Waters renders obvious Claims 21 and 30 for the same reasons discussed above with respect to 1[a]-[b]. *See supra* §VII.A.i.1[a]-[b].

Dependent Claims 22, 31: the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch

Waters discloses Claims 22 and 31 for the same reasons discussed above with respect to 20[f]. *See supra* §VII.A.iv.20[f].

Dependent Claim 23: the mechanical switch must be activated and the state stored in the state memory must be an ON state before the second RF signal is transmitted

Waters renders obvious Claim 23 for the same reasons discussed above with respect to 1[g] and 20[a]. *See supra* §§VII.A.i.1[g], VII.A.iv.20[a].

Dependent Claim 24: a key memory configured for storing a key for changing the state stored in the state memory, the switch logic being further configured to read the key from the key memory, to compare the received data with the read key, and to change the state stored in the state memory responsive to the comparison between the received data with the read key

Waters renders obvious Claim 24 for the same reasons discussed above with respect to 1[f]. *See supra* §VII.A.i.1[f].

Dependent Claim 52: the state memory is non-volatile memory

Waters renders obvious Claim 52 for the same reasons discussed above with respect to 1[d] and claims 3 and 16. *See supra* §§VII.A.i.1[d], VII.A.xi (claims 3, 16). As discussed above, it would have been obvious to a POSITA to store the ON/OFF state of near field tag 41 as a value of a state variable. EX1013, ¶¶165-66; EX1026, 26, 47, 72-74. It also would have been obvious to a POSITA that data memory (which stores variable values) would be implemented as non-volatile memory, such that the stored data can be retained after the device is powered off, as this was a well-known practice at the time of invention. EX1013, ¶¶165-66; EX1026, 34, 47.

B. GROUND 1B: *WATERS WITH PONT*

Waters with *Pont* renders obvious claims 1-33 and 51-60.

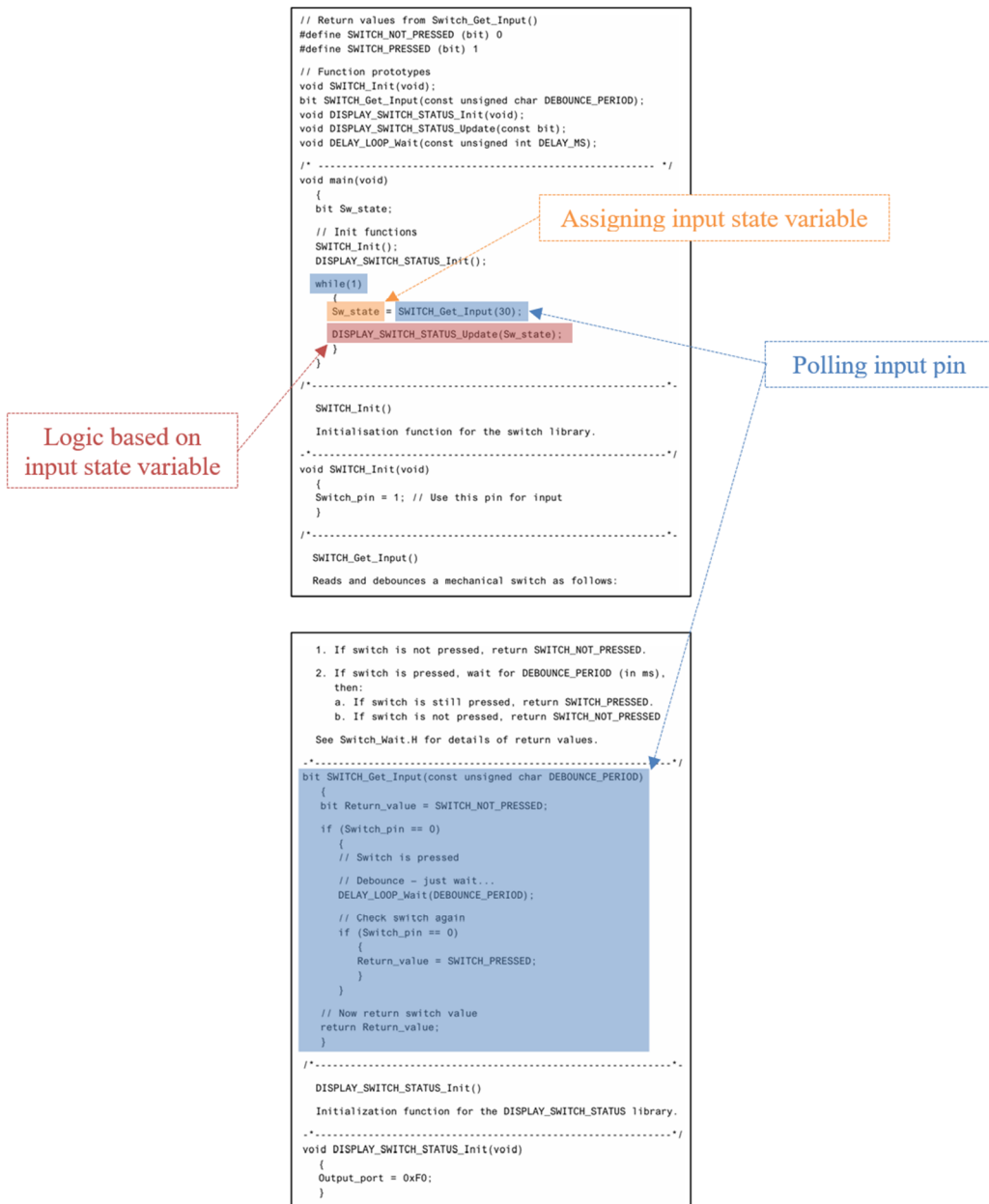
i. Motivation to Combine

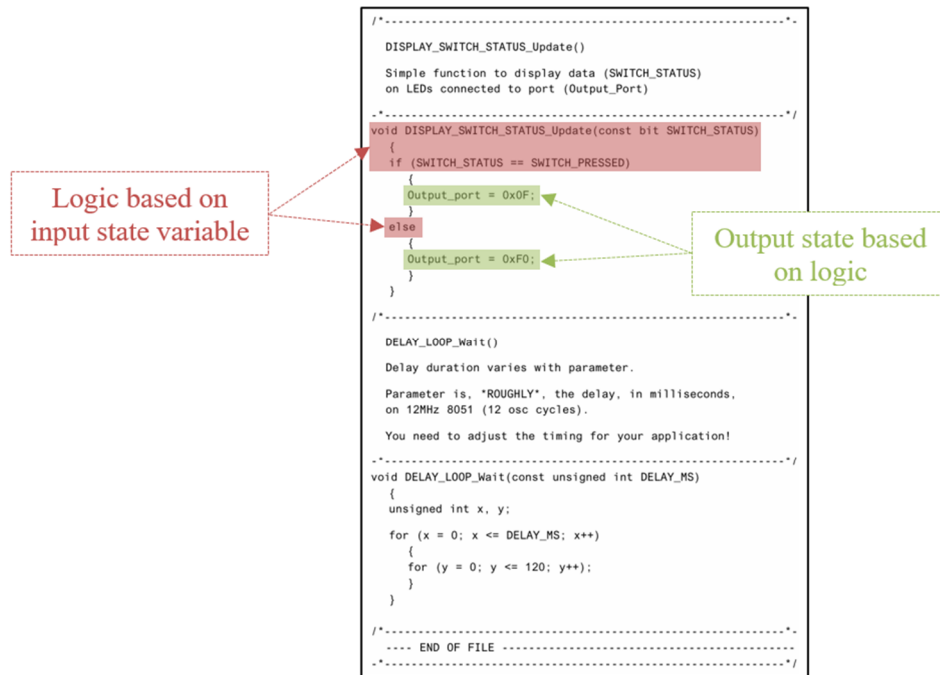
Both *Waters* and *Pont* are directed to mobile phone applications. *Waters* describes a mobile phone that performs RFID-based financial transactions. EX1024, [0020], [0034]. *Pont* is directed to software development using embedded devices, including mobile phone and smart card/SIM processors. EX1026, xi.

Specifically, *Waters* uses SIM 15 and near field tag 41 to carry out its RFID functionality. EX1024, [0036]-[0037]. While *Waters* describes these features in functional terms, it lacks specific disclosure of how these features would be implemented at a software level. For example, *Waters* discloses that SIM 15 and near field tag 41 would interact with inputs and memory, but does not disclose *how* these components would read a switch input or *how* they would interact with memory. *Pont* fills this gap. Indeed, a POSITA would turn to *Pont* for such knowledge, as *Pont* is a contemporary textbook which provides teachings related to programming embedded processors in C. EX1026, xi. Such processors can include mobile phone processors, similar to the control components of SIM 15 and near field tag 41 of *Waters*. *Id.* *Pont* therefore provides useful guidance to a POSITA related to specific methods of programming a microprocessor to carry out mobile phone applications.

Pont discloses that a controller can interface with a switch, and change a device state based on the value of the switch, similar to the functionality described in *Waters*. EX1026, 71-74; EX1024, [0053]. As shown below, *Pont* teaches that to enable such functionality, a switch can be polled. EX1026, 72. On each iteration of the polling loop, the current value of the switch can be checked, and assigned to a switch state variable. *Id.* (storing the value of SWITCH_Get_Input() in the Sw_state variable). Then, the value of the switch state variable can be passed into a controller function, to carry out logic based on the switch state. *Id.* (passing Sw_state into DISPLAY_SWITCH_STATUS_Update()). In the example provided by *Pont*, the controller changes the value of an output state variable, depending on the value of the switch state, to control the state of an LED based on a switch. *Id.*, 74 (assigning different values to the Output_port variable depending on the value of the Sw_state variable), *see also* 192-198.

```
/*-----*/
Switch_read.C (v1.00)
/*-----*/
A simple 'switch input' program for the 8051.
- Reads (and debounces) switch input on Pin1*0
- If switch is pressed, changes Port 3 output
/*-----*/
#include <Reg52.h>
// Connect switch to this pin
sbit Switch_pin = P1^0;
// Display switch status on this port
#define Output_port P3
```





EX1026, 71-74.

Pont teaches the output state variable is stored in RAM. EX1026, 26 (variables are stored in memory). This memory location corresponds to state memory, as it stores information representing the current device state. EX1013, ¶171.

Thus, a POSITA would have been motivated to apply *Pont*'s control structure to *Waters*, such that an output state variable stores the active state of the RFID functionality. EX1013, ¶¶171-73. For example, according to *Pont*'s teachings, a POSITA would understand that in *Waters*, a polling loop would be used to check the current value of a mechanical switch. *Id.* On each iteration of the polling loop, the switch value would be assigned to a switch state variable. *Id.* Then, the value of the switch state variable would be passed to a controller function. *Id.* The controller

function would then apply logic to determine the current state of the RFID transaction functionality, as taught by *Waters*. *Id.* The function would assign this state to an RFID state variable and use the value of this variable to control the downstream functions of the device. *Id.* As taught by *Pont*, the implementation of such logic would require that the RFID state is stored in RAM, which can correspond to a state memory. *Id.*

Moreover, a POSITA would have had a reasonable expectation of success in making this combination. *Id.* For example, *Pont* discloses that its teachings are directly applicable to embedded processors in mobile phones, as well as low-cost and low-power devices (similar to smart cards). EX1026, xi, 2-5, 33; *id.* The *Waters-Pont* combination therefore involves nothing more than applying known elements (software controllers) in a known structure (mobile phones) using known methods (programming in C) to achieve a well-understood and predictable benefit (reliable control of mobile phone processes). EX1013, ¶¶171-74. A POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established programming techniques and produces understood results. *Id.*

ii. **“State Memory” Claims: 1, 4, 6-7, 11, 14, 20, 23-24, 29, 51-54, 57, 60**

Waters-Pont renders obvious a “state memory,” as recited in claims 1, 4, 6-7, 11, 14, 20, 23-24, 29, 51-54, 57, and 60.

As discussed above, based on *Pont*'s teachings, a POSITA would have understood that the device of *Waters* would include memory, which would store information representing the current state of the device. EX1013, ¶¶174-77; *see supra* §VII.A.i.1[d]. The device memory (state memory) would store the current value of a device state variable (jamming (first ON state), transaction (second ON state), or deactivated (OFF state)). *Id.*; *see also* §VII.A.i.1[d].

Except for the implementation of the state memory described above, *Waters-Pont* is identical to *Waters*. Thus, the remaining limitations of claims 1, 4, 6-7, 11, 14, 20, 23-24, 29, 51-54, 57, and 60 are disclosed and/or rendered obvious by *Waters-Pont* for the same reasons discussed above, with respect to *Waters*. *See supra* §VII.A.

iii. **Claims 2-3, 5, 8-10, 12-13, 15-19, 21-22, 25-28, 30-33, 55-56, 58-59**

As discussed above, except for the implementation of the state memory described above, *Waters-Pont* is identical to *Waters*. Thus, claims 2-3, 5, 8-10, 12-13, 15-19, 21-22, 25-28, 30-33, 55-56, and 58-59 are disclosed and/or rendered obvious by *Waters-Pont* for the same reasons discussed above, with respect to *Waters*. *See supra* §VII.A.

C. GROUND 1C: *WATERS WITH SELKER*

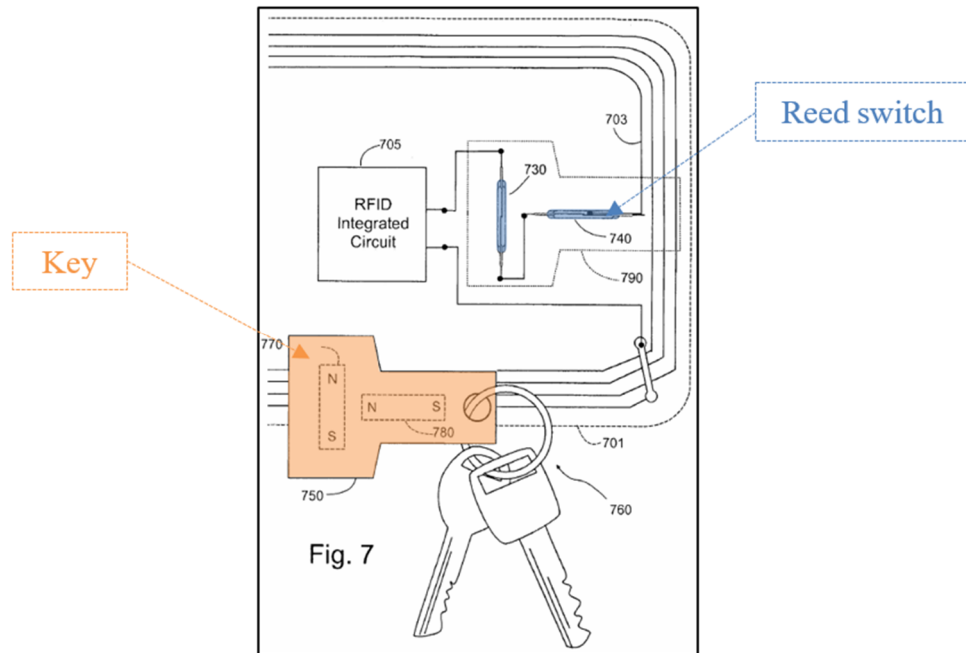
Waters with *Selker* renders obvious claims 39-43.

i. **Motivation to Combine**

Both *Waters* and *Selker* are directed to RFID payment technologies. *Waters* is directed to a mobile phone including components to control and carry out financial transactions using RFID communication. EX1024, [0034], [0043]. *Selker* is directed to a mechanism to protect RFID payment cards from unauthorized misuse. EX1027, [0004].

As discussed above, *Waters* discloses a pressure sensor (mechanical switch), which enables and disables RFID communication to improve data security in RFID applications. EX1024, [0050], [0053]. According to *Waters*, this pressure sensor can prevent skimming. *Id.* *Selker* similarly addresses the issue that “because RF-enabled devices such [as] payment cards can be read at a distance with a suitable transmitter and receiver, it is possible to surreptitiously obtain information from the card while it remains in its cardholder’s possession. In addition to non-contact data transfer, wireless communication can also allow non-line-of-sight communication, meaning that an RF-enabled device may be read while it remains in the cardholder’s wallet or purse.” EX1027, [0003]. Thus, *Selker* teaches that security can be further improved by implementing a reed switch and key mechanism, which is “functionally flexible in order to work in cards and other devices having a variety of shapes and sizes.” *Id.*, [0004], [0027], [0031], FIG. 7. According to *Selker*, this mechanism

provides “enhanced security” and “helps protect” the RFID device “from unauthorized misuse.” *Id.*, [0004], [0019].



Id., FIG. 7.

Based on these teachings, a POSITA would have been motivated to implement *Selker*’s reed switch and key mechanism in the device of *Waters* to achieve improved device security as taught in *Selker*. *Id.*, [0004], [0027], [0031], FIG. 7; EX1013, ¶¶182-83. To do so, a POSITA would have replaced *Waters*’s pressure sensor (mechanical switch) with a set of two perpendicular reed switches, as taught by *Selker*, to securely authenticate a user in possession of a key. EX1013, ¶¶182-83; EX1027, FIG. 7 (reproduced above), [0031]. As discussed above, the jamming functionality of *Waters*’s device is disabled when “authorized use” is required. EX1024, [0055]; *see supra* §VII.A.i.1[d]. Thus, a POSITA would

implement the *Waters-Selker* device such that the near field tag 41 transitions from the jamming state (first ON state) to a transaction state (second ON state), when the magnetic key is placed in close proximity to the set of reed switches. EX1013, ¶¶182-83. As taught by *Waters*, near field tag 41 can later automatically enter a deactivated state (OFF state), in which RFID communication is disabled, after it has been read by an RFID reader. EX1024, [0057]; *id.*

Moreover, a POSITA would have had a reasonable expectation of success in making this combination. EX1013, ¶¶182-83. For example, *Waters* discloses similar security measures. EX1024, [0050], [0053] (discussing pressure sensors to prevent skimming). Meanwhile, *Selker* provides an alternative reed switch and key mechanism, which provides further enhanced security. EX1027, [0004], [0019]. The *Waters-Selker* combination therefore involves nothing more than applying known elements (a reed switch and key mechanism) in a known structure (mobile phones) using known methods (basic circuit design) to achieve a well-understood and predictable benefit (improved device security). EX1013, ¶¶182-83. A POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established circuit design techniques and produces understood results. *Id.*

ii. **Independent Claim 39**

39[pre]

Except for the implementation of the reed switch and key mechanism described above, *Waters-Selker* is identical to *Waters*. Thus, 39[pre] is rendered obvious by *Waters-Selker* for the same reasons discussed above, with respect to *Waters*. See *supra* §VII.A.i.1[pre].

39[a]: mechanical switch responsive to a state of a mechanical security device

As discussed above, based on *Selker*'s teachings, a POSITA would have replaced the pressure sensor of *Waters* with a set of two perpendicular reed switches (mechanical switch), as taught by *Selker*, to achieve enhanced security. EX1013, ¶¶185-87; see *supra* §VII.C.i. As further taught by *Selker*, the set of reed switches (mechanical switch) is normally open. EX1013, ¶¶185-87; EX1027, [0027], FIG. 7. When a magnetic key (mechanical security device) is brought in close proximity to the set of reed switches (mechanical switch), the circuit is closed, and the key-holding user is authenticated. See *supra* §VII.C.i; EX1027, [0027]; EX1013, ¶¶185-87. Thus, in *Waters-Selker*, the set of reed switches (mechanical switch) is responsive to the magnetic key (mechanical security device). *Id.*

Thus, *Waters-Selker* renders obvious 39[a].

39[b]-[f]

Except for the implementation of the reed switch and key mechanism described above, *Waters-Selker* is identical to *Waters*. Thus, 39[b]-[f] are rendered obvious by *Waters-Selker* for the same reasons discussed above, with respect to *Waters*. See *supra* §§VII.A.i.1[a]-[d], VII.A.iv.20[f].

iii. Dependent Claims

Dependent Claim 40: the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch

Waters-Selker discloses Claim 40 for the same reasons discussed above with respect to 20[f]. See *supra* §VII.A.iv.20[f].

Dependent Claim 41: the RFID tag is disposed within a cellular telephone

Waters-Selker discloses Claim 41 for the same reasons discussed above with respect to claims 8, 13, 18, 25-26, 32, 55, and 58. See *supra* §VII.A.xi (claims 8, 13, 18, 25-26, 32, 55, 58).

Dependent Claim 42: the RFID tag is disposed within passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document

Waters-Selker discloses Claim 42 for the same reasons discussed above with respect to claims 9, 19, 27, and 33. See *supra* §VII.A.xi (claims 9, 19, 27, 33).

Dependent Claim 43: the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard

Waters-Selker discloses Claim 43 for the same reasons discussed above with respect to claims 9, 19, 27, and 33. *See supra* §VII.A.xi (claims 9, 19, 27, 33).

D. GROUND 2A: DUA

Dua renders obvious claims 1-10, 14-38, and 44-59.

i. Independent Claim 1

1[pre]: A RFID tag

Dua's device is equipped with hardware and software that enables RFID communication (RFID tag), which transmits credentials to facilitate a transaction. EX1023, [0378], [0383], [0423], [0495]; EX1021, 250.

Thus, *Dua* discloses 1[pre].

1[a]: an antenna configured to receive data in a first RF signal, to receive energy from the first RF signal, and to transmit data in a second RF signal, the transmission of the second RF signal being powered by the energy received from the first RF signal

Dua explains its techniques relate to smart card technology, including a “contactless smart card” with an “antenna[]” which “receive[s] power for on-card electronic functions” from a “reader” in “close proximity” therewith via an “electromagnetic signal” (first RF signal) and which transmits a credential to a reader, such as payment data, to perform a contactless transaction (second RF signal). *Id.*, [0009], [0315], [0352]-[0353].

To the extent *Dua*'s express disclosure is insufficient, an RFID antenna configured to receive and transmit data necessarily flows or is a natural result of *Dua*'s RFID communication functionality. *See, e.g.*, EX1023, [0009]; EX1029, 41; EX1013, ¶¶198-202. Additionally, it would have been further obvious to a POSITA that the device could be "passive," such that energy is also received by the antenna from the signal emitted by the RFID reader (first RF signal) and used to power transmission of the payment credentials (second RF signal), as such technology was well-known at the time of invention. EX1023, [0009]; EX1013, ¶¶198-202.

Thus, *Dua* renders obvious 1[a].

1[b]: integrated circuitry including an input configured to receive data from the antenna and to receive power resulting from the energy received from the antenna

Dua discloses that similar devices include "integrated circuits." EX1023, [0007]. Further, *Dua* discloses an RFID interface, which enables RFID communication. *Id.*, [0309], [0378], [0383], [0495]. An input to receive input data and power from the antenna and an output to provide output data to the antenna necessarily flows or is a natural result of *Dua*'s RFID interface and related integrated circuitry. EX1013, ¶¶203-207. Indeed, a POSITA would understand that the antenna must be electrically coupled to the integrated circuitry through an input/interface that conveys the received data and power, as without such an input, the integrated

circuitry could neither process the reader communication nor operate from the received RF energy. *Id.*

To the extent *Dua*'s disclosure is insufficient, as discussed above with respect to 1[a], *Dua*'s device receives data and power from an RFID reader. *See supra* §VII.D.i.1[a]. An input to receive data and energy from the RFID antenna, necessarily flows or is a natural result of such functionality, which cannot be implemented without an input. EX1013, ¶¶203-207.

Further, it would have been obvious to a POSITA that the functionality discussed above would be implemented as integrated circuitry. EX1013, ¶¶203-207. For example, a POSITA would understand that at the time of invention, integrated circuits were commonly used in mobile phone and RFID applications to provide communications and control functionality, with increased efficiency and decreased cost, compared to other methods. *Id.*; EX1029, 292-293; EX1026, 4.

Thus, *Dua* renders obvious 1[b].

1[c]: integrated circuitry including...an output configured to provide the second RF signal to the antenna for transmission

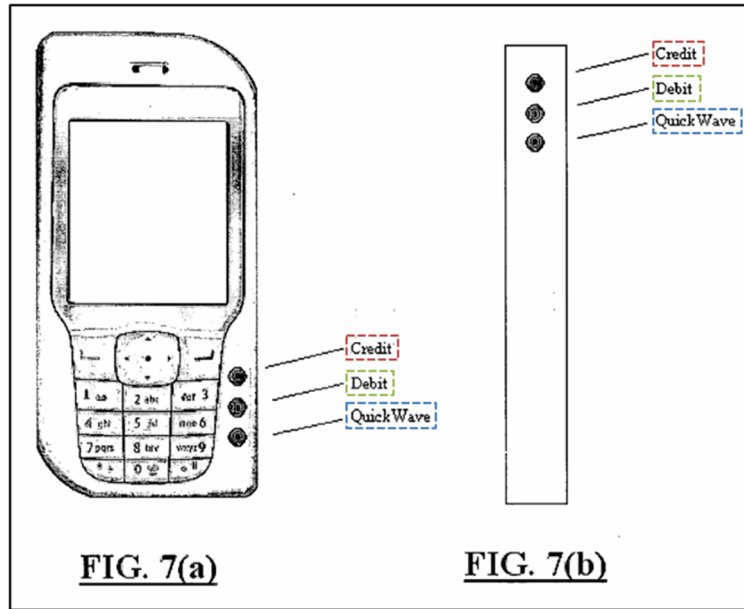
Similar to 1[b], integrated circuitry including an output to provide output data to the antenna necessarily flows or is a natural result of *Dua*'s RFID interface and RFID communication functionality, which cannot be implemented without such an output. EX1013, ¶¶208-11; *see supra* §VII.D.i.1[b].

To the extent *Dua*'s disclosure is insufficient, *Dua*'s device transmits data, including payment credentials (second RF signal) to an RFID reader via an RFID interface. EX1023, [0309], [0378], [0383], [0423]. It would have been obvious to a POSITA that such functionality would be implemented using an output to provide the payment credential data (second RF signal) to the antenna, such that the data can be transmitted to the RFID reader by the antenna. EX1013, ¶¶208-11.

Thus, *Dua* renders obvious 1[c].

1[d]: integrated circuitry including...a state memory configured to store an ON/OFF state including two or more ON states of the RFID tag

By default, *Dua*'s device is in a deactivated state (OFF state), in which no credentials will be transmitted to an RFID reader. EX1023, [0383], [0395]. *Dua*'s device can transition from the deactivated state (OFF state) to one of several transaction states (ON states), in which payment credentials are transmitted to an RFID reader, when a "hot button" associated with a particular transaction state is pushed by a user. These hot buttons include (1) a "QuickWave" hot button, which activates a QuickWave state (first ON state), (2) a "Credit" hot button, which activates a credit card state (second ON state), and (3) a "Debit/ATM" hot button, which activates a debit card state (third ON state). *Id.*, [0388]-[0395], FIG. 7.



EX1023, FIG. 7.

In the QuickWave state (first ON state), the device can transmit credentials which have a reader key associated with them. EX1023, [0392]; *see infra* §VII.D.i.1[e] (discussing QuickWave and reader key functionality in detail). In the credit card state (second ON state), the device can transmit the QuickWave credentials, plus credit card credentials. *Id.*, [0392]-[0393]. In the debit card state (third ON state), the device can transmit the QuickWave credentials, plus debit card credentials. *Id.* Each of these states corresponds to a unique ON state, because the device will transmit different data via RFID communication, depending on the transmission type.

Dua's device includes memory, and it would have been obvious to a POSITA to store the current state (deactivated, QuickWave, credit card, or debit card) of the

device in this memory (state memory), to enable implementation of the logic described above (transitioning from the deactivated state to a QuickWave state, credit card state, or debit card state, depending on which hot button was pressed by the user). EX1013, ¶¶212-17; EX1023, [0193]. For example, the device includes a “wallet application,” which controls the device to carry out this logic. EX1023, [0333], [0354]. As discussed above with respect to Ground 1, it would have been obvious to a POSITA to store the current state as a variable in memory (state memory), such that the wallet application can interact with the RFID circuitry to carry out the functionality described above. *See supra* §VII.A.i.1[d].

Thus, *Dua* renders obvious 1[d].

1[e]: integrated circuitry including...a key memory configured for storing a key for changing the ON/OFF state stored in the state memory

Dua’s device can store reader keys (keys) in memory (key memory) to associate specific credentials with certain readers. A reader key is transmitted by a credential issuer to the device during the issuance process of a credential that is associated with the reader key. EX1023, [0353], [0365]. The key is then stored in the device’s memory (key memory). *Id.*, [0354]. All RFID readers associated with the issuer also store a corresponding key. *Id.*, [0353]. At the start of a transaction, an RFID reader associated with the issuer transmits its key to the device. *Id.* The device then passes the key to the wallet application, which uses the key to look up a

credential associated with the corresponding reader key (key), which was received and stored during the issuance process. *Id.*, [0353], [0354]. Then, the wallet application completes a transaction using the relevant credential. *Id.* Such functionality “allows a reader device to automatically capture certain credential information from a device without the end-user having to scroll through different screens within the wallet application and pressing multiple buttons on his device.” *Id.*, [0355]. Thus, the reader key (key), which is stored in memory (key memory) is used to transition from a deactivated state (OFF state) to a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state), depending on which credential (QuickWave, credit, or debit) is associated with a particular reader key (key). As discussed above with respect to 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §VII.D.i.1[d].

Thus, *Dua* discloses 1[e].

1[f]: integrated circuitry including...a switch logic configured to receive data from the input, to read the key from the key memory, to compare the received data with the read key, and to change the ON/OFF state stored in the state memory responsive to this comparison

As discussed above with respect to 1[e], *Dua* discloses logic to receive a key (data) from an RFID reader via RFID communication (from the input), read a reader key (key) from memory (key memory), and compare the key (data) with the reader

key (key), to determine a transition from a deactivated state (OFF state) to a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state). *See supra* §VII.D.i.1[e].

As further discussed above with respect to 1[d], it would have been obvious to a POSITA to store the current state in state memory. *See supra* §VII.D.i.1[d].

Thus, *Dua* renders obvious 1[f].

1[g]: the switch logic being further configured to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the ON/OFF state stored in the state memory

As discussed above with reference to 1[d], *Dua* discloses logic to determine whether to provide payment credentials (second RF signal) to the antenna for transmission, depending on the current state (QuickWave, credit, debit, or deactivated) stored in state memory. *See supra* §VII.D.i.1[d].

Thus, *Dua* renders obvious 1[g].

ii. Independent Claim 14

14[pre]-[c]

Dua discloses and/or renders obvious 14[pre]-[c] for the same reasons discussed above with respect to 1[pre]-[c]. *See supra* §VII.D.i.1[pre]-[c].

14[d]: integrated circuitry including...a state memory configured to store an ON/OFF state of the RFID tag, the

ON/OFF state being responsive to timing using a resistor-capacitor circuit

When a hot button is pressed, the device transitions from a deactivated state (OFF state) to a QuickWave state (first ON state), credit state (second ON state), or debit state (third ON state) for a 30-second period. EX1023, [0395]. After this 30-second period, the device returns to the deactivated state (OFF state). *Id.*; *see also id.*, [0383]. As discussed with reference to Ground 1, it would have been obvious to a POSITA that this timing functionality could be implemented using a resistor-capacitor circuit, as it was known in the art to build timers using such circuits. EX1013, ¶¶229-31; *see, e.g.*, EX1028, 10-1; EX1029, 276-78 (discussing RC timers in RFID applications). A POSITA implementing such predetermined-time deactivation functionality would have recognized a resistor-capacitor timing circuit as a conventional, inexpensive, and predictable circuit for defining the duration of the temporary ON state. EX1013, ¶¶229-31.

Dua renders obvious 14[d].

14[e]-[g]

Dua discloses and/or renders obvious 14[e]-[g] for the same reasons discussed above with respect to 1[e]-[g]. *See supra* §VII.D.i.1[e]-[g].

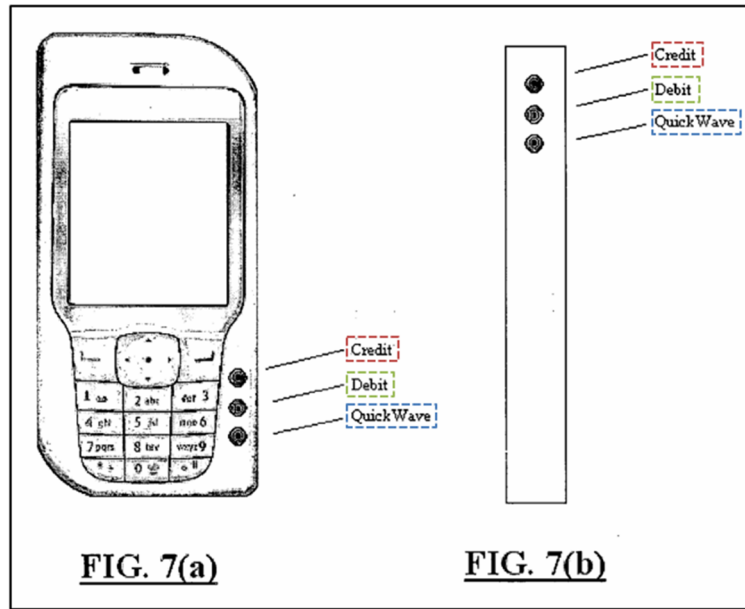
iii. **Independent Claim 20**

20[pre]

Dua discloses 20[pre] for the same reasons discussed above with respect to 1[pre]. *See supra* §VII.D.i.1[pre].

20[a]: a mechanical switch configured for selecting between two or more ON states of the RFID tag

As discussed with reference to 1[d], *Dua*'s device includes hot buttons (mechanical switches), each of which allows a user to select between ON states by pressing and activating the hot button. *See supra* §VII.D.i.1[d]; EX1013, ¶¶234-39. Each hot button discloses a mechanical switch because it controls circuit components by making or breaking an electrical connection in the device circuitry, responsive to its components being pressed (moved) by a user. EX1013, ¶¶234-39; *see supra* §V.B (a POSITA would have understood “mechanical switch” to mean “a control device that makes or breaks an electrical connection in a circuit responsive to movement of one or more components of the control device.”). In particular, a “QuickWave” hot button selects a QuickWave state (first ON state), a “Credit” hot button selects a credit card state (second ON state), and a “Debit/ATM” hot button selects a debit card state (third ON state). EX1023, [0388]-[0395], FIG. 7.



EX1023, FIG. 7.

When a hot button is pressed, communication of QuickWave, credit, or debit credentials is enabled for a 30-second period, depending on which button was pressed. *Id.*, [0395], *see also* [0393] (the credit/debit buttons can also be programmed to enable transmission of both a credit/debit credential and a QuickWave credential). Thus, a POSITA would have understood that in the scenario where a first hot button is pressed (and an ON state is activated for 30 seconds), and then a second hot button is pressed within the 30-second window, the second hot button will cause a transition from one ON state to a different ON state. EX1013, ¶¶234-39. For example, if a user first presses the “QuickWave” button, and then 15 seconds later, presses the “Credit” button (mechanical switch), the device will transition from (select between) a QuickWave state (first ON state) to a credit card

state (second ON state). *Id.*; compare EX1001, 21:41-49. Indeed, this functionality is similar to the enabling embodiment of the '156 Patent, which includes an RFID tag that “will transmit a limited amount of data when Switch 170 is off and a less limited amount of data when Switch 170 is on.” EX1001, 8:65-9:10.

Alternatively, *Dua* emphasizes flexibility in the design of its hot buttons. EX1023, [0396]. Accordingly, a POSITA would have considered it an obvious design choice to implement *Dua*’s three wallet buttons as a single, three-way selector switch, having a first position for “QuickWave” functionality, a second position for “Credit” functionality, and a third position for “Debit” functionality, because this implementation would preserve the functionality of *Dua*’s device, while reducing the number of components and complexity of its design. EX1013, ¶¶234-39.

Thus, *Dua* discloses 20[a].

20[b]-[e]

Dua discloses and/or renders obvious 20[b]-[e] for the same reasons discussed above with respect to 1[a]-[d]. *See supra* §VII.D.i.1[a]-[d].

20[f]: integrated circuitry including...a switch logic configured to receive data from the input, and to determine whether or not to provide the second RF signal to the antenna for transmission, the determination being responsive to the state stored in the state memory or the mechanical switch

As discussed above with respect to 1[b], the device receives data from an input. *See supra* §VII.D.i.1[b].

As discussed above with respect to 20[a], the device determines whether to provide payment credentials (second RF signal) to the antenna for transmission, based on whether a hot button (mechanical switch) was pressed. *See supra* §VII.D.iii.20[a]. Alternatively, as discussed above with respect to 1[g], such determination can be based on the state stored in state memory. *See supra* §VII.D.i.1[g].

Thus, *Dua* renders obvious 20[f].

iv. Independent Claim 29

29[pre]

Dua discloses 29[pre] for the same reasons discussed above with respect to 1[pre]. *See supra* §VII.D.i.1[pre].

29[a]: a mechanical switch configured to set a state of the RFID tag stored in a state memory

As discussed above with reference to 20[a], *Dua* discloses hot buttons (mechanical switches) configured to select between a QuickWave state (first ON state), credit card state (second ON state), and a debit card state (third ON state). *See supra* §VII.D.iii.20[a]. As further discussed above, the current state (set by the mechanical switch) is stored in memory (state memory). *See supra* §VII.D.i.1[d].

Thus, *Dua* discloses 29[a].

29[b]-[f]

As discussed above with reference to claim 1, *Dua* discloses and/or renders obvious 29[b]-[e]. *See supra* §VII.D.i.1[a]-[d]. As discussed above with reference to claim 20, *Dua* renders obvious 29[f]. *See supra* §VII.D.iii.20[f].

v. Independent Claim 34

34[pre]

As discussed above with reference to 1[pre], *Dua* discloses 34[pre]. *See supra* §VII.D.i.1[pre].

34[a]

As discussed above with reference to 20[a], *Dua* discloses 34[a]. *See supra* §VII.D.iii.20[a].

34[b]-[e]

As discussed above with reference to 1[a]-[d], *Dua* discloses 34[b]-[e]. *See supra* §VII.D.i.1[a]-[d].

34[f]

As discussed above with reference to 20[f], *Dua* discloses 34[f]. *See supra* §VII.D.iii.20[f].

34[g]: the state logic being further configured to store a plurality of alternative ON states

As an initial matter, “the state logic” is not introduced or defined in the claim. However, to the extent that the Board may interpret “state logic” as referring to “state memory,” as discussed above with respect to 1[d], it would have been obvious to a

POSITA to store a QuickWave state (first ON state), a credit card state (second ON state), and a debit card state (third ON state) in the device memory (state memory).

See supra §VII.D.i.1[d]; EX1013, ¶¶254-56.

Thus, *Dua* renders obvious 34[g].

34[h]: the mechanical switch being configured for switching the RFID tag from an OFF state to one of the plurality of alternative ON states

As discussed above with respect to 20[a], each hot button (mechanical switch) can select a QuickWave state (first ON state), credit card state (second ON state), or debit card state (third ON state). *See supra* §VII.D.iii.20[a]. In the scenario where the device is in a deactivated state (OFF state), and a hot button (mechanical switch) is then pressed, the device will switch from an OFF state to an ON state. EX1023, [0383], [0386]; EX1013, ¶¶257-59.

Thus, *Dua* discloses 34[h].

vi. Independent Claim 44

44[pre]: A method of changing a state of an RFID Tag

Dua discloses 44[pre] for the same reasons discussed above with respect to 1[d]-[f]. *See supra* §VII.D.i.1[d]-[f].

44[a]-[b]

Dua discloses 44[a]-[b] for the same reasons discussed above with respect to 1[a]-[b]. *See supra* §VII.D.i.1[a]-[b].

44[c]: reading a key from a key memory

Dua discloses 44[c] for the same reasons discussed above with respect to 1[e]-[f]. *See supra* §VII.D.i.1[e]-[f].

44[d]: using an integrated circuit to compare the first data received through the RF antenna with the key read from the key memory, the integrated circuit powered by the received energy

Dua discloses 44[d] for the same reasons discussed above with respect to 1[a]-[b] and 1[f]. *See supra* §§VII.D.i.1[a]-[b] (integrated circuit is powered by received energy), VII.D.i.1[f] (first data is compared to key).

44[e]: determining a state of a mechanical switch in the RFID tag

Dua discloses 44[e] for the same reasons discussed above with respect to 20[a]. *See supra* §VII.D.iii.20[a].

44[f]: writing data to state memory responsive to the comparison only if the mechanical switch is activated, the data written to the state memory being configured to change the RFID tag from a first state to a second state

Dua renders obvious 44[f] for the same reasons discussed above with respect to 1[f] and 20[a]. *See supra* §§VII.D.i.1[f] (writing data to state memory responsive to comparison), VII.D.iii.20[a] (changing ON states only if mechanical switch is activated).

vii. Independent Claim 51

51[pre]-[e]

Dua discloses and/or renders obvious 51[pre]-[e] for the same reasons discussed above with respect to 44[pre]-[f]. *See supra* §VII.D.vi.44[pre]-[f].

51[f]: the first state and the second state are alternative ON states

Dua discloses 51[f] for the same reasons discussed above with respect to 1[d]. *See supra* §VII.D.i.1[d].

viii. Independent Claim 53

53[pre]-[e]

Dua discloses and/or renders obvious 53[pre]-[e] for the same reasons discussed above with respect to 44[pre]-[f]. *See supra* §VII.D.vi.44[pre]-[f].

53[f]: providing an RF response, a content of data in the RF response being responsive to the comparison

As discussed above with respect to 1[d] and 1[f], after receiving a key from an RFID reader, the device can provide a response transmission (RF response) including specific payment credentials (content of data in the RF response), depending on which stored reader key corresponds to the received key (responsive to the comparison). *See supra* §§VII.D.i.1[d], VII.D.i.1[f].

Dua discloses 53[f].

ix. **Independent Claim 54**

54[pre]-[a]

Dua discloses 54[pre]-[a] for the same reasons discussed above with respect to 44[pre] and 44[b]. *See supra* §§VII.D.vi.44[pre], VII.D.vi.44[b].

54[b]: reading a state from a state memory, the state memory being configured to alternatively store an OFF state, a first ON state and a second ON state

Dua renders obvious 54[b] for the same reasons discussed above with respect to 1[d] and 1[g]. *See supra* §§VII.D.i.1[d] (storing an OFF state, a first ON state, and a second ON state in state memory), VII.D.i.1[g] (reading the state from state memory to determine whether to provide a response signal).

54[c]-[d]

Dua discloses 54[c]-[d] for the same reasons discussed above with respect to 1[d] and 1[g]. *See supra* §§VII.D.i.1[d] (contents of response signal depend on whether the current state is the first ON state or the second ON state), VII.D.i.1[g] (sending response signal using antenna depending on whether the current state is the first ON state or the second ON state).

x. **Independent Claim 57**

57[pre]-[a]

Dua discloses 57[pre]-[a] for the same reasons discussed above with respect to 44[pre] and 44[b]. *See supra* §§VII.D.vi.44[pre], VII.D.vi.44[b].

57[b]-[c]

Dua discloses 57[b]-[c] for the same reasons discussed above with respect to 54[b]-[c]. *See supra* §§VII.D.ix.54[b]-[c].

57[d]: sending the response signal is responsive to a mechanical switch

Dua discloses 57[d] for the same reasons discussed above with respect to 20[f]. *See supra* §VII.D.iii.20[f].

xi. Dependent Claims

Dependent Claims 2, 15: the ON/OFF state of the RFID tag is OFF by default and temporally ON

As discussed above with respect to 1[d], *Dua*'s device is in a deactivated state (OFF state) by default, and transitions to one of several transaction states (ON states) only temporarily, when a "hot button" is pressed by the user. *See supra* §VII.D.i.1[d]. When RF communication is enabled, the device remains in an ON state for a 30-second window, after which "the application will disable RF communication and the application may shutdown or go into its normal dormant state" (OFF state). EX1023, [0383], [0395].

Thus, *Dua* renders obvious Claims 2 and 15.

Dependent Claims 3, 16: the ON/OFF state of the RFID tag is stored in static memory

Dua renders obvious Claims 3 and 16 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.D.i.1[d]. As discussed above, it would have

been obvious to a POSITA to store the current state (deactivated, QuickWave, credit card, or debit card) of the device in device memory (state memory). *Id.* It also would have been obvious to a POSITA that device memory storing variable values would be implemented as static RAM, as this was a well-known practice at the time of invention. EX1013, ¶¶280-81; EX1026, 24, 26, 34, 47.

Thus, *Dua* renders obvious Claims 3 and 16.

Dependent Claim 4: the determination is responsive to which of the alternative ON states are stored in the state memory

Dua renders obvious Claim 4 for the same reasons discussed above with respect to 1[g]. *See supra* §VII.D.i.1[g].

Dependent Claim 5: the RFID tag is disposed within a passport

Dua discloses that the device may include contactless smart card technology, and specifically discusses the use of such technology in access control applications. EX1023, [0009], [0011]-[0012]. *Dua* further discloses that the device with the wallet application can serve as a replacement for identity documents with RFID functionality. *Id.*, [0333], [0342]. It therefore would have been obvious to a POSITA to incorporate the RFID functionality of *Dua*'s device within a passport, as such identity documents with RFID capability were well-known at the time of invention. EX1013, ¶¶283-84; EX1030, 4, 14.

Thus, *Dua* renders obvious Claim 5.

Dependent Claim 6: the state memory is configured to store in the alternative, an OFF state, a first ON state and a second ON state

Dua renders obvious Claim 6 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.D.i.1[d].

Dependent Claim 7: the state memory is configured to store a first value indicating an ON/OFF state and a second value indicating one of at least two alternative ON states

Dua renders obvious Claim 7 for the same reasons discussed above with respect to 1[d]. *See supra* §VII.D.i.1[d].

Dependent Claims 8, 18, 25-26, 32, 37, 55, 58: the RFID tag is disposed within a cellular telephone

Dua's hardware and software enabling RFID communication (RFID tag) is disposed within a device, which is preferably a cellular telephone. EX1023, [0026], [0041], FIG. 7.

Thus, *Dua* discloses Claims 8, 18, 25-26, 32, 37, 55, and 58.

Dependent Claims 9, 19, 27, 33, 38: the RFID tag is disposed within a passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document

Dua renders obvious Claims 9, 19, 27, 33, and 38 for the same reasons discussed above with respect to claim 5. *See supra* §VII.D.xi (claim 5).

Dependent Claims 10, 28, 50, 56, 59: the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard

Dua renders obvious Claims 10, 28, 50, 56, and 59 for the same reasons discussed above with respect to claim 5. *See supra* §VII.D.xi (claim 5).

Dependent Claim 17: the RFID tag is not remotely detectable using an RF signal when the ON/OFF state is OFF

As discussed above with respect to 1[d], *Dua*'s device can enter a deactivated state (OFF state). *See supra* §VII.D.i.1[d]. In this state, the device does not transmit credentials, and thus the RFID interface (RFID tag) is not remotely detectable using an RF signal. EX1023, [0383], [0386], [0395].

Thus, *Dua* discloses Claim 17.

Dependent Claims 21, 30, 35: the input is further configured to receive power resulting from the first RF signal and to power the integrated circuitry using the power

Dua renders obvious Claims 21, 30, and 35 for the same reasons discussed above with respect to 1[a]-[b]. *See supra* §VII.D.i.1[a]-[b].

Dependent Claims 22, 31, 36: the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch

Dua discloses Claims 22, 31, and 36 for the same reasons discussed above with respect to 20[f]. *See supra* §VII.D.iii.20[f].

Dependent Claim 23: the mechanical switch must be activated and the state stored in the state memory must be an ON state before the second RF signal is transmitted

Dua renders obvious Claim 23 for the same reasons discussed above with respect to 1[g] and 20[a]. *See supra* §§VII.D.i.1[g], VII.D.iii.20[a]. As discussed above, a hot button (mechanical switch) must be pressed to transition from the deactivated state (OFF state) to an ON state, and the device will only transmit payment credentials (second RF signal) when it is in an ON state. *Id.*

Dependent Claim 24: a key memory configured for storing a key for changing the state stored in the state memory, the switch logic being further configured to read the key from the key memory, to compare the received data with the read key, and to change the state stored in the state memory responsive to the comparison between the received data with the read key

Dua renders obvious Claim 24 for the same reasons discussed above with respect to 1[f]. *See supra* §VII.D.i.1[f].

Dependent Claim 45: the first state is a state in which the RFID tag will not transmit an RF signal

As discussed above with respect to 1[d], *Dua*'s device can be in a deactivated state (first state/OFF state), in which no credentials will be transmitted (the RFID tag will not transmit an RF signal). *See supra* §§VII.D.i.1[d], VII.D.xi (claim 17).

Thus, *Dua* discloses Claim 45.

Dependent Claim 46: using an integrated circuit to compare the first data received through the RF antenna with the key is only performed if the state of the mechanical switch is ON

As discussed above with respect to 1[f] and 20[a], *Dua* discloses logic to receive a key (first data) from an RFID reader, compare the received key with a stored reader key (key), and transition from a deactivated state (OFF state) to an ON state. *See supra* §§VII.D.i.1[f], VII.D.iii.20[a]. *Dua* further discloses that a hot button (mechanical switch) must be pressed to enable RF communication. EX1023, [0383], [0386], [0395]. It would have been obvious to a POSITA that this comparison would only be performed after the hot button (mechanical switch) is activated (ON), as the RF communication that enables receipt of the first data is only enabled after pressing a hot button (mechanical switch). EX1013, ¶¶229-30.

Thus, *Dua* renders obvious Claim 46.

Dependent Claims 47, 52: the state memory is non-volatile memory

Dua renders obvious Claims 47 and 52 for the same reasons discussed above with respect to 1[d] and claims 3 and 16. *See supra* §§VII.D.i.1[d], VII.D.xi (claims 3, 16). As discussed above, it would have been obvious to a POSITA to store the current state of *Dua*'s device in device memory (state memory). *Id.* It also would have been obvious to a POSITA that device memory storing variable values would be implemented as non-volatile memory, such that the stored data can be retained

after the device is powered off, as this was a well-known practice at the time of invention. EX1013, ¶¶301-02; *see, e.g.*, EX1026, 34, 47.

Dependent Claim 48: automatically returning to the OFF state

As discussed above with respect to 1[d] and 14[d], when a hot button is pressed, the device transitions from a deactivated state (OFF state) to an ON state for a 30-second period, after which the device automatically returns to the deactivated state (OFF state). *See supra* §§VII.D.i.1[d], VII.D.ii.14[d]; EX1023, [0383], [0395].

Thus, *Dua* discloses Claim 48.

Dependent Claim 49: sending a response signal using the RF antenna if the second state is an ON state

Dua discloses Claim 49 for the same reasons discussed above with respect to 53[f]. *See supra* §VII.D.viii.53[f].

E. GROUND 2B: DUA WITH PONT

Dua with *Pont* renders obvious claims 1-10, 14-38, and 44-59.

i. Motivation to Combine

Both *Dua* and *Pont* are directed to mobile phone applications. *Dua* is directed to a mobile phone including components to control and carry out financial transactions using RFID communication. EX1023, [0025], [0333]. *Pont* is directed to mobile phone processors, which can be used to control operations. EX1026, xi.

Specifically, *Dua* uses the device's processor, running a software-based "wallet application," to control the RFID interface and related components to carry out RFID transaction functionality. EX1023, [0041], [0333]. While *Dua* describes these features in functional terms, it lacks specific disclosure of how these features would be implemented at a software level. For example, *Dua* discloses that the wallet application can read a hot button input and interact with device memory to select and transmit credentials, but does not disclose *how* a processor would read such a switch input or *how* a processor would interact with memory. EX1023, [0388]-[0395]. *Pont* fills this gap. A POSITA would turn to *Pont* for such knowledge, as *Pont* is a contemporary textbook which provides teachings related to programming embedded processors in C. EX1026, xi. Such processors can include mobile phone processors, similar to the mobile phone processor of *Dua*. *Id.* *Pont* therefore provides useful guidance to a POSITA related to specific methods of programming a microprocessor to carry out mobile phone applications.

As discussed above with reference to *Waters-Pont*, *Pont* discloses that a controller can interface with a switch and change a device state based on the value of the switch, similar to the functionality described in *Dua*, and that to enable such functionality, the state would be stored in an output state variable. *See supra* §VII.B.i.

Pont further teaches that the value of the output state variable is stored in RAM. EX1026, 26 (variables are stored in memory). This memory location can

correspond to a state memory, as it will store information representative of the current state of the device. EX1013, ¶308.

Based on these teachings, a POSITA would have been motivated to apply *Pont*'s control structure to *Dua*, such that an output state variable stores the active state of the RFID functionality. EX1013, ¶¶309-10. For example, according to *Pont*'s teachings, a POSITA would understand that in *Dua*, a polling loop would be used to check the current value of a hot button (mechanical switch). EX1013, ¶¶309-10. On each iteration of the polling loop, the switch value would be assigned to a switch state variable. *Id.* Then, the value of the switch state variable would be passed to a controller function of the wallet application. *Id.* The controller function would then apply logic to determine the current state of the RFID transaction functionality, as taught by *Dua*. *Id.* The function would assign this state to an RFID state variable and use the value of this variable to control the downstream functions of the device. *Id.* As taught by *Pont*, the implementation of such logic would require that the RFID state is stored in RAM, which can correspond to a state memory. *Id.*

Moreover, a POSITA would have had a reasonable expectation of success in making this combination. *Id.* For example, *Pont* discloses that its teachings are directly applicable to embedded processors in mobile phones. EX1026, xi, 2. The *Dua-Pont* combination therefore involves nothing more than applying known elements (software control) in a known structure (mobile phones) using known

methods (programming in C) to achieve a well-understood and predictable benefit (reliable control of mobile phone processes). EX1013, ¶¶309-10. A POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established programming techniques and produces understood results. *Id.*

ii. **“State Memory” Claims: 1, 4, 6-7, 14, 20, 23-24, 29, 34, 44, 47, 51-54, 57**

Dua-Pont renders obvious a “state memory,” as recited in claims 1, 4, 6-7, 14, 20, 23-24, 29, 34, 44, 47, 51-54, and 57.

As discussed above, based on *Pont*’s teachings, a POSITA would have understood that the device of *Dua* would include RAM, which would store information representing the current state of the device. EX1013, ¶¶311-14; *see supra* §VII.D.i.1[d]. For example, the device RAM (state memory) would store the current value of a device state variable (QuickWave (first ON state), credit card (second ON state), debit card (third ON state), or deactivated (OFF state)). EX1013, ¶¶311-14; *see also* §VII.D.i.1[d].

Except for the implementation of the state memory described above, *Dua-Pont* is identical to *Dua*. Thus, the remaining limitations of claims 1, 4, 6-7, 14, 20, 23-24, 29, 34, 44, 47, 51-54, and 57 are disclosed and/or rendered obvious by *Dua-Pont* for the same reasons discussed above, with respect to *Dua*. *See supra* §VII.D.

iii. **Claims 2-3, 5, 8-10, 15-19, 21-22, 25-28, 30-33, 35-38, 45-46, 48-50, 55-56, 58-59**

As discussed above, except for the implementation of the state memory described above, *Dua-Pont* is identical to *Dua*. Thus, claims 2-3, 5, 8-10, 15-19, 21-22, 25-28, 30-33, 35-38, 45-46, 48-50, 55-56, and 58-59 are disclosed and/or rendered obvious by *Dua-Pont* for the same reasons discussed above, with respect to *Dua*. See *supra* §VII.D.

F. GROUND 2C: DUA WITH SELKER

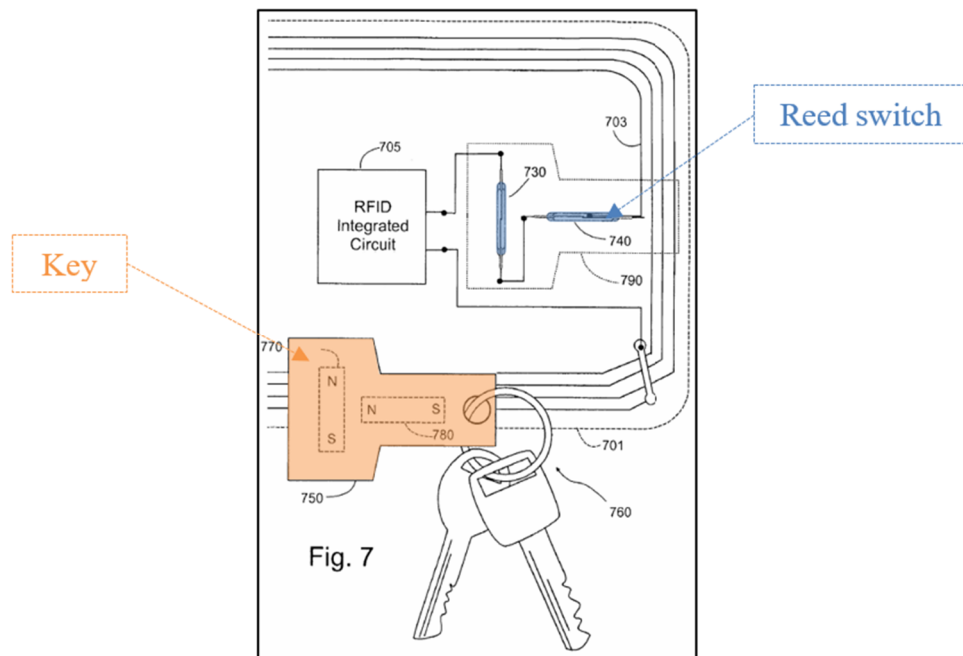
Dua with *Selker* renders obvious claims 39-43.

i. **Motivation to Combine**

Both *Dua* and *Selker* are directed to RFID payment technologies. *Dua* relates to a device (e.g., cellphone), that carries out transactions using RFID. EX1023, [0026], [0041], [0296], FIG. 7. *Selker* relates to mechanisms to protect RFID payment cards from unauthorized misuse. EX1027, [0004].

Dua discloses hot buttons (mechanical switches), which enable RFID and control credential transmission, to improve data security in RFID applications. EX1023, [0382]-[0383], [0392]-[0395]. As discussed above, implementation of hot buttons can prevent unauthorized bad actors from reading/skimming credentials. *Id.* *Selker* similarly addresses the issue that “because RF-enabled devices such [as] payment cards can be read at a distance with a suitable transmitter and receiver, it is possible to surreptitiously obtain information from the card while it remains in its

cardholder's possession. In addition to non-contact data transfer, wireless communication can also allow non-line-of-sight communication, meaning that an RF-enabled device may be read while it remains in the cardholder's wallet or purse." EX1027, [0003]. Thus, *Selker* teaches that security can be further improved by implementing a reed switch and key mechanism, which is "functionally flexible in order to work in cards and other devices having a variety of shapes and sizes." *Id.*, [0004], [0027], [0031], FIG. 7.



Id., FIG. 7.

According to *Selker*, this mechanism provides "enhanced security" and "helps protect" the RFID device "from unauthorized misuse." *Id.*, [0004], [0019]. Thus, a POSITA would have been motivated to implement *Selker*'s reed switch and key mechanism in the device of *Dua* to achieve the heightened security taught by *Selker*,

with respect to especially sensitive financial accounts, such as debit accounts. *Id.*, [0004], [0027], [0031], FIG. 7. To do so, a POSITA would have understood to replace *Dua*'s "Debit" hot button (mechanical switch) with a set of perpendicular reed switches, as taught by *Selker*. *Id.*; EX1013, ¶¶319-20. Thus, to authenticate themselves and enable a sensitive debit transaction, a user can place the magnetic key in close proximity to the reed switches, which would close the switch circuit, similar to pressing *Dua*'s original hot button. EX1013, ¶¶319-20.

Moreover, a POSITA would have had a reasonable expectation of success in making this combination. *Id.* For example, *Dua* discloses similar security measures. EX1023, [0392]-[0395] (discussing hot buttons to prevent skimming). Meanwhile, *Selker* provides an alternative reed switch and key mechanism, which provides further enhanced security. EX1027, [0004], [0019]. The *Dua-Selker* combination therefore involves nothing more than applying known elements (a reed switch and key mechanism) in a known structure (mobile phones) using known methods (basic circuit design) to achieve a well-understood and predictable benefit (improved security). EX1013, ¶¶319-20. A POSITA would reasonably expect this combination to succeed without undue experimentation, as it relies on established circuit design techniques and produces understood results. *Id.*

ii. **Independent Claim 39**

39[pre]

Except for the implementation of the reed switch and key mechanism described above, *Dua-Selker* is identical to *Dua*. Thus, 39[pre] is rendered obvious by *Dua-Selker* for the same reasons discussed above, with respect to *Dua*. *See supra* §VII.D.i.1[pre].

39[a]: mechanical switch responsive to a state of a mechanical security device

As discussed above, based on *Selker*'s teachings, a POSITA would have replaced *Dua*'s "Debit" hot button (mechanical switch) with a set of two perpendicular reed switches (mechanical switch), as taught by *Selker*, to achieve enhanced security. EX1013, ¶¶322-24; *see supra* §VII.F.i. As further taught by *Selker*, the set of reed switches (mechanical switch) is normally open. EX1013, ¶¶322-24; EX1027, [0027], FIG. 7. When a magnetic key (mechanical security device) is brought in close proximity to the set of reed switches (mechanical switch), the circuit is closed. *Id.* Thus, in *Dua-Selker*, the set of reed switches (mechanical switch) is responsive to the magnetic key (mechanical security device). *Id.*

Thus, *Dua-Selker* renders obvious 39[a].

39[b]-[f]

Except for the implementation of the reed switch and key mechanism described above, *Dua-Selker* is identical to *Dua*. Thus, 39[b]-[f] are rendered

obvious by *Dua-Selker* for the same reasons discussed above, with respect to *Dua*.
See supra §§VII.D.i.1[a]-[d], VII.D.iii.20[f].

iii. **Dependent Claims**

Dependent Claim 40: the integrated circuitry is configured for authorizing a transaction responsive to the mechanical switch

Dua-Selker discloses Claim 40 for the same reasons discussed above with respect to 20[f]. *See supra* §VII.D.iii.20[f].

Dependent Claim 41: the RFID tag is disposed within a cellular telephone

Dua-Selker discloses Claim 41 for the same reasons discussed above with respect to claims 8, 18, 25-26, 32, 37, 55, and 58. *See supra* §VII.D.xi (claims 8, 18, 25-26, 32, 37, 55, 58).

Dependent Claim 42: the RFID tag is disposed within passport, identity card, driver's license, immigration document, student identity card, library card, financial card, social security card, military ID card, key, keycard, or identification document

Dua-Selker discloses Claim 42 for the same reasons discussed above with respect to claims 9, 19, 27, 33, and 38. *See supra* §VII.D.xi (claims 9, 19, 27, 33, 38).

Dependent Claim 43: the RFID tag is disposed within a passport, driver's license, financial card, military ID card, key, or keycard

Dua-Selker discloses Claim 43 for the same reasons discussed above with respect to claims 10, 28, 50, 56, and 59. *See supra* §VII.D.xi (claims 10, 28, 50, 56, 59).

VIII. SECONDARY CONSIDERATIONS

Petitioners are aware of no evidence of secondary considerations that would rebut a finding of obviousness and reserve the right to rebut any purported evidence raised by Patent Owner.

IX. CONCLUSION

Petitioners respectfully request that IPR be instituted and the Challenged Claims be cancelled.

Respectfully submitted,

Dated: September 22, 2026

/ Eliot D. Williams /
Eliot D. Williams, Reg. No. 50,822
eliot.williams@bakerbotts.com
Baker Botts L.L.P.
700 K Street, N.W.
Washington, D.C. 20001-5692
Phone: 202.639.1334
Fax: 202.639.7890

Neil Sirota, Reg. No. 38,306
Baker Botts L.L.P.
30 Rockefeller Plaza, Ste 4340
New York, NY 10112-4498
Phone: 212.408.2548

Fax: 212.259.2548
neil.sirota@bakerbotts.com

Megan LaDriere White, Reg. No. 75,995
Baker Botts L.L.P.
2001 Ross Avenue
Suite 900
Dallas, Texas 75201-2980
Phone: 214.953.6948
megan.white@bakerbotts.com

Eric Faragi, Reg. No. 51,259
Baker Botts L.L.P.
30 Rockefeller Plaza, Ste 4340
New York, NY 10112-4498
Phone: 212.408.2591
eric.faragi@bakerbotts.com

Benjamin Rosen, Reg. No. 84,598
Baker Botts L.L.P.
30 Rockefeller Plaza, Ste 4340
New York, NY 10112-4498
Phone: 212.408.2691
benjamin.rosen@bakerbotts.com

Coleman Strine, Reg. No. 79,981
Baker Botts L.L.P.
30 Rockefeller Plaza, Ste 4340
New York, NY 10112-4498
Phone: 212.408.2595
coleman.strine@bakerbotts.com

CERTIFICATION UNDER 37 C.F.R. §42.24(d)

Pursuant to 37 C.F.R. §42.24(d), the undersigned hereby certifies that the word count under §42.24(a)(1) for the foregoing Petition for *Inter Partes* Review totals 13,988 words, within the 14,000 word limit allowed under §42.24(a)(1)(i).

Dated: September 22, 2026

/ Eliot D. Williams /
Eliot D. Williams

CERTIFICATE OF SERVICE

In accordance with 37 C.F.R. §§42.6(e) and 42.105, the undersigned certifies that, on this date, the foregoing was served via FedEx Overnight Delivery on the Patent Owner at the correspondence addresses of record (as listed in Patent Center and on the Patent Assignment Cover Sheet) for the subject patent at:

Patent Center	Patent Assignment Cover Sheet
Steven Colby Rimon Law, P.C. 1655 W. Fairview Ave., Suite 102 Boise, Idaho 83702	SureCell Transactions, LLC P.O. Box 837 Verdi, Nevada 89439

A complete copy was also served via electronic mail to counsel of record for Patent Owner in the litigation pending before the U.S. District Court for the Eastern District of Texas entitled *SureCell Transactions LLC v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, No. 2:26-cv-00106 at:

sdavis@stafforddavisfirm.com
cbartles@stafforddavisfirm.com

Dated: September 22, 2026

/ Eliot D. Williams /
Eliot D. Williams