US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12393926
Kind Code	B2
Date of Patent	August 19, 2025
Inventor(s)	Ilincic; Rajko

Systems and methods for data access control using a short-range transceiver

Abstract

Systems and methods for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device are presented. An exemplary system and method may include establishing a database storing information for a plurality of accounts, receiving from a client device of the second account holder an account link request to link a first account with a second account, the account link request generated in response to a tap action between a contactless card and the client device, transmitting to a client device of the first account holder a link approval request to approve the account link request, receiving from the first account holder client device, a link approval message generated in response to an indication by the first account holder approving the account link request, and transmitting to the second account holder client device an account link.

Inventors: **Ilincic; Rajko (Annandale, VA)**

Applicant: **Capital One Services, LLC** (McLean, VA)

Family ID: **1000008762703**

Assignee: **Capital One Services, LLC (McLean, VA)**

Appl. No.: **17/589803**

Filed: **January 31, 2022**

Prior Publication Data

Document Identifier	Publication Date
US 20220156720 A1	May. 19, 2022

Related U.S. Application Data

continuation parent-doc US 17088117 20201103 US 11270291 child-doc US 17589803
continuation parent-doc US 16863952 20200430 US 10861006 20201208 child-doc US 17088117

Publication Classification

Int. Cl.: **G06Q20/34** (20120101); **G06Q20/36** (20120101)

U.S. Cl.:

CPC **G06Q20/352** (20130101); **G06Q20/341** (20130101); **G06Q20/3672** (20130101); **G06Q20/3674** (20130101);

Field of Classification Search

CPC: G06Q (20/352); G06Q (20/341); G06Q (20/3672); G06Q (20/3674)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
4683553	12/1986	Mollier	N/A	N/A
4827113	12/1988	Rikuna	N/A	N/A
4910773	12/1989	Hazard et al.	N/A	N/A
5036461	12/1990	Elliott et al.	N/A	N/A
5363448	12/1993	Koopman, Jr. et al.	N/A	N/A
5377270	12/1993	Koopman, Jr. et al.	N/A	N/A
5533126	12/1995	Hazard	N/A	N/A
5537314	12/1995	Kanter	N/A	N/A
5592553	12/1996	Guski et al.	N/A	N/A
5616901	12/1996	Crandall	N/A	N/A
5666415	12/1996	Kaufman	N/A	N/A
5764789	12/1997	Pare, Jr. et al.	N/A	N/A
5768373	12/1997	Lohstroh et al.	N/A	N/A
5778072	12/1997	Samar	N/A	N/A
5796827	12/1997	Coppersmith et al.	N/A	N/A
5832090	12/1997	Raspotnik	N/A	N/A
5883810	12/1998	Franklin et al.	N/A	N/A
5901874	12/1998	Deters	N/A	N/A
5929413	12/1998	Gardner	N/A	N/A
5960411	12/1998	Hartman et al.	N/A	N/A
6021203	12/1999	Douceur et al.	N/A	N/A
6049328	12/1999	Vanderheiden	N/A	N/A
6058373	12/1999	Blinn et al.	N/A	N/A
6061666	12/1999	Do et al.	N/A	N/A
6105013	12/1999	Curry et al.	N/A	N/A
6199114	12/2000	White et al.	N/A	N/A
6199762	12/2000	Hohle	N/A	N/A
6216227	12/2000	Goldstein et al.	N/A	N/A
6227447	12/2000	Campisano	N/A	N/A
6282522	12/2000	Davis et al.	N/A	N/A
6324271	12/2000	Sawyer et al.	N/A	N/A
6342844	12/2001	Rozin	N/A	N/A
6367011	12/2001	Lee et al.	N/A	N/A

6402028	12/2001	Graham, Jr. et al.	N/A	N/A
6438550	12/2001	Doyle et al.	N/A	N/A
6501847	12/2001	Helot et al.	N/A	N/A
6631197	12/2002	Taenzer	N/A	N/A
6641050	12/2002	Kelley et al.	N/A	N/A
6655585	12/2002	Shinn	N/A	N/A
6662020	12/2002	Aaro et al.	N/A	N/A
6721706	12/2003	Strubbe et al.	N/A	N/A
6731778	12/2003	Oda et al.	N/A	N/A
6779115	12/2003	Naim	N/A	N/A
6792533	12/2003	Jablon	N/A	N/A
6829711	12/2003	Kwok et al.	N/A	N/A
6834271	12/2003	Hodgson et al.	N/A	N/A
6834795	12/2003	Rasmussen et al.	N/A	N/A
6852031	12/2004	Rowe	N/A	N/A
6865547	12/2004	Brake, Jr. et al.	N/A	N/A
6873260	12/2004	Lancos et al.	N/A	N/A
6877656	12/2004	Jaros et al.	N/A	N/A
6889198	12/2004	Kawan	N/A	N/A
6905411	12/2004	Nguyen et al.	N/A	N/A
6910627	12/2004	Simpson-Young et al.	N/A	N/A
6971031	12/2004	Haala	N/A	N/A
6990588	12/2005	Yasukura	N/A	N/A
7006986	12/2005	Sines et al.	N/A	N/A
7085931	12/2005	Smith et al.	N/A	N/A
7127605	12/2005	Montgomery et al.	N/A	N/A
7128274	12/2005	Kelley et al.	N/A	N/A
7140550	12/2005	Ramachandran	N/A	N/A
7152045	12/2005	Hoffman	N/A	N/A
7165727	12/2006	de Jong	N/A	N/A
7175076	12/2006	Block et al.	N/A	N/A
7202773	12/2006	Oba et al.	N/A	N/A
7206806	12/2006	Pineau	N/A	N/A
7232073	12/2006	de Jong	N/A	N/A
7246752	12/2006	Brown	N/A	N/A
7254569	12/2006	Goodman et al.	N/A	N/A
7263507	12/2006	Brake, Jr. et al.	N/A	N/A
7270276	12/2006	Vayssiere	N/A	N/A
7278025	12/2006	Saito et al.	N/A	N/A
7287692	12/2006	Patel et al.	N/A	N/A
7290709	12/2006	Tsai et al.	N/A	N/A
7306143	12/2006	Bonneau, Jr. et al.	N/A	N/A
7319986	12/2007	Praisner et al.	N/A	N/A
7325132	12/2007	Takayama et al.	N/A	N/A
7373515	12/2007	Owen et al.	N/A	N/A
7374099	12/2007	de Jong	N/A	N/A
7375616	12/2007	Rowse et al.	N/A	N/A
7380710	12/2007	Brown	N/A	N/A
7424977	12/2007	Smets et al.	N/A	N/A
7453439	12/2007	Kushler et al.	N/A	N/A

7472829	12/2008	Brown	N/A	N/A
7487357	12/2008	Smith et al.	N/A	N/A
7568631	12/2008	Gibbs et al.	N/A	N/A
7584153	12/2008	Brown et al.	N/A	N/A
7597250	12/2008	Finn	N/A	N/A
7628322	12/2008	Holtmanns et al.	N/A	N/A
7652578	12/2009	Braun et al.	N/A	N/A
7689832	12/2009	Talmor et al.	N/A	N/A
7703142	12/2009	Wilson et al.	N/A	N/A
7748609	12/2009	Sachdeva et al.	N/A	N/A
7748617	12/2009	Gray	N/A	N/A
7748636	12/2009	Finn	N/A	N/A
7762457	12/2009	Bonalle et al.	N/A	N/A
7789302	12/2009	Tame	N/A	N/A
7793851	12/2009	Mullen	N/A	N/A
7796013	12/2009	Murakami et al.	N/A	N/A
7801799	12/2009	Brake, Jr. et al.	N/A	N/A
7801829	12/2009	Gray et al.	N/A	N/A
7805755	12/2009	Brown et al.	N/A	N/A
7809643	12/2009	Phillips et al.	N/A	N/A
7827115	12/2009	Weller et al.	N/A	N/A
7828214	12/2009	Narendra et al.	N/A	N/A
7848746	12/2009	Juels	N/A	N/A
7882553	12/2010	Tuliani	N/A	N/A
7900048	12/2010	Andersson	N/A	N/A
7908216	12/2010	Davis et al.	N/A	N/A
7922082	12/2010	Muscato	N/A	N/A
7933589	12/2010	Mamdani et al.	N/A	N/A
7949559	12/2010	Freiberg	N/A	N/A
7954716	12/2010	Narendra et al.	N/A	N/A
7954723	12/2010	Charrat	N/A	N/A
7962369	12/2010	Rosenberg	N/A	N/A
7993197	12/2010	Mamdani et al.	N/A	N/A
8005426	12/2010	Huomo et al.	N/A	N/A
8010405	12/2010	Bortolin et al.	N/A	N/A
RE42762	12/2010	Shin	N/A	N/A
8041954	12/2010	Plesman	N/A	N/A
8060012	12/2010	Sklovsky et al.	N/A	N/A
8074877	12/2010	Mullen et al.	N/A	N/A
8082450	12/2010	Frey et al.	N/A	N/A
8095113	12/2011	Kean et al.	N/A	N/A
8099332	12/2011	Lemay et al.	N/A	N/A
8103249	12/2011	Markison	N/A	N/A
8108687	12/2011	Ellis et al.	N/A	N/A
8127143	12/2011	Abdallah et al.	N/A	N/A
8135648	12/2011	Oram et al.	N/A	N/A
8140010	12/2011	Symons et al.	N/A	N/A
8141136	12/2011	Lee et al.	N/A	N/A
8150321	12/2011	Winter et al.	N/A	N/A
8150767	12/2011	Wankmueller	N/A	N/A
8186602	12/2011	Itay et al.	N/A	N/A

8196131	12/2011	von Behren et al.	N/A	N/A
8215563	12/2011	Levy et al.	N/A	N/A
8224753	12/2011	Atef et al.	N/A	N/A
8232879	12/2011	Davis	N/A	N/A
8233841	12/2011	Griffin et al.	N/A	N/A
8245292	12/2011	Buer	N/A	N/A
8249654	12/2011	Zhu	N/A	N/A
8266451	12/2011	Leydier et al.	N/A	N/A
8285329	12/2011	Zhu	N/A	N/A
8302872	12/2011	Mullen	N/A	N/A
8312519	12/2011	Bailey et al.	N/A	N/A
8316237	12/2011	Felsher et al.	N/A	N/A
8332272	12/2011	Fisher	N/A	N/A
8365988	12/2012	Medina, III et al.	N/A	N/A
8369960	12/2012	Tran et al.	N/A	N/A
8371501	12/2012	Hopkins	N/A	N/A
8381307	12/2012	Cimino	N/A	N/A
8391719	12/2012	Alameh et al.	N/A	N/A
8417231	12/2012	Sanding et al.	N/A	N/A
8439271	12/2012	Smets et al.	N/A	N/A
8475367	12/2012	Yuen et al.	N/A	N/A
8489112	12/2012	Roeding et al.	N/A	N/A
8511542	12/2012	Pan	N/A	N/A
8559872	12/2012	Butler	N/A	N/A
8566916	12/2012	Vernon et al.	N/A	N/A
8567670	12/2012	Stanfield et al.	N/A	N/A
8572386	12/2012	Takekawa et al.	N/A	N/A
8577810	12/2012	Dalit et al.	N/A	N/A
8583454	12/2012	Beraja et al.	N/A	N/A
8589335	12/2012	Smith et al.	N/A	N/A
8594730	12/2012	Bona et al.	N/A	N/A
8615468	12/2012	Varadarajan	N/A	N/A
8620218	12/2012	Awad	N/A	N/A
8667285	12/2013	Coulier et al.	N/A	N/A
8723941	12/2013	Shirbabadi et al.	N/A	N/A
8726405	12/2013	Bailey et al.	N/A	N/A
8740073	12/2013	Vijayshankar et al.	N/A	N/A
8750514	12/2013	Gallo et al.	N/A	N/A
8752189	12/2013	De Jong	N/A	N/A
8794509	12/2013	Bishop et al.	N/A	N/A
8799668	12/2013	Cheng	N/A	N/A
8806592	12/2013	Ganesan	N/A	N/A
8807440	12/2013	Von Behren et al.	N/A	N/A
8811892	12/2013	Khan et al.	N/A	N/A
8814039	12/2013	Bishop et al.	N/A	N/A
8814052	12/2013	Bona et al.	N/A	N/A
8818867	12/2013	Baldwin et al.	N/A	N/A
8850538	12/2013	Vernon et al.	N/A	N/A
8861733	12/2013	Benteo et al.	N/A	N/A
8880027	12/2013	Darringer	N/A	N/A
8888002	12/2013	Chesney et al.	N/A	N/A

8898088	12/2013	Springer et al.	N/A	N/A
8934837	12/2014	Zhu et al.	N/A	N/A
8977569	12/2014	Rao	N/A	N/A
8994498	12/2014	Agrafioti et al.	N/A	N/A
9004365	12/2014	Bona et al.	N/A	N/A
9038894	12/2014	Khalid	N/A	N/A
9042814	12/2014	Royston et al.	N/A	N/A
9047531	12/2014	Showering et al.	N/A	N/A
9069976	12/2014	Toole et al.	N/A	N/A
9081948	12/2014	Magne	N/A	N/A
9104853	12/2014	Mathur et al.	N/A	N/A
9118663	12/2014	Bailey et al.	N/A	N/A
9122964	12/2014	Krawczewicz	N/A	N/A
9129280	12/2014	Bona et al.	N/A	N/A
9152832	12/2014	Royston et al.	N/A	N/A
9203800	12/2014	Izu et al.	N/A	N/A
9209867	12/2014	Royston	N/A	N/A
9251330	12/2015	Boivie et al.	N/A	N/A
9251518	12/2015	Levin et al.	N/A	N/A
9258715	12/2015	Borghei	N/A	N/A
9270337	12/2015	Zhu et al.	N/A	N/A
9306626	12/2015	Hall et al.	N/A	N/A
9306942	12/2015	Bailey et al.	N/A	N/A
9324066	12/2015	Archer et al.	N/A	N/A
9324067	12/2015	Van Os et al.	N/A	N/A
9332587	12/2015	Salahshoor	N/A	N/A
9338622	12/2015	Bjontegard	N/A	N/A
9373141	12/2015	Shakkarwar	N/A	N/A
9379841	12/2015	Fine et al.	N/A	N/A
9406011	12/2015	Bartenstein et al.	N/A	N/A
9413430	12/2015	Royston et al.	N/A	N/A
9413768	12/2015	Gregg et al.	N/A	N/A
9420496	12/2015	Indurkar	N/A	N/A
9426132	12/2015	Alikhani	N/A	N/A
9432339	12/2015	Bowness	N/A	N/A
9455968	12/2015	Machani et al.	N/A	N/A
9473509	12/2015	Arsanjani et al.	N/A	N/A
9491626	12/2015	Sharma et al.	N/A	N/A
9553637	12/2016	Yang et al.	N/A	N/A
9619952	12/2016	Zhao et al.	N/A	N/A
9635000	12/2016	Muftic	N/A	N/A
9665858	12/2016	Kumar	N/A	N/A
9674705	12/2016	Rose et al.	N/A	N/A
9679286	12/2016	Colnot et al.	N/A	N/A
9680942	12/2016	Dimmick	N/A	N/A
9710804	12/2016	Zhou et al.	N/A	N/A
9740342	12/2016	Paulsen et al.	N/A	N/A
9740988	12/2016	Levin et al.	N/A	N/A
9763097	12/2016	Robinson et al.	N/A	N/A
9767329	12/2016	Forster	N/A	N/A
9769662	12/2016	Queru	N/A	N/A

9773151	12/2016	Mil'shtein et al.	N/A	N/A
9780953	12/2016	Gaddam et al.	N/A	N/A
9891823	12/2017	Feng et al.	N/A	N/A
9940571	12/2017	Herrington	N/A	N/A
9953323	12/2017	Candelore et al.	N/A	N/A
9961194	12/2017	Wiechman et al.	N/A	N/A
9965756	12/2017	Davis et al.	N/A	N/A
9965911	12/2017	Wishne	N/A	N/A
9978058	12/2017	Wurmfeld et al.	N/A	N/A
10043164	12/2017	Dogin et al.	N/A	N/A
10075437	12/2017	Costigan et al.	N/A	N/A
10129648	12/2017	Hernandez et al.	N/A	N/A
10133979	12/2017	Eidam et al.	N/A	N/A
10217105	12/2018	Sangi et al.	N/A	N/A
10706400	12/2019	Puffer et al.	N/A	N/A
10861006	12/2019	Ilincic	N/A	G06Q 20/341
2001/0010723	12/2000	Pinkas	N/A	N/A
2001/0029485	12/2000	Brody et al.	N/A	N/A
2001/0034702	12/2000	Mockett et al.	N/A	N/A
2001/0054003	12/2000	Chien et al.	N/A	N/A
2002/0078345	12/2001	Sandhu et al.	N/A	N/A
2002/0093530	12/2001	Krothapalli et al.	N/A	N/A
2002/0100808	12/2001	Norwood et al.	N/A	N/A
2002/0120583	12/2001	Keresman, III et al.	N/A	N/A
2002/0152116	12/2001	Yan et al.	N/A	N/A
2002/0153424	12/2001	Li	N/A	N/A
2002/0165827	12/2001	Gien et al.	N/A	N/A
2003/0023554	12/2002	Yap et al.	N/A	N/A
2003/0034873	12/2002	Chase et al.	N/A	N/A
2003/0055727	12/2002	Walker et al.	N/A	N/A
2003/0078882	12/2002	Sukeda et al.	N/A	N/A
2003/0167350	12/2002	Davis et al.	N/A	N/A
2003/0208449	12/2002	Diao	N/A	N/A
2004/0015958	12/2003	Veil et al.	N/A	N/A
2004/0039919	12/2003	Takayama et al.	N/A	N/A
2004/0127256	12/2003	Goldthwaite et al.	N/A	N/A
2004/0215674	12/2003	Odinak et al.	N/A	N/A
2004/0230799	12/2003	Davis	N/A	N/A
2004/0235450	12/2003	Rosenberg	N/A	N/A
2005/0044367	12/2004	Gasparini et al.	N/A	N/A
2005/0075985	12/2004	Cartmell	N/A	N/A
2005/0081038	12/2004	Arditti Modiano et al.	N/A	N/A
2005/0138387	12/2004	Lam et al.	N/A	N/A
2005/0156026	12/2004	Ghosh et al.	N/A	N/A
2005/0160049	12/2004	Lundholm	N/A	N/A
2005/0195975	12/2004	Kawakita	N/A	N/A
2005/0247797	12/2004	Ramachandran	N/A	N/A
2006/0006230	12/2005	Bear et al.	N/A	N/A
2006/0040726	12/2005	Szrek et al.	N/A	N/A
2006/0041402	12/2005	Baker	N/A	N/A

2006/0044153	12/2005	Dawidowsky	N/A	N/A
2006/0047954	12/2005	Sachdeva et al.	N/A	N/A
2006/0085848	12/2005	Aissi et al.	N/A	N/A
2006/0136334	12/2005	Atkinson et al.	N/A	N/A
2006/0173985	12/2005	Moore	N/A	N/A
2006/0174331	12/2005	Schuetz	N/A	N/A
2006/0242698	12/2005	Inskeep et al.	N/A	N/A
2006/0280338	12/2005	Rabb	N/A	N/A
2007/0033642	12/2006	Ganesan et al.	N/A	N/A
2007/0055630	12/2006	Gauthier et al.	N/A	N/A
2007/0061266	12/2006	Moore et al.	N/A	N/A
2007/0061487	12/2006	Moore et al.	N/A	N/A
2007/0116292	12/2006	Kurita et al.	N/A	N/A
2007/0118745	12/2006	Buer	N/A	N/A
2007/0197261	12/2006	Humbel	N/A	N/A
2007/0224969	12/2006	Rao	N/A	N/A
2007/0241182	12/2006	Buer	N/A	N/A
2007/0256134	12/2006	Lehtonen et al.	N/A	N/A
2007/0258594	12/2006	Sandhu et al.	N/A	N/A
2007/0278291	12/2006	Rans et al.	N/A	N/A
2008/0008315	12/2007	Fontana et al.	N/A	N/A
2008/0011831	12/2007	Bonalle et al.	N/A	N/A
2008/0014867	12/2007	Finn	N/A	N/A
2008/0035738	12/2007	Mullen	N/A	N/A
2008/0071681	12/2007	Khalid	N/A	N/A
2008/0072303	12/2007	Syed	N/A	N/A
2008/0086767	12/2007	Kulkarni et al.	N/A	N/A
2008/0103968	12/2007	Bies et al.	N/A	N/A
2008/0109309	12/2007	Landau et al.	N/A	N/A
2008/0110983	12/2007	Ashfield	N/A	N/A
2008/0120711	12/2007	Dispensa	N/A	N/A
2008/0134295	12/2007	Bailey	726/4	G06F 21/30
2008/0156873	12/2007	Wilhelm et al.	N/A	N/A
2008/0162312	12/2007	Sklovsky et al.	N/A	N/A
2008/0164308	12/2007	Aaron et al.	N/A	N/A
2008/0207307	12/2007	Cunningham, II et al.	N/A	N/A
2008/0209543	12/2007	Aaron	N/A	N/A
2008/0223918	12/2007	Williams et al.	N/A	N/A
2008/0285746	12/2007	Landrock et al.	N/A	N/A
2008/0308641	12/2007	Finn	N/A	N/A
2009/0037275	12/2008	Pollio	N/A	N/A
2009/0048026	12/2008	French	N/A	N/A
2009/0132417	12/2008	Scipioni et al.	N/A	N/A
2009/0143104	12/2008	Loh et al.	N/A	N/A
2009/0171682	12/2008	Dixon et al.	N/A	N/A
2009/0210308	12/2008	Toomer et al.	N/A	N/A
2009/0235339	12/2008	Mennes et al.	N/A	N/A
2009/0249077	12/2008	Gargaro et al.	N/A	N/A
2009/0282264	12/2008	Amiel et al.	N/A	N/A
2010/0023449	12/2009	Skowronek et al.	N/A	N/A

2010/0023455	12/2009	Dispensa et al.	N/A	N/A
2010/0029202	12/2009	Jolivet et al.	N/A	N/A
2010/0033310	12/2009	Narendra et al.	N/A	N/A
2010/0036769	12/2009	Winters et al.	N/A	N/A
2010/0078471	12/2009	Lin et al.	N/A	N/A
2010/0082491	12/2009	Rosenblatt et al.	N/A	N/A
2010/0094754	12/2009	Bertran et al.	N/A	N/A
2010/0095130	12/2009	Bertran et al.	N/A	N/A
2010/0100480	12/2009	Altman et al.	N/A	N/A
2010/0114731	12/2009	Kingston et al.	N/A	N/A
2010/0192230	12/2009	Steeves et al.	N/A	N/A
2010/0207742	12/2009	Buhot et al.	N/A	N/A
2010/0211797	12/2009	Westerveld et al.	N/A	N/A
2010/0240413	12/2009	He et al.	N/A	N/A
2010/0257357	12/2009	McClain	N/A	N/A
2010/0312634	12/2009	Cervenka	N/A	N/A
2010/0312635	12/2009	Cervenka	N/A	N/A
2011/0028160	12/2010	Roeding et al.	N/A	N/A
2011/0035604	12/2010	Habraken	N/A	N/A
2011/0060631	12/2010	Grossman et al.	N/A	N/A
2011/0068170	12/2010	Lehman	N/A	N/A
2011/0084132	12/2010	Tofighbakhsh	N/A	N/A
2011/0101093	12/2010	Ehrensvard	N/A	N/A
2011/0113245	12/2010	Varadrajan	N/A	N/A
2011/0125638	12/2010	Davis et al.	N/A	N/A
2011/0131415	12/2010	Schneider	N/A	N/A
2011/0153437	12/2010	Archer et al.	N/A	N/A
2011/0153496	12/2010	Royyuru	N/A	N/A
2011/0208658	12/2010	Makhotin	N/A	N/A
2011/0208965	12/2010	Machani	N/A	N/A
2011/0211219	12/2010	Bradley	N/A	N/A
2011/0218911	12/2010	Spodak	N/A	N/A
2011/0238564	12/2010	Lim et al.	N/A	N/A
2011/0246780	12/2010	Yeap et al.	N/A	N/A
2011/0258452	12/2010	Coulier et al.	N/A	N/A
2011/0280406	12/2010	Ma et al.	N/A	N/A
2011/0282785	12/2010	Chin	N/A	N/A
2011/0294418	12/2010	Chen	N/A	N/A
2011/0312271	12/2010	Ma et al.	N/A	N/A
2012/0024947	12/2011	Naelon	N/A	N/A
2012/0030047	12/2011	Fuentes et al.	N/A	N/A
2012/0030121	12/2011	Grellier	N/A	N/A
2012/0047071	12/2011	Mullen et al.	N/A	N/A
2012/0079281	12/2011	Lowenstein et al.	N/A	N/A
2012/0109735	12/2011	Krawczewicz et al.	N/A	N/A
2012/0109764	12/2011	Martin et al.	N/A	N/A
2012/0143754	12/2011	Patel	N/A	N/A
2012/0150737	12/2011	Rottink	N/A	N/A
2012/0178366	12/2011	Levy et al.	N/A	N/A
2012/0196583	12/2011	Kindo	N/A	N/A
2012/0207305	12/2011	Gallo et al.	N/A	N/A

2012/0209773	12/2011	Ranganathan	N/A	N/A
2012/0238206	12/2011	Singh et al.	N/A	N/A
2012/0239560	12/2011	Pourfallah et al.	N/A	N/A
2012/0252350	12/2011	Steinmetz et al.	N/A	N/A
2012/0254394	12/2011	Barras	N/A	N/A
2012/0284194	12/2011	Liu et al.	N/A	N/A
2012/0290472	12/2011	Mullen et al.	N/A	N/A
2012/0296818	12/2011	Nuzzi et al.	N/A	N/A
2012/0316992	12/2011	Oborne	N/A	N/A
2012/0317035	12/2011	Royyuru et al.	N/A	N/A
2012/0317628	12/2011	Yeager	N/A	N/A
2012/0331529	12/2011	Maximilian et al.	N/A	N/A
2013/0005245	12/2012	Royston	N/A	N/A
2013/0008956	12/2012	Ashfield	N/A	N/A
2013/0026229	12/2012	Jarman et al.	N/A	N/A
2013/0048713	12/2012	Pan	N/A	N/A
2013/0054474	12/2012	Yeager	N/A	N/A
2013/0065564	12/2012	Conner et al.	N/A	N/A
2013/0080228	12/2012	Fisher	N/A	N/A
2013/0080229	12/2012	Fisher	N/A	N/A
2013/0099587	12/2012	Lou	N/A	N/A
2013/0104251	12/2012	Moore et al.	N/A	N/A
2013/0106576	12/2012	Hinman et al.	N/A	N/A
2013/0119130	12/2012	Braams	N/A	N/A
2013/0130614	12/2012	Busch-Sorensen	N/A	N/A
2013/0144793	12/2012	Royston	N/A	N/A
2013/0171929	12/2012	Adams et al.	N/A	N/A
2013/0179351	12/2012	Wallner	N/A	N/A
2013/0185772	12/2012	Jaudon et al.	N/A	N/A
2013/0191279	12/2012	Calman et al.	N/A	N/A
2013/0200999	12/2012	Spodak et al.	N/A	N/A
2013/0216108	12/2012	Hwang et al.	N/A	N/A
2013/0226791	12/2012	Springer et al.	N/A	N/A
2013/0226796	12/2012	Jiang et al.	N/A	N/A
2013/0232082	12/2012	Krawczewicz et al.	N/A	N/A
2013/0238894	12/2012	Ferg et al.	N/A	N/A
2013/0282360	12/2012	Shimota et al.	N/A	N/A
2013/0303085	12/2012	Boucher et al.	N/A	N/A
2013/0304651	12/2012	Smith	N/A	N/A
2013/0312082	12/2012	Izu et al.	N/A	N/A
2013/0314593	12/2012	Reznik et al.	N/A	N/A
2013/0344857	12/2012	Berionne et al.	N/A	N/A
2014/0002238	12/2013	Taveau et al.	N/A	N/A
2014/0019352	12/2013	Shrivastava	N/A	N/A
2014/0027506	12/2013	Heo et al.	N/A	N/A
2014/0032409	12/2013	Rosano	N/A	N/A
2014/0032410	12/2013	Georgiev et al.	N/A	N/A
2014/0040120	12/2013	Cho et al.	N/A	N/A
2014/0040139	12/2013	Brudnicki et al.	N/A	N/A
2014/0040147	12/2013	Varadarakan et al.	N/A	N/A
2014/0047235	12/2013	Lessiak et al.	N/A	N/A

2014/0067690	12/2013	Pitroda et al.	N/A	N/A
2014/0074637	12/2013	Hammad	N/A	N/A
2014/0074655	12/2013	Lim et al.	N/A	N/A
2014/0081720	12/2013	Wu	N/A	N/A
2014/0138435	12/2013	Khalid	N/A	N/A
2014/0171034	12/2013	Aleksin et al.	N/A	N/A
2014/0171039	12/2013	Bjontegard	N/A	N/A
2014/0172700	12/2013	Teuwen et al.	N/A	N/A
2014/0180851	12/2013	Fisher	N/A	N/A
2014/0208112	12/2013	McDonald et al.	N/A	N/A
2014/0214674	12/2013	Narula	N/A	N/A
2014/0229375	12/2013	Zaytzsev et al.	N/A	N/A
2014/0245391	12/2013	Adenuga	N/A	N/A
2014/0256251	12/2013	Caceres et al.	N/A	N/A
2014/0258099	12/2013	Rosano	N/A	N/A
2014/0258113	12/2013	Gauthier et al.	N/A	N/A
2014/0258125	12/2013	Gerber et al.	N/A	N/A
2014/0274179	12/2013	Zhu et al.	N/A	N/A
2014/0279479	12/2013	Maniar et al.	N/A	N/A
2014/0337235	12/2013	Van Heerden et al.	N/A	N/A
2014/0339315	12/2013	Ko	N/A	N/A
2014/0346860	12/2013	Aubry et al.	N/A	N/A
2014/0365780	12/2013	Movassaghi	N/A	N/A
2014/0379361	12/2013	Mahadkar et al.	N/A	N/A
2015/0012444	12/2014	Brown et al.	N/A	N/A
2015/0032635	12/2014	Guise	N/A	N/A
2015/0071486	12/2014	Rhoads et al.	N/A	N/A
2015/0088757	12/2014	Zhou et al.	N/A	N/A
2015/0089586	12/2014	Ballesteros	N/A	N/A
2015/0121541	12/2014	Fay	N/A	N/A
2015/0134452	12/2014	Williams	N/A	N/A
2015/0140960	12/2014	Powell et al.	N/A	N/A
2015/0154595	12/2014	Collinge et al.	N/A	N/A
2015/0170138	12/2014	Rao	N/A	N/A
2015/0178724	12/2014	Ngo et al.	N/A	N/A
2015/0178725	12/2014	Poetsch	N/A	N/A
2015/0186871	12/2014	Laracey	N/A	N/A
2015/0205379	12/2014	Mag et al.	N/A	N/A
2015/0271200	12/2014	Shane et al.	N/A	N/A
2015/0302409	12/2014	Malek	N/A	N/A
2015/0317626	12/2014	Ran et al.	N/A	N/A
2015/0332266	12/2014	Friedlander et al.	N/A	N/A
2015/0339474	12/2014	Paz et al.	N/A	N/A
2015/0371234	12/2014	Huang et al.	N/A	N/A
2016/0012465	12/2015	Sharp	N/A	N/A
2016/0019536	12/2015	Ortiz et al.	N/A	N/A
2016/0026997	12/2015	Tsui et al.	N/A	N/A
2016/0034887	12/2015	Lee	N/A	N/A
2016/0048913	12/2015	Rausaria et al.	N/A	N/A
2016/0055480	12/2015	Shah	N/A	N/A
2016/0057619	12/2015	Lopez	N/A	N/A

2016/0065370	12/2015	Le Saint et al.	N/A	N/A
2016/0087957	12/2015	Shah et al.	N/A	N/A
2016/0092696	12/2015	Guglani et al.	N/A	N/A
2016/0148193	12/2015	Kelley et al.	N/A	N/A
2016/0232523	12/2015	Venot et al.	N/A	N/A
2016/0239672	12/2015	Khan et al.	N/A	N/A
2016/0253651	12/2015	Park et al.	N/A	N/A
2016/0255072	12/2015	Liu	N/A	N/A
2016/0267486	12/2015	Mitra et al.	N/A	N/A
2016/0277383	12/2015	Guyomarc'h et al.	N/A	N/A
2016/0277388	12/2015	Lowe et al.	N/A	N/A
2016/0307187	12/2015	Guo et al.	N/A	N/A
2016/0307189	12/2015	Zarakas et al.	N/A	N/A
2016/0314472	12/2015	Ashfield	N/A	N/A
2016/0330027	12/2015	Ebrahimi	N/A	N/A
2016/0335531	12/2015	Mullen et al.	N/A	N/A
2016/0379217	12/2015	Hammad	N/A	N/A
2017/0004502	12/2016	Quentin et al.	N/A	N/A
2017/0011395	12/2016	Pillai et al.	N/A	N/A
2017/0011406	12/2016	Tunnell et al.	N/A	N/A
2017/0017957	12/2016	Radu	N/A	N/A
2017/0017964	12/2016	Janefalkar et al.	N/A	N/A
2017/0024716	12/2016	Jiam et al.	N/A	N/A
2017/0039566	12/2016	Schipperheijn	N/A	N/A
2017/0041759	12/2016	Gantert et al.	N/A	N/A
2017/0068950	12/2016	Kwon	N/A	N/A
2017/0103388	12/2016	Pillai et al.	N/A	N/A
2017/0104739	12/2016	Lansler et al.	N/A	N/A
2017/0109509	12/2016	Baghdasaryan	N/A	N/A
2017/0109730	12/2016	Locke et al.	N/A	N/A
2017/0116447	12/2016	Cimino et al.	N/A	N/A
2017/0124568	12/2016	Moghadam	N/A	N/A
2017/0140379	12/2016	Deck	N/A	N/A
2017/0154328	12/2016	Zarakas et al.	N/A	N/A
2017/0154333	12/2016	Gleeson et al.	N/A	N/A
2017/0180134	12/2016	King	N/A	N/A
2017/0230189	12/2016	Toll et al.	N/A	N/A
2017/0237301	12/2016	Elad et al.	N/A	N/A
2017/0289127	12/2016	Hendrick	N/A	N/A
2017/0295013	12/2016	Claes	N/A	N/A
2017/0316696	12/2016	Bartel	N/A	N/A
2017/0317834	12/2016	Smith et al.	N/A	N/A
2017/0330173	12/2016	Woo et al.	N/A	N/A
2017/0374070	12/2016	Shah et al.	N/A	N/A
2018/0034507	12/2017	Wobak et al.	N/A	N/A
2018/0039986	12/2017	Essebag et al.	N/A	N/A
2018/0068316	12/2017	Essebag et al.	N/A	N/A
2018/0129945	12/2017	Saxena et al.	N/A	N/A
2018/0160255	12/2017	Park	N/A	N/A
2018/0191501	12/2017	Lindemann	N/A	N/A
2018/0205712	12/2017	Versteeg et al.	N/A	N/A

2018/0219867	12/2017	Patterson et al.	N/A	N/A
2018/0240106	12/2017	Garrett et al.	N/A	N/A
2018/0254909	12/2017	Hancock	N/A	N/A
2018/0268132	12/2017	Buer et al.	N/A	N/A
2018/0270214	12/2017	Caterino et al.	N/A	N/A
2018/0294959	12/2017	Traynor et al.	N/A	N/A
2018/0300716	12/2017	Carlson	N/A	N/A
2018/0302396	12/2017	Camenisch et al.	N/A	N/A
2018/0315050	12/2017	Hammad	N/A	N/A
2018/0316666	12/2017	Koved et al.	N/A	N/A
2018/0322486	12/2017	Deliwala et al.	N/A	N/A
2018/0359100	12/2017	Gaddam et al.	N/A	N/A
2019/0014107	12/2018	George	N/A	N/A
2019/0019375	12/2018	Foley	N/A	N/A
2019/0036678	12/2018	Ahmed	N/A	N/A
2019/0238517	12/2018	D'Agostino et al.	N/A	N/A
2019/0392416	12/2018	Bernholc	N/A	N/A
2020/0028841	12/2019	Mars	N/A	H04B 10/1141
2020/0104833	12/2019	Rule et al.	N/A	N/A
2022/0058633	12/2021	Yantis	N/A	G06Q 20/3676

FOREIGN PATENT DOCUMENTS

Patent No.	**Application Date**	**Country**	**CPC**
2847636	12/2010	CA	G06Q 20/10
3010336	12/2016	CA	N/A
101192295	12/2007	CN	N/A
103023643	12/2012	CN	N/A
103417202	12/2012	CN	N/A
1 085 424	12/2000	EP	N/A
1 223 565	12/2001	EP	N/A
1 265 186	12/2001	EP	N/A
1 783 919	12/2006	EP	N/A
2 852 070	12/2008	EP	N/A
2 139 196	12/2008	EP	N/A
1 469 419	12/2011	EP	N/A
2 457 221	12/2008	GB	N/A
2 516 861	12/2014	GB	N/A
2 551 907	12/2017	GB	N/A
2004199534	12/2003	JP	N/A
2007516513	12/2006	JP	N/A
2012147945	12/2011	JP	N/A
2014211873	12/2013	JP	N/A
2018508091	12/2017	JP	N/A
101508320	12/2014	KR	N/A
101560440	12/2014	KR	N/A
WO 00/49586	12/1999	WO	N/A
WO 2006070189	12/2005	WO	N/A
WO 2008055170	12/2007	WO	N/A

WO 2009025605	12/2008	WO	N/A
WO 2010049252	12/2009	WO	N/A
WO 2011112158	12/2010	WO	N/A
WO 2012001624	12/2011	WO	N/A
WO 2013039395	12/2012	WO	N/A
WO 2013155562	12/2012	WO	N/A
WO 2013192358	12/2012	WO	N/A
WO 2014043278	12/2013	WO	N/A
WO 2014170741	12/2013	WO	N/A
WO 2015179649	12/2014	WO	N/A
WO 2015183818	12/2014	WO	N/A
WO 2016097718	12/2015	WO	N/A
WO 2016160816	12/2015	WO	N/A
WO 2016168394	12/2015	WO	N/A
WO 2017042375	12/2016	WO	N/A
WO 2017042400	12/2016	WO	N/A
WO 2017157859	12/2016	WO	N/A
WO 2017208063	12/2016	WO	N/A
WO 2018063809	12/2017	WO	N/A
WO 2018137888	12/2017	WO	N/A

OTHER PUBLICATIONS

Batina, Lejla and Poll, Erik, “SmartCards and RFID”, Course PowerPoint Presentation for IPA Security Course, Digital Security at University of Nijmegen, Netherlands (date unknown) 75 pages. cited by applicant

Haykin M. and Warnar, R., “Smart Card Technology: New Methods for Computer Access Control,” Computer Science and Technology NIST Special Publication 500-157:1-60 (1988). cited by applicant

Lehpamer, Harvey, “Component of the RFID System,” RFID Design Principles, 2nd edition pp. 133-201 (2012). cited by applicant

Pourghomi, Pardis et al., “A Proposed NFC Payment Application, International Journal of Advanced Computer Science and Applications,” vol. 4, No. 8, 2013. cited by applicant

Author Unknown, “CardrefresherSM from American Express®,” [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://merchant-channel.americanexpress.com/merchant/en_US/cardrefresher, 2 pages. cited by applicant

Author Unknown, “Add Account Updater to your recurring payment tool,” [online] 2018-19 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.authorize.net/our-features/account-updater/, 5 pages. cited by applicant

Author Unknown, “Visa® Account Updater for Merchants,” [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://usa.visa.com/dam/VCOM/download/merchants/visa-account-updater-product-information-fact-sheet-for-merchants.pdf, 2 pages. cited by applicant

Author Unknown, “Manage the cards that you use with Apple Pay,” Apple Support [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://support.apple.com/en-us/HT205583, 5 pages. cited by applicant

Author Unknown, “Contactless Specifications for Payment Systems,” EMV Book B—Entry Point Specification [online] 2016 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.emvco.com/wp-content/uploads/2017/05/BookB_Entry_Point_Specification_v2_6_20160809023257319.pdf, 52 pages. cited by applicant

Author Unknown, “EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management,” Version 3.4, [online] 2011 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.emvco.com/wp-

content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf, 174 pages. cited by applicant
Author unknown, “NFC Guide: All You Need to Know About Near Field Communication” Square Guide [online] 2018[retrieved on Nov. 13, 2018]. Retrieved from Internet URL: https://squareup.com/guides/nfc, 8 pages. cited by applicant
Profis, S., “Everything you need to know about NFC and mobile payments” CNET Directory [online], 2014 [retrieved on Mar. 25, 2019]. Retrieved from the Internet URL: https://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/, 6 pages. cited by applicant
Cozma, N., “Copy data from other devices in Android 5.0 Lollipop setup” CNET Directory [online] 2014 [retrieved on Mar. 25, 2019]. Retrieved from the Internet URL: https://www.cnet.com/how-to/copy-data-from-other-devices-in-android-5-0-lollipop-setup/, 5 pages. cited by applicant
Kevin, Android Enthusiast, “How to copy text string from nfc tag” StackExchange [online] 2013 [retrieved on Mar. 25, 2019]. Retrieved from the Internet URL: https://android.stackexchange.com/questions/55689/how-to-copy-text-string-from-nfc-tag, 11 pages. cited by applicant
Author unknown, “Tap & Go Device Setup” Samsung [online] date unknown [retrieved on Mar. 25, 2019]. Retrieved from the Internet URL: https://www.samsung.com/us/switch-me/switch-to-the-galaxy-s-5/app/partial/setup-device/tap-go.html, 1 page. cited by applicant
Author Unknown, “Multiple encryption”, Wikipedia [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://en.wikipedia.org/wiki/Multiple_encryption, 4 pages. cited by applicant
Krawczyk, et al., “HMAC: Keyed-Hashing for Message Authentication”, Network Working Group RFC:2104 memo [online] 1997 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://tools.ietf.org/html/rfc2104, 12 pages. cited by applicant
Song, et al., “The AES-CMAC Algorithm”, Network Working Group RFC: 4493 memo [online] 2006 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://tools.ietf.org/html/rfc4493, 21 pages. cited by applicant
Katz, J., and Lindell, Y., “Aggregate Message Authentication Codes”, Topics in Cryptology [online] 2008 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.cs.umd.edu/˜jkatz/papers/aggregateMAC.pdf, 11 pages. cited by applicant
Adams, D., and Maier, A-K, “Goldbug Big Seven open source crypto-messengers to be compared-: or Comprehensive Confidentiality Review & Audit of GoldBug Encrypting E-Mail—Client & Secure Instant Messenger”, Big Seven Study 2016 [online] [retrieved on Mar. 25, 2018]. Retrieved from Internet URL: https://sf.net/projects/goldbug/files/bigseven-crypto-audit.pdf, 309 pages. cited by applicant
Author Unknown, “Triple DES”, Wikipedia [online] 2018 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://simple.wikipedia.org/wiki/Triple_DES, 2 pages. cited by applicant
Song, F., and Yun, A.1, “Quantum Security of NMAC and Related Constructions—PRF domain extension against quantum attacks”, IACR Cryptology ePrint Archive [online] 2017 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://eprint.iacr.org/2017/509.pdf, 41 pages. cited by applicant
Saxena, N., “Lecture 10: NMAC, HMAC and Number Theory”, CS 6903 Modern Cryptography [online] 2008 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: http://isis.poly.edu/courses/cs6903/Lectures/lecture10.pdf, 8 pages. cited by applicant
Berg, Guy, “Fundamentals of EMV” Smart Card Alliance [online] date unknown [retrieved on Mar. 27, 2019]. Retrieved from Internet URL: https://www.securetechalliance.org/resources/media/scap13_preconference/02.pdf, 37 pages. cited by applicant
Pierce, Kevin, “Is the amazon echo NFC compatible,?” Amazon.com Customer Q&A [online] 2016 [retrieved on Mar. 26, 2019]. Retrieved from Internet URL: https://www.amazon.com/ask/questions/Tx1RJXYSPE6XLJD?_encodi . . . , 2 pages. cited by applicant
Author Unknown, “Multi-Factor Authentication”, idaptive [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.centrify.com/products/application-services/adaptive-multi-factor-authentication/risk-based-mfa/, 10 pages. cited by applicant

Author Unknown, “Adaptive Authentication”, SecureAuth [online] 2019 [retrieved on Mar. 25, 2019}. Retrieved from Internet URL: https://www.secureauth.com/products/access-management/adaptive-authentication, 7 pages. cited by applicant
Van den Breekel, J., et al., “EMV in a nutshell”, Technical Report, 2016 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.cs.ru.nl/E.Poll/papers/EMVtechreport.pdf, 37 pages. cited by applicant
Author Unknown, “Autofill”, Computer Hope [online] 2018 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.computerhope.com/jargon/a/autofill.htm, 2 pages. cited by applicant
Author Unknown, “Fill out forms automatically”, Google Chrome Help [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://support.google.com/chrome/answer/142893?co=GENIE.Platform%3DDesktop&hl=en, 3 pages. cited by applicant
Author unknown, “Autofill credit cards, contacts, and passwords in Safari on Mac”, Apple Safari User Guide [online] 2019 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://support.apple.com/guide/safari/use-autofill-ibrw1103/mac, 3 pages. cited by applicant
Menghin, M.J., “Power Optimization Techniques for Near Field Communication Systems” 2014 Dissertation at Technical University of Graz [online]. Retrieved from Internet URL: https://diglib.tugraz.at/download.php?id=576a7b910d2d6&location=browse, 135 pages. cited by applicant
Mareli, M., et al., “Experimental evaluation of NFC reliability between an RFID tag and a smartphone” Conference paper (2013) IEEE AFRICON At Mauritius [online] [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://core.ac.uk/download/pdf/54204839.pdf, 5 pages. cited by applicant
Davison, A., et al., “MonoSLAM: Real-Time Single Camera SLAM”, IEEE Transactions on Pattern Analysis and Machine Intelligence 29(6): 1052-1067 (2007). cited by applicant
Barba, R., “Sharing your location with your bank sounds creepy, but it's also useful”, Bankrate, LLC [online] 2017 [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.bankrate.com/banking/banking-app-location-sharing/, 6 pages. cited by applicant
Author unknown: “onetappayment™M”, [online] Jan. 24, 2019, [retrieved on Mar. 25, 2019]. Retrieved from Internet URL: https://www.payubiz.in/onetap, 4 pages. cited by applicant
Vu et al., (2012). “Distinguishing users with capacitive touch communication” Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM. 10.1145/2348543.2348569. cited by applicant
EMVCo, EMV Card Personalization Specification, version 1.0 (Jun. 2003), 81 pages. cited by applicant
Ullmann et al., (2012). “On-Card User Authentication for Contactless Smart Cards based on Gesture Recognition”, LNI, 223-234, 12 pages. cited by applicant
Faraj et al. (2008). “Investigation of Java Smart Card Technology for Multi-Task Applications” J. of Al-Anbar University for Pure Science, vol. 2: No. 1: 2008, 11 pages. cited by applicant
Dhamdhere (2017) “Key Benefits of a Unified Platform for Loyalty, Referral Marketing, and UGC” Annex Cloud [retrieved on Jul. 3, 2019]. Retrieved from Internet URL: https://www.annexcloude.com/blog/benefits-unified-platform/, 13 pages. cited by applicant
European Extended Search Report issued in related European Patent Application No. EP 21156457.0, mailed Jun. 21, 2021. cited by applicant
Singapore Patent Office Search Report and Written Opinion issued in related Singapore Patent Application No. 10202101473Q mailed Apr. 11, 2023, 11 pages. cited by applicant
European Examination Report issued in related European Patent Application No. EP 21156457.0, dated Jul. 5, 2023. cited by applicant
Canadian Examination Report for related Canadian Application No. 3,108,475, dated Nov. 8, 2023, 5 pages. cited by applicant

---

Primary Examiner: Johnson; Sonji N

Attorney, Agent or Firm: KDW Firm PLLC

Background/Summary

CROSS-REFERENCE TO RELATED APPLICATIONS (1) This application is a continuation of U.S. patent application Ser. No. 17/088,117 filed Nov. 3, 2020, which is a continuation of U.S. patent application Ser. No. 16/863,952 filed Apr. 30, 2020, now U.S. Pat. No. 10,861,006, the complete disclosure of which is incorporated herein by reference in their entireties.

FIELD OF THE DISCLOSURE

(1) The present disclosure relates generally to user data control and, more specifically, to an exemplary system and method for active control of user access to data through the interaction of a short-range transceiver with a client device.

BACKGROUND

(2) A typical user has multiple different accounts with one or more entities. When a user creates an account, the user will generally provide a certain amount of personal, identifying information regarding the user, as well as information for account access such as a username and password. Each entity may have, for example, different user data retention policies, different use policies, and different user data sharing policies. The policies of using user-information may further change without any notification to the user. In addition, the possessor of the user information may also change through a merger or buy-out of one entity by another, many times without any notice to the user.

(3) Account access will often rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised, another person could have access to the user's account. In addition, the more entities or individuals that a user shares their personal information with, the greater the risk of the user's information being stolen by a breach at one of the entities. Further, a user may only desire to share certain pieces of personal information with an entity or individual for limited purposes or limited in time.

(4) Thus, it may be beneficial to provide exemplary systems and methods which allow users to control the use of user information to overcome at least some of the deficiencies described herein.

SUMMARY

(5) Aspects of the disclosed technology include systems and methods for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device. Data access control may be provided in the context of account information, including handling requests to link a first account with a second account, via the interaction of a short-range transceiver, such as a contactless card, with a client device such that disclosure of certain account identifier information, or account login information, need not be disclosed to individuals or entities requesting access to account data of another individual or entity.

(6) Embodiments of the present disclosure provide a data access control system, comprising: a database storing information for a plurality of accounts comprising, for a first account associated with a first account holder, a first account identifier and first account data, and, for a second account associated with a second account holder, a second account identifier; a server configured to communicate over a network with a plurality of client devices, including a first client device associated with the first account holder and a second client device associated with the second account holder; a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a token, wherein the contactless card is associated with the first account holder; a client application comprising instructions for execution on at least one of the first client device or the second client device, the client application configured to: when executed on the second client device: in response to a tap action between the contactless card and the second client device: receive the token from the contactless card, and transmit to the server the token and an

account link request to link the first account with the second account; and receive from the server an account link confirmation message including instructions for access to the first account data; and, when executed on the first client device: in response to a link approval request from the server to approve the account link request, transmit to the server a link approval message approving the account link request; and, a processor in data communication with the server and the database, the processor configured to: receive from the second client device the token and the account link request; identify the first account based on the token; transmit to the first client device the link approval request to approve the account link request; receive from the first client device the link approval message approving the account link request; and transmit to the second client device the account link confirmation message including instructions for access to the first account data.

(7) Embodiments of the present disclosure provide a method for controlling data access, comprising: establishing a database storing information for a plurality of accounts comprising, for a first account associated with a first account holder, a first account identifier, first account data and data control parameters, and, for a second account associated with a second account holder, a second account identifier; receiving from a client device of the second account holder, via a network, an account link request to link the first account with the second account, the account link request generated in response to a tap action between a contactless card and the second account holder client device, the account link request accompanied by a token stored on the contactless card, wherein the contactless card is associated with the first account holder; identifying the first account based on the token; transmitting to a client device of the first account holder, via the network, a link approval request to approve the account link request; receiving from the first account holder client device, via the network, a link approval message, the link approval message generated in response to an indication by the first account holder approving the account link request; and transmitting to the second account holder client device, via the network, an account link confirmation message, the account link confirmation message confirming approval of the account link request and providing instructions for access to the first account data.

(8) Embodiments of the present disclosure provide a method for controlling data access, comprising: establishing a database storing information for a plurality of accounts comprising, for a first account associated with a first account holder, a first account identifier, first account data and data control parameters, and, for a second account associated with a second account holder, a second account identifier; providing a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a token, wherein the communications interface is configured to support at least one of near field communication, Bluetooth, or Wi-Fi, and wherein the contactless card is associated with the first account holder; and providing a client application comprising instructions for execution on at least one of a first client device of the first account holder or a second client device of the second account holder, the client application configured to: when executed on the second client device: in response to a tap action between the contactless card and the second client device: receive the token from the contactless card, and transmit to the server the token and an account link request to link the first account with the second account; and receive from the server an account link confirmation message including instructions for access to the first account data, the data access provided according to the data control parameters; and, when executed on the first client device: determine a tap action between the contactless card and the first client device, the tap action in response to a link approval request to approve the account link request, the tap action indicating approval of the account link request; and transmit to the server a link approval message approving the account link request.

(9) Further features of the disclosed design, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments described below and illustrated in the accompanying drawings.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) FIG. **1**A is a diagram of a data access control system according to one or more example embodiments.

(2) FIG. **1**B is a diagram illustrating a sequence for providing data access control according to one or more example embodiments.

(3) FIG. **2** illustrates components of a client device used in a data access control system according to one or more example embodiments.

(4) FIG. **3** illustrates components of a short-range transceiver used in a data access control system according to one or more example embodiments.

(5) FIG. **4** is diagram illustrating interaction between a client device and a short-range transceiver used in a data access control system according to one or more example embodiments.

(6) FIG. **5** is diagram illustrating interaction between a client device and a short-range transceiver used in a data access control system according to one or more example embodiments.

(7) FIG. **6** is a flowchart illustrating a method of data access control according to one or more example embodiments.

(8) FIG. **7** is a flowchart illustrating a method of data access control according to one or more example embodiments.

(9) FIG. **8** is a flowchart illustrating a method of data access control according to one or more example embodiments.

DETAILED DESCRIPTION

(10) The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

(11) Exemplary embodiments of the disclosed systems and methods provide for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device. Data access control may be provided in the context of controlling access to account information. Requests to link a first account with a second account may be handled via the interaction of a short-range transceiver, such as a contactless card, with a client device such that disclosure of certain account identifier information, or account login information, need not be disclosed to individuals or entities requesting access to account data of another individual or entity. Benefits of the disclosed technology may include improved data security for account information, improved fraud prevention, and improved user experience.

(12) FIG. **1**A shows a diagram illustrating a data access control system **100** according to one or more example embodiments. As discussed further below, system **100** may include client device **101**, client device **103**, short-range transceiver **105**, server **110**, processor **120** and database **130**. Client device **101** and client device **103** may communicate with server **110** via network **115**. Although FIG. **1** illustrates certain components connected in certain ways, system **100** may include additional or multiple components connected in various ways.

(13) System **100** may include one or more client devices, such as client device **101** and/or client device **103**, which may each be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a thin client, a fat client, an Internet browser, or other

device. Each of client devices **101** and **103** also may be a mobile device; for example, a mobile device may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device. Additional features that may be included in a client device, such as client device **101** and/or client device **103**, are further described below with reference to FIG. **2**.

(14) System **100** may include one or more short-range transceivers, such as short-range transceiver **105**. Short-range transceiver **105** may be in wireless communication with a client device, such as client device **101** and/or client device **103**, within a short-range communications field such as, for example, near field communication (NFC). Short-range transceiver **105** may include, for example, a contactless card, a smart card, or may include a device with a varying form factor such as a fob, pendant or other device configured to communicate within a short-range communications field. In other embodiments, the short-range transceiver **105** may be the same or similar as the client devices **101**, **103**. Additional features that may be included in a short-range transceiver, such as such as short-range transceiver **105**, are further described below with reference to FIG. **3**.

(15) System **100** may include one or more servers **110**. In some example embodiments, server **110** may include one or more processors (such as, e.g., a microprocessor) which are coupled to memory. Server **110** may be configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Server **110** may be a dedicated server computer, such as bladed servers, or may be personal computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, or any processor-controlled device capable of supporting the system **100**.

(16) Server **110** may be configured for data communication (such as, e.g., via a connection) with one or more processors, such as processor **120**. In some example embodiments, server **110** may incorporate processor **120**. In some example embodiments, server **110** may be physically separate and/or remote from processor **120**. Processor **120** may be configured to serve as a back-end processor. Processor **120** may be configured for data communication (such as, e.g., via a connection) with database **130** and/or server **110**. Processor **120** may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., along with associated processing circuitry. Processor **120** may include, or be connected to, memory storing executable instructions and/or data. Processor **120** may communicate, send or receive messages, requests, notifications, data, etc. to/from other devices, such as client devices **101** and/or **103**, via server **110**.

(17) Server **110** may be configured for data communication (such as, e.g., via a connection) with one or more databases, such as database **130**. Database **130** may be a relational or non-relational database, or a combination of more than one database. In some example embodiments, server **110** may incorporate database **130**. In some example embodiments, database **130** may be physically separate and/or remote from server **110**, located in another server, on a cloud-based platform, or in any storage device that is in data communication with server **110**.

(18) Connections between server **110**, processor **120** and database **130** may be made via any communications line, link or network, or combination thereof, wired and/or wireless, suitable for communicating between these components. Such network may include network **115** and/or one or more networks of same or similar type as those described herein with reference to network **115**. In some example embodiments, connections between server **110**, processor **120** and database **130** may include a corporate LAN.

(19) Server **110** and/or database **130** may include user login credentials used to control access to user accounts. The login credentials may include, without limitation, user names, passwords, access codes, security questions, swipe patterns, image recognition, identification scans (e.g., driver's license scan and passport scan), device registrations, telephone numbers, email addresses, social media account access information, and biometric identification (e.g., voice recognition, fingerprint scans, retina scans, and facial scans).

(20) Database **130** may contain data relating to one or more accounts. Accounts may be maintained

by (or on behalf of) and/or relate to any one or more of a variety of entities, such as, for example (and without limitation) a bank, merchant, online retailer, service provider, merchandizer, manufacturer, social media provider, provider or promoter of sporting or entertainment events, or hotel chain. For example, database **130** may include, without limitation, account identification information (e.g., account number, account owner identification number, account owner name and contact information—any one or more of which may comprise an account identifier), account characteristics (e.g., type of account, funding and trading limitations, and restrictions on access and other activity), and may include data pertinent to the account, including financial (such as balance information, payment history, and transaction history), social and/or personal information. Data stored in database **130** may be stored in any suitable format, and may be encrypted and stored in a secure format to prevent unauthorized access. Any suitable algorithm/procedure may be used for data encryption and for authorized decryption.

(21) Server **110** may be configured to communicate with one or more client devices, such as such as client device **101** and/or client device **103**, via one or more networks, such as network **115**. Network **115** may include one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect client devices **101** and/or **103** to server **110**. For example, network **115** may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless local area network (LAN), a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

(22) In addition, network **115** may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, network **115** may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network **115** may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. Network **115** may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network **115** may translate to or from other protocols to one or more protocols of network devices. Although network **115** is depicted as a single network, it should be appreciated that according to one or more example embodiments, network **115** may comprise a plurality of interconnected networks, such as, for example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, a LAN, and/or home networks.

(23) In some example embodiments, server **110** may access records, including records in database **130**, to determine a method or methods for communicating with client device **101** and/or client device **103**. The communication method may include an actionable push notification with an application stored on client device **101** and/or client device **103**. Other communication methods may include a text message or an e-mail, or other messaging techniques appropriate in a network-based client/server configuration. Messages or requests by client devices **101** and/or **103** may be communicated to server **110** via an application on the client device, or may be sent by a text message or an e-mail, or other messaging techniques appropriate in a network-based client/server configuration. Communications originating with client device **101** or client device **103** may be sent to server **110** using the same communications method as communications originating with server **110**, or via a different communications method.

(24) FIG. **1**B shows a diagram illustrating a sequence for providing data access control according to one or more example embodiments, which may include a request to link two accounts, each account held by separate account holders. FIG. **1**B references similar components of example embodiment

system **100** as illustrated in FIG. **1**A. Client device **101** may be associated with a first account holder. The first account holder may have an associated first account, which may include a first account identifier and first account data. Client device **101** may include application **102**, which may include instructions for execution by client device **101**. Client device **101** may include features further described below with reference to FIG. **2**. Application **102** may be configured to provide a user interface for the first account holder when using client device **101**. Application **102** may be configured to communicate, via client device **101**, with other client devices, with short-range transceiver **105**, and with server **110**. Application **102** may be configured to receive requests and send messages as described herein with reference to client device **101**. Account information, including account identifiers and account data, may be stored in database **130**.

(25) Client device **103** may be associated with a second account holder. The second account holder may have an associated second account, which may include a second account identifier. Client device **103** may include application **104**, which may include instructions for execution by client device **103**. Client device **103** may include features further described below with reference to FIG. **2**. Application **104** may be configured to provide a user interface for the second account holder when using client device **103**. Application **104** may be configured to communicate, via client device **103**, with other client devices, with short-range transceiver **105**, and with server **110**. Application **104** may be configured to send requests and receive messages as described herein with reference to client device **103**.

(26) Short-range transceiver **105** may be associated with the first account holder. Short-range transceiver **105** may include, for example, a contactless card, and may include features further described below with reference to FIG. **3**. Short-range transceiver **105** may have memory storing an applet **106** and/or a token **107**, token **107** being associated with the first account holder.

(27) A token may be used to increase security through token authorization. Server **110** may send a validation request to client device **101** and/or **103**, receive responsive information from client device **101** and/or **103**, and if validated, send a validation token back to client device **101** and/or **103**. The validation token may be based on a pre-determined token, or may be a dynamic token based on an algorithm that can be secret and known only to server **110** and client device **101** and/or **103**; the algorithm may include live parameters independently verifiable by the participants, such as the temperature at a particular location or the time. The token may be used to verify the identity of the first account holder or the second account holder. The validation request and/or validation token may be based on token **107** stored on short-range transceiver **105**.

(28) In some example embodiments, application **104** may display an instruction on client device **103** prompting the second account holder to initiate a tap action between short-range transceiver **105** and client device **103**. As used herein, a tap action may include tapping short-range transceiver **105** against client device **103** (or vice-versa). For example, if short-range transceiver **105** is a contactless card and client device **103** is a mobile device, the tap action may include tapping the contactless card on a screen or other portion of client device **103**. However, a tap action is not limited to a physical tap by short-range transceiver **105** against client device **103**, and may include other gestures, such as, e.g., a wave or other movement of short-range transceiver **105** in the vicinity of client device **103** (or vice-versa).

(29) At label **150**, there may be a tap action between short-range transceiver **105** and client device **103**. The tap action may be in response to a prompt displayed on client device **103**.

(30) At label **152**, application **104** may communicate (via client device **103**) with short-range transceiver **105** (e.g., after short-range transceiver **105** is brought near client device **103**). Communication between application **104** and short-range transceiver **105** may involve short-range transceiver **105** (such as, e.g., a contactless card) being sufficiently close to a card reader (not shown) of the client device **103** to enable NFC data transfer between application **104** and short-range transceiver **105**, and may occur in conjunction with (or response to) a tap action between short-range transceiver **105** and client device **103** (such as, e.g., the tap action at label **150**). The communication may include exchange of data or commands to establish a communication session between

application **104** and short-range transceiver **105**. The exchange of data may include transfer or exchange of one or more keys, which may be preexisting keys or generated as session keys. In some example embodiments, the communication may occur upon entry of short-range transceiver **105** into a short-range communication field of client device **103** prior to a tap action between short-range transceiver **105** and client device **103**.

(31) At label **154**, short-range transceiver **105** may send token **107** associated with the first account holder to application **104**. Token **107** may include the first account identifier, which may be unique to a specific user account. In an example embodiment, token **107** may include an identifier unique to the first account holder, but not to a specific account; in which case if the first account holder has more than one account, the second account holder would need to select the account to be linked. In some example embodiments, token **107** may include a key associated with the first account holder. In some example embodiments, the sending of token **107** to application **104** may be in conjunction with (or response to) a tap action between short-range transceiver **105** and client device **103** (such as, e.g., the tap action at label **150**). In some example embodiments, the sending of token **107** to application **104** may occur upon entry of short-range transceiver **105** into a short-range communication field of client device **103** prior to a tap action between short-range transceiver **105** and client device **103**.

(32) At label **156**, application **104** may send token **107** to server **110**, along with an account link request to link the first account (associated with the first account holder) with the second account (associated with the second account holder). This may be carried out in response to a tap action between short-range transceiver **105** and client device **103** (such as, e.g., the tap action at label **150**).

(33) At label **158**, processor **120** may receive (e.g., via server **110**) the token and the account link request. Processor **120** may use the token to identify the first account associated with the first account holder. In some example embodiments, identifying the first account may be carried out by using the first account identifier in the token to look up account information in database **130**. In some example embodiments, at label **159**, if the token includes the key associated with the first account holder, processor **120** may use the key in the token to authenticate the first account holder as the first account holder associated with short-range transceiver **105**.

(34) At label **160**, processor **120** may send (e.g., via server **110**) a link approval request to client device **101**, requesting that the first account holder approve the account link request, by the second account holder, to link the first account with the second account. The link approval request may include, for example, the name of the second account holder, and any information or instructions required by the first account holder to consider the request. The link approval request may include a notice that the first account holder may approve or deny the request. The link approval request may be sent as a push notification to application **102** (via client device **101**). In some example embodiments, application **102** may display an instruction on client device **101** prompting the first account holder to initiate a tap action between short-range transceiver **105** and client device **101**.

(35) At label **162**, there may be a tap action between short-range transceiver **105** and client device **101**. The tap action may be responsive to the link approval request (and/or to a prompt displayed on client device **101**), and may indicate approval by the first account holder of the account link request.

(36) At label **164**, application **102** may send a link approval message to the server, indicating approval by the first account holder of the account link request. This may be carried out in response to a tap action between short-range transceiver **105** and client device **101** (such as, e.g., the tap action at label **162**). In an example embodiment, application **102** may instead send a denial message (not shown) to the server, indicating denial by the first account holder of the account link request.

(37) At label **166**, processor **120** may send (e.g., via server **110**) a link confirmation message to client device **103**, confirming approval of the request to link the first account with the second account. The link confirmation message may be sent as a push notification to application **104** (via client device **103**). In some example embodiments, information for the first account and/or the second account in database **130** may be updated with the permission granted by the first account holder to link the first and second accounts.

(38) In an example embodiment, processor **120** may instead send a denial notification (not shown) to client device **103**, indicating denial by the first account holder of the account link request.
(39) At label **168**, processor **120** may send (e.g., via server **110**) to client device **103** instructions for obtaining access to first account data in the first account. The instructions for access to the first account data may be included with the link confirmation message (at label **166**), or may be sent as part of a separate communication, including a push notification to application **104**.
(40) Processor **120** may retrieve the requested first account data from database **130** and transmit the data to client device **103**. Processor **120** may encrypt the requested first account data, prior to transmission to client device **103**, using any suitable encryption method, such as Triple DES, RSA public-key private-key encryption, asymmetric encryption, Blowfish encryption, Twofish encryption, Advanced Encryption Standard (AES), quantum key distribution, Honey Encryption, etc. In some embodiments, the requested first account data may already be encrypted as stored in database **130** prior to retrieval by processor **120**.
(41) Upon receipt of the requested first account data, client device **103** may decrypt the information, if the information was encrypted prior to transmission by processor **120**. Client device **103** may receive a decryption key separate from the first communication of encrypted first account data. The encryption may allow for control of access to first account data according to data control parameters. For example, the first account data may be encrypted in a manner that requires a new key to be requested by client device **103** from processor **120** each time client device **103** desires to gain access to the first account data, such that the data would need to be decrypted for each access by client device **103**; this procedure would permit processor **120** to keep track of and ensure that the first account data is not accessed in a manner inconsistent with data control parameters.
(42) In an example embodiment, the second account holder may login to the second account and, via data sharing on the backend, obtain access to first account data, in accordance with any data control parameters.
(43) Application **104** executing on client device **103** may through the use of application programming interfaces (APIs), perform the steps of sending and receiving messages and requests with server **110**/processor **120**. Application **104** may be configured to receive, decrypt, and access the requested first account data. Through interaction with application **104**, processor **120** may monitor access of the requested first account data by client device **103**, including in accordance with data control parameters. For example, processor **120** may through interaction with application **104** determine the number of times client device **103** has obtained access to the requested first account data, or the period(s) of time such access occurred. In some embodiments, application **104** may be permitted to store the requested first account data on a time-limited, or limited number of uses, basis.
(44) In an example embodiment, processor **120** may be configured to determine whether the first account is eligible to be linked with the second account. Eligibility for account linking may be based on, for example, the type of accounts involved (e.g., business accounts), or identity of the account holders (e.g., family members or members of the same business entity). Eligibility may also be based on whether the first account holder has previously approved or revoked approval of account linking, or whether requested access would violate data control parameters (discussed further below). Eligibility for account linking may, e.g., be indicated in a flag stored in database **130** or in memory of short-range transceiver **105**.
(45) In one or more example embodiments, access by the second account holder to first account data may be limited in accordance with data control parameters. In an example embodiment, data control parameters may be stored in database **130** with the first account information. Application **102** may provide an interface for the first account holder to select the data control parameters stored in database **130**. The selected data control parameters may be stored in database **130** and may be applied to limit access by the second account holder to first account data. Application **102** may also transmit the selected data control parameters to short-range transceiver **105**. In an example embodiment, data control parameters may be stored in memory of short-range transceiver **105**. Data control parameters stored in memory of short-range transceiver **105** may be sent to application **104**

and used by application **104** to limit access by the second account holder to first account data. Applet **106** may be configured to receive the data control parameters and store the data control parameters in memory of short-range transceiver **105**. Applet **106** may be further configured to transmit the data control parameters to client device **103**. In some example embodiments, the first account holder may select data control parameters at the time of approving the request to link accounts, and application **102** may transmit the selected data control parameters to server **110** along with the link approval message. The selected data control parameters may be stored in database **130** and may be applied to limit access by the second account holder to first account data.

(46) In one or more example embodiments, data control parameters may be used to limit access by the second account holder to first account data in one or more ways. For example, the data control parameters may permit access only for a specific or limited period of time. As another example, the data control parameters may permit access to a single use by the second account holder. As another example, the data control parameters may permit access for an unlimited period of time, unless the first account holder revokes the approval of the request to link the first account with the second account. As another example, the data control parameters may permit access only to portions of first account data corresponding to a predefined category. As another example, the data control parameters may provide different access permissions based on the identity of the second account holder. As another example, the data control parameters may permit access only when short-range transceiver **105** is detected within range of a short-range communication field of client device **103**. In some example embodiments, each time the second account holder attempts to access first account data after account linking approval is obtained, processor **120** may check to determine whether such access is permitted based on data control parameters and any revocation by the first account holder.

(47) In an example embodiment, application **104** may be launched in response to a tap action between short-range transceiver **105** and client device **103**. In an example embodiment, application **102** may be launched in response to a tap action between short-range transceiver **105** and client device **101**.

(48) FIG. **2** illustrates components of a client device **200** used in a data access control system according to one or more example embodiments. In one or more example embodiments, client device **200** may be one or more of client devices **101** and/or **103**, described above with reference to FIG. **1**A and FIG. **1**B. Client device **200** may include one or more applications **201**, one or more processors **202**, a short-range communications interface **203**, and a network interface **204**. Application **201** may include a software application or executable program code to be executed on processor **202** and configured to carry out features described herein for any of the client devices, such as client devices **101** and/or **103**, and/or any of the features described herein with reference to application **102**. Application **201** may be configured, for example, to transmit and/or receive data with other devices via client device **200**, such as via short-range communications interface **203** and/or network interface **204**. For example, application **201** may be configured to initiate one or more requests, such as near field data exchange requests to a short-range transceiver (such as a contactless card). Application **201** may also be configured to provide a user interface via a display (not shown) for a user of the client device. Application **201** may be stored in memory in client device **200**; the memory may include a read-only memory, write-once read-multiple memory and/or read/write memory, e.g., RAM, ROM, and EEPROM.

(49) Processor **202** may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., and may include associated processing circuitry. Processor **202** may include, or be connected to, memory storing executable instructions and/or data, as may be necessary or appropriate to control, operate or interface with the other features of client device **200**, including application **201**. Processor **202** (including any associated processing circuitry) may contain additional components including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

(50) Short-range communications interface **203** may support communication via a short-range

wireless communication field, such as NFC, RFID, or Bluetooth. Short-range communications interface **203** may include a reader, such as a mobile device NFC reader. Short-range communications interface **203** may be incorporated into network interface **204**, or may be provided as a separate interface.

(51) Network interface **204** may include wired or wireless data communication capability. These capabilities may support data communication with a wired or wireless communication network, including the Internet, a cellular network, a wide area network, a local area network, a wireless personal area network, a wide body area network, any other wired or wireless network for transmitting and receiving a data signal, or any combination thereof. Such network may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a local area network, a wireless personal area network, a wide body area network or a global network such as the Internet.

(52) Client device **200** may also include a display (not shown). Such display may be any type of device for presenting visual information such as a computer monitor, a flat panel display, or a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays.

(53) Client device **200** may also include one or more device inputs (not shown). Such inputs may include any device for entering information into the client device that is available and supported by the client device **300**, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder, or camcorder. The device inputs may be used to enter information and interact with the client device **200** and, by extension, with the systems described herein.

(54) FIG. **3** illustrates components of a short-range transceiver **300** used in a data access control system according to one or more example embodiments. In one or more example embodiments, short-range transceiver **300** may be one or more of short-range transceiver **105**, described above with reference to FIG. **1**A and FIG. **1**B. Short-range transceiver **300** may include, for example, a contactless card, or may include a device with a varying form factor such as a fob, pendant or other device configured to communicate within a short-range communications field. Short-range transceiver **300** may include a processor **301**, memory **302**, and short-range communications interface **305**.

(55) Processor **301** may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., and may include associated processing circuitry. Processor **301** may include, or be connected to, memory storing executable instructions and/or data, as may be necessary or appropriate to control, operate or interface with the other features of short-range transceiver **300**, including applet **303**. Processor **301** (including any associated processing circuitry) may contain additional components including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

(56) Memory **302** may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM. Memory **302** may be configured to store one or more applets **303**, and one or more tokens **304**. Applet **303** may comprise one or more software applications configured to execute on processor **301**, such as a Java Card applet that may be executable on a contactless card. However, it is understood that applet **303** is not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. Applet **303** may be configured to respond to one or more requests, such as near field data exchange requests from a client device, including requests from a device having a reader such as a mobile device NFC reader. Applet **303** may be configured to read (or write) data, including token **304**, from (or to) memory **302** and provide the data, including token **304**, in response to a request.

(57) Token **304** may include a unique alphanumeric identifier assigned to a user of the short-range transceiver **300**, and the identifier may distinguish the user of the short-range transceiver **300** from

other users of other short-range transceivers (such as other contactless card users). In some example embodiments, token **304** may identify both a customer and an account assigned to that customer and may further identify the short-range transceiver (such as a contactless card) associated with the customer's account. In some example embodiments, token **304** may include a key unique to the user or customer with which the short-range transceiver is associated.

(58) Short-range communications interface **305** may support communication via a short-range wireless communication field, such as NFC, RFID, or Bluetooth. Short-range transceiver **300** may also include one or more antennas (not shown) connected to short-range communications interface **305** to provide connectivity with a short-range wireless communications field.

(59) FIG. **4** is diagram illustrating the interaction **400** between a client device **401** and a short-range transceiver **420** used in a data access control system according to one or more example embodiments, including embodiments described above with reference to FIGS. **1**A-**1**B. Client device **401** may be client device **103** described above with reference to FIG. **1**A and FIG. **1**B. Client device **401** may be associated with the second account holder. User interface **402** may be generated by application **104** described above with reference to FIG. **1**B. Short-range transceiver **420** may be short-range transceiver **105** described above with reference to FIG. **1**A and FIG. **1**B. Upon entry of short-range transceiver **420** into a short-range communication field of client device **401** (such as, e.g., via a tap action), client device **401** may communicate with short-range transceiver **420**. Client device **401** may send data or commands to short-range transceiver **420** via transmit signal **431**, and may receive data from short-range transceiver **420**, including token **422**, via receive signal **432**. Communication between client device **401** and short-range transceiver **420** may proceed as described above with reference to FIG. **1**B (e.g., client device **101** or **103** and short-range transceiver **105**).

(60) User interface **402** may present on client device **401** a screen display for an account link request **410**, which may include field **411** and field **412**. If necessary, the second account holder may enter a username in field **411** and password in field **412**. The screen display may include an instruction **414** prompting the second account holder to tap short-range transceiver **420** (in the example shown, short-range transceiver **420** may be a contactless card) to initiate an account link request to link the first account with the second account. Instruction **414** may be a push notification from server **110** (shown in FIGS. **1**A and **1**B). Client device **401** may transmit an account link request to server **110** (shown in FIG. **1**A and FIG. **1**B) in response to a tap action.

(61) FIG. **5** is diagram illustrating the interaction **500** between a client device **501** and a short-range transceiver **520** used in a data access control system according to one or more example embodiments, including embodiments described above with reference to FIGS. **1**A-**1**B. Client device **501** may be client device **101** described above with reference to FIG. **1**A and FIG. **1**B. Client device **501** may be associated with the first account holder. User interface **502** may be generated by application **102** described above with reference to FIG. **1**B. Short-range transceiver **520** may be short-range transceiver **105** described above with reference to FIG. **1**A and FIG. **1**B. Upon entry of short-range transceiver **520** into a short-range communication field of client device **501** (such as, e.g., via a tap action), client device **501** may communicate with short-range transceiver **520**. Client device **501** may send data or commands to short-range transceiver **520** via transmit signal **531**, and may receive data from short-range transceiver **520**, including token **522**, via receive signal **532**. Communication between client device **501** and short-range transceiver **520** may proceed as described above with reference to FIG. **1**B (e.g., client device **101** or **103** and short-range transceiver **105**).

(62) User interface **502** may present on client device **501** a screen display for an account link request **510**, which may include field **511** and field **512**. If necessary, the first account holder may enter a username in field **511** and password in field **512**. The screen display may include an instruction **514** notifying the first account holder that the second account holder (named 2_Acc_Hldr as shown in the example) has requested to link the first account with the second account, and prompting the first account holder to tap short-range transceiver **520** (in the example shown, short-range transceiver **520**

may be a contactless card) to approve the account link request to link the first account with the second account. Instruction **514** may result from a push notification from server **110** (shown in FIG. **1**A and FIG. **1**B). Client device **501** may transmit an account link approval message to server **110** in response to a tap action. In some example embodiments, user interface **502** may provide the first account holder the option to select data control parameters at the time of approving the request to link accounts. Client device **501** may transmit the selected data control parameters to server **110** along with the link approval message; the selected data control parameters may be stored and may be applied to limit access by the second account holder to first account data, as discussed above.

(63) FIG. **6** is a flowchart illustrating a method of data access control **600** according to one or more example embodiments, with reference to components and features described above including but not limited to the figures and associated description. Data access control method **600** may be carried out by application **104** executing on client device **103** associated with the second account holder. Short-range transceiver **105** is associated with the first account holder.

(64) At block **610**, application **104** may cause client device **103** to display an account link request screen (such as shown in, and described above with reference to, FIG. **4**). The account link request screen may include an instruction to tap short-range transceiver **105** with/against client device **103** to initiate the account link request. As described above with reference to FIG. **4**, short-range transceiver **420** (and, hence, short-range transceiver **105**) may be a contactless card.

(65) At block **620**, a tap action may be detected between short-range transceiver **105** and client device **103**.

(66) At block **630**, token **107** may be received from short-range transceiver **105**. Receiving token **107** may be in response to the tap action of block **620**. Token **107** may include the first account identifier. In some example embodiments, token **107** may include a key associated with the first account holder.

(67) At block **640**, token **107** may be transmitted to server **110** along with an account link request to link the first account with the second account. Transmission of token **107** and the account link request to server **110** may be in response to the tap action of block **620**.

(68) At block **650**, an account link confirmation message may be received from server **110** along with instructions for access to first account data. As discussed above, the instructions may be part of the account link confirmation message, or part of a separate message.

(69) At block **660**, the second account holder may access the first account data according to the received instructions. As discussed above, in some example embodiments access to first account data may be only provided in accordance with data control parameters. In some example embodiments, the data control parameters are stored in database **130** with the first account information, and data access is limited by processor **120**. In some example embodiments, the data control parameters are stored in memory of short-range transceiver **105** and are received by application **104** from short-range transceiver **105**. In some example embodiments, the first account data may be encrypted prior to receiving instructions for access to the first account data. Decryption of the encrypted first account data may be performed using the key associated with the first account holder.

(70) FIG. **7** is a flowchart illustrating a method of data access control **700** according to one or more example embodiments, with reference to components and features described above including but not limited to the figures and associated description. Data access control method **700** may be carried out by application **102** executing on client device **101** associated with the first account holder. Short-range transceiver **105** is associated with the first account holder.

(71) At block **710**, a link approval request may be received from server **110** seeking approval to link the first account with the second account.

(72) At block **720**, application **102** may cause client device **101** to display an account link request screen (such as shown in, and described above with reference to, FIG. **5**). The account link request screen may include an instruction to tap short-range transceiver **105** with/against client device **101** to approve the account link request. As described above with reference to FIG. **5**, short-range transceiver **520** (and, hence, short-range transceiver **105**) may be a contactless card.

(73) At block **730**, a tap action may be detected between short-range transceiver **105** and client device **101** indicating approval of the link approval request. The tap action may be responsive to the link approval request. In an example embodiment, approval may be indicated by other methods (such as, e.g. selecting a button).
(74) At block **740**, token **107** may be received from short-range transceiver **105**. Token **107** may include the first account identifier. In some example embodiments, token **107** may include a key associated with the first account holder.
(75) At block **750**, a link approval message may be sent to server **110** indicating approval of the request to link the first account with the second account.
(76) FIG. **8** is a flowchart illustrating a method of data access control **800** according to one or more example embodiments, with reference to components and features described above including but not limited to the figures and associated description. Data access control method **800** may be carried out by processor **120** in communication with, via server **110**, client device **101** associated with the first account holder and/or client device **103** associated with the second account holder.
(77) At block **810** an account link request may be received, along with token **107**, from client device **103** associated with the second account holder, requesting to link the first account with the second account. Token **107** may include the first account identifier. In some example embodiments, token **107** may include a key associated with the first account holder.
(78) At block **820**, the sender of the account link request may be identified as the second account holder.
(79) At block **830**, the first account may be identified based on received token **107**. In some example embodiments, when token **107** includes the key associated with the first account holder, the key associated with the first account holder may be used to authenticate the first account holder.
(80) At block **840**, the processor may confirm that the first account is eligible to be linked with the second account. As discussed above with reference to FIG. **1**B, eligibility for account linking may be based on, for example, the type of accounts involved (e.g., business accounts), or identity of the account holders (e.g., family members or members of the same business entity).
(81) At block **850**, a link approval request may be sent to client device **101** associated with the first account holder seeking approval to link the first account with the second account.
(82) At block **860**, a link approval message may be received from client device **101**, indicating approval of the request to link the first account with the second account.
(83) At block **870**, an account link confirmation message may be sent to client device **103** associated with the second account holder, along with instructions for access to first account data. As discussed above, the instructions may be part of the account link confirmation message, or part of a separate message. In some example embodiments, access to first account data may be limited in accordance with data control parameters. In some example embodiments, processor **120** may encrypt the first account data prior to providing client device **103** instructions for access to the first account data. Encryption of the first account data may be performed using the key associated with the first account holder.
(84) The description of embodiments in this disclosure provides non-limiting representative examples referencing figures and numerals to particularly describe features and teachings of different aspects of the disclosure. The embodiments described should be recognized as capable of implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the disclosure. The description of embodiments should facilitate understanding of the disclosure to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the disclosure.
(85) Throughout the specification and the claims, the following terms take at least the meanings explicitly associated herein, unless the context clearly dictates otherwise. The term “or” is intended

to mean an inclusive “or.” Further, the terms “a,” “an,” and “the” are intended to mean one or more unless specified otherwise or clear from the context to be directed to a singular form.
(86) In this description, numerous specific details have been set forth. It is to be understood, however, that implementations of the disclosed technology may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description. References to “some examples,” “other examples,” “one example,” “an example,” “various examples,” “one embodiment,” “an embodiment,” “some embodiments,” “example embodiment,” “various embodiments,” “one implementation,” “an implementation,” “example implementation,” “various implementations,” “some implementations,” etc., indicate that the implementation(s) of the disclosed technology so described may include a particular feature, structure, or characteristic, but not every implementation necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrases “in one example,” “in one embodiment,” or “in one implementation” does not necessarily refer to the same example, embodiment, or implementation, although it may.
(87) As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.
(88) While certain implementations of the disclosed technology have been described in connection with what is presently considered to be the most practical and various implementations, it is to be understood that the disclosed technology is not to be limited to the disclosed implementations, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.
(89) This written description uses examples to disclose certain implementations of the disclosed technology, including the best mode, and also to enable any person skilled in the art to practice certain implementations of the disclosed technology, including making and using any devices or systems and performing any incorporated methods. The patentable scope of certain implementations of the disclosed technology is defined in the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal language of the claims.

Claims

1. A method for controlling data access, comprising: receiving, by a server via a network, an account link request to link a first account associated with a first account holder with a second account associated with a second account holder, the account link request accompanied by a token; identifying, by the server, the first account based on the token; determining whether the first account is eligible for linking to the second account based on at least one selected from the group of an identity of the first account holder and an identity of the second account holder and based on at least one selected from the group of an account type of the first account and an account type of the second account, wherein the identity of the first account holder and the identity of the second account holder are at least one selected from the group of family members and members of the same business entity: transmitting, by the server via the network, a link approval request to approve the account link request; receiving, by the server via the network, a link approval message generated in response to an indication by the first account holder approving the account link request and one or more data control parameters for limiting access by the second account holder to the first account; and transmitting, by the server via the network, an account link confirmation message and the one or more data control parameters, the account link confirmation message confirming approval of the

account link request.
2. The method of claim 1, wherein the token comprises a key associated with the first account holder.
3. The method of claim 2, wherein identifying the first account based on the token comprises identifying the first account based on the key.
4. The method of claim 1, wherein the token comprise a first identifier associated with the first account holder.
5. The method of claim 1, wherein: the server is in data communication with a database storing information for a plurality of accounts, and the plurality of accounts includes at least the first account and the second account.
6. The method of claim 5, wherein: for the first account, the database stores information comprising a first account identifier and first account data, and for the second account, the database stores information comprising a second account identifier.
7. The method of claim 1, wherein the account type of the first account and the account type of the second account are corporate accounts.
8. The method of claim 1, wherein: the account link confirmation message includes instructions for access to first account data associate with the first account holder, and access to the first account data is limited by at least one of the one or more data control parameters.
9. The method of claim 8, wherein the data control parameters permit access to the first account data for a limited period of time.
10. A server, comprising: a processor; and a memory, wherein the processor: receives, via a network, an account link request and a token, wherein the account link request is to link a first account associated with a first account holder with a second account associated with a second account holder, identifies the first account based on the token, determines whether the first account is eligible for linking to the second account based on at least one selected from the group of an identity of the first account holder and an identity of the second account holder and based on at least one selected from the group of an account type of the first account and an account type of the second account, wherein the identity of the first account holder and the identity of the second account holder are at least one selected from the group of family members and members of the same business entity, transmits, via the network, a link approval request to approve the account link request, receives, via the network, a link approval message generated in response to an indication by the first account holder approving the account link request and one or more data control parameters for limiting access by the second account holder to the first account, and transmits, via the network, an account link confirmation message and the one or more data control parameters, the account link confirmation message confirming approval of the account link request.
11. The server of claim 10, wherein: the processor is in data communication with a database, and the database stores information for a plurality of accounts, the information including: for the first account associated with the first account holder, a first account identifier and first account data, and, for the second account associated with a second account holder, a second account identifier.
12. The server of claim 11, wherein the processor: retrieves at least a portion of the first account data from the database, encrypts the at least a portion of the first account data to generate encrypted first account data, and following transmission of the account link confirmation message, transmits the encrypted first account data.
13. The server of claim 12, wherein the processor transmits, in a separate communication from the encrypted first account data, a decryption key.
14. The server of claim 13, wherein the decryption key is a key associated with the first account holder.
15. A system for data access control, comprising: a short-range transceiver comprising a processor and a memory, wherein: the short-range transceiver is associated with a first account holder, and the memory of the short-range transceiver contains a token; and a server comprising a processor and a memory, wherein the server is in data communication with a database storing information for a

plurality of accounts, the information including, for a first account associated with the first account holder, a first account identifier, first account data, and, for a second account associated with a second account holder, a second account identifier, wherein the short-range transceiver transmits an account link request to link the first account with the second account and the token to the server, and wherein, after receipt of the account link request, the server: identifies the first account based on the token, and transmits a link approval request to approve the account link request, receives a link approval message generated in response to an indication by the first account holder approving the account link request and one or more data control parameters for limiting access by the second account holder to the first account, and transmits an account link confirmation message and the one or more data control parameters, the account link confirmation message confirming approval of the account link request.

16. The system of claim 15, wherein the server transmits instructions for access to the first account data.

17. The system of claim 16, wherein access to the first account data is limited by at least one of the one or more data control parameters selected by the first account holder.

18. The system of claim 15, wherein the token comprises a key associated with the first account holder.

19. The system of claim 18, wherein identifying the first account based on the token comprises identifying the first account based on the key.

20. The system of claim 18, wherein the key comprises a session key generated by the short-range transceiver.