US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12389217
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Raleigh; Gregory G.

Device assisted services install

Abstract

Device assisted services (DAS) install techniques are provided in accordance with some embodiments. In some embodiments, DAS install techniques for providing service processors for mobile devices are provided. In some embodiments, DAS install techniques for downloading/installing new and/or updated service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing verified service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing secured service processors for mobile devices are provided. In some embodiments, DAS install techniques include determining if a communications device in communication with a wireless network includes a service processor for assisting control of the communications device use of a service on the wireless network, in which the service processor includes a service profile that includes a plurality of service policy settings, and in which the service profile is associated with a service plan that provides for access to the service; and verifying the service processor. In some embodiments, DAS install techniques include providing a generic first version service processor for downloading and installing a second version service processor.

Inventors: **Raleigh; Gregory G. (Incline Village, NV)**

Applicant: **Headwater Research LLC** (Tyler, TX)

Family ID: **42398597**

Assignee: **Headwater Research LLC (Tyler, TX)**

Appl. No.: **17/742190**

Filed: **May 11, 2022**

Prior Publication Data

Document Identifier	Publication Date
US 20220272523 A1	Aug. 25, 2022

Related U.S. Application Data

continuation parent-doc US 16804983 20200228 US 11337059 child-doc US 17742190
continuation parent-doc US 16118374 20180830 US 10582375 20200303 child-doc US 16804983
continuation parent-doc US 15210619 20160714 US 10070305 child-doc US 16118374
continuation parent-doc US 14158206 20140117 ABANDONED child-doc US 15210619
continuation parent-doc US 12694455 20100127 US 8402111 20130319 child-doc US 13674808
continuation-in-part parent-doc US 12380780 20090302 US 8839388 20140916 child-doc US 12694455
division parent-doc US 13674808 20121112 US 8634821 20140121 child-doc US 14158206
us-provisional-application US 61264120 20091124
us-provisional-application US 61207739 20090213
us-provisional-application US 61207393 20090210
us-provisional-application US 61206944 20090204
us-provisional-application US 61206354 20090128

Publication Classification

Int. Cl.: **H04W8/22** (20090101); **H04L41/0806** (20220101); **H04L41/082** (20220101); **H04L67/00** (20220101); **H04M15/00** (20240101); **H04W4/24** (20240101); **H04W8/18** (20090101); **H04W28/18** (20090101)

U.S. Cl.:

CPC **H04W8/22** (20130101); **H04L41/0806** (20130101); **H04L41/082** (20130101); **H04L67/34** (20130101); **H04M15/61** (20130101); **H04M15/8094** (20130101); **H04W4/24** (20130101); **H04W8/183** (20130101); **H04W28/18** (20130101);

Field of Classification Search

CPC: H04W (8/22); H04W (4/24); H04W (8/183); H04W (28/18); H04L (41/0806); H04L (41/082); H04L (67/34); H04M (15/61)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
5131020	12/1991	Liebesny et al.	N/A	N/A
5283904	12/1993	Carson et al.	N/A	N/A
5325532	12/1993	Crosswy et al.	N/A	N/A
5572528	12/1995	Shuen	N/A	N/A
5577100	12/1995	McGregor et al.	N/A	N/A
5594777	12/1996	Makkonen et al.	N/A	N/A
5617539	12/1996	Ludwig et al.	N/A	N/A
5630159	12/1996	Zancho	N/A	N/A
5633484	12/1996	Zancho et al.	N/A	N/A
5633868	12/1996	Baldwin et al.	N/A	N/A
5754953	12/1997	Briancon et al.	N/A	N/A
5764693	12/1997	Taylor et al.	N/A	N/A
5774532	12/1997	Gottlieb et al.	N/A	N/A
5794142	12/1997	Vanttila et al.	N/A	N/A
5814798	12/1997	Zancho	N/A	N/A
5889477	12/1998	Fastenrath	N/A	N/A
5892900	12/1998	Ginter et al.	N/A	N/A
5903845	12/1998	Buhrmann et al.	N/A	N/A
5915008	12/1998	Dulman	N/A	N/A
5915226	12/1998	Martineau	N/A	N/A
5933778	12/1998	Buhrmann et al.	N/A	N/A
5940472	12/1998	Newman et al.	N/A	N/A
5974439	12/1998	Bollella	N/A	N/A
5983270	12/1998	Abraham et al.	N/A	N/A
6035281	12/1999	Crosskey et al.	N/A	N/A
6038452	12/1999	Strawczynski et al.	N/A	N/A
6038540	12/1999	Krist et al.	N/A	N/A
6047268	12/1999	Bartoli et al.	N/A	N/A
6058434	12/1999	Wilt et al.	N/A	N/A
6061571	12/1999	Tamura	N/A	N/A
6064878	12/1999	Denker et al.	N/A	N/A
6078953	12/1999	Vaid et al.	N/A	N/A
6081591	12/1999	Skoog	N/A	N/A
6098878	12/1999	Dent et al.	N/A	N/A
6104700	12/1999	Haddock et al.	N/A	N/A
6115823	12/1999	Velasco et al.	N/A	N/A
6119933	12/1999	Wong et al.	N/A	N/A
6125391	12/1999	Meltzer et al.	N/A	N/A
6141565	12/1999	Feuerstein et al.	N/A	N/A
6141686	12/1999	Jackowski et al.	N/A	N/A
6148336	12/1999	Thomas et al.	N/A	N/A
6154738	12/1999	Call	N/A	N/A
6157636	12/1999	Voit et al.	N/A	N/A
6185576	12/2000	Mcintosh	N/A	N/A
6198915	12/2000	McGregor et al.	N/A	N/A
6219786	12/2000	Cunningham et al.	N/A	N/A
6226277	12/2000	Chuah	N/A	N/A
6246870	12/2000	Dent et al.	N/A	N/A
6263055	12/2000	Garland et al.	N/A	N/A
6292828	12/2000	Williams	N/A	N/A
6317584	12/2000	Abu-Amara et al.	N/A	N/A
6370139	12/2001	Redmond	N/A	N/A
6381316	12/2001	Joyce et al.	N/A	N/A
6393014	12/2001	Daly et al.	N/A	N/A
6397259	12/2001	Lincke et al.	N/A	N/A
6401113	12/2001	Lazaridis et al.	N/A	N/A
6418147	12/2001	Wiedeman	N/A	N/A
6421722	12/2001	Bauer et al.	N/A	N/A
6438575	12/2001	Khan et al.	N/A	N/A
6445777	12/2001	Clark	N/A	N/A
6449479	12/2001	Sanchez	N/A	N/A
6466984	12/2001	Naveh et al.	N/A	N/A
6470182	12/2001	Nelson	N/A	N/A
6477670	12/2001	Ahmadvand	N/A	N/A
6502131	12/2001	Vaid et al.	N/A	N/A
6505114	12/2002	Luciani	N/A	N/A
6510152	12/2002	Gerszberg et al.	N/A	N/A
6522629	12/2002	Anderson, Sr.	N/A	N/A
6532235	12/2002	Benson et al.	N/A	N/A
6532579	12/2002	Sato et al.	N/A	N/A

6535855	12/2002	Cahill et al.	N/A	N/A
6535949	12/2002	Parker	N/A	N/A
6539082	12/2002	Lowe et al.	N/A	N/A
6542500	12/2002	Gerszberg et al.	N/A	N/A
6542992	12/2002	Peirce et al.	N/A	N/A
6546016	12/2002	Gerszberg et al.	N/A	N/A
6556823	12/2002	Clapton et al.	N/A	N/A
6563806	12/2002	Yano et al.	N/A	N/A
6570974	12/2002	Gerszberg et al.	N/A	N/A
6574321	12/2002	Cox et al.	N/A	N/A
6574465	12/2002	Marsh et al.	N/A	N/A
6578076	12/2002	Putzolu	N/A	N/A
6581092	12/2002	Motoyama	N/A	N/A
6591098	12/2002	Shieh et al.	N/A	N/A
6598034	12/2002	Kloth	N/A	N/A
6601040	12/2002	Kolls	N/A	N/A
6603969	12/2002	Vuoristo et al.	N/A	N/A
6603975	12/2002	Inouchi et al.	N/A	N/A
6606744	12/2002	Mikurak	N/A	N/A
6615034	12/2002	Alloune et al.	N/A	N/A
6628934	12/2002	Rosenberg et al.	N/A	N/A
6631122	12/2002	Arunachalam et al.	N/A	N/A
6636721	12/2002	Threadgill et al.	N/A	N/A
6639975	12/2002	O'Neal et al.	N/A	N/A
6640097	12/2002	Corrigan et al.	N/A	N/A
6640334	12/2002	Rasmussen	N/A	N/A
6650887	12/2002	McGregor et al.	N/A	N/A
6651101	12/2002	Gai et al.	N/A	N/A
6654786	12/2002	Fox et al.	N/A	N/A
6654814	12/2002	Britton et al.	N/A	N/A
6658254	12/2002	Purdy et al.	N/A	N/A
6662014	12/2002	Walsh	N/A	N/A
6678516	12/2003	Nordman et al.	N/A	N/A
6683853	12/2003	Kannas et al.	N/A	N/A
6684244	12/2003	Goldman et al.	N/A	N/A
6690918	12/2003	Evans et al.	N/A	N/A
6694362	12/2003	Secor et al.	N/A	N/A
6697821	12/2003	Ziff et al.	N/A	N/A
6725031	12/2003	Watler et al.	N/A	N/A
6725256	12/2003	Albal et al.	N/A	N/A
6732176	12/2003	Stewart et al.	N/A	N/A
6735206	12/2003	Oki et al.	N/A	N/A
6748195	12/2003	Phillips	N/A	N/A
6748437	12/2003	Mankude et al.	N/A	N/A
6751296	12/2003	Albal et al.	N/A	N/A
6754470	12/2003	Hendrickson et al.	N/A	N/A
6757717	12/2003	Goldstein	N/A	N/A
6760417	12/2003	Wallenius	N/A	N/A
6763000	12/2003	Walsh	N/A	N/A
6763226	12/2003	McZeal, Jr.	N/A	N/A
6765864	12/2003	Natarajan et al.	N/A	N/A
6765925	12/2003	Sawyer et al.	N/A	N/A
6782412	12/2003	Brophy et al.	N/A	N/A
6785889	12/2003	Williams	N/A	N/A
6792461	12/2003	Hericourt	N/A	N/A
6829596	12/2003	Frazee	N/A	N/A
6829696	12/2003	Balmer et al.	N/A	N/A
6839340	12/2004	Voit et al.	N/A	N/A
6842628	12/2004	Arnold et al.	N/A	N/A
6873988	12/2004	Herrmann et al.	N/A	N/A
6876653	12/2004	Ambe et al.	N/A	N/A
6879825	12/2004	Daly	N/A	N/A
6882718	12/2004	Smith	N/A	N/A
6885997	12/2004	Roberts	N/A	N/A
6901440	12/2004	Bimm et al.	N/A	N/A
6920455	12/2004	Weschler	N/A	N/A
6922562	12/2004	Ward et al.	N/A	N/A
6928280	12/2004	Xanthos et al.	N/A	N/A
6934249	12/2004	Bertin et al.	N/A	N/A
6934751	12/2004	Jayapalan et al.	N/A	N/A
6947723	12/2004	Gurnani et al.	N/A	N/A
6947985	12/2004	Hegli et al.	N/A	N/A
6952428	12/2004	Necka et al.	N/A	N/A
6957067	12/2004	Iyer et al.	N/A	N/A
6959202	12/2004	Heinonen et al.	N/A	N/A

6959393	12/2004	Hollis et al.	N/A	N/A
6965667	12/2004	Trabandt et al.	N/A	N/A
6965872	12/2004	Grdina	N/A	N/A
6967958	12/2004	Ono et al.	N/A	N/A
6970692	12/2004	Tysor	N/A	N/A
6970927	12/2004	Stewart et al.	N/A	N/A
6982733	12/2005	McNally et al.	N/A	N/A
6983370	12/2005	Eaton et al.	N/A	N/A
6996062	12/2005	Freed et al.	N/A	N/A
6996076	12/2005	Forbes et al.	N/A	N/A
6996393	12/2005	Pyhalammi et al.	N/A	N/A
6998985	12/2005	Reisman et al.	N/A	N/A
7002920	12/2005	Ayyagari et al.	N/A	N/A
7007295	12/2005	Rose et al.	N/A	N/A
7013469	12/2005	Smith et al.	N/A	N/A
7017189	12/2005	DeMello et al.	N/A	N/A
7024200	12/2005	McKenna et al.	N/A	N/A
7024460	12/2005	Koopmas et al.	N/A	N/A
7027055	12/2005	Anderson et al.	N/A	N/A
7027408	12/2005	Nabkel et al.	N/A	N/A
7031733	12/2005	Alminana et al.	N/A	N/A
7032072	12/2005	Quinn et al.	N/A	N/A
7039027	12/2005	Bridgelall	N/A	N/A
7039037	12/2005	Wang et al.	N/A	N/A
7039403	12/2005	Wong	N/A	N/A
7039713	12/2005	Van Gunter et al.	N/A	N/A
7042988	12/2005	Juitt et al.	N/A	N/A
7043225	12/2005	Patel et al.	N/A	N/A
7043226	12/2005	Yamauchi	N/A	N/A
7043268	12/2005	Yukie et al.	N/A	N/A
7047276	12/2005	Liu et al.	N/A	N/A
7058022	12/2005	Carolan et al.	N/A	N/A
7058968	12/2005	Rowland et al.	N/A	N/A
7068600	12/2005	Cain	N/A	N/A
7069248	12/2005	Huber	N/A	N/A
7082422	12/2005	Zirngibi et al.	N/A	N/A
7084775	12/2005	Smith	N/A	N/A
7092696	12/2005	Hosain et al.	N/A	N/A
7095754	12/2005	Benveniste	N/A	N/A
7102620	12/2005	Harries et al.	N/A	N/A
7110753	12/2005	Campen	N/A	N/A
7113780	12/2005	McKenna et al.	N/A	N/A
7113997	12/2005	Jayapalan et al.	N/A	N/A
7120133	12/2005	Joo et al.	N/A	N/A
7133386	12/2005	Holur et al.	N/A	N/A
7133695	12/2005	Beyda	N/A	N/A
7136361	12/2005	Benveniste	N/A	N/A
7139569	12/2005	Kato	N/A	N/A
7142876	12/2005	Trossen et al.	N/A	N/A
7149229	12/2005	Leung	N/A	N/A
7149521	12/2005	Sundar et al.	N/A	N/A
7151764	12/2005	Heinonen et al.	N/A	N/A
7158792	12/2006	Cook et al.	N/A	N/A
7162237	12/2006	Silver et al.	N/A	N/A
7165040	12/2006	Ehrman et al.	N/A	N/A
7167078	12/2006	Pourchot	N/A	N/A
7174156	12/2006	Mangal	N/A	N/A
7174174	12/2006	Boris et al.	N/A	N/A
7177919	12/2006	Truong et al.	N/A	N/A
7180855	12/2006	Lin	N/A	N/A
7181017	12/2006	Nagel et al.	N/A	N/A
7191248	12/2006	Chattopadhyay et al.	N/A	N/A
7197321	12/2006	Erskine et al.	N/A	N/A
7200112	12/2006	Sundar et al.	N/A	N/A
7200551	12/2006	Senez	N/A	N/A
7203169	12/2006	Okholm et al.	N/A	N/A
7203721	12/2006	Ben-Efraim et al.	N/A	N/A
7203752	12/2006	Rice et al.	N/A	N/A
7212491	12/2006	Koga	N/A	N/A
7219123	12/2006	Flechter et al.	N/A	N/A
7222190	12/2006	Klinker et al.	N/A	N/A
7222304	12/2006	Beaton et al.	N/A	N/A
7224968	12/2006	Dobson et al.	N/A	N/A
7228354	12/2006	Chambliss et al.	N/A	N/A
7236780	12/2006	Benco	N/A	N/A

7242668	12/2006	Kan et al.	N/A	N/A
7242920	12/2006	Morris	N/A	N/A
7245901	12/2006	McGregor et al.	N/A	N/A
7248570	12/2006	Bahl et al.	N/A	N/A
7251218	12/2006	Jorgensen	N/A	N/A
7260382	12/2006	Lamb et al.	N/A	N/A
7266371	12/2006	Amin et al.	N/A	N/A
7269157	12/2006	Klinker et al.	N/A	N/A
7271765	12/2006	Stilp et al.	N/A	N/A
7272660	12/2006	Powers et al.	N/A	N/A
7280816	12/2006	Fratti et al.	N/A	N/A
7280818	12/2006	Clayton	N/A	N/A
7283561	12/2006	Picher-Dempsey	N/A	N/A
7283963	12/2006	Fitzpatrick et al.	N/A	N/A
7286834	12/2006	Walter	N/A	N/A
7286848	12/2006	Vireday et al.	N/A	N/A
7289489	12/2006	Kung et al.	N/A	N/A
7290283	12/2006	Copeland, III	N/A	N/A
7310424	12/2006	Gehring et al.	N/A	N/A
7313237	12/2006	Bahl et al.	N/A	N/A
7315892	12/2007	Freimuth et al.	N/A	N/A
7317699	12/2007	Godfrey et al.	N/A	N/A
7318050	12/2007	Musgrave	N/A	N/A
7318111	12/2007	Zhao	N/A	N/A
7320029	12/2007	Rinne et al.	N/A	N/A
7322044	12/2007	Hrastar	N/A	N/A
7324447	12/2007	Morford	N/A	N/A
7325037	12/2007	Lawson	N/A	N/A
7336960	12/2007	Zavalkovsky et al.	N/A	N/A
7340772	12/2007	Panasyuk et al.	N/A	N/A
7346410	12/2007	Uchiyama	N/A	N/A
7349695	12/2007	Oommen et al.	N/A	N/A
7353533	12/2007	Wright et al.	N/A	N/A
7356011	12/2007	Waters et al.	N/A	N/A
7356337	12/2007	Florence	N/A	N/A
7366497	12/2007	Nagata	N/A	N/A
7366654	12/2007	Moore	N/A	N/A
7366934	12/2007	Narayan et al.	N/A	N/A
7369848	12/2007	Jiang	N/A	N/A
7369856	12/2007	Ovadia	N/A	N/A
7373136	12/2007	Watler et al.	N/A	N/A
7373179	12/2007	Stine et al.	N/A	N/A
7379731	12/2007	Natsuno et al.	N/A	N/A
7388950	12/2007	Elsey et al.	N/A	N/A
7389412	12/2007	Sharma et al.	N/A	N/A
7391724	12/2007	Alakoski et al.	N/A	N/A
7395056	12/2007	Petermann	N/A	N/A
7395244	12/2007	Kingsford	N/A	N/A
7401338	12/2007	Bowen et al.	N/A	N/A
7403763	12/2007	Maes	N/A	N/A
7409447	12/2007	Assadzadeh	N/A	N/A
7409569	12/2007	Illowsky et al.	N/A	N/A
7411930	12/2007	Montojo et al.	N/A	N/A
7418253	12/2007	Kavanah	N/A	N/A
7418257	12/2007	Kim	N/A	N/A
7421004	12/2007	Feher	N/A	N/A
7423971	12/2007	Mohaban et al.	N/A	N/A
7428750	12/2007	Dunn et al.	N/A	N/A
7433362	12/2007	Mallya et al.	N/A	N/A
7436816	12/2007	Mehta et al.	N/A	N/A
7440433	12/2007	Rink et al.	N/A	N/A
7444669	12/2007	Bahl et al.	N/A	N/A
7450591	12/2007	Korling et al.	N/A	N/A
7450927	12/2007	Creswell et al.	N/A	N/A
7454191	12/2007	Dawson et al.	N/A	N/A
7457265	12/2007	Julka et al.	N/A	N/A
7457870	12/2007	Lownsbrough et al.	N/A	N/A
7460837	12/2007	Diener	N/A	N/A
7466652	12/2007	Lau et al.	N/A	N/A
7467160	12/2007	McIntyre	N/A	N/A
7472189	12/2007	Mallya et al.	N/A	N/A
7478420	12/2008	Wright et al.	N/A	N/A
7486185	12/2008	Culpepper et al.	N/A	N/A
7486658	12/2008	Kumar	N/A	N/A
7493659	12/2008	Wu et al.	N/A	N/A

7496652	12/2008	Pezzutti	N/A	N/A
7499438	12/2008	Hinman et al.	N/A	N/A
7499537	12/2008	Elsey et al.	N/A	N/A
7502672	12/2008	Kolls	N/A	N/A
7505756	12/2008	Bahl	N/A	N/A
7505795	12/2008	Lim et al.	N/A	N/A
7508799	12/2008	Sumner et al.	N/A	N/A
7512128	12/2008	DiMambro et al.	N/A	N/A
7512131	12/2008	Svensson et al.	N/A	N/A
7515608	12/2008	Yuan et al.	N/A	N/A
7515926	12/2008	Bu et al.	N/A	N/A
7516219	12/2008	Moghaddam et al.	N/A	N/A
7522549	12/2008	Karaoguz et al.	N/A	N/A
7522576	12/2008	Du et al.	N/A	N/A
7526541	12/2008	Roese et al.	N/A	N/A
7529204	12/2008	Bourlas et al.	N/A	N/A
7535880	12/2008	Hinman et al.	N/A	N/A
7536695	12/2008	Alam et al.	N/A	N/A
7539132	12/2008	Werner et al.	N/A	N/A
7539862	12/2008	Edgett et al.	N/A	N/A
7540408	12/2008	Levine et al.	N/A	N/A
7545782	12/2008	Rayment et al.	N/A	N/A
7546460	12/2008	Maes	N/A	N/A
7546629	12/2008	Albert et al.	N/A	N/A
7548875	12/2008	Mikkelsen et al.	N/A	N/A
7548976	12/2008	Bahl et al.	N/A	N/A
7551921	12/2008	Petermann	N/A	N/A
7551922	12/2008	Roskowski et al.	N/A	N/A
7554983	12/2008	Muppala	N/A	N/A
7555757	12/2008	Smith et al.	N/A	N/A
7561899	12/2008	Lee	N/A	N/A
7562213	12/2008	Timms	N/A	N/A
7564799	12/2008	Holland et al.	N/A	N/A
7565141	12/2008	Macaluso	N/A	N/A
7574509	12/2008	Nixon et al.	N/A	N/A
7574731	12/2008	Fascenda	N/A	N/A
7577431	12/2008	Jiang	N/A	N/A
7580356	12/2008	Mishra et al.	N/A	N/A
7580857	12/2008	VanFleet et al.	N/A	N/A
7583964	12/2008	Wong	N/A	N/A
7584298	12/2008	Klinker et al.	N/A	N/A
7585217	12/2008	Lutnick et al.	N/A	N/A
7586871	12/2008	Hamilton et al.	N/A	N/A
7593417	12/2008	Wang et al.	N/A	N/A
7593730	12/2008	Khandelwal et al.	N/A	N/A
7596373	12/2008	Mcgregor et al.	N/A	N/A
7599288	12/2008	Cole et al.	N/A	N/A
7599714	12/2008	Kuzminskiy	N/A	N/A
7602746	12/2008	Calhoun et al.	N/A	N/A
7606918	12/2008	Holzman et al.	N/A	N/A
7607041	12/2008	Kraemer et al.	N/A	N/A
7609650	12/2008	Roskowski et al.	N/A	N/A
7609700	12/2008	Ying et al.	N/A	N/A
7610047	12/2008	Hicks, III et al.	N/A	N/A
7610057	12/2008	Bahl et al.	N/A	N/A
7610328	12/2008	Haase et al.	N/A	N/A
7610396	12/2008	Taglienti et al.	N/A	N/A
7614051	12/2008	Glaum et al.	N/A	N/A
7616962	12/2008	Oswal et al.	N/A	N/A
7617516	12/2008	Huslak et al.	N/A	N/A
7620041	12/2008	Dunn et al.	N/A	N/A
7620065	12/2008	Falardeau	N/A	N/A
7620162	12/2008	Aaron et al.	N/A	N/A
7620383	12/2008	Taglienti et al.	N/A	N/A
7627314	12/2008	Carlson et al.	N/A	N/A
7627600	12/2008	Citron et al.	N/A	N/A
7627767	12/2008	Sherman et al.	N/A	N/A
7627872	12/2008	Hebeler et al.	N/A	N/A
7633438	12/2008	Tysowski	N/A	N/A
7634388	12/2008	Archer et al.	N/A	N/A
7636574	12/2008	Poosala	N/A	N/A
7636626	12/2008	Oesterling et al.	N/A	N/A
7643411	12/2009	Andreasen et al.	N/A	N/A
7644151	12/2009	Jerrim et al.	N/A	N/A
7644267	12/2009	Ylikoski et al.	N/A	N/A

7644414	12/2009	Smith et al.	N/A	N/A
7647047	12/2009	Moghaddam et al.	N/A	N/A
7650137	12/2009	Jobs et al.	N/A	N/A
7653394	12/2009	McMillin	N/A	N/A
7656271	12/2009	Ehrman et al.	N/A	N/A
7657920	12/2009	Arseneau et al.	N/A	N/A
7660419	12/2009	Ho	N/A	N/A
7661124	12/2009	Ramanathan et al.	N/A	N/A
7664494	12/2009	Jiang	N/A	N/A
7668176	12/2009	Chuah	N/A	N/A
7668612	12/2009	Okkonen	N/A	N/A
7668903	12/2009	Edwards et al.	N/A	N/A
7668966	12/2009	Klinker et al.	N/A	N/A
7672695	12/2009	Rainnie et al.	N/A	N/A
7676673	12/2009	Weller et al.	N/A	N/A
7680086	12/2009	Eglin	N/A	N/A
7681226	12/2009	Kraemer et al.	N/A	N/A
7684370	12/2009	Kezys	N/A	N/A
7685131	12/2009	Batra et al.	N/A	N/A
7685254	12/2009	Pandya	N/A	N/A
7685530	12/2009	Sherrard et al.	N/A	N/A
7688792	12/2009	Babbar et al.	N/A	N/A
7693107	12/2009	De Froment	N/A	N/A
7693720	12/2009	Kennewick et al.	N/A	N/A
7697540	12/2009	Haddad et al.	N/A	N/A
7710932	12/2009	Muthuswamy et al.	N/A	N/A
7711848	12/2009	Maes	N/A	N/A
7719966	12/2009	Luft et al.	N/A	N/A
7720206	12/2009	Devolites et al.	N/A	N/A
7720464	12/2009	Batta	N/A	N/A
7720505	12/2009	Gopi et al.	N/A	N/A
7720960	12/2009	Pruss et al.	N/A	N/A
7721296	12/2009	Ricagni	N/A	N/A
7724716	12/2009	Fadell	N/A	N/A
7725570	12/2009	Lewis	N/A	N/A
7729326	12/2009	Sekhar	N/A	N/A
7730123	12/2009	Erickson et al.	N/A	N/A
7734784	12/2009	Araujo et al.	N/A	N/A
7742406	12/2009	Muppala	N/A	N/A
7746854	12/2009	Ambe et al.	N/A	N/A
7747240	12/2009	Briscoe et al.	N/A	N/A
7747699	12/2009	Prueitt et al.	N/A	N/A
7747730	12/2009	Harlow	N/A	N/A
7752330	12/2009	Olsen et al.	N/A	N/A
7756056	12/2009	Kim et al.	N/A	N/A
7756534	12/2009	Anupam et al.	N/A	N/A
7756757	12/2009	Oakes, III	N/A	N/A
7760137	12/2009	Martucci et al.	N/A	N/A
7760711	12/2009	Kung et al.	N/A	N/A
7760861	12/2009	Croak et al.	N/A	N/A
7765294	12/2009	Edwards et al.	N/A	N/A
7769397	12/2009	Funato et al.	N/A	N/A
7770785	12/2009	Jha et al.	N/A	N/A
7774323	12/2009	Helfman	N/A	N/A
7774412	12/2009	Schnepel	N/A	N/A
7774456	12/2009	Lownsbrough et al.	N/A	N/A
7778176	12/2009	Morford	N/A	N/A
7778643	12/2009	Laroia et al.	N/A	N/A
7792257	12/2009	Vanier et al.	N/A	N/A
7792538	12/2009	Kozisek	N/A	N/A
7792708	12/2009	Alva	N/A	N/A
7797019	12/2009	Friedmann	N/A	N/A
7797060	12/2009	Grgic et al.	N/A	N/A
7797204	12/2009	Balent	N/A	N/A
7797401	12/2009	Stewart et al.	N/A	N/A
7801523	12/2009	Kenderov	N/A	N/A
7801783	12/2009	Kende et al.	N/A	N/A
7801985	12/2009	Pitkow et al.	N/A	N/A
7802724	12/2009	Nohr	N/A	N/A
7805140	12/2009	Friday et al.	N/A	N/A
7805522	12/2009	Schlüter et al.	N/A	N/A
7805606	12/2009	Birger et al.	N/A	N/A
7809351	12/2009	Panda et al.	N/A	N/A
7809372	12/2009	Rajaniemi	N/A	N/A
7813746	12/2009	Rajkotia	N/A	N/A

7817615	12/2009	Breau et al.	N/A	N/A
7817983	12/2009	Cassett et al.	N/A	N/A
7822837	12/2009	Urban et al.	N/A	N/A
7822849	12/2009	Titus	N/A	N/A
7826427	12/2009	Sood et al.	N/A	N/A
7826607	12/2009	De Carvalho Resende et al.	N/A	N/A
7835275	12/2009	Swan et al.	N/A	N/A
7843831	12/2009	Morrill et al.	N/A	N/A
7843843	12/2009	Papp, III et al.	N/A	N/A
7844034	12/2009	Oh et al.	N/A	N/A
7844728	12/2009	Anderson et al.	N/A	N/A
7848768	12/2009	Omori et al.	N/A	N/A
7849161	12/2009	Koch et al.	N/A	N/A
7849170	12/2009	Hargens et al.	N/A	N/A
7849310	12/2009	Watt et al.	N/A	N/A
7849477	12/2009	Cristofalo et al.	N/A	N/A
7853255	12/2009	Karaoguz et al.	N/A	N/A
7853656	12/2009	Yach et al.	N/A	N/A
7856226	12/2009	Wong et al.	N/A	N/A
7860088	12/2009	Lioy	N/A	N/A
7865182	12/2010	Macaluso	N/A	N/A
7865187	12/2010	Ramer et al.	N/A	N/A
7868778	12/2010	Kenwright	N/A	N/A
7873001	12/2010	Silver	N/A	N/A
7873344	12/2010	Bowser et al.	N/A	N/A
7873346	12/2010	Petersson et al.	N/A	N/A
7873540	12/2010	Arumugam	N/A	N/A
7873705	12/2010	Kalish	N/A	N/A
7877090	12/2010	Maes	N/A	N/A
7881199	12/2010	Krstulich	N/A	N/A
7881267	12/2010	Crosswy et al.	N/A	N/A
7881697	12/2010	Baker et al.	N/A	N/A
7882029	12/2010	White	N/A	N/A
7882247	12/2010	Sturniolo et al.	N/A	N/A
7882560	12/2010	Kraemer et al.	N/A	N/A
7886047	12/2010	Potluri	N/A	N/A
7889384	12/2010	Armentrout et al.	N/A	N/A
7890084	12/2010	Dudziak et al.	N/A	N/A
7890111	12/2010	Bugenhagen	N/A	N/A
7894431	12/2010	Goring et al.	N/A	N/A
7899039	12/2010	Andreasen et al.	N/A	N/A
7899438	12/2010	Baker et al.	N/A	N/A
7903553	12/2010	Liu	N/A	N/A
7907970	12/2010	Park et al.	N/A	N/A
7908358	12/2010	Prasad et al.	N/A	N/A
7911975	12/2010	Droz et al.	N/A	N/A
7912025	12/2010	Pattenden et al.	N/A	N/A
7912056	12/2010	Brassem	N/A	N/A
7920529	12/2010	Mahler et al.	N/A	N/A
7921463	12/2010	Sood et al.	N/A	N/A
7925740	12/2010	Nath et al.	N/A	N/A
7925778	12/2010	Wijnands et al.	N/A	N/A
7929959	12/2010	DeAtley et al.	N/A	N/A
7929960	12/2010	Martin et al.	N/A	N/A
7929973	12/2010	Zavalkovsky et al.	N/A	N/A
7930327	12/2010	Craft et al.	N/A	N/A
7930446	12/2010	Kesselman et al.	N/A	N/A
7930553	12/2010	Satarasinghe et al.	N/A	N/A
7933274	12/2010	Verma et al.	N/A	N/A
7936736	12/2010	Proctor, Jr. et al.	N/A	N/A
7937069	12/2010	Rassam	N/A	N/A
7937450	12/2010	Janik	N/A	N/A
7940685	12/2010	Breslau et al.	N/A	N/A
7940751	12/2010	Hansen	N/A	N/A
7941184	12/2010	Prendergast et al.	N/A	N/A
7944948	12/2010	Chow et al.	N/A	N/A
7945238	12/2010	Baker et al.	N/A	N/A
7945240	12/2010	Klock et al.	N/A	N/A
7945945	12/2010	Graham et al.	N/A	N/A
7948952	12/2010	Hurtta et al.	N/A	N/A
7948953	12/2010	Melkote et al.	N/A	N/A
7948968	12/2010	Voit et al.	N/A	N/A
7949529	12/2010	Weider et al.	N/A	N/A
7953808	12/2010	Sharp et al.	N/A	N/A
7953877	12/2010	Vemula et al.	N/A	N/A

7957020	12/2010	Mine et al.	N/A	N/A
7957381	12/2010	Clermidy et al.	N/A	N/A
7957511	12/2010	Drudis et al.	N/A	N/A
7958029	12/2010	Bobich et al.	N/A	N/A
7962622	12/2010	Friend et al.	N/A	N/A
7965983	12/2010	Swan et al.	N/A	N/A
7966405	12/2010	Sundaresan et al.	N/A	N/A
7969950	12/2010	Iyer et al.	N/A	N/A
7970350	12/2010	Sheynman	N/A	N/A
7970426	12/2010	Poe et al.	N/A	N/A
7974624	12/2010	Gallagher et al.	N/A	N/A
7975184	12/2010	Goff et al.	N/A	N/A
7978627	12/2010	Taylor et al.	N/A	N/A
7978686	12/2010	Goyal et al.	N/A	N/A
7979069	12/2010	Hupp et al.	N/A	N/A
7979889	12/2010	Gladstone et al.	N/A	N/A
7979896	12/2010	McMurtry et al.	N/A	N/A
7984130	12/2010	Bogineni et al.	N/A	N/A
7984511	12/2010	Kocher et al.	N/A	N/A
7986935	12/2010	D'Souza et al.	N/A	N/A
7987496	12/2010	Bryce et al.	N/A	N/A
7987510	12/2010	Kocher et al.	N/A	N/A
7990049	12/2010	Shioya	N/A	N/A
8000276	12/2010	Scherzer et al.	N/A	N/A
8000318	12/2010	Wiley et al.	N/A	N/A
8005009	12/2010	McKee et al.	N/A	N/A
8005459	12/2010	Balsillie	N/A	N/A
8005726	12/2010	Bao	N/A	N/A
8005913	12/2010	Carlander	N/A	N/A
8005988	12/2010	Maes	N/A	N/A
8010080	12/2010	Thenthiruperai et al.	N/A	N/A
8010081	12/2010	Roskowski	N/A	N/A
8010082	12/2010	Sutaria et al.	N/A	N/A
8010990	12/2010	Ferguson et al.	N/A	N/A
8015133	12/2010	Wu et al.	N/A	N/A
8015234	12/2010	Lum et al.	N/A	N/A
8015249	12/2010	Nayak et al.	N/A	N/A
8019687	12/2010	Wang et al.	N/A	N/A
8019820	12/2010	Son et al.	N/A	N/A
8019846	12/2010	Roelens et al.	N/A	N/A
8019868	12/2010	Rao et al.	N/A	N/A
8019886	12/2010	Harrang et al.	N/A	N/A
8023425	12/2010	Raleigh	N/A	N/A
8024397	12/2010	Erickson et al.	N/A	N/A
8024424	12/2010	Freimuth et al.	N/A	N/A
8027339	12/2010	Short et al.	N/A	N/A
8031601	12/2010	Feroz et al.	N/A	N/A
8032168	12/2010	Ikaheimo	N/A	N/A
8032409	12/2010	Mikurak	N/A	N/A
8032899	12/2010	Archer et al.	N/A	N/A
8036387	12/2010	Kudelski et al.	N/A	N/A
8036600	12/2010	Garrett et al.	N/A	N/A
8044792	12/2010	Orr et al.	N/A	N/A
8045973	12/2010	Chambers	N/A	N/A
8046449	12/2010	Yoshiuchi	N/A	N/A
8050275	12/2010	Iyer	N/A	N/A
8050690	12/2010	Neeraj	N/A	N/A
8050705	12/2010	Sicher et al.	N/A	N/A
8059530	12/2010	Cole	N/A	N/A
8060017	12/2010	Schlicht et al.	N/A	N/A
8060463	12/2010	Spiegel	N/A	N/A
8060603	12/2010	Caunter et al.	N/A	N/A
8060748	12/2010	Johansson et al.	N/A	N/A
8064417	12/2010	Maki	N/A	N/A
8064418	12/2010	Maki	N/A	N/A
8064896	12/2010	Bell et al.	N/A	N/A
8065365	12/2010	Saxena et al.	N/A	N/A
8068824	12/2010	Shan et al.	N/A	N/A
8068829	12/2010	Lemond et al.	N/A	N/A
8073427	12/2010	Koch et al.	N/A	N/A
8073721	12/2010	Lewis	N/A	N/A
8078140	12/2010	Baker et al.	N/A	N/A
8078163	12/2010	Lemond et al.	N/A	N/A
8085808	12/2010	Brusca et al.	N/A	N/A
8086398	12/2010	Sanchez et al.	N/A	N/A

8086497	12/2010	Oakes, III	N/A	N/A
8086791	12/2010	Caulkins	N/A	N/A
8090359	12/2011	Proctor, Jr. et al.	N/A	N/A
8090361	12/2011	Hagan	N/A	N/A
8090616	12/2011	Proctor, Jr. et al.	N/A	N/A
8091087	12/2011	Ali et al.	N/A	N/A
8094551	12/2011	Huber et al.	N/A	N/A
8095112	12/2011	Chow et al.	N/A	N/A
8095124	12/2011	Balia	N/A	N/A
8095640	12/2011	Guingo et al.	N/A	N/A
8095666	12/2011	Schmidt et al.	N/A	N/A
8098579	12/2011	Ray et al.	N/A	N/A
8099077	12/2011	Chowdhury et al.	N/A	N/A
8099517	12/2011	Jia et al.	N/A	N/A
8102814	12/2011	Rahman et al.	N/A	N/A
8103285	12/2011	Kalhan	N/A	N/A
8104080	12/2011	Burns et al.	N/A	N/A
8107953	12/2011	Zimmerman et al.	N/A	N/A
8108520	12/2011	Ruutu et al.	N/A	N/A
8108680	12/2011	Murray	N/A	N/A
8112435	12/2011	Epstein et al.	N/A	N/A
8116223	12/2011	Tian et al.	N/A	N/A
8116749	12/2011	Proctor, Jr. et al.	N/A	N/A
8116781	12/2011	Chen et al.	N/A	N/A
8122128	12/2011	Burke, II et al.	N/A	N/A
8122249	12/2011	Falk et al.	N/A	N/A
8125897	12/2011	Ray et al.	N/A	N/A
8126123	12/2011	Cai et al.	N/A	N/A
8126396	12/2011	Bennett	N/A	N/A
8126476	12/2011	Vardi et al.	N/A	N/A
8126722	12/2011	Robb et al.	N/A	N/A
8130793	12/2011	Edwards et al.	N/A	N/A
8131256	12/2011	Martti et al.	N/A	N/A
8131281	12/2011	Hildner et al.	N/A	N/A
8131840	12/2011	Denker	N/A	N/A
8131858	12/2011	Agulnik et al.	N/A	N/A
8132256	12/2011	Bari	N/A	N/A
8134954	12/2011	Godfrey et al.	N/A	N/A
8135388	12/2011	Gailloux et al.	N/A	N/A
8135392	12/2011	Marcellino et al.	N/A	N/A
8135657	12/2011	Kapoor et al.	N/A	N/A
8140690	12/2011	Ly et al.	N/A	N/A
8144591	12/2011	Ghai et al.	N/A	N/A
8145194	12/2011	Yoshikawa et al.	N/A	N/A
8146142	12/2011	Lortz et al.	N/A	N/A
8149748	12/2011	Bata et al.	N/A	N/A
8149823	12/2011	Turcan et al.	N/A	N/A
8150394	12/2011	Bianconi et al.	N/A	N/A
8150431	12/2011	Wolovitz et al.	N/A	N/A
8151205	12/2011	Follmann et al.	N/A	N/A
8155155	12/2011	Chow et al.	N/A	N/A
8155620	12/2011	Wang et al.	N/A	N/A
8155666	12/2011	Alizadeh-Shabdiz	N/A	N/A
8155670	12/2011	Fullam et al.	N/A	N/A
8156206	12/2011	Kiley et al.	N/A	N/A
8159520	12/2011	Dhanoa et al.	N/A	N/A
8160015	12/2011	Rashid et al.	N/A	N/A
8160056	12/2011	Van der Merwe et al.	N/A	N/A
8160598	12/2011	Savoor	N/A	N/A
8165576	12/2011	Raju et al.	N/A	N/A
8166040	12/2011	Brindisi et al.	N/A	N/A
8166554	12/2011	John	N/A	N/A
8170553	12/2011	Bennett	N/A	N/A
8174378	12/2011	Richman et al.	N/A	N/A
8174970	12/2011	Adamczyk et al.	N/A	N/A
8175574	12/2011	Panda et al.	N/A	N/A
8180333	12/2011	Wells et al.	N/A	N/A
8180881	12/2011	Seo et al.	N/A	N/A
8180886	12/2011	Overcash et al.	N/A	N/A
8184530	12/2011	Swan et al.	N/A	N/A
8184590	12/2011	Rosenblatt	N/A	N/A
8185088	12/2011	Klein et al.	N/A	N/A
8185093	12/2011	Jheng et al.	N/A	N/A
8185127	12/2011	Cai et al.	N/A	N/A
8185152	12/2011	Goldner	N/A	N/A

8185158	12/2011	Tamura et al.	N/A	N/A
8190087	12/2011	Fisher et al.	N/A	N/A
8190122	12/2011	Alexander et al.	N/A	N/A
8190675	12/2011	Tribbett	N/A	N/A
8191106	12/2011	Choyi et al.	N/A	N/A
8191116	12/2011	Gazzard	N/A	N/A
8191124	12/2011	Wynn et al.	N/A	N/A
8194549	12/2011	Huber et al.	N/A	N/A
8194553	12/2011	Liang et al.	N/A	N/A
8194572	12/2011	Horvath et al.	N/A	N/A
8194581	12/2011	Schroeder et al.	N/A	N/A
8195093	12/2011	Garrett et al.	N/A	N/A
8195153	12/2011	Frencel et al.	N/A	N/A
8195163	12/2011	Gisby et al.	N/A	N/A
8195661	12/2011	Kalavade	N/A	N/A
8196199	12/2011	Hrastar et al.	N/A	N/A
8200163	12/2011	Hoffman	N/A	N/A
8200200	12/2011	Belser et al.	N/A	N/A
8200509	12/2011	Kenedy et al.	N/A	N/A
8200775	12/2011	Moore	N/A	N/A
8200818	12/2011	Freund et al.	N/A	N/A
8204190	12/2011	Bang et al.	N/A	N/A
8204505	12/2011	Jin et al.	N/A	N/A
8208788	12/2011	Ando et al.	N/A	N/A
8208919	12/2011	Kotecha	N/A	N/A
8213296	12/2011	Shannon et al.	N/A	N/A
8213363	12/2011	Ying et al.	N/A	N/A
8214536	12/2011	Zhao	N/A	N/A
8214890	12/2011	Kirovski et al.	N/A	N/A
8219134	12/2011	Maharajh et al.	N/A	N/A
8223655	12/2011	Heinz et al.	N/A	N/A
8223741	12/2011	Bartlett et al.	N/A	N/A
8224382	12/2011	Bultman	N/A	N/A
8224773	12/2011	Spiegel	N/A	N/A
8228818	12/2011	Chase et al.	N/A	N/A
8229394	12/2011	Karlberg	N/A	N/A
8229914	12/2011	Ramer et al.	N/A	N/A
8233433	12/2011	Kalhan	N/A	N/A
8233883	12/2011	De Froment	N/A	N/A
8233895	12/2011	Tysowski	N/A	N/A
8234583	12/2011	Sloo et al.	N/A	N/A
8238287	12/2011	Gopi et al.	N/A	N/A
8238913	12/2011	Bhattacharyya et al.	N/A	N/A
8239520	12/2011	Grah	N/A	N/A
8242959	12/2011	Mia et al.	N/A	N/A
8244241	12/2011	Montemurro	N/A	N/A
8249601	12/2011	Emberson et al.	N/A	N/A
8254880	12/2011	Aaltonen et al.	N/A	N/A
8254915	12/2011	Kozisek	N/A	N/A
8255515	12/2011	Melman et al.	N/A	N/A
8255534	12/2011	Assadzadeh	N/A	N/A
8255669	12/2011	Kim et al.	N/A	N/A
8259692	12/2011	Bajko	N/A	N/A
8260252	12/2011	Agarwal	N/A	N/A
8264965	12/2011	Dolganow et al.	N/A	N/A
8265004	12/2011	Toutonghi	N/A	N/A
8266249	12/2011	Hu	N/A	N/A
8266681	12/2011	Deshpande et al.	N/A	N/A
8270955	12/2011	Ramer et al.	N/A	N/A
8270972	12/2011	Otting et al.	N/A	N/A
8271025	12/2011	Brisebois et al.	N/A	N/A
8271045	12/2011	Parolkar et al.	N/A	N/A
8271049	12/2011	Silver et al.	N/A	N/A
8271992	12/2011	Chatley et al.	N/A	N/A
8275415	12/2011	Huslak	N/A	N/A
8275830	12/2011	Raleigh	N/A	N/A
8279067	12/2011	Berger et al.	N/A	N/A
8279864	12/2011	Wood	N/A	N/A
8280354	12/2011	Smith et al.	N/A	N/A
8284740	12/2011	O'Connor	N/A	N/A
8285249	12/2011	Baker et al.	N/A	N/A
8285992	12/2011	Mathur et al.	N/A	N/A
8290820	12/2011	Plastina et al.	N/A	N/A
8291238	12/2011	Ginter et al.	N/A	N/A
8291439	12/2011	Jethi et al.	N/A	N/A

8296404	12/2011	McDysan et al.	N/A	N/A
8300575	12/2011	Willars	N/A	N/A
8306518	12/2011	Gailloux	N/A	N/A
8306741	12/2011	Tu	N/A	N/A
8307067	12/2011	Ryan	N/A	N/A
8310943	12/2011	Mehta et al.	N/A	N/A
8315198	12/2011	Corneille et al.	N/A	N/A
8315593	12/2011	Gallant et al.	N/A	N/A
8315594	12/2011	Mauser et al.	N/A	N/A
8315718	12/2011	Caffrey et al.	N/A	N/A
8315999	12/2011	Chatley et al.	N/A	N/A
8320244	12/2011	Muqattash et al.	N/A	N/A
8320949	12/2011	Matta	N/A	N/A
8325638	12/2011	Jin et al.	N/A	N/A
8325906	12/2011	Fullarton et al.	N/A	N/A
8326319	12/2011	Davis	N/A	N/A
8326828	12/2011	Zhou et al.	N/A	N/A
8331223	12/2011	Hill et al.	N/A	N/A
8331293	12/2011	Sood	N/A	N/A
8332375	12/2011	Chatley et al.	N/A	N/A
8339991	12/2011	Biswas et al.	N/A	N/A
8340625	12/2011	Johnson et al.	N/A	N/A
8340628	12/2011	Taylor et al.	N/A	N/A
8340678	12/2011	Pandey	N/A	N/A
8340718	12/2011	Colonna et al.	N/A	N/A
8346210	12/2012	Balsan et al.	N/A	N/A
8346225	12/2012	Raleigh	N/A	N/A
8346923	12/2012	Rowles et al.	N/A	N/A
8347104	12/2012	Pathiyal	N/A	N/A
8347362	12/2012	Cai et al.	N/A	N/A
8347378	12/2012	Merkin et al.	N/A	N/A
8350700	12/2012	Fast et al.	N/A	N/A
8351592	12/2012	Freeny, Jr. et al.	N/A	N/A
8351898	12/2012	Raleigh	N/A	N/A
8352360	12/2012	De Judicibus et al.	N/A	N/A
8352980	12/2012	Howcroft	N/A	N/A
8353001	12/2012	Herrod	N/A	N/A
8355570	12/2012	Karsanbhai et al.	N/A	N/A
8355696	12/2012	Olding et al.	N/A	N/A
8356336	12/2012	Johnston et al.	N/A	N/A
8358638	12/2012	Scherzer et al.	N/A	N/A
8358975	12/2012	Bahl et al.	N/A	N/A
8363658	12/2012	Delker et al.	N/A	N/A
8363799	12/2012	Gruchala et al.	N/A	N/A
8364089	12/2012	Phillips	N/A	N/A
8364806	12/2012	Short et al.	N/A	N/A
8369274	12/2012	Sawai	N/A	N/A
8370477	12/2012	Short et al.	N/A	N/A
8370483	12/2012	Choong et al.	N/A	N/A
8374090	12/2012	Morrill et al.	N/A	N/A
8374592	12/2012	Proctor, Jr. et al.	N/A	N/A
8375128	12/2012	Tofighbakhsh et al.	N/A	N/A
8375136	12/2012	Roman et al.	N/A	N/A
8380247	12/2012	Engstrom	N/A	N/A
8385199	12/2012	Coward et al.	N/A	N/A
8385896	12/2012	Proctor, Jr. et al.	N/A	N/A
8385964	12/2012	Haney	N/A	N/A
8385975	12/2012	Forutanpour et al.	N/A	N/A
8386386	12/2012	Zhu	N/A	N/A
8391262	12/2012	Maki et al.	N/A	N/A
8391834	12/2012	Raleigh	455/414.1	H04L 41/5054
8392982	12/2012	Harris et al.	N/A	N/A
8396458	12/2012	Raleigh	N/A	N/A
8396929	12/2012	Helfman et al.	N/A	N/A
8401968	12/2012	Schattauer et al.	N/A	N/A
8402111	12/2012	Raleigh	709/224	H04L 67/34
8402165	12/2012	Deu-Ngoc et al.	N/A	N/A
8402540	12/2012	Kapoor et al.	N/A	N/A
8406427	12/2012	Chand et al.	N/A	N/A
8406736	12/2012	Das et al.	N/A	N/A
8407763	12/2012	Weller et al.	N/A	N/A
8411587	12/2012	Curtis et al.	N/A	N/A
8411691	12/2012	Aggarwal	N/A	N/A
8412798	12/2012	Wang	N/A	N/A
8413245	12/2012	Kraemer et al.	N/A	N/A

8418168	12/2012	Tyhurst et al.	N/A	N/A
8422988	12/2012	Keshav	N/A	N/A
8423016	12/2012	Buckley et al.	N/A	N/A
8429403	12/2012	Moret et al.	N/A	N/A
8437734	12/2012	Ray et al.	N/A	N/A
8442015	12/2012	Behzad et al.	N/A	N/A
8446831	12/2012	Kwan et al.	N/A	N/A
8447324	12/2012	Shuman et al.	N/A	N/A
8447607	12/2012	Weider et al.	N/A	N/A
8447980	12/2012	Godfrey et al.	N/A	N/A
8448015	12/2012	Gerhart	N/A	N/A
8452858	12/2012	Wu et al.	N/A	N/A
8457603	12/2012	El-Kadri et al.	N/A	N/A
8461958	12/2012	Saenz et al.	N/A	N/A
8463194	12/2012	Erlenback et al.	N/A	N/A
8463232	12/2012	Tuli et al.	N/A	N/A
8468337	12/2012	Gaur et al.	N/A	N/A
8472371	12/2012	Bari et al.	N/A	N/A
8477778	12/2012	Lehmann, Jr. et al.	N/A	N/A
8478840	12/2012	Skutela et al.	N/A	N/A
8483057	12/2012	Cuervo	N/A	N/A
8483135	12/2012	Cai et al.	N/A	N/A
8483694	12/2012	Lewis et al.	N/A	N/A
8484327	12/2012	Werner et al.	N/A	N/A
8488597	12/2012	Nie et al.	N/A	N/A
8489110	12/2012	Frank et al.	N/A	N/A
8489720	12/2012	Morford et al.	N/A	N/A
8494559	12/2012	Malmi	N/A	N/A
8495181	12/2012	Venkatraman et al.	N/A	N/A
8495207	12/2012	Lee	N/A	N/A
8495227	12/2012	Kaminsky et al.	N/A	N/A
8495360	12/2012	Falk et al.	N/A	N/A
8495700	12/2012	Shahbazi	N/A	N/A
8495743	12/2012	Kraemer et al.	N/A	N/A
8499087	12/2012	Hu	N/A	N/A
RE44412	12/2012	Naqvi et al.	N/A	N/A
8500533	12/2012	Lutnick et al.	N/A	N/A
8503358	12/2012	Hanson et al.	N/A	N/A
8503455	12/2012	Heikens	N/A	N/A
8504032	12/2012	Lott et al.	N/A	N/A
8504574	12/2012	Dvorak et al.	N/A	N/A
8504687	12/2012	Maffione et al.	N/A	N/A
8504690	12/2012	Shah et al.	N/A	N/A
8504729	12/2012	Pezzutti	N/A	N/A
8505073	12/2012	Taglienti et al.	N/A	N/A
8509082	12/2012	Heinz et al.	N/A	N/A
8514927	12/2012	Sundararajan et al.	N/A	N/A
8516552	12/2012	Raleigh	N/A	N/A
8520589	12/2012	Bhatt et al.	N/A	N/A
8520595	12/2012	Yadav et al.	N/A	N/A
8521110	12/2012	Rofougaran	N/A	N/A
8521775	12/2012	Poh et al.	N/A	N/A
8522039	12/2012	Hyndman et al.	N/A	N/A
8522249	12/2012	Beaule	N/A	N/A
8522337	12/2012	Adusumilli et al.	N/A	N/A
8523547	12/2012	Pekrul	N/A	N/A
8526329	12/2012	Mahany et al.	N/A	N/A
8526350	12/2012	Xue et al.	N/A	N/A
8527013	12/2012	Guba et al.	N/A	N/A
8527410	12/2012	Markki et al.	N/A	N/A
8527662	12/2012	Biswas et al.	N/A	N/A
8528068	12/2012	Weglein et al.	N/A	N/A
8531954	12/2012	McNaughton et al.	N/A	N/A
8531995	12/2012	Khan et al.	N/A	N/A
8532610	12/2012	Manning Cassett et al.	N/A	N/A
8533775	12/2012	Alcorn et al.	N/A	N/A
8535160	12/2012	Lutnick et al.	N/A	N/A
8538394	12/2012	Zimmerman et al.	N/A	N/A
8538421	12/2012	Brisebois et al.	N/A	N/A
8538458	12/2012	Haney	N/A	N/A
8539544	12/2012	Garimella et al.	N/A	N/A
8543265	12/2012	Ekhaguere et al.	N/A	N/A
8543814	12/2012	Laitinen et al.	N/A	N/A
8544105	12/2012	Mclean et al.	N/A	N/A
8548427	12/2012	Chow et al.	N/A	N/A

8549173	12/2012	Wu et al.	N/A	N/A
8554876	12/2012	Winsor	N/A	N/A
8559369	12/2012	Barkan	N/A	N/A
8561138	12/2012	Rothman et al.	N/A	N/A
8565746	12/2012	Hoffman	N/A	N/A
8566236	12/2012	Busch	N/A	N/A
8571474	12/2012	Chavez et al.	N/A	N/A
8571501	12/2012	Miller et al.	N/A	N/A
8571598	12/2012	Valavi	N/A	N/A
8571993	12/2012	Kocher et al.	N/A	N/A
8572117	12/2012	Rappaport	N/A	N/A
8572256	12/2012	Babbar	N/A	N/A
8583499	12/2012	De Judicibus et al.	N/A	N/A
8588240	12/2012	Ramankutty et al.	N/A	N/A
8589955	12/2012	Roundtree et al.	N/A	N/A
8594665	12/2012	Anschutz	N/A	N/A
8595186	12/2012	Mandyam et al.	N/A	N/A
8600895	12/2012	Felsher	N/A	N/A
8601125	12/2012	Huang et al.	N/A	N/A
8605691	12/2012	Soomro et al.	N/A	N/A
8612967	12/2012	Delker	717/169	G06F 8/61
8615507	12/2012	Varadarajulu et al.	N/A	N/A
8619735	12/2012	Montemurro et al.	N/A	N/A
8620257	12/2012	Qiu et al.	N/A	N/A
8630630	12/2013	Raleigh	N/A	N/A
8630925	12/2013	Bystrom et al.	N/A	N/A
8631428	12/2013	Scott et al.	N/A	N/A
8634425	12/2013	Gorti et al.	N/A	N/A
8635164	12/2013	Rosenhaft et al.	N/A	N/A
8639215	12/2013	McGregor et al.	N/A	N/A
8644702	12/2013	Kalajan	N/A	N/A
8644813	12/2013	Gailloux et al.	N/A	N/A
8645518	12/2013	David	N/A	N/A
8655357	12/2013	Gazzard et al.	N/A	N/A
8656472	12/2013	McMurtry et al.	N/A	N/A
8660853	12/2013	Robb et al.	N/A	N/A
8666395	12/2013	Silver	N/A	N/A
8667542	12/2013	Bertz et al.	N/A	N/A
8670334	12/2013	Keohane et al.	N/A	N/A
8675852	12/2013	Maes	N/A	N/A
8676682	12/2013	Kalliola	N/A	N/A
8676925	12/2013	Liu et al.	N/A	N/A
8693323	12/2013	McDysan	N/A	N/A
8694772	12/2013	Kao et al.	N/A	N/A
8700729	12/2013	Dua	N/A	N/A
8701015	12/2013	Bonnat	N/A	N/A
8705361	12/2013	Venkataraman et al.	N/A	N/A
8706863	12/2013	Fadell	N/A	N/A
8713535	12/2013	Malhotra et al.	N/A	N/A
8713641	12/2013	Pagan et al.	N/A	N/A
8719397	12/2013	Levi et al.	N/A	N/A
8719423	12/2013	Wyld	N/A	N/A
8724486	12/2013	Seto et al.	N/A	N/A
8725899	12/2013	Short et al.	N/A	N/A
8730842	12/2013	Collins et al.	N/A	N/A
8731519	12/2013	Flynn et al.	N/A	N/A
8732808	12/2013	Sewall et al.	N/A	N/A
8739035	12/2013	Trethewey	N/A	N/A
8744339	12/2013	Halfmann et al.	N/A	N/A
8761711	12/2013	Grignani et al.	N/A	N/A
8780857	12/2013	Balasubramanian et al.	N/A	N/A
8787249	12/2013	Giaretta et al.	N/A	N/A
8792857	12/2013	Cai et al.	N/A	N/A
8793304	12/2013	Lu et al.	N/A	N/A
8798610	12/2013	Prakash et al.	N/A	N/A
8799440	12/2013	Zhou et al.	N/A	N/A
8804695	12/2013	Branam	N/A	N/A
8811338	12/2013	Jin et al.	N/A	N/A
8811991	12/2013	Jain et al.	N/A	N/A
8818394	12/2013	Bienas et al.	N/A	N/A
8819253	12/2013	Simeloff et al.	N/A	N/A
8825109	12/2013	Montemurro et al.	N/A	N/A
8826411	12/2013	Moen et al.	N/A	N/A
8831561	12/2013	Sutaria et al.	N/A	N/A
8838752	12/2013	Lor et al.	N/A	N/A

8843849	12/2013	Neil et al.	N/A	N/A
8845415	12/2013	Lutnick et al.	N/A	N/A
8849297	12/2013	Balasubramanian	N/A	N/A
8855620	12/2013	Sievers et al.	N/A	N/A
8862751	12/2013	Faccin et al.	N/A	N/A
8863111	12/2013	Selitser et al.	N/A	N/A
8875042	12/2013	LeJeune et al.	N/A	N/A
8880047	12/2013	Konicek et al.	N/A	N/A
8891483	12/2013	Connelly et al.	N/A	N/A
8898748	12/2013	Burks et al.	N/A	N/A
8908516	12/2013	Tzamaloukas et al.	N/A	N/A
8923824	12/2013	Masterman	N/A	N/A
8929374	12/2014	Tönsing et al.	N/A	N/A
8930238	12/2014	Coffman et al.	N/A	N/A
8930551	12/2014	Pandya et al.	N/A	N/A
8943551	12/2014	Ganapathy et al.	N/A	N/A
8948726	12/2014	Smith et al.	N/A	N/A
8949382	12/2014	Cornett et al.	N/A	N/A
8949597	12/2014	Reeves et al.	N/A	N/A
8955038	12/2014	Nicodemus et al.	N/A	N/A
8966018	12/2014	Bugwadia et al.	N/A	N/A
8971912	12/2014	Chou et al.	N/A	N/A
8977284	12/2014	Reed	N/A	N/A
8995952	12/2014	Baker et al.	N/A	N/A
9002342	12/2014	Tenhunen et al.	N/A	N/A
9014973	12/2014	Ruckart	N/A	N/A
9015331	12/2014	Lai et al.	N/A	N/A
9026100	12/2014	Castro et al.	N/A	N/A
9030934	12/2014	Shah et al.	N/A	N/A
9049010	12/2014	Jueneman et al.	N/A	N/A
9064275	12/2014	Lu et al.	N/A	N/A
9105031	12/2014	Shen et al.	N/A	N/A
9111088	12/2014	Ghai et al.	N/A	N/A
9137286	12/2014	Yuan	N/A	N/A
9172553	12/2014	Dawes et al.	N/A	N/A
9177455	12/2014	Remer	N/A	N/A
9191394	12/2014	Novak et al.	N/A	N/A
9204282	12/2014	Raleigh	N/A	N/A
9282460	12/2015	Souissi	N/A	N/A
9286469	12/2015	Kraemer et al.	N/A	N/A
9286604	12/2015	Aabye et al.	N/A	N/A
9313708	12/2015	Nam et al.	N/A	N/A
9325737	12/2015	Gutowski et al.	N/A	N/A
9326173	12/2015	Luft	N/A	N/A
9344557	12/2015	Gruchala et al.	N/A	N/A
9363285	12/2015	Kitamura	N/A	N/A
9367680	12/2015	Mahaffey et al.	N/A	N/A
9413546	12/2015	Meier et al.	N/A	N/A
9418381	12/2015	Ahuja et al.	N/A	N/A
9459767	12/2015	Cockcroft et al.	N/A	N/A
9501803	12/2015	Bilac et al.	N/A	N/A
9544397	12/2016	Raleigh et al.	N/A	N/A
9589117	12/2016	Ali et al.	N/A	N/A
9609459	12/2016	Raleigh	N/A	N/A
9712476	12/2016	Boynton et al.	N/A	N/A
9942796	12/2017	Raleigh	N/A	N/A
9986413	12/2017	Raleigh	N/A	N/A
10021251	12/2017	Aaron et al.	N/A	N/A
10285025	12/2018	Baker et al.	N/A	N/A
10326800	12/2018	Raleigh et al.	N/A	N/A
10492102	12/2018	Raleigh et al.	N/A	N/A
10582375	12/2019	Raleigh	N/A	H04L 41/082
10694385	12/2019	Raleigh	N/A	G06Q 10/06375
10779177	12/2019	Raleigh	N/A	N/A
10855559	12/2019	Raleigh	N/A	H04L 47/824
11337059	12/2021	Raleigh	N/A	H04M 15/61
2001/0048738	12/2000	Baniak et al.	N/A	N/A
2001/0053694	12/2000	Igarashi et al.	N/A	N/A
2002/0013844	12/2001	Garrett et al.	N/A	N/A
2002/0022472	12/2001	Watler et al.	N/A	N/A
2002/0022483	12/2001	Thompson et al.	N/A	N/A
2002/0049074	12/2001	Eisinger et al.	N/A	N/A
2002/0099848	12/2001	Lee	N/A	N/A
2002/0116338	12/2001	Gonthier et al.	N/A	N/A
2002/0120370	12/2001	Parupudi et al.	N/A	N/A

2002/0120540	12/2001	Kende et al.	N/A	N/A
2002/0131404	12/2001	Mehta et al.	N/A	N/A
2002/0138599	12/2001	Dilman et al.	N/A	N/A
2002/0138601	12/2001	Piponius et al.	N/A	N/A
2002/0154751	12/2001	Thompson et al.	N/A	N/A
2002/0161601	12/2001	Nauer et al.	N/A	N/A
2002/0164983	12/2001	Raviv et al.	N/A	N/A
2002/0176377	12/2001	Hamilton	N/A	N/A
2002/0188732	12/2001	Buckman et al.	N/A	N/A
2002/0191573	12/2001	Whitehill et al.	N/A	N/A
2002/0199001	12/2001	Wenocur et al.	N/A	N/A
2003/0004937	12/2002	Salmenkaita et al.	N/A	N/A
2003/0005112	12/2002	Krautkremer	N/A	N/A
2003/0013434	12/2002	Rosenberg et al.	N/A	N/A
2003/0018524	12/2002	Fishman et al.	N/A	N/A
2003/0028623	12/2002	Hennessey et al.	N/A	N/A
2003/0046396	12/2002	Richter et al.	N/A	N/A
2003/0050070	12/2002	Mashinsky et al.	N/A	N/A
2003/0050837	12/2002	Kim	N/A	N/A
2003/0084321	12/2002	Tarquini et al.	N/A	N/A
2003/0088671	12/2002	Klinker et al.	N/A	N/A
2003/0133408	12/2002	Cheng et al.	N/A	N/A
2003/0134650	12/2002	Sundar et al.	N/A	N/A
2003/0159030	12/2002	Evans	N/A	N/A
2003/0161265	12/2002	Cao et al.	N/A	N/A
2003/0171112	12/2002	Lupper et al.	N/A	N/A
2003/0182420	12/2002	Jones et al.	N/A	N/A
2003/0182435	12/2002	Redlich et al.	N/A	N/A
2003/0184793	12/2002	Pineau	N/A	N/A
2003/0188006	12/2002	Bard	N/A	N/A
2003/0188117	12/2002	Yoshino et al.	N/A	N/A
2003/0220984	12/2002	Jones et al.	N/A	N/A
2003/0224781	12/2002	Milford et al.	N/A	N/A
2003/0229900	12/2002	Reisman	N/A	N/A
2003/0233332	12/2002	Keeler et al.	N/A	N/A
2003/0236745	12/2002	Hartsell et al.	N/A	N/A
2004/0019539	12/2003	Raman et al.	N/A	N/A
2004/0019564	12/2003	Goldthwaite et al.	N/A	N/A
2004/0021697	12/2003	Beaton et al.	N/A	N/A
2004/0024756	12/2003	Rickard	N/A	N/A
2004/0030705	12/2003	Bowman-Amuah	N/A	N/A
2004/0039792	12/2003	Nakanishi	N/A	N/A
2004/0044623	12/2003	Wake et al.	N/A	N/A
2004/0047358	12/2003	Chen et al.	N/A	N/A
2004/0054779	12/2003	Takeshima et al.	N/A	N/A
2004/0073672	12/2003	Fascenda	N/A	N/A
2004/0082346	12/2003	Skytt et al.	N/A	N/A
2004/0098715	12/2003	Aghera et al.	N/A	N/A
2004/0102182	12/2003	Reith et al.	N/A	N/A
2004/0103193	12/2003	Pandya et al.	N/A	N/A
2004/0107360	12/2003	Herrmann et al.	N/A	N/A
2004/0116140	12/2003	Babbar et al.	N/A	N/A
2004/0123153	12/2003	Wright et al.	N/A	N/A
2004/0127200	12/2003	Shaw et al.	N/A	N/A
2004/0127208	12/2003	Nair et al.	N/A	N/A
2004/0127256	12/2003	Goldthwaite et al.	N/A	N/A
2004/0132427	12/2003	Lee et al.	N/A	N/A
2004/0133668	12/2003	Nicholas, III	N/A	N/A
2004/0137890	12/2003	Kalke	N/A	N/A
2004/0148237	12/2003	Bittmann et al.	N/A	N/A
2004/0165596	12/2003	Garcia et al.	N/A	N/A
2004/0167958	12/2003	Stewart et al.	N/A	N/A
2004/0168052	12/2003	Clisham et al.	N/A	N/A
2004/0170191	12/2003	Guo et al.	N/A	N/A
2004/0176104	12/2003	Arcens	N/A	N/A
2004/0198331	12/2003	Coward et al.	N/A	N/A
2004/0203755	12/2003	Brunet et al.	N/A	N/A
2004/0203833	12/2003	Rathunde et al.	N/A	N/A
2004/0225561	12/2003	Hertzberg et al.	N/A	N/A
2004/0225898	12/2003	Frost et al.	N/A	N/A
2004/0236547	12/2003	Rappaport et al.	N/A	N/A
2004/0243680	12/2003	Mayer	N/A	N/A
2004/0243992	12/2003	Gustafson et al.	N/A	N/A
2004/0249918	12/2003	Sunshine	N/A	N/A
2004/0255145	12/2003	Chow	N/A	N/A

2004/0259534	12/2003	Chaudhari et al.	N/A	N/A
2004/0260766	12/2003	Barros et al.	N/A	N/A
2004/0267872	12/2003	Serdy et al.	N/A	N/A
2005/0007993	12/2004	Chambers et al.	N/A	N/A
2005/0009499	12/2004	Koster	N/A	N/A
2005/0021995	12/2004	Lal et al.	N/A	N/A
2005/0041617	12/2004	Huotari et al.	N/A	N/A
2005/0048950	12/2004	Morper	N/A	N/A
2005/0055291	12/2004	Bevente et al.	N/A	N/A
2005/0055309	12/2004	Williams et al.	N/A	N/A
2005/0055595	12/2004	Frazer et al.	N/A	N/A
2005/0060266	12/2004	Demello et al.	N/A	N/A
2005/0060525	12/2004	Schwartz et al.	N/A	N/A
2005/0075115	12/2004	Corneille et al.	N/A	N/A
2005/0079863	12/2004	Macaluso	N/A	N/A
2005/0091505	12/2004	Riley et al.	N/A	N/A
2005/0096024	12/2004	Bicker et al.	N/A	N/A
2005/0097516	12/2004	Donnelly et al.	N/A	N/A
2005/0101323	12/2004	De Beer	N/A	N/A
2005/0107091	12/2004	Vannithamby et al.	N/A	N/A
2005/0108075	12/2004	Douglis et al.	N/A	N/A
2005/0108534	12/2004	Bajikar et al.	N/A	N/A
2005/0111463	12/2004	Leung et al.	N/A	N/A
2005/0128967	12/2004	Scobbie	N/A	N/A
2005/0135264	12/2004	Popoff et al.	N/A	N/A
2005/0163320	12/2004	Brown et al.	N/A	N/A
2005/0166043	12/2004	Zhang et al.	N/A	N/A
2005/0183143	12/2004	Anderholm et al.	N/A	N/A
2005/0186948	12/2004	Gallagher et al.	N/A	N/A
2005/0198377	12/2004	Ferguson et al.	N/A	N/A
2005/0216421	12/2004	Barry et al.	N/A	N/A
2005/0228985	12/2004	Ylikoski et al.	N/A	N/A
2005/0238046	12/2004	Hassan et al.	N/A	N/A
2005/0239447	12/2004	Holzman et al.	N/A	N/A
2005/0245241	12/2004	Durand et al.	N/A	N/A
2005/0246282	12/2004	Naslund et al.	N/A	N/A
2005/0250508	12/2004	Guo et al.	N/A	N/A
2005/0250536	12/2004	Deng et al.	N/A	N/A
2005/0254435	12/2004	Moakley et al.	N/A	N/A
2005/0266825	12/2004	Clayton	N/A	N/A
2005/0266880	12/2004	Gupta	N/A	N/A
2006/0014519	12/2005	Marsh et al.	N/A	N/A
2006/0015749	12/2005	Mittal	N/A	N/A
2006/0019632	12/2005	Cunningham et al.	N/A	N/A
2006/0020781	12/2005	Scarlata et al.	N/A	N/A
2006/0020787	12/2005	Choyi et al.	N/A	N/A
2006/0026679	12/2005	Zakas	N/A	N/A
2006/0030306	12/2005	Kuhn	N/A	N/A
2006/0034256	12/2005	Addagatla et al.	N/A	N/A
2006/0035631	12/2005	White et al.	N/A	N/A
2006/0040642	12/2005	Boris et al.	N/A	N/A
2006/0045245	12/2005	Aaron et al.	N/A	N/A
2006/0048223	12/2005	Lee et al.	N/A	N/A
2006/0068796	12/2005	Millen et al.	N/A	N/A
2006/0072451	12/2005	Ross	N/A	N/A
2006/0072550	12/2005	Davis et al.	N/A	N/A
2006/0072646	12/2005	Feher	N/A	N/A
2006/0075506	12/2005	Sanda et al.	N/A	N/A
2006/0085543	12/2005	Hrastar et al.	N/A	N/A
2006/0093107	12/2005	Chien	N/A	N/A
2006/0095517	12/2005	O'Connor et al.	N/A	N/A
2006/0098627	12/2005	Karaoguz et al.	N/A	N/A
2006/0099970	12/2005	Morgan et al.	N/A	N/A
2006/0101507	12/2005	Camenisch	N/A	N/A
2006/0112016	12/2005	Ishibashi	N/A	N/A
2006/0112427	12/2005	Shahbazi	N/A	N/A
2006/0114821	12/2005	Willey et al.	N/A	N/A
2006/0114832	12/2005	Hamilton et al.	N/A	N/A
2006/0126562	12/2005	Liu	N/A	N/A
2006/0135144	12/2005	Jothipragasam	N/A	N/A
2006/0136882	12/2005	Noonan et al.	N/A	N/A
2006/0143066	12/2005	Calabria	N/A	N/A
2006/0143098	12/2005	Lazaridis	N/A	N/A
2006/0156398	12/2005	Ross et al.	N/A	N/A
2006/0160536	12/2005	Chou	N/A	N/A

2006/0165060	12/2005	Dua	N/A	N/A
2006/0168128	12/2005	Sistla et al.	N/A	N/A
2006/0173959	12/2005	Mckelvie et al.	N/A	N/A
2006/0174035	12/2005	Tufail	N/A	N/A
2006/0178917	12/2005	Merriam et al.	N/A	N/A
2006/0178918	12/2005	Mikurak	N/A	N/A
2006/0182137	12/2005	Zhou et al.	N/A	N/A
2006/0183461	12/2005	Pearce	N/A	N/A
2006/0183462	12/2005	Kolehmainen	N/A	N/A
2006/0190314	12/2005	Hernandez	N/A	N/A
2006/0190987	12/2005	Ohta et al.	N/A	N/A
2006/0193280	12/2005	Lee et al.	N/A	N/A
2006/0199608	12/2005	Dunn et al.	N/A	N/A
2006/0200663	12/2005	Thornton	N/A	N/A
2006/0206709	12/2005	Labrou et al.	N/A	N/A
2006/0206904	12/2005	Watkins et al.	N/A	N/A
2006/0218395	12/2005	Maes	N/A	N/A
2006/0233108	12/2005	Krishnan	N/A	N/A
2006/0233166	12/2005	Bou-Diab et al.	N/A	N/A
2006/0236095	12/2005	Smith et al.	N/A	N/A
2006/0242685	12/2005	Heard et al.	N/A	N/A
2006/0258289	12/2005	Dua	N/A	N/A
2006/0258341	12/2005	Miller et al.	N/A	N/A
2006/0274706	12/2005	Chen et al.	N/A	N/A
2006/0277590	12/2005	Limont et al.	N/A	N/A
2006/0286977	12/2005	Khandelwal	455/435.2	H04W 12/02
2006/0291419	12/2005	McConnell et al.	N/A	N/A
2006/0291477	12/2005	Croak et al.	N/A	N/A
2007/0005795	12/2006	Gonzalez	N/A	N/A
2007/0006289	12/2006	Limont et al.	N/A	N/A
2007/0019670	12/2006	Falardeau	N/A	N/A
2007/0022289	12/2006	Alt et al.	N/A	N/A
2007/0025301	12/2006	Petersson et al.	N/A	N/A
2007/0033194	12/2006	Srinivas et al.	N/A	N/A
2007/0033197	12/2006	Scherzer et al.	N/A	N/A
2007/0035390	12/2006	Thomas et al.	N/A	N/A
2007/0036312	12/2006	Cai et al.	N/A	N/A
2007/0055694	12/2006	Ruge et al.	N/A	N/A
2007/0060200	12/2006	Boris et al.	N/A	N/A
2007/0061243	12/2006	Ramer et al.	N/A	N/A
2007/0061535	12/2006	Xu et al.	N/A	N/A
2007/0061800	12/2006	Cheng et al.	N/A	N/A
2007/0061878	12/2006	Hagiu et al.	N/A	N/A
2007/0073899	12/2006	Judge et al.	N/A	N/A
2007/0076616	12/2006	Ngo et al.	N/A	N/A
2007/0093243	12/2006	Kapadekar et al.	N/A	N/A
2007/0100981	12/2006	Adamczyk et al.	N/A	N/A
2007/0101426	12/2006	Lee et al.	N/A	N/A
2007/0104126	12/2006	Calhoun et al.	N/A	N/A
2007/0104169	12/2006	Polson	370/338	H04W 28/24
2007/0109983	12/2006	Shankar et al.	N/A	N/A
2007/0111740	12/2006	Wandel	N/A	N/A
2007/0117538	12/2006	Weiser et al.	N/A	N/A
2007/0130283	12/2006	Klein et al.	N/A	N/A
2007/0130315	12/2006	Friend et al.	N/A	N/A
2007/0140113	12/2006	Gemelos	N/A	N/A
2007/0140145	12/2006	Kumar et al.	N/A	N/A
2007/0140275	12/2006	Bowman et al.	N/A	N/A
2007/0143824	12/2006	Shahbazi	N/A	N/A
2007/0147317	12/2006	Smith et al.	N/A	N/A
2007/0147324	12/2006	McGary	N/A	N/A
2007/0149252	12/2006	Jobs et al.	N/A	N/A
2007/0155365	12/2006	Kim et al.	N/A	N/A
2007/0165630	12/2006	Rasanen et al.	N/A	N/A
2007/0168499	12/2006	Chu	N/A	N/A
2007/0171856	12/2006	Bruce et al.	N/A	N/A
2007/0174490	12/2006	Choi et al.	N/A	N/A
2007/0178888	12/2006	Alfano et al.	N/A	N/A
2007/0191006	12/2006	Carpenter	N/A	N/A
2007/0192460	12/2006	Chol et al.	N/A	N/A
2007/0198656	12/2006	Mazzaferri et al.	N/A	N/A
2007/0201502	12/2006	Abramson	N/A	N/A
2007/0213054	12/2006	Han	N/A	N/A
2007/0220251	12/2006	Rosenberg et al.	N/A	N/A
2007/0226225	12/2006	Yiu et al.	N/A	N/A

2007/0226775	12/2006	Andreasen et al.	N/A	N/A
2007/0234402	12/2006	Khosravi et al.	N/A	N/A
2007/0243862	12/2006	Coskun et al.	N/A	N/A
2007/0248100	12/2006	Zuberi et al.	N/A	N/A
2007/0254646	12/2006	Sokondar	N/A	N/A
2007/0254675	12/2006	Zorlu Ozer et al.	N/A	N/A
2007/0255769	12/2006	Agrawal et al.	N/A	N/A
2007/0255797	12/2006	Dunn et al.	N/A	N/A
2007/0255848	12/2006	Sewall et al.	N/A	N/A
2007/0257767	12/2006	Beeson	N/A	N/A
2007/0259656	12/2006	Jeong	N/A	N/A
2007/0259673	12/2006	Willars et al.	N/A	N/A
2007/0263558	12/2006	Salomone	N/A	N/A
2007/0266422	12/2006	Germano et al.	N/A	N/A
2007/0274327	12/2006	Kaarela et al.	N/A	N/A
2007/0280453	12/2006	Kelley	N/A	N/A
2007/0282896	12/2006	Wydroug et al.	N/A	N/A
2007/0288989	12/2006	Aarnos et al.	N/A	N/A
2007/0293191	12/2006	Mir et al.	N/A	N/A
2007/0294395	12/2006	Strub et al.	N/A	N/A
2007/0294410	12/2006	Pandya et al.	N/A	N/A
2007/0297378	12/2006	Poyhonen et al.	N/A	N/A
2007/0298764	12/2006	Clayton	N/A	N/A
2007/0299965	12/2006	Nieh et al.	N/A	N/A
2007/0300252	12/2006	Acharya et al.	N/A	N/A
2008/0005285	12/2007	Robinson et al.	N/A	N/A
2008/0005561	12/2007	Brown et al.	N/A	N/A
2008/0010379	12/2007	Zhao	N/A	N/A
2008/0010452	12/2007	Holtzman et al.	N/A	N/A
2008/0018494	12/2007	Waite et al.	N/A	N/A
2008/0020738	12/2007	Ho et al.	N/A	N/A
2008/0022354	12/2007	Grewal et al.	N/A	N/A
2008/0025230	12/2007	Patel et al.	N/A	N/A
2008/0032715	12/2007	Jia et al.	N/A	N/A
2008/0034063	12/2007	Yee	N/A	N/A
2008/0034419	12/2007	Mullick et al.	N/A	N/A
2008/0039102	12/2007	Sewall et al.	N/A	N/A
2008/0049630	12/2007	Kozisek et al.	N/A	N/A
2008/0050715	12/2007	Golczewski et al.	N/A	N/A
2008/0051076	12/2007	O'Shaughnessy et al.	N/A	N/A
2008/0052387	12/2007	Heinz et al.	N/A	N/A
2008/0056273	12/2007	Pelletier et al.	N/A	N/A
2008/0059474	12/2007	Lim	N/A	N/A
2008/0059743	12/2007	Bychkov et al.	N/A	N/A
2008/0060066	12/2007	Wynn et al.	N/A	N/A
2008/0062900	12/2007	Rao	N/A	N/A
2008/0064367	12/2007	Nath et al.	N/A	N/A
2008/0066149	12/2007	Lim	N/A	N/A
2008/0066150	12/2007	Lim	N/A	N/A
2008/0066181	12/2007	Haveson et al.	N/A	N/A
2008/0070550	12/2007	Hose	N/A	N/A
2008/0077705	12/2007	Li et al.	N/A	N/A
2008/0080457	12/2007	Cole	N/A	N/A
2008/0081606	12/2007	Cole	N/A	N/A
2008/0082643	12/2007	Storrie et al.	N/A	N/A
2008/0083013	12/2007	Soliman et al.	N/A	N/A
2008/0085707	12/2007	Fadell	N/A	N/A
2008/0089295	12/2007	Keeler et al.	N/A	N/A
2008/0089303	12/2007	Wirtanen et al.	N/A	N/A
2008/0095339	12/2007	Elliott et al.	N/A	N/A
2008/0096559	12/2007	Phillips et al.	N/A	N/A
2008/0098062	12/2007	Balia	N/A	N/A
2008/0109679	12/2007	Wright et al.	N/A	N/A
2008/0117958	12/2007	Pattenden et al.	N/A	N/A
2008/0120129	12/2007	Seubert et al.	N/A	N/A
2008/0120174	12/2007	Li	N/A	N/A
2008/0120668	12/2007	Yau	N/A	N/A
2008/0120688	12/2007	Qiu et al.	N/A	N/A
2008/0122796	12/2007	Jobs et al.	N/A	N/A
2008/0125079	12/2007	O'Neil et al.	N/A	N/A
2008/0126287	12/2007	Cox et al.	N/A	N/A
2008/0127304	12/2007	Ginter et al.	N/A	N/A
2008/0130534	12/2007	Tomioka	N/A	N/A
2008/0130656	12/2007	Kim et al.	N/A	N/A
2008/0132201	12/2007	Karlberg	N/A	N/A

2008/0132268	12/2007	Choi-Grogan et al.	N/A	N/A
2008/0134330	12/2007	Kapoor et al.	N/A	N/A
2008/0139210	12/2007	Gisby et al.	N/A	N/A
2008/0147454	12/2007	Walker et al.	N/A	N/A
2008/0160958	12/2007	Abichandani et al.	N/A	N/A
2008/0162637	12/2007	Adamczyk et al.	N/A	N/A
2008/0162704	12/2007	Poplett et al.	N/A	N/A
2008/0164304	12/2007	Narasimhan et al.	N/A	N/A
2008/0166993	12/2007	Gautier et al.	N/A	N/A
2008/0167027	12/2007	Gautier et al.	N/A	N/A
2008/0167033	12/2007	Beckers	N/A	N/A
2008/0168275	12/2007	DeAtley et al.	N/A	N/A
2008/0168523	12/2007	Ansari et al.	N/A	N/A
2008/0177998	12/2007	Apsangi et al.	N/A	N/A
2008/0178300	12/2007	Brown et al.	N/A	N/A
2008/0181117	12/2007	Acke et al.	N/A	N/A
2008/0183812	12/2007	Paul et al.	N/A	N/A
2008/0184127	12/2007	Rafey et al.	N/A	N/A
2008/0189760	12/2007	Rosenberg et al.	N/A	N/A
2008/0201266	12/2007	Chua et al.	N/A	N/A
2008/0207167	12/2007	Bugenhagen	N/A	N/A
2008/0212470	12/2007	Castaneda et al.	N/A	N/A
2008/0212751	12/2007	Chung	N/A	N/A
2008/0219268	12/2007	Dennison	N/A	N/A
2008/0221951	12/2007	Stanforth et al.	N/A	N/A
2008/0222692	12/2007	Andersson et al.	N/A	N/A
2008/0225748	12/2007	Khemani et al.	N/A	N/A
2008/0229385	12/2007	Feder et al.	N/A	N/A
2008/0229388	12/2007	Maes	N/A	N/A
2008/0235511	12/2007	O'Brien et al.	N/A	N/A
2008/0240373	12/2007	Wilhelm	N/A	N/A
2008/0244018	12/2007	Chen et al.	N/A	N/A
2008/0250053	12/2007	Aaltonen et al.	N/A	N/A
2008/0256593	12/2007	Vinberg et al.	N/A	N/A
2008/0259924	12/2007	Gooch et al.	N/A	N/A
2008/0262798	12/2007	Kim et al.	N/A	N/A
2008/0263348	12/2007	Zaltsman et al.	N/A	N/A
2008/0268813	12/2007	Maes	N/A	N/A
2008/0270212	12/2007	Blight et al.	N/A	N/A
2008/0279216	12/2007	Sharif-Ahmadi et al.	N/A	N/A
2008/0282319	12/2007	Fontijn et al.	N/A	N/A
2008/0291872	12/2007	Henriksson	N/A	N/A
2008/0293395	12/2007	Mathews et al.	N/A	N/A
2008/0298230	12/2007	Luft et al.	N/A	N/A
2008/0305793	12/2007	Gallagher et al.	N/A	N/A
2008/0311885	12/2007	Dawson et al.	N/A	N/A
2008/0313315	12/2007	Karaoguz et al.	N/A	N/A
2008/0313730	12/2007	Iftimie et al.	N/A	N/A
2008/0316923	12/2007	Fedders et al.	N/A	N/A
2008/0318547	12/2007	Ballou et al.	N/A	N/A
2008/0318550	12/2007	DeAtley	N/A	N/A
2008/0319879	12/2007	Carroll et al.	N/A	N/A
2008/0320497	12/2007	Tarkoma et al.	N/A	N/A
2009/0005000	12/2008	Baker et al.	N/A	N/A
2009/0005005	12/2008	Forstall et al.	N/A	N/A
2009/0006116	12/2008	Baker et al.	N/A	N/A
2009/0006200	12/2008	Baker et al.	N/A	N/A
2009/0006229	12/2008	Sweeney et al.	N/A	N/A
2009/0013157	12/2008	Beaule	N/A	N/A
2009/0016310	12/2008	Rasal	N/A	N/A
2009/0017809	12/2008	Jethi et al.	N/A	N/A
2009/0036111	12/2008	Danford et al.	N/A	N/A
2009/0042536	12/2008	Bernard et al.	N/A	N/A
2009/0044185	12/2008	Krivopaltsev	N/A	N/A
2009/0046707	12/2008	Smires et al.	N/A	N/A
2009/0046723	12/2008	Rahman et al.	N/A	N/A
2009/0047989	12/2008	Harmon et al.	N/A	N/A
2009/0048913	12/2008	Shenfield et al.	N/A	N/A
2009/0049156	12/2008	Aronsson et al.	N/A	N/A
2009/0049518	12/2008	Roman et al.	N/A	N/A
2009/0054030	12/2008	Golds	N/A	N/A
2009/0065571	12/2008	Jain	N/A	N/A
2009/0066999	12/2008	Ito	N/A	N/A
2009/0067372	12/2008	Shah et al.	N/A	N/A
2009/0068984	12/2008	Burnett	N/A	N/A

2009/0070379	12/2008	Rappaport	N/A	N/A
2009/0077622	12/2008	Baum et al.	N/A	N/A
2009/0077643	12/2008	Schmidt et al.	N/A	N/A
2009/0079699	12/2008	Sun	N/A	N/A
2009/0113514	12/2008	Hu	N/A	N/A
2009/0125619	12/2008	Antani	N/A	N/A
2009/0132860	12/2008	Liu et al.	N/A	N/A
2009/0149154	12/2008	Bhasin et al.	N/A	N/A
2009/0149165	12/2008	Minborg et al.	N/A	N/A
2009/0157792	12/2008	Fiatal	N/A	N/A
2009/0163173	12/2008	Williams	N/A	N/A
2009/0172077	12/2008	Roxburgh et al.	N/A	N/A
2009/0180391	12/2008	Petersen et al.	N/A	N/A
2009/0181662	12/2008	Fleischman et al.	N/A	N/A
2009/0197585	12/2008	Aaron	N/A	N/A
2009/0197612	12/2008	Kiiskinen	N/A	N/A
2009/0203352	12/2008	Fordon et al.	N/A	N/A
2009/0217065	12/2008	Araujo, Jr.	N/A	N/A
2009/0217364	12/2008	Salmela et al.	N/A	N/A
2009/0219170	12/2008	Clark et al.	N/A	N/A
2009/0248883	12/2008	Suryanarayana et al.	N/A	N/A
2009/0249247	12/2008	Tseng et al.	N/A	N/A
2009/0253409	12/2008	Slavov et al.	N/A	N/A
2009/0254857	12/2008	Romine et al.	N/A	N/A
2009/0257379	12/2008	Robinson et al.	N/A	N/A
2009/0262715	12/2008	Juang	N/A	N/A
2009/0265754	12/2008	Hinds	N/A	N/A
2009/0271514	12/2008	Thomas et al.	N/A	N/A
2009/0282127	12/2008	Leblanc et al.	N/A	N/A
2009/0286507	12/2008	O'Neil et al.	N/A	N/A
2009/0287921	12/2008	Zhu et al.	N/A	N/A
2009/0288140	12/2008	Huber et al.	N/A	N/A
2009/0291665	12/2008	Gaskarth et al.	N/A	N/A
2009/0299857	12/2008	Brubaker	N/A	N/A
2009/0307696	12/2008	Vals et al.	N/A	N/A
2009/0307746	12/2008	Di et al.	N/A	N/A
2009/0315735	12/2008	Bhavani et al.	N/A	N/A
2009/0320110	12/2008	Nicolson et al.	N/A	N/A
2010/0017506	12/2009	Fadell	N/A	N/A
2010/0020822	12/2009	Zerillo et al.	N/A	N/A
2010/0027469	12/2009	Gurajala et al.	N/A	N/A
2010/0027559	12/2009	Lin et al.	N/A	N/A
2010/0029273	12/2009	Bennett	N/A	N/A
2010/0030890	12/2009	Dutta et al.	N/A	N/A
2010/0041364	12/2009	Lott et al.	N/A	N/A
2010/0041365	12/2009	Lott et al.	N/A	N/A
2010/0041391	12/2009	Spivey et al.	N/A	N/A
2010/0042675	12/2009	Fujii	N/A	N/A
2010/0043068	12/2009	Varadhan et al.	N/A	N/A
2010/0069074	12/2009	Kodialam et al.	N/A	N/A
2010/0071053	12/2009	Ansari et al.	N/A	N/A
2010/0075666	12/2009	Garner	N/A	N/A
2010/0077035	12/2009	Li et al.	N/A	N/A
2010/0080202	12/2009	Hanson	N/A	N/A
2010/0082431	12/2009	Ramer et al.	N/A	N/A
2010/0088387	12/2009	Calamera	N/A	N/A
2010/0103820	12/2009	Fuller et al.	N/A	N/A
2010/0113020	12/2009	Subramanian et al.	N/A	N/A
2010/0121744	12/2009	Belz et al.	N/A	N/A
2010/0131584	12/2009	Johnson	N/A	N/A
2010/0142478	12/2009	Forssell et al.	N/A	N/A
2010/0144310	12/2009	Bedingfield	N/A	N/A
2010/0151866	12/2009	Karpov et al.	N/A	N/A
2010/0153781	12/2009	Hanna	N/A	N/A
2010/0167696	12/2009	Smith et al.	N/A	N/A
2010/0177663	12/2009	Johansson et al.	N/A	N/A
2010/0183132	12/2009	Satyavolu et al.	N/A	N/A
2010/0188975	12/2009	Raleigh	N/A	N/A
2010/0188990	12/2009	Raleigh	N/A	N/A
2010/0188992	12/2009	Raleigh	N/A	N/A
2010/0188994	12/2009	Raleigh	N/A	N/A
2010/0190469	12/2009	Vanderveen et al.	N/A	N/A
2010/0191576	12/2009	Raleigh	N/A	N/A
2010/0191612	12/2009	Raleigh	N/A	N/A
2010/0191846	12/2009	Raleigh	N/A	N/A

2010/0192170	12/2009	Raleigh	N/A	N/A
2010/0192212	12/2009	Raleigh	N/A	N/A
2010/0195503	12/2009	Raleigh	N/A	N/A
2010/0197268	12/2009	Raleigh	N/A	N/A
2010/0198698	12/2009	Raleigh et al.	N/A	N/A
2010/0198939	12/2009	Raleigh	N/A	N/A
2010/0222024	12/2009	Sigmund et al.	N/A	N/A
2010/0235329	12/2009	Koren et al.	N/A	N/A
2010/0241544	12/2009	Benson et al.	N/A	N/A
2010/0248719	12/2009	Scholaert	N/A	N/A
2010/0284327	12/2009	Miklos	N/A	N/A
2010/0284388	12/2009	Fantini et al.	N/A	N/A
2010/0287599	12/2009	He et al.	N/A	N/A
2010/0311402	12/2009	Srinivasan et al.	N/A	N/A
2010/0325420	12/2009	Kanekar	N/A	N/A
2011/0004917	12/2010	Saisa et al.	N/A	N/A
2011/0013569	12/2010	Scherzer et al.	N/A	N/A
2011/0019574	12/2010	Malomsoky et al.	N/A	N/A
2011/0081881	12/2010	Baker et al.	N/A	N/A
2011/0082790	12/2010	Baker et al.	N/A	N/A
2011/0088025	12/2010	Basmov	717/170	G06F 8/61
2011/0110309	12/2010	Bennett	N/A	N/A
2011/0126141	12/2010	King et al.	N/A	N/A
2011/0130119	12/2010	Gupta et al.	N/A	N/A
2011/0145920	12/2010	Mahaffey et al.	N/A	N/A
2011/0159818	12/2010	Scherzer et al.	N/A	N/A
2011/0173678	12/2010	Kaippallimalil et al.	N/A	N/A
2011/0177811	12/2010	Heckman et al.	N/A	N/A
2011/0182220	12/2010	Black et al.	N/A	N/A
2011/0185202	12/2010	Black et al.	N/A	N/A
2011/0244837	12/2010	Murata et al.	N/A	N/A
2011/0249668	12/2010	Milligan et al.	N/A	N/A
2011/0264923	12/2010	Kocher et al.	N/A	N/A
2011/0277019	12/2010	Pritchard, Jr.	N/A	N/A
2012/0011017	12/2011	Wolcott et al.	N/A	N/A
2012/0020296	12/2011	Scherzer et al.	N/A	N/A
2012/0124647	12/2011	Simula	709/217	H04L 63/0815
2012/0144025	12/2011	Melander et al.	N/A	N/A
2012/0166364	12/2011	Ahmad et al.	N/A	N/A
2012/0185636	12/2011	Leon et al.	N/A	N/A
2012/0196644	12/2011	Scherzer et al.	N/A	N/A
2012/0236760	12/2011	Ionescu et al.	N/A	N/A
2012/0238287	12/2011	Scherzer	N/A	N/A
2013/0029653	12/2012	Baker et al.	N/A	N/A
2013/0058274	12/2012	Scherzer et al.	N/A	N/A
2013/0065555	12/2012	Baker et al.	N/A	N/A
2013/0072177	12/2012	Ross et al.	N/A	N/A
2013/0084835	12/2012	Scherzer et al.	N/A	N/A
2013/0144789	12/2012	Aaltonen et al.	N/A	N/A
2013/0165075	12/2012	Rishy-Maharaj et al.	N/A	N/A
2013/0225151	12/2012	King et al.	N/A	N/A
2013/0326356	12/2012	Zheng et al.	N/A	N/A
2014/0073291	12/2013	Hildner et al.	N/A	N/A
2014/0099916	12/2013	Mallikarjunan	455/406	H04W 8/20
2014/0241342	12/2013	Constantinof	N/A	N/A
2015/0181628	12/2014	Haverinen et al.	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
2688553	12/2007	CA	N/A
1310401	12/2000	CN	N/A
1345154	12/2001	CN	N/A
1508734	12/2003	CN	N/A
1538730	12/2003	CN	N/A
1567818	12/2004	CN	N/A
101035308	12/2005	CN	N/A
1801829	12/2005	CN	N/A
1802839	12/2005	CN	N/A
1889777	12/2005	CN	N/A
101155343	12/2005	CN	N/A
1867024	12/2005	CN	N/A
1878160	12/2005	CN	N/A
1937511	12/2006	CN	N/A
101123553	12/2006	CN	N/A
101080055	12/2006	CN	N/A

101115248	12/2007	CN	N/A
101127988	12/2007	CN	N/A
101183958	12/2007	CN	N/A
101335666	12/2007	CN	N/A
101341764	12/2008	CN	N/A
101815275	12/2009	CN	N/A
1098490	12/2000	EP	N/A
1247411	12/2001	EP	N/A
1289326	12/2002	EP	N/A
1463238	12/2003	EP	N/A
1503548	12/2004	EP	N/A
1545114	12/2004	EP	N/A
1739518	12/2006	EP	N/A
1772988	12/2006	EP	N/A
1850575	12/2006	EP	N/A
1887732	12/2007	EP	N/A
1942698	12/2007	EP	N/A
1978772	12/2007	EP	N/A
2007065	12/2007	EP	N/A
2026514	12/2008	EP	N/A
3148713	12/2000	JP	N/A
2005339247	12/2004	JP	N/A
2006041989	12/2005	JP	N/A
2006155263	12/2005	JP	N/A
2006197137	12/2005	JP	N/A
2006344007	12/2005	JP	N/A
2007318354	12/2006	JP	N/A
2008301121	12/2007	JP	N/A
2009111919	12/2008	JP	N/A
2009212707	12/2008	JP	N/A
2009218773	12/2008	JP	N/A
2009232107	12/2008	JP	N/A
20040053858	12/2003	KR	N/A
100958566	12/2009	KR	N/A
1998058505	12/1997	WO	N/A
1999027723	12/1998	WO	N/A
1999065185	12/2000	WO	N/A
0208863	12/2001	WO	N/A
2002045315	12/2001	WO	N/A
2002067616	12/2001	WO	N/A
2002093877	12/2001	WO	N/A
03017065	12/2002	WO	N/A
2003014891	12/2002	WO	N/A
2003017063	12/2002	WO	N/A
2003017065	12/2002	WO	N/A
2003058880	12/2002	WO	N/A
2004028070	12/2003	WO	N/A
2004064306	12/2003	WO	N/A
2004095753	12/2004	WO	N/A
2005008995	12/2004	WO	N/A
2005053335	12/2004	WO	N/A
2005083934	12/2004	WO	N/A
2006004467	12/2005	WO	N/A
2006004784	12/2005	WO	N/A
2006012610	12/2005	WO	N/A
2006050758	12/2005	WO	N/A
2006077481	12/2005	WO	N/A
2006093961	12/2005	WO	N/A
2006120558	12/2005	WO	N/A
2006130960	12/2005	WO	N/A
2007001833	12/2006	WO	N/A
2007014630	12/2006	WO	N/A
2007018363	12/2006	WO	N/A
2007053848	12/2006	WO	N/A
2007068288	12/2006	WO	N/A
2007097786	12/2006	WO	N/A
2007107701	12/2006	WO	N/A
2007120310	12/2006	WO	N/A
2007124279	12/2006	WO	N/A
2007126352	12/2006	WO	N/A
2007129180	12/2006	WO	N/A
2007133844	12/2006	WO	N/A
2004077797	12/2007	WO	N/A
2008017837	12/2007	WO	N/A
2008051379	12/2007	WO	N/A

2008066419	12/2007	WO	N/A
2008080139	12/2007	WO	N/A
2008080430	12/2007	WO	N/A
2008099802	12/2007	WO	N/A
2009002949	12/2007	WO	N/A
2009008817	12/2008	WO	N/A
2009002949	12/2008	WO	N/A
2006073837	12/2008	WO	N/A
2007069245	12/2008	WO	N/A
2009091295	12/2008	WO	N/A
2010088413	12/2009	WO	N/A
2010128391	12/2009	WO	N/A
2010128391	12/2010	WO	N/A
2011002450	12/2010	WO	N/A

OTHER PUBLICATIONS

Rivadeneyra et al., “A communication architecture to access data services through GSM,” San Sebastian, Spain, 1998. cited by applicant
Ruckus Wireless—White Paper; “Smarter Wi-Fi for Mobile Operator Infrastructures” 2010. cited by applicant
Sabat, “The evolving mobile wireless value chain and market structure,” Nov. 2002. cited by applicant
Sadeh et al., “Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application,” ISR School of Computer Science, Carnegi
Schiller et al., “Location-Based Services,” The Morgan Kaufmann Series in Data Management Systems, 2004. cited by applicant
Sharkey, “Coding for Life—Battery Life, That Is,” May 27, 2009. cited by applicant
Steglich, Stephan, “I-Centric User Interaction,” Nov. 21, 2003. cited by applicant
Sun et al., “Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm,” Dept. of El
Oulu, Finland, 2004. cited by applicant
Van Eijk, et al., “GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage,” Jul. 1, 2002. cited by applicant
VerizonWireless.com news, “Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaper
Solution,” Aug. 18, 2008. cited by applicant
Windows7 Power Management, published Apr. 2009. cited by applicant
Wireless Broadband Alliance, “WISPr 2.0, Apr. 8, 2010”; Doc. Ref. No. WBA/RM/WISPr, Version 01.00. cited by applicant
Zhu et al., “A Survey of Quality of Service in IEEE 802.11 Networks,” IEEE Wireless Communications, Aug. 2004. cited by applicant
“Ads and movies on the run,” the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008. cited by applicant
“ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example,” Document ID 70917, Jan. 10, 2008. cited by applicant
“Communication Concepts for Mobile Agent Systems,” by Joachim Baumann et al.; Inst. of Parallel and Distributed High-Performance Systems, Univ. of Stu
applicant
“End to End QoS Solution for Real-time Multimedia Application;” Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang We
Normal College, Zhan jiang, Guangdong 524048, China. cited by applicant
“Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices,” The Mobile Internet, Boston, MA, Feb. 2008.
“The Construction of Intelligent Residential District in Use of Cable Television Network,” Shandong Science, vol. 13, No. 2, Jun. 2000. cited by applicant
3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for E
Network (E-UTRAN) Access,” Release 8, Document No. 3GPP TS 23.401, V8.4.0, Dec. 2008. cited by applicant
3rd Generation Partnership Project, “Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture,” Release 8, Docu
cited by applicant
Accuris Networks, “The Business Value of Mobile Data Offload—a White Paper”, 2010. cited by applicant
Ahmed et al., “A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and Its Performance,” BenQ Mobile, Munich Germa
2006. cited by applicant
Alonistioti et al., “Intelligent Architectures Enabling Flexible Service Provision and Adaptability,” 2002. cited by applicant
Amazon Technologies, Inc., “Kindle™ User's Guide,” 3rd Edition, Copyright 2004-2009. cited by applicant
Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009. cited by applicant
Anton, B. et al., “Best Current Practices for Wireless Internet Service Provider (WISP) Roaming”; Release Date Feb. 2003, Version 1.0; Wi-Fi Alliance—Wire
Blackberry Mobile Data System, version 4.1, Technical Overview, 2006. cited by applicant
Byrd, “Open Secure Wireless,” May 5, 2010. cited by applicant
Chandrasekhar et al., “Ferntocell Networks: A Survey,” Jun. 28, 2008. cited by applicant
Chaouchi et al., “Policy Based Networking in the Integration Effort of 4G Networks and Services,” 2004 IEEE. cited by applicant
Cisco Systems, Inc., “Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2—Overview of GSM, GPRS, and UMTS,” Nov. 4, 2008. cited by applicant
Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007. cited by applicant
Dikaiakos et al., “A Distributed Middleware Infrastructure for Personalized Services,” Nov. 24, 2003. cited by applicant
Dixon et al., Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), Aug. 2007. cited by applicant
Droid Wall 1.3.7 description Apr. 28, 2010 obtained from https://www.freewarelovers.com/android/apps/droid-wall. cited by applicant
Ehnert, “Small application to monitor IP trafic on a Blackberry—1.01.03”, Mar. 27, 2008; http://www.ehnert.net/MiniMoni/. cited by applicant
European Commission, “Data Roaming Tariffs—Transparency Measures,” obtained from EUROPA—Europe's Information Society Thematic Portal website,
“http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm.” cited by applicant
Farooq et al., “An IEEE 802.16 WiMax Module for the NS-3 Simulator,” Mar. 2-6, 2009. cited by applicant
Fujitsu, “Server Push Technology Survey and Bidirectional Communication in HTTP Browser,” Jan. 9, 2008 (JP). cited by applicant
Han et al., “Information Collection Services for Qos-Aware Mobile Applications,” 2005. cited by applicant
Hartmann et al., “Agent-Based Banking Transactions & Information Retrieval—What About Performance Issues?” 1999. cited by applicant
Hewlett-Packard Development Company, LP, “IP Multimedia Services Charging,” white paper, Jan. 2006. cited by applicant
Hossain et al., “Gain-Based Selection of Ambient Media Services in Pervasive Environments,” Mobile Networks and Applications. Oct. 3, 2008. cited by appl
Jing et al., “Client-Server Computing in Mobile Environments,” GTE Labs. Inc., Purdue University, ACM Computing Surveys, vol. 31, No. 2, Jun. 1999. cite
Kasper et al., “Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing,” Fraunhofer-Institute f
Darmstadt, Germany; ICACT 2008. cited by applicant
Kassar et al., “An overview of vertical handover decision strategies in heterogeneous wireless networks,” ScienceDirect, University Pierre & Marie Curie, Par
Kim, “Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits,” San Francisco Chronicle, Aug. 21, 2006. cited by applica
Knight et al., “Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts,” IEEE Communications Magazine, Jun. 2004. cite
Koutsopoulou et al., “Charging, Accounting and Billing Management Schemes in Mobile Telecommunication Networks and the Internet,” IEEE Communicati

6, No. 1. cited by applicant
Koutsopoulou et al., “Middleware Platform for the Support of Charging Reconfiguration Actions,” 2005. cited by applicant
Kuntze et al., “Trustworthy content push,” Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE. cited by a
Kyriakakos et al., “Ubiquitous Service Provision in Next Generation Mobile Networks,” Proceedings of the 13th IST Mobile and Wireless Communications S
applicant
Li, Yu, “Dedicated E-Reading Device: The State of the Art and The Challenges,” Scroll, vol. 1, No. 1, 2008. cited by applicant
Loopt User Guide, metroPCS, Jul. 17, 2008. cited by applicant
Muntermann et al., “Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen,” Chair of Mobile Commer
Frankfurt, 2004. cited by applicant
NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007. cited by applicant
Nilsson et al., “A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA,” Feb. 2006. cited by applicant
Nuzman et al., “A compund model for TCP connection arrivals for LAN and WAN applications,” Oct. 22, 2002. cited by applicant
Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C. cited by applicant
Oppliger, Rolf, “Internet Security: Firewalls and Bey,” Communications of the ACM, May 1997, vol. 40. No. 5. cited by applicant
Rao et al., “Evolution of Mobile Location-Based Services,” Communication of the ACM, Dec. 2003. cited by applicant
Richtel, “Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition],” National Post, Canada, Oc
Arm TrustZone Microprocessor Report, dated Aug. 25, 2033. cited by applicant
Arm TrustZone Paper, TrustZone: Integrated Hardware and Software Security, dated Jul. 2004. cited by applicant
Limont Prosecution History Excerpt, U.S. Appl. No. 11/171,850, filed Jun. 30, 2005. cited by applicant
Plaintiff's Infringement Contention in Case No. 6:23-CV-00352-JRG-RSP, *Headwater Research LLC* v. *Cellco Partnership, d/b/a Verizon Wireless, Verizon C*
28, 2023). cited by applicant
IPR2024-00809 Petition for Inter Partes Review of U.S. Pat. No. 9,198,042, filed Apr. 19, 2024. cited by applicant
IPR2024-00809 File History of Inter Partes Review of U.S. Pat. No. 9,198,042, filed Apr. 19, 2024. cited by applicant
Federal Communications Commission (FCC) Regulation (2010), available at, https://www.govinfo.gov/content/pkg/FR-2010-06-22/pdf/2010-15073.pdf. cite
Samsung Galaxy SII Mobile Phone User Manual (2011), available at https://ringtones.specialtyansweringservice.net/wpcontent/uploads/2014/08/manuals/sam
IPhone User Guide for iPhone OS 3.1 Software (2009), available at https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf
Architecture and Enablers for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks (2009), available at
https://www.researchgate.net/publication/224371987_Architecture_and_Enablers_for_Optimized_Radio_Resource_Usage_in_Heterogeneous_Wireless_Acce
cited by applicant
Characterizing Radio Resource Allocation for 3G Networks (2010), available at https://www.cs.columbia.edu/~lierranli/coms6998-7Spring2014/papers/RRC3
Operating System Implications of Fast, Cheap, Non-Volatile Memory (2011), available at https://www.usenix.org/legacy/events/hotos11/tech/final_files/Baile
IPod touch User Guide for iOS 5.1 Software (2012), available at https://cdsassets.apple.com/live/6GJYWVAV/user/ma1627_ipod_touch_ios5_user_guide.pdf
Samsung Galaxy SIII 4G LTE Smartphone User Manual (2013), available at
https://downloadcenter.samsung.com/content/UM/202101/20210101045744723/ATT_SGHI747_Galaxy_SIII_English_User_Manual_KK_NE4_F1.pdf. cited
Jacob et al., Memory Systems: Cache, DRAM, Disk (2007). cited by applicant
European Telecommunications Standards Institute (ETSI) Technical Specification 23.003 v8.11.0 (2011), available at
https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/08.11.00_60/ts_123003v081100p.pdf. cited by applicant
Control Servers in the Core Network (2000), available at https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1247211968f9167dbc5e7ea896b
Wireless Application Protocol (WAP) Architectural Overview (2001), available at https://www.openmobilealliance.org/release/Push/V2_1-20051122-C/WAP-
applicant
Complaint for Patent Infringement in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd. et al*., 2-24-cv-00228 (EDTX) (Apr. 3, 2024). cited by applic
Docket Control Order in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd. et al*., Case No. 2:24-cv-00228 (EDTX) (Aug. 9, 2024). cited by applican
Disclosure of Asserted Claims and Infringement Contentions in *Headwater Research LLC* v. *Samsung Electronics Co., Ltd. et al*., 2-24-cv-00228 (EDTX) (Ju
File History of IPR2025-00483, filed Feb. 10, 2025. cited by applicant
Petition for Inter Partes Review in IPR2025-00483, filed Feb. 10, 2025. cited by applicant
File History of IPR2025-00484, filed Feb. 10, 2025. cited by applicant
Petition for Inter Partes Review in IPR2025-00484, filed Feb. 10, 2025. cited by applicant
Complaint, *Headwater Research LLC* v. *Samsung Elec-tronics Co., Ltd. et al*, 2-24-cv-00228, E.D. Tex., filed Apr. 3, 2024. cited by applicant
(Excerpts) Smith, et al., 2005. “Virtual Machines: Versa-tile Platforms for Systems and Processes,” Elsevier, Inc, 2005, ISBN 1-55860-910-5. cited by applica
(Excerpts) Telecom Dictionary, Athos Publishing, 2007. cited by applicant
(Excerpts) Eberspächer, Jörg (2001). GSM Switching, Services and Protocols, Second Edition. John Wiley & Sons Ltd. ISBN: 978-0-470-85394-8. cited by ap
3rd Generation Partnership Project; Technical Specifica-tion Group Terminals; “Characteristics of the USIM application” (Release 7), 3GPP TS 31.102 V7.0.0
Kasper, et al., Feb. 2008. “Subscriber authentication in cellular networks with trusted virtual sims.” In 2008 10th International Conference on Advanced Comm
IEEE. cited by applicant
TCG Mobile Reference Architecture, version 1.0, Revi-sion 1, Jun. 12, 2007. (“TCG Mobile Reference Archi-tecture”). cited by applicant
TCG Mobile Trusted Module Specification, version 1.0, Revision 6, Jun. 26, 2008. (“TCG Mobile Trusted Mod-ule Specification”). cited by applicant
Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp. 10-21. cited by applicant
David K. Gifford. 1982. Cryptographic sealing for infor-mation secrecy and authentication. Commun. ACM 25, 4 (Apr. 1982), 274-286. https://doi.org/10.114
Jansen, Wayne A. and Richard P. Ayers. “Forensic Tools for Mobile Phone Subscriber Identity Modules.” J. Digit. Forensics Secur. Law 1 (2006): 75-94. cited
National Institute of Standards and Technology. 2001. Security Requirements for Cryptographic Modules, downloaded from the Internet at https://nvl-pubs.nis
Dec. 5, 2024. cited by applicant
Verma, et. al., (2002). Policy-based management of con-tent distribution networks. IEEE network, 16(2), 34-39. cited by applicant
Lobo, et al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298. cited by applicant
Westerinen, et al., IETF RFC 3198, Terminology for Pol-icy-Based Management, Nov. 2001, downloaded from the Internet on May 27, 2024. cited by applica
(Excerpts) Keith Mayes and Konstantinos Markantona-kis. 2008. Smart Cards, Tokens, Security and Applica-tions (1st. ed.). cited by applicant
(Excerpts) Gasser, Morrie. Building a Secure Computer System. New York, NY: Van Nostrand Reinhold, 1988. (“Gasser”). cited by applicant
(Excerpts) Malhotra, Ravi. 2002. IP Routing: Help for Network Administrators. O'Reilly Media. ISBN: 978-0-596-00275-0 (“Malhotra”). cited by applicant
Jude, Michael. “Policy-Based Management: Beyond the Hype.” Business Communications Review 31.3 (2001): 52-56. (“Jude”). cited by applicant
Merkle, Ralph C. 1978. Secure communications over in-secure channels. Commun. ACM 21, 4 (Apr. 1978), 294-299. https://doi.org/10.1145/359460.359473
ARM. 2004. PrimeCell Infrastructure AMBA 3 TrustZone Protection Controller (BP147) Revision: r0p0 Technical Overview, downloaded from the Internet a
vice.arm.com/static/5e9565afc8052b1608762aae%3Fto-ken%3D&ved=2ahUKEwiZq56_3pGKAxVUCnkGHcR9OGIQFnoECAwQAQ&usg=AOv-Vaw2PG
by applicant
Network Associates, Inc. 1999. PGP, Version 6.5.1. An Introduction to Cryptography. cited by applicant
Stuart E. Madnick and John J. Donovan. 1973. Applica-tion and analysis of the virtual machine approach to information system security and isolation. In Proc
systems. Associa-tion for Computing Machinery, New York, NY, USA, 210-224. https://doi.org/10.1145/800122.803961. cited by applicant

European Telecommunications Standards Institute. 1998. Terrestrial Trunked Radio (TETRA); Security Aspects; Subscriber Identity Module to Mobile Equipr
(Nov. 1998), downloaded from the Internet at https://www.etsi.org/de-liver/etsi_i_ets/300800_300899/300812/01_20_9826/ets_300812e01c.pdf on Dec. 12, 2
IETF RFC 1122, Requirements for Internet Hosts—Com-munication Layers, Oct. 1989, downloaded from the internet at https://datatracker.ietf.org/doc/html/r
IETF RFC 793, Transmission Control Protocol, Sep. 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc793.txt on Dec. 11, 2024. cited by appl
Smith, et al., 2005. "The architecture of virtual machines. Computer," 38(5). cited by applicant
ISO/IEC 7498-1, "Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model," downloaded from the internet at htt
loads/s020269e.pdf on Jan. 10, 2025. cited by applicant
Gonçalves, et al., Oct. 2009. A graphical user inter-face for policy composition in CIM-SPL. In 2009 Inter-national Conference on Ultra Modern Telecommun
applicant
Agrawal, et. al., May 2007. Issues in designing a policy language for distributed management of IT infrastruc-tures. In 2007 10th IFIP/IEEE International Syn
30-39). IEEE. cited by applicant
File History of IPR2025-00482, filed Jan. 28, 2025. cited by applicant
Petition for Inter Partes Review in IPR2025-00482, filed Jan. 28, 2025. cited by applicant

---

Primary Examiner: Miller; Brandon J

Attorney, Agent or Firm: Farjami & Farjami LLP

Background/Summary

BACKGROUND OF THE INVENTION

(1) With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access). LTE (Long Term Evolution). WiMax (Worldwide Interoperability for Microwave Access), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

(2) Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

(1) Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

(2) FIG. **1** illustrates a wireless network architecture for providing device assisted services (DAS) install techniques in accordance with some embodiments.

(3) FIG. **2** illustrates another wireless network architecture for providing DAS install techniques in accordance with some embodiments.

(4) FIG. **3** illustrates a flow diagram for DAS install techniques in accordance with some embodiments.

(5) FIG. **4** illustrates another flow diagram for DAS install techniques in accordance with some embodiments.

(6) FIG. **5** illustrates another flow diagram for DAS install techniques in accordance with some embodiments.

(7) FIG. **6** illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

(8) FIG. **7** illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

(9) FIG. **8** illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

(10) FIG. **9** is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

(11) FIG. **10** illustrates a network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments.

DETAILED DESCRIPTION

(12) The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

(13) A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

(14) Device assisted services (DAS) install techniques are provided in accordance with some embodiments. In some embodiments. DAS install techniques for providing service processors for mobile devices are provided. In some embodiments, DAS install techniques for downloading/installing new and/or updated service processors for mobile devices are provided. In some embodiments. DAS install techniques for providing verified service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing secured service processors for mobile devices are provided. In some embodiments, DAS install techniques include providing a generic first version service processor for downloading and installing a second version service processor. These and other DAS install techniques are described herein with respect to

various embodiments.
(15) In some embodiments, a virtual network overlay includes a device service processor, a network service controller and a control plane communication link to manage various aspects of device based network service policy implementation. In some embodiments, the virtual network overlay networking solution is applied to an existing hierarchical network (e.g., for wireless services), and in some embodiments, is applied to simplify or flatten the network architecture as will be further described below. In some embodiments, the large majority of the complex data path network processing required to implement the richer service management objectives of existing hierarchical networks (e.g., for wireless services) are moved into the device, leaving less data path processing required in the edge network and in some cases even less in the core network. Because the control plane traffic between the service control servers and the device agents that implement service policies can be several orders of magnitude slower than the data plane traffic, service control server network placement and back-haul infrastructure is much less performance sensitive than the data plane network. In some embodiments, as described further below, this architecture can be overlaid onto all the important existing access network architectures used today. In some embodiments, this architecture can be employed to greatly simplify core access network routing and data plane traffic forwarding and management. For example, in the case of wireless networks, the incorporation of device assisted service policy implementation architectures can result in base stations that directly connect to the Internet local loop and the data traffic does not need to be concentrated into a dedicated core network. This results, for example, in a large reduction in backhaul cost, core network cost and maintenance cost. These cost savings can be re-deployed to purchase and install more base stations with smaller cells, which results in higher data capacity for the access network leading to better user experience, more useful applications and lower service costs. This flattened networking architecture also results in latency reduction as fewer routes are needed to move traffic through the Internet. In some embodiments, the present invention provides the necessary teaching to enable this powerful transformation of centralized network service architectures to a more distributed device based service architectures.
(16) FIG. **6** illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments. As shown. FIG. **6** includes a 4G/3G/2G HSPA/Transport access network operated by a central provider and two mobile virtual network operator (MVNO) networks **210** operated by two MVNO partners. In some embodiments, the central provider can offer improved service capabilities using a conventional UMTS network. As shown, the base stations **125** do not connect directly to the Internet **120**, and instead the base stations **125** connect to the conventional UMTS network. However, the service processor **115** still connects through the secure control plane link to service controller **122**. In some embodiments, the data plane traffic is backhauled across the various UMTS network routers and gateways as is the control plane traffic, and the Internet protocol detail records (IPDRs) are obtained from the access network AAA server **121**. Referring now to the 4G/3G/2G HSPA/Transport access network as shown in FIG. **6**, the LTE/HSPA and HSPA/GPRS base stations/nodes **125** are in communication with 4G/3G/2G Service/Serving GPRS Support Nodes (SGSNs) cluster **410** via a radio access network **405**, which are in communication with 4G/3G/2G Gateway GPRS Support Nodes (GGSNs) cluster **420** via an access transport network **415** (e.g., a GPRS-IP network), which are then in communication with central provider core network **110**.
(17) As shown in FIG. **6**, service usage data store **118** is a functional descriptor for a network level service usage information collection and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks in the figure (e.g., RAN, transport and/or core networks). As shown in FIG. **6**, service usage **118** is an isolated function connected to the central provider core network **110** and the intention of this depiction is to facilitate all the possible embodiments for locating the service usage **118** function. In some UMTS network embodiments, the service usage **118** function is located or partially located in the GGSN gateway (or gateway cluster) **420**. In some embodiments, service usage **118** functionality is located or partially located in the SGSN gateway (or gateway cluster) **410**. In some embodiments, service usage **118** functionality is located or partially located in the equipment cluster that includes the AAA **121** and/or the mobile wireless center **132**. In some embodiments, service usage **118** functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station **125** in FIG. **6**. In some embodiments, service usage **118** functionality is located or partially located in a networking component in the transport network **415**, a networking component in the core network **110**, the billing system **123** and/or in another network component or function. This discussion on the possible locations for the network based service usage history logging and reporting function can be easily generalized by one of ordinary skill in the art (e.g., RAN Gateway **410** and/or Transport Gateway **420**), and this background will be assumed even if not directly stated in all discussion above and below.
(18) In some embodiments, a central provider provides open development services to MVNO. Master Value Added Reseller (MVAR) and/or Original Equipment Manufacturer (OEM) partners. In some embodiments, all three service providers, central provider service provider, MVNO #1 service provider and MVNO #2 service provider have service control and billing control of their own respective devices **100** through the unique pairing of the service processors **115** and service controllers **122**. For example, MVNO #1 and MVNO #2 can each have open development billing agreements with the central provider and each can own their respective billing systems **123**. As shown in FIG. **6**. MVNO #1 core network **210** is in communication with the central provider core network **110** via the Internet **120**, and MVNO #2 core network **210** is in communication with the central provider core network **110** via an alternate landline (LL)/VPN connection **425**. In some embodiments, the two MVNOs each offer completely different devices and/or services, and the devices and/or services also differ significantly from those offered by the central provider, and the service profiles are adapted as required to service the different devices and respective service offerings. In addition, the central billing system **123** allows all three service provider user populations to access ecommerce experiences from transaction provider partners operating transaction servers **134**, to choose central provider billing options that combine their third party transaction bills on their service provider bill, and each subscriber population can experience a service provider specified look and feel that is unique to the respective service provider even though the different user populations are interfacing to the same transaction servers and the transaction partners do not need to require significant custom development to provide the unique central billing and unique consistent user experience look and feel.
(19) In some embodiments, a central provider offers open network device and service developer services using one service controller server **122** (e.g., a service controller server farm) and allows the open development partners to lease server time and server tools to build their own service profiles. The central provider also provides service billing on behalf of services to the open development partners. For example, this reduces costs associated with setting up an MVNO network for the open development partners and does not require the partners to give up significant control or flexibility in device and/or service control.
(20) In some embodiments, virtual service provider (VSP) capabilities include making available to a third party service partner one or more of the following: (1) device group definition, control and security. (2) provisioning definition and execution, (3) ATS activation owner, (4) service profile definitions, (5) activation and ambient service definition. (6) billing rules definition, (7) billing process and branding controls, (8) bill by account settings. (9) service usage analysis capabilities by device, sub-group or group, (10) beta test publishing capabilities by device, sub-group or group, and (11) production publishing, fine tuning and re-publishing.
(21) FIG. **7** illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments. As shown, the service controller design, policy analysis, definition, test, publishing system **4835** is configured so that multiple “service group owners” (e.g., the service provider for certain smart phones) or “device group owners” (e.g., eReader devices for the eReader service provider(s)) or “user group owners” (e.g., IT for Company X for their employees' corporate mobile devices), collectively referred to as the “Virtual Service Provider” (VSP), are serviced with the same service controller infrastructure and the same (or substantially similar) service processor design from virtual service provider workstation server **4910** and/or virtual service provider remote workstation(s) **4920**. As shown, the virtual service provider remote workstation(s) **4920** communicates with the virtual service provider workstation server **4910** via VPN, leased line or secure Internet connections. The dashed lines shown in FIG. **7** are depicted to represent that, in some embodiments, the virtual service provider workstation server

4910 is networked with the service controller device control system **4825** and/or, in some embodiments, the service controller design, policy analysis, definition, test, publishing system **4835**. Based on the discussion herein, it will be apparent to one of ordinary skill in the art that the VSP workstation server **4910** can also be networked in various embodiments with billing system **123**. AAA server **121**, gateways **410** or **420**, or other network components to perform, for example, various network provisioning and activation related functions discussed herein for the device group assigned to one or more VSPs, or for other reasons as will be apparent to a given VSP embodiment.

(22) In some embodiments, the service controller functionality is partitioned for a VSP by setting up one or more secure workstations, secure portals, secure websites, secure remote software terminals and/or other similar techniques to allow the service managers who work for the VSP to analyze, fine tune, control or define the services they decide to publish to one or more groups of devices or groups of users that the VSP "owns." In some embodiments, the VSP "owns" such groups by virtue of a relationship with the central provider in which the VSP is responsible for the service design and profitability. In some embodiments, the central provider receives payment from the VSP for wholesale access services. In some embodiments, the VSP workstations **4910** and **4920** only have access to the service analysis, design, beta testing and publishing functions for the devices or users "owned" by the VSP. In some embodiments, the user or device base serviced by the central provider network is securely partitioned into those owned by the central provider, those owned by the VSP, and those owned by any other VSPs.

(23) In some embodiments, the VSP manages their devices from the VSP workstations **4910** and **4920** using device based service control techniques as described herein. In some embodiments, the VSP manages their devices from the VSP workstations **4910** and **4920** using device assisted and network based service control techniques as described herein. In some embodiments, the VSP manages their devices from the VSP workstations **4910** and **4920** using network based service control techniques (e.g., DPI techniques) as described herein.

(24) For example, this approach is particularly well suited for "open developer programs" offered by the central providers in which the central provider brings in VSPs who offer special value in the devices or service plans, and using this approach, neither the central provider nor the VSP needs to do as much work as would be required to set up a conventional MVNO or MVNE system, which often requires some degree of customization in the network solution, the billing solution or the device solution for each new device application and/or service application that is developed and deployed. In some embodiments, the service customization is simplified by implementing custom policy settings on the service processor and service controller, and the custom device is quickly brought onto the network using the SDK and test/certification process. In some embodiments, the VSP functionality is also offered by an entity other than the central provider. For example, an MVNE entity can develop a wholesale relationship with one or more carriers, use the service controller to create the VSP capabilities, and then offer VSP services for one network or for a group of networks. In some embodiments, the service customization is simplified by implementing custom policy settings through the VSP embodiments on the network equipment, including, in some embodiments, service aware or DPI based network equipment that has a relatively deep level of service activity control capability. For example, using the embodiments described herein, and possibly also including some of the activation and provisioning embodiments, it is possible to efficiently design and implement custom ambient service plans that are different for different types of devices, different OEMs, different VSPs, different distributors, or different user groups all using the same general infrastructure, whether the service control policy implementation is accomplished primarily (or exclusively) with networking equipment (network) based service control, primarily (or exclusively) with device based service control or with a combination of both (e.g., hybrid device and network based service control).

(25) As discussed herein, various VSP embodiments for performing one or more of analyzing traffic usage and defining, managing service profiles or plans, dry lab testing service profiles or plans, beta testing service profiles or plans, fine tuning service profiles or plans, publishing service profiles or plans, or other policy related settings can involve programming settings in the network equipment and/or programming settings or software on the device. For example, as discussed herein, the service processor settings are controlled by the service controller, which can be partitioned to allow groups of devices to be controlled. As another example, equipment in the network involved with network based service control, such as DPI based gateways, routers or switches, can similarly be programmed to utilize various VSP embodiments to implement that portion of the service profile (or service activity usage control) that is controlled by network level functions, and it will be appreciated that substantially all or all of the service activity control for certain embodiments can be accomplished with the network functions instead of the device. Continuing this example, just as the device service processor settings control functions of the service processor can have a group of devices that are partitioned off and placed under the control of a VSP, various VSP control embodiments can partition off a group of devices that have service usage activity controlled by the networking equipment, including, in some embodiments, sophisticated service aware DPI based service control equipment, to achieve similar objectives. It will be appreciated that the discussion herein regarding service controller design, policy analysis, test, publishing 4835, and the discussion regarding device group, user group and other VSP related embodiments, should be understood as applicable to various embodiments described in view of device based services control, control assistance and/or monitoring, or network based services control, control assistance and/or monitoring, or a combination of device based services control, control assistance and/or monitoring and network based services control, control assistance and/or monitoring. The various embodiments described herein related to service activation and provisioning also make apparent how the programming of network equipment service control, service control assistance and/or monitoring can be implemented prior to and following activation of the device. It will also be appreciated that the VSP capabilities described herein can also be applied to those devices that have services controlled by, provided by and/or billed by the central provider, so these techniques can be applied to central provider service embodiments, MVNO embodiments and other embodiments.

(26) In some embodiments, an SDK is provided that allows developers, such as device manufacturers, service providers, MVNO. MVNE and/or VSPs, to develop various service processors (e.g., different versions of the service processor **115**) for various devices (e.g., various types of devices **100**) and corresponding service controllers (e.g., different versions of the service controller **122**) for various types of services and network environments. For example, a device manufacturer can use the SDK to develop a new service processor for their new device (e.g., mobile phone, PDA, eBook reader, portable music device, computer, laptop, netbook, or any other network accessible device). The device manufacturer can also preload/preinstall their new service processor on their new devices. In this example, users of the new device would then be able to utilize the new device to access network based services using the new service processor, which communicates with the deployed new service controller, as similarly discussed herein in various embodiments. For example, the device can be preinstalled with the new service processor to provide ambient services, as similarly discussed herein in various embodiments. For example, the SDK can allow for substantially similar service processors to be installed on similar and/or different devices thereby minimizing any unnecessary differences between service processor elements for device assisted services. In some embodiments, for ambient services for a group of devices, or devices associated with a certain service provider, a set of numbers (e.g., dummy numbers) can be assigned for use for attempting access via the access network using a new device that is not yet otherwise subscribed for service. In some embodiments, the set of (dummy) numbers used for ambient access by the device can also be used for associating the device with a service provider or a type of device (e.g., eReader or some other type of network accessible device), and upon activation, the service provider assigns a real number for the activated device (e.g., which can be provided at the time of manufacture of the device, point of sale of the device, or after the point of sale of the device, such as upon activation of the device). For example, ambient access of the device can use the device ID. SIM ID, assigned phone (real or dummy) number, and/or other information associated with the device for assigning appropriate service control and service policy/profile for the device.

(27) In some embodiments, the service processor **115** is distributed as an SDK to any device that the central provider or the VSP desires to offer services with so that the service processor **115** can be efficiently designed or adapted by the device OEM, ODM or manufacturer for operation on the service network. In some embodiments, the SDK includes either a complete set of service processor **115** agent software designed for and/or tested for the OS (Operating System) and processor set being used on the device, or a mature reference design for the OS and processor set being used on the

device, or a less mature reference design (potentially for the same OS and/or processor set or a different OS and/or processor set being used on the device) that the OEM (Original Equipment Manufacturer) ports to the desired OS or processor set, or a basic set of example software programs that the OEM or ODM (Original Design Manufacturer) can use to develop software compatible with the service, or a set of specifications and descriptions (possibly forming an interoperability standard) of how to design the software to be compatible with the service. In some embodiments, the SDK includes a set of OEM lab test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the SDK includes a set of network certification test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the certification procedures are approved for testing by the OEM, the central provider, the VSP and/or a trusted third party. For example, the central provider is typically in control of the SDK and the test procedures, but others can be in control. In some embodiments, the test procedures are at least in part common across multiple central provider networks. In some embodiments, the SDK concept is extended to include one or more modem modules where one or more of the SDK embodiments described above is combined with a standard reference design or a standard hardware sales package for one or more modems so that the entire package forms a turn-key product that allows a device manufacturer, central provider, VSP or other entity bring new devices or device applications onto the central provider network possibly in combination with other networks in a manner that requires less engineering time and resources and less network certification time and resources than would be required in some designs that do not use this standard SDK plus module approach. For example, the standard SDK plus module product embodiments can be pre-certified and tested with one or more central providers to further reduce development time and expense. The standard SDK plus module embodiments can also use a multi-mode modem (e.g., modems based on a multimode CDMA, EVDO, UMTS, HSPA chipset as in the Gobi global multimode chipset product or modems based on other recently announced LTE plus HSPA chipsets, WiMax plus Wi-Fi chipsets or LTE plus EVDO chipsets) and a multi-mode connection manager agent so that the same SDK plus modem embodiment may satisfy a wide range of applications for many service providers around the world.

(28) In some embodiments, at the time of manufacture, the device is associated with an MVNO. For example, the MVNO can provide an ambient service that provides a service provider clearing house, in which the device can access a network in ambient access mode (e.g., a wholesale MVNO connection through the access network) for purposes of selecting a service provider (e.g., a VSP. MVNO or carrier). Based on the service provider selection, the device credentials and/or service processor are reprogrammed and/or new software is downloaded/installed to activate the device with the selected service provider, as described herein for provisioning the device and the account on that service provider network (e.g., the activation tracking service (ATS) can track such activation, for example, for revenue sharing purposes, as an activation incentive fee).

(29) In some embodiments ATS is implemented entirely in the network. At the time of manufacture or at sometime during device distribution, the device master agent programs a unique credential in the device that cannot be re-programmed or removed (or is difficult to re-program or remove) and that can be recognized and recorded by the network at the time of activation or at some other time. In this manner, even if other, possibly primary, device credentials are reprogrammed or removed, there will still be a credential that is associated with the device master agent. The ATS process can then be implemented by using a database search function to scan through the database of activated devices to form a list of devices that have been activated for the purpose of master agent reconciliation. Example credentials that can suffice are MEID, hardware MAC address, and/or serial number, that are picked up and recorded by the service provider or other service entity at time of activation or before or after activation.

(30) In some embodiments, the service processor **115** includes various components, such as device agents, that perform service policy implementation or management functions. In some embodiments, these functions include service policy or implementation verification, service policy implementation tamper prevention, service allowance or denial, application access control, traffic control, network access control services, various network authentication services, service control plane communication, device heartbeat services, service billing, transaction billing, simplified activation services and/or other service implementations or service policy implementations. It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice, that the functional lines can be re-drawn in any technically feasible way that the product designers see fit, and that the placing divisions on the naming and functional breakouts for device agents aids in understanding, although in more complex embodiments, for example, it can make sense to the product designer to break out device agent functionality specifications in some other manner in order to manage development specification and testing complexity and workflow.

(31) FIG. **8** illustrates a hardware diagram of a device **100** that includes a service processor **115** in accordance with some embodiments. As shown in FIG. **8**, the service processor **115** is stored in a non volatile memory **910** and a memory **920** of the device **100**. As will be appreciated by those of ordinary skill in the art, the present invention can operate with virtually any device architecture, and the device architectures discussed herein are examples of various implementations on certain devices (e.g., of different representations of device **100**).

(32) As shown in FIG. **8**, device **100** also includes a processor **930**, sometimes referred to as a CPU or central processor unit, an APU or application processor unit, a core processor, a computing device, or many other well known terms. In some embodiments, device **100** includes one or more processors and/or a multicore processor. As shown, processor **930** includes a sub-processor **935**. In some embodiments, processor **930** and/or sub-processor **935** are based on an architecture sometimes referred to as a complex instruction set computer or CISC, a reduced instruction set computer or RISC, a parallel processor, a combination of two or more architectures or any other processor architecture. In some embodiments, processor **930** has a design that is based on logic and circuitry from one or more standard design library or published architecture, or includes specialized logic and circuitry designed for a given device **100** or collection of such devices. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, one processor and/or sub-processor can have one architecture while another may have a somewhat different or completely different architecture. In some embodiments, one or more of the processors and/or sub-processors can have a general purpose architecture or instruction set, can have an architecture or instruction set that is partially general or partially specialized, or can have an instruction set or architecture that is entirely specialized. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, there can be a division of the functionality for one or more processors and/or sub-processors. For example, one or more processors and/or sub-processors can perform general operating system or application program execution functions, while one or more others can perform communication modem functions, input/output functions, user interface functions, graphics or multimedia functions, communication stack functions, security functions, memory management or direct memory access functions, computing functions, and/or can share in these or other specialized or partially specialized functions. In some embodiments, any processor **930** and/or any sub-processor **935** can run a low level operating system, a high level operating system, a combination of low level and high level operating systems, or can include logic implemented in hardware and/or software that does not depend on the divisions of functionality or hierarchy of processing functionality common to operating systems.

(33) As shown in FIG. **8**, device **100** also includes non-volatile memory **910**, memory **920**, graphics memory **950** and/or other memory used for general and/or specialized purposes. As shown, device **100** also includes a graphics processor **938** (e.g., for graphics processing functions). In some embodiments, graphics processing functions are performed by processor **930** and/or sub-processor **935**, and a separate graphics process **938** is not included in device **100**. As shown in FIG. **8**, device **100** includes the following modems: wire line modem **940**. WWAN modem **942**, USB modem **944**. Wi-Fi modem **946**, Bluetooth modem **948**, and Ethernet modem **949**. In some embodiments, device **100** includes one or more of these modems and/or other modems (e.g., for other networking/access technologies). In some embodiments, some or all of the functions performed by one or more of these modems are performed by the processor **930** and/or sub processor **935**. For example, processor **930** can implement some or all of certain WWAN functional aspects, such as the modem management, modem physical layer and/or MAC layer DSP, modem I/O, modem radio circuit interface, or other aspects of modem operation. In some embodiments, processor **930** as functionality discussed above is provided in a separate specialized processor as similarly shown with respect to the graphics and/or multimedia processor **938**.

(34) As also shown in FIG. **8**, device **100** includes an internal (or external) communication bus structure **960**. The internal communication bus structure **960** generally connects the components in the device **100** to one another (e.g., allows for intercommunication). In some embodiments, the

internal communication bus structure **960** is based on one or more general purpose buses, such as AMBA, AHP, USB, PCIe, GPIO, UART, SPI, I2C, Fire wire, DisplayPort, Ethernet, Wi-Fi, Bluetooth, Zigbee, IRDA, and/or any other bus and/or I/O standards (open or proprietary). In some embodiments, the bus structure is constructed with one or more custom serial or parallel interconnect logic or protocol schemes. As will be apparent to one of ordinary skill in the art, any of these or other bus schemes can be used in isolation and/or in combination for various interconnections between device **100** components.

(35) In some embodiments, all or a portion of the service processor **115** functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor **115** functions are implemented in hardware. In some embodiments, all or substantially all of the service processor **115** functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device **100**. FIG. **8** illustrates an embodiment in which service processor **115** is stored in device memory, as shown, in memory **920** and/or non-volatile memory **910**, or a combination of both. In some embodiments, it is advantageous to store or implement certain portions or all of service processor **115** in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor **115**. In some embodiments, service processor **115**, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory **930** can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor **115** software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor **115** software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader **1663** as discussed below (and as shown in FIG. **9**). In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board. In some embodiments, the service processor **115** which as shown in FIG. **8** is stored or implemented in non volatile memory **910** and memory **920**, can be implemented in part on other components in device **100**.

(36) FIG. **9** is a functional diagram illustrating a device based service processor **115** and a service controller **122** in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller **122** is connected to the Internet **120** and not directly to the access network **1610**. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As previously discussed, it is understood that the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, as discussed below in some embodiments, one or more of the policy implementation or service monitoring functions can be placed on one of the access modems located below the modem driver and modem bus in the communication stack as illustrated in certain figures and described herein. As discussed below, some simplified embodiment figures illustrate that not all the functions illustrated in all the figures are necessary for many designs, so a product/service designer can choose to implement those functions believed to be most advantageous or sufficient for the desired purposes and/or environment. The functional elements shown in FIG. **9** are described below.

(37) In some embodiments, the service control device link **1691** facilitates another important function, which is the download of new service processor software elements, revisions of service processor software elements, and/or dynamic refreshes of service processor software elements. There are many embodiments for such operations. In some embodiments, the software is received as a single file over the service control device link **1691**. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself. In some embodiments, the software files are segmented into smaller packets that are communicated in multiple messages sent over the service control device link **1691**. In some embodiments, once the file(s) are received, or the segmented portions of the file(s) are received, they are communicated to a service downloader **1663** for file aggregation and installation, which, in some embodiments, is performed after further measures to verify the service processor software are completed. In some embodiments, the files are sent using other delivery means, such a direct TCP socket connection to the service downloader **1663** or some other software installer, which can also involve secure transport and additional levels of encryption.

(38) In some embodiments, the policy control agent **1692** adapts low level service policy rules/settings to perform one or more of the following objectives: achieve higher level service usage or cost objectives, reduce network control channel capacity drain, reduce network control plane server processing bandwidth, and/or provide a higher level of user privacy or network neutrality while satisfying service usage or service activity objectives. In some embodiments, the policy control agent **1692** performs a policy control function to adapt instantaneous service policies to achieve a service usage objective. In some embodiments, the policy control agent **1692** receives service usage information from the service monitor agent **1696** to evaluate service usage history as compared to service usage goals. In some embodiments, the policy control agent **1692** uses service monitor **1696** service usage or service activity history and various possible algorithm embodiments to create an estimate of the future projected service usage. In some embodiments, the policy control agent **1692** uses a future projection of service usage to determine what service usage or service activity controls need to be changed to maintain service usage goals. In some embodiments, the policy control agent **1692** uses service usage history to perform a service usage or service activity analysis to determine the distribution of service usage across service usage elements within categories, such as usage by application, usage by URL, usage by address, usage by content type, usage by time of day, usage by access network, usage by location, and/or any other categories for classifying service usage. In some embodiments, the policy control agent **1692** uses the service usage distribution analysis to determine which service usage elements or service activities are creating the largest service usage (e.g., if e-mail, social networking, or multimedia/online video application categories are creating the largest service usage).

(39) In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. In some embodiments, ambient access generally refers to an initial service access in which such service access is in some manner limited, such as where service options are significantly limited (e.g., low bandwidth network browsing and/or access to a specific transactional service), limited bandwidth, limited duration access before which a service plan must be purchased to maintain service or have service suspended/disabled or throttled or otherwise limited/reduced/downgraded, and/or any other time based, quality based, scope of service limited initial access for the network enabled device. In some embodiments, ambient activation is provided by setting access control to a fixed destination (e.g., providing access to a portal, such as a web page (e.g., for a hotspot) or WAP (Wireless Application Protocol) page, that provides the user with service plan options for obtaining a service plan for the user desired access, such as the service plan options for data usage, service types, time period for access (e.g., a day pass, a week pass or some other duration), and costs of service plan(s)). In some embodiments, service data usage of the ambient activated device is verified using IPDRs (e.g., using the device ID/device number for the device **101** to determine if the device has been used in a manner that is out of plan for the service plan associated with the device **101**, such as based on the amount of data usage exceeding the service plan's service data usage limits, out of plan/unauthorized access to certain websites, and/or out of plan/unauthorized transactions). In some embodiments, service data usage of the ambient activated device is verified by setting a maximum data rate in the policy control agent **1692** and if/when it is determined that the device is exceeding a specified data rate/data usage, then the service data usage is throttled accordingly. In some embodiments, various other verification approaches are used for ambient activation purposes.

(40) In some embodiments, the billing agent **1695** detects and reports service billing events. In some embodiments, the billing agent **1695** plays a key role in transaction billing. In some embodiments, the billing agent **1695** performs one or more of the following functions: provides the user with service plan options, accepts service plan selections, provides options on service usage notification policies, accepts user preference specifications on service usage notification policies, provides notification on service usage levels, provides alerts when service usage threatens to go over plan limits or to generate excess cost, provides options on service usage control policy, accepts choices on service usage control policy, informs policy control agent **1692** of user preference on service usage control policy, provides billing transaction options and/or accepts billing transaction choices. In some embodiments, the billing agent **1695** interacts with transaction servers (e.g., open content transaction partner sites **134**) to conduct ecommerce transactions with central billing **1619**.

(41) In some embodiments, the service notification and billing interface notifies the user of expected network coverage (e.g., based on the device's current geography/location and the accessible networks for the device from that current geography/location) and displays options to the user based on the expected network coverage information. In some embodiments, the service notification and billing interface notifies the user of their current service usage at specified service usage points and displays various options to the user (e.g., service usage options and/or billing options). For example, the user's responses to the presented options are recorded (e.g., stored locally on the device at least temporarily for reporting purposes or permanently in a local configuration data store until such configuration settings are otherwise modified or reset) and reported, such as to the billing server (e.g., central billing **1619**). For example, user input, such as selected options and/or corresponding policy settings, can be stored locally on the device via a cache system. As another example, the service notification and billing interface displays options to the user for how the user wants to be notified and how the user wants to control service usage costs, the user's input on such notification options is recorded, and the cost control options (e.g., and the billing agent **1695** and policy control agent **1692**) are configured accordingly. Similarly, the user's input on service plan options/changes can be recorded, and the service plan options/changes (e.g., and the billing agent **1695** and policy control agent **1692**) are configured/updated accordingly. In another example, the service notification and billing interface provides various traffic control profiles, such as for where the user requests assistance in controlling service usage costs (e.g., service data usage and/or transactional usage related activities/costs). Similarly, the service notification and billing interface can provide various notification options, such as for where the user wants advance warning on service coverage. In another example, the service notification and billing interface provides options for automatic pre-buy at a set point in service usage. In another example, the service notification and billing interface provides the option to choose different notification and cost control options for alternative networks or roaming networks.

(42) As shown in FIG. **9**, the service processor **115** includes a service interface or user interface **1697**. In some embodiments, the user interface **1697** provides the user with information and accepts user choices or preferences on one or more of the following: user service information, user billing information, service activation, service plan selection or change, service usage or service activity counters, remaining service status, service usage projections, service usage overage possibility warnings, service cost status, service cost projections, service usage control policy options, privacy/CRM/GPS related options, and/or other service related information, settings, and/or options. For example, the user interface **1697** can collect service usage information from service monitor agent **1696** to update the local service usage counter (and/or, alternatively, the service usage information is obtained from the service controller **122**) to update user interface service usage or service cost information for display to the user. As another example, service billing records obtained from central billing system **1619** can be used to synchronize local service usage counters and service monitor agent **1696** information to perform real-time updating of local service usage counters between billing system **1619** synchronizations. As another example, the user interface **1697** can display options and accept user preference feedback, such as similarly discussed above with respect to user privacy/CRM/GPS filtering, traffic monitoring and service controls. For example, the user interface **1697** can allow the user of the device to modify their privacy settings, provide user feedback on service preferences and/or service experiences, modify their service profiles (e.g., preferences, settings, configurations, and/or network settings and options), to review service usage data (e.g., based on local service usage counters and/or other data monitored by the service processor **115**), to receive various events or triggers (e.g., based on projected service usage/costs), and/or the user interface **1697** can provide/support various other user input/output for service control and service usage.

(43) In some embodiments, by providing the service policy implementation and the control of service policy implementation to the preferences of the user, and/or by providing the user with the option of specifying or influencing how the various service notification and control policies or control algorithms are implemented, the user is provided with options for how to control the service experience, the service cost, the capabilities of the service, the manner in which the user is notified regarding service usage or service cost, the level of sensitive user information that is shared with the network or service provider entity, and the manner in which certain service usage activities may or may not be throttled, accelerated, blocked, enabled and/or otherwise controlled. Accordingly, some embodiments provide the service control to beneficially optimize user cost versus service capabilities or capacities in a manner that facilitates an optimized user experience and does not violate network neutrality goals, regulations and/or requirements. For example, by offering the user with a set of choices, ranging from simple choices between two or more pre-packaged service control settings options to advanced user screens where more detailed level of user specification and control is made available, some embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other “entity” to implement valuable or necessary service controls while allowing the user to decide or influence the decision on which service usage activities are controlled, such as how they are controlled or throttled and which service usage activities may not be throttled or controlled in some manner. These various embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, or other “entity” to assist the user in managing services in a manner that is network neutral with respect to their implementation and service control policies, because the user is making or influencing the decisions, for example, on cost versus service capabilities or quality. By further providing user control or influence on the filtering settings for the service usage reporting or CRM reporting, various levels of service usage and other user information associated with device usage can be transmitted to the network, service provider, device manufacturer, device distributor, MVNO. VSP, service provider partner, and/or other “entity” in a manner specified or influenced by the user to maintain the user's desired level of information privacy.

(44) As shown in FIG. **9**, the service processor **115** includes the service downloader **1663**. In some embodiments, the service downloader **1663** provides a download function to install or update service software elements on the device. In some embodiments, the service downloader **1663** requires a secure signed version of software before a download is accepted. For example, the download can require a unique key for a particular service downloader **1663**. As another example, the service downloader **1663** can be stored or execute in secure memory or execute a secure memory partition in the CPU memory space. Those of ordinary skill in the art will appreciate that there are a variety of other security techniques that can be used to ensure the integrity of the service downloader **1663**.

(45) In some embodiments, improved and simplified processes for provisioning a device or user for service on a central provider network, an MVNO network or a virtual service provider (VSP) on the central provider network are provided. In some embodiments, provisioning includes one or more of the following: a process or result of assigning, programming, storing or embedding into the device and/or network a set of credentials, or otherwise providing the credentials to the user; the credentials being at least in part carried on the device or with the user; and/or at least a portion of or a counterpart to the credentials being stored or recognized by the network so that the various network elements responsible for admitting the device access to the appropriate service activities do so once the device or user service is active.

(46) As an example, as discussed herein, the credentials can include one or more of the following: phone number, device identification number. MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version,

device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user.

(47) In some embodiments, provisioning includes assigning, programming or embedding into the device and/or network the information to define the level of service activity, referred to as a service profile, that the device is authorized to receive. In some embodiments, provisioning also includes establishing the device settings and/or network settings to define an ambient activation experience in which the device user receives a set of services after (e.g., within a short period of time after) purchasing or otherwise obtaining or installing the device whether the device has or has not been registered and activated with the device user or device owner.

(48) In some embodiments, the ambient experience is the user experience that is available at the time the device is sold in the event the user has not yet signed up for a service plan. For example, the ambient experience is defined by an ambient service profile, an ambient service plan and/or the other service usage activity control policies in effect in the network, on the device, or a combination of both. For example, if the device service processor is used in large part to define the ambient service profile, then the initial provisioning and activation settings in the service processor, and possibly the service controller, can define the user service upgrade offering choices, network destination access control possibilities, traffic control policies, mobile commerce transaction capabilities (e.g., which transaction websites. WAP sites or portals the user can access to purchase information, content, music, games and/or eBooks), possibly free news or weather or other modest bandwidth Internet services that are provided free of charge to entice the user into using/upgrading the service or using the transactions or viewing advertisements, what advertisements are displayed to the user or what advertisement based websites the user is exposed to, certain applications may have access while others are blocked (e.g., Internet based text services have access but email downloads do not), or other example service capabilities. It will be apparent to one of ordinary skill in the art that allowing all of these services, and blocking other ambient user service attempts (e.g., unpaid large file size Internet downloads or uploads or movie viewing or other access that would consume bandwidth and cause the ambient service to be a potential source of losses for the service provider) is made possible by the service profile control capabilities of the service processor and/or the service controller. The bill by account embodiments, as discussed herein, in which each service activity can, for example, be separately tracked with the service monitor and other agents and server functions to produce a billing offset that allows categorization and mediation of different billing entities (accounts) provides the capability for the service provider to individually account for the costs of each ambient service element. This allows business models wherein the free access to the end user is paid for or partially paid for by one or more service provider partners who are billed for service access using the bill by account capabilities (e.g., the transaction partners pay for user access to their transaction experience and perhaps pay a revenue share for transaction billing, the advertising sponsored website partners pay for their access service share).

(49) In some embodiments, automated provisioning and activation includes automation of one or more of the following functions: (1) programming device credentials or partial credentials and recording them in a database (or providing same when they are programmed into the device), (2) associating these credentials with the proper provisioning and/or activation actions to be taken on the device and in the network, (3) directing the device to the proper activation function (e.g., activation server) sequence when it attempts to connect to the network, (4) completing provisioning of the device, (5) programming the AAA, billing system, gateways, mobile wireless center and other network equipment to the proper initial device service control settings, and (6) establishing a service account for the device.

(50) In some embodiments, improved processes for activating service for a device or user with a network service provided by a central provider network, an MVNO network or a VSP on the central provider network are provided. In some embodiments, activation includes one or more of the following: a process or result of associating a service account with device or user credentials; with the service account potentially further being associated with a service profile defining the service activities that the device is authorized to access; creating or updating a service usage or billing record and associating it with the service account to create a service plan; and/or initiating service to the device or user in which the network equipment allows access to the appropriate level of service activities. In some embodiments, VSP embodiments include the provisioning and activation apparatus embodiments of any or all forms.

(51) In conventional mobile device provisioning systems, the provisioning and activation process required to create a user service account and enable the device to access the desired level of service activities can limit mass market, low cost or user friendly applications of the device or service, because the process can often be cumbersome, time consuming and/or expensive for the service provider, service owner, master agent (service distributor), MVNO, VSP and/or user. Accordingly, the various embodiments for provisioning and activation described herein simplify the provisioning and activation process for mobile devices. In some embodiments, provisioning and activation for the device and/or the network accommodates a wide variety of device types and service profile types, with the capability to perform the provisioning and activation at a number of points in the manufacturing, distribution, sales and usage progression for the device, and the ability to either pre-activate before first device use or very quickly activate during first device use (or during some later use of the device).

(52) In some embodiments, as described herein, the term provisioning generally refers to those actions/processes associated with programming the device with credentials or other device settings or software installations used to later activate the device, as well as, in some embodiments, creating database entries and other credential associations in the network so that the network and/or device have the information used to recognize the device or credentials and implement the service policies in the service profile and/or service plan once the service profile and/or service plan are activated. In some embodiments, as described herein, the term activation generally refers to the process of creating or selecting the service plan and/or service profile, programming the settings that are used in each (e.g., required) network function and/or each (e.g., required) device function so that the system can properly associate the device credentials with the appropriate service activity policies, and then admitting the device onto the network. The term activation can also refer in some embodiments to the creation of a user or device service account, in some cases, with user or device owner information or billing information. In some embodiments, the process of provisioning amounts to assigning credentials to the device and programming a portion or all of the credentials on the device, entering a portion or all of the credentials in the various necessary network equipment databases so that the network components are capable of identifying the device and associating it with the network based portion of the admission, traffic processing, service monitoring, billing, service limits and other policies that are eventually defined by the service profile and service plan.

(53) Further examples of the network based service profile policies include network access level, traffic routing, service monitoring, service limits and actions taken upon reaching service limits. Once the service profile is created and activated during the activation process, the device credentials and the associated service profile are communicated throughout the necessary network elements so that each element can implement its part of the network portion of the service profile policies. This process of propagating the service profile settings to all the required network equipment components is a portion of what is referred to herein as activation in accordance with some embodiments. In some embodiments, the activation process includes associating the credentials with the proper service plan and/or service profile, and possibly completing the process of programming the device functions and/or network functions so that the device can be admitted to the appropriate level of network services. In some embodiments, activation also includes the service processor software settings, configurations or installs for each function or agent in the service processor to

implement its part of the service profile, service plan, service billing or transaction billing policies. In some embodiments, activation also includes the creation of entries in the various service account databases and/or billing databases to create a user account or device owner account for the purpose of managing the user choices for service plan and other account information storage and management aspects, such as maintaining status information, maintaining the central service profile configuration, conducting reconciliation and billing exchanges, service usage history, and/or account history.

(54) In some embodiments, the term credentials generally refers to the set of information parameters that the network and/or device uses (e.g., requires) to admit the device onto the network and associate it with the appropriate service profile and/or service plan. For example, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider. OEM, master agent (service distributor). VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user. In some embodiments, at least some of the credentials are unique to the device, and, in some embodiments, groups of devices share one or more aspects of the credentials. In some embodiments, the term permanent credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a permanent basis. In some embodiments, the term temporary credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a temporary basis. In some embodiments, temporary credentials are eventually replaced by permanent credentials. In some embodiments, at least some elements in the temporary credentials (e.g., phone number and/or access or authorization security credential) are used for more than one device. In some embodiments, the temporary credentials are recycled from one or more devices and used for one or more other devices, for example, when they remain unused for a period of time or when they are replaced with permanent credentials on one or more devices. It should not be inferred from the term permanent credentials that permanent credentials are never recycled, for example, when the user discontinues service or use of the credentials. Also, the term temporary credentials does not imply that temporary credentials are always temporary. In some embodiments, partial credentials or pre-activation credentials generally refer to a subset of credentials that are to gain access to limited network services for the purpose of provisioning of credentials and/or activation of a service plan or service profile. For example, prior to a phone number being assigned, a device can gain access to a limited set of network server destinations in which embedded information contained in the device (e.g., the partial credentials) is provided to the server, the server associates that information with the proper additional credentials (including the phone number) to assign to the device and/or associates the information with the proper service profile to activate service. In this example, partial credentials can include device type, OEM, service provider, VSP, device identification number, SIM, service processor configuration or some other information used by the server to determine what the credentials should be and the proper service profile.

(55) In some embodiments, a permanent service account generally refers to the service account that is permanently associated with the user and/or device. For example, this account includes an association with the device or user credentials, user information or billing information, service profile, billing profile, network authorization status and other aspects that define the device or user service policies and billing policies. In some embodiments, the term temporary service account generally refers to a service account that is temporarily set up and associated with the device before some or all of the required permanent account information is available or entered for a device or user. For example, this account can be set up with an association with an actual user, or can be set up with a mock user or unassigned user association so that the network and billing system can recognize the credentials, authenticate the device, admit the device, provide the proper level of service activity control according to the service profile associated with the temporary service account, or collect the service activity usage information for various network and billing system accounting needs before actual user information or billing information has been entered into the network systems. For example, a temporary service account can make it possible or easier to use existing billing systems or other network systems to provide simplified provisioning, simplified activation or ambient services. A temporary service account can also become a permanent service account by replacing mock user or unassigned user information with actual user information, or a temporary service account may need to be replaced by a permanent service account when actual user information needs to be entered into the network systems, possibly including the billing or service profile databases.

(56) In some embodiments, temporary or permanent device credentials and other information used/required for provisioning the device are generated with apparatus located at the manufacturer or in the distribution channel as discussed below. In some embodiments, the apparatus includes a local onsite server that typically shares some aspects of the provisioning information (e.g., phone number, phone number range. MEID or MEID range. SIM number or SIM number range, IP address or IP address range. MAC address or MAC address range, other secure device credential elements) with a network provisioning database. In some embodiments, the apparatus includes a server terminal, and the aforementioned portion of the credentials is generated by the network and shared with the local provisioning apparatus. In some embodiments, as will be discussed below, the provisioning credentials are in part generated in the network and shared with the device while it is connected online to an activation server (e.g., activation server **160**) that is connected to the access network. Similarly, there can be activation servers connected to apparatus in the manufacturing or distribution channel that service device activation, or over the air or over the network apparatus connected to an activation server, which in turn connects to the device, can be used to accomplish activation programming of the network and device as further discussed below.

(57) In some embodiments, when a device is provisioned and entered into the network provisioning database, it is associated with the automatic provisioning and/or activation sequence the device is intended to go through once it connects to the network or to the apparatus that will complete the process. In some embodiments, one or more device parameters (e.g., service owner, device type. OEM, plan type. IP address, security credential and/or software version) are used to determine what the appropriate network provisioning steps and/or settings are for completing the provisioning and/or activation process, and this association information is stored in the network provisioning database for propagation of the provisioning profiles or activation profiles to the various network equipment elements. In some embodiments, the network provisioning database is provided (e.g., in the network) that associates the pre-activation provisioning information (e.g., generated, as described herein, at time of manufacture, sometime during distribution, by the user on a website by a sales associate or other activation assistant, or by the network when a new device enters the automatic activation process). For example, the pre-activation provisioning information informs the network whether or not to let the device onto an activation sequence when the device attempts access, and in some cases, also instructs the network to direct the device to a specific activation sequence including, for example, an activation server (or other activation sequencing apparatus) sequence as described herein. In some embodiments, a central database is queried by other network equipment or the central database is included in one or more of the network elements (e.g., the AAA server and/or billing system, mobile wireless center **132**), or the database is copied in pail or in whole in various network elements (e.g., the central database, AAA server, mobile wireless center, billing system and/or gateways).

(58) In some embodiments, propagating the network equipment provisioning information for a given device or group of devices is accomplished with a network provisioning system that has access to the network provisioning database and is capable of programming the appropriate network equipment. In some embodiments, this network equipment is referred to as “network management” equipment or “network provisioning” equipment. In some embodiments, there are several functions that take part individually or in concert, including, for example, the AAA server **121**, service controller **122** (either with device based/assisted services through the service processor related embodiments or with network only embodiments as described herein), the mobile wireless center **132** (e.g., including the home location register (HLR) or other similar function referred to by other industry terms), the activation server(s) **160**, other network provisioning or management equipment attached to or associated with the billing database system, and/or some other equipment apparatus. In some embodiments, the local database on the device, database in the AAA server and/or database elsewhere in network is provisioned to inform the gateway of the process for handling the pre-provisioned device according to, for example, the credentials. For example, if the device is not recognized or not authenticated onto the access network as an activated device with associated active service profile and/or service plan, the device connection or communication can be directed (or routed) to a generic activation server that provides an activation sequence that is not necessarily determined by one or more of the specific device credential elements, partial credential elements, device profile or partial device profile that define something specific about the activation sequence for the device. In another example, in which the device is not recognized or authenticated as an activated device with associated service profile and/or service plan, the device can be directed (or routed) to an activation service (or other activation sequencing apparatus) that uses some part of the credentials or range of partial credentials or a portion of a partial or complete device profile to determine a desired pre-determined device specific or device group specific activation sequence that is implemented by a specific activation service sequence or other activation sequence apparatus. In another example, in which the device is not recognized or authenticated as an activated device with associated active service profile and/or service plan, a portion of the device credentials or partial credentials can be used as a look-up index into a database that determines what the specific device activation sequence should be, and the device can be directed (or routed) to a specific activation server sequence or other activation sequencing apparatus.

(59) In some embodiments, a database in the AAA server or database elsewhere in network is provisioned to inform the gateway what to do with a pre-provisioned device according to the credentials. For example, devices can be authenticated (for activated devices), routed to activation servers (or other activation sequencing apparatus) or denied access. In some embodiments, the AAA server (and/or other network elements) provide the above discussed look-up function for the above gateway description in which a lookup database, locally stored or stored in a central database, is queried to provide secondary routing information to the specific or generic activation servers.

(60) In some embodiments, the pre-provisioned database is located in the billing system. In some embodiments, the billing system accesses the pre-provisioned database (e.g., stored on the billing system or another network element) for the purpose of setting up temporary accounts or permanent accounts and associating those accounts with pre-activation status, activated free ambient or activated paying customer.

(61) In some embodiments, for zero activation, all the required pre-provisioning or programming of the above network elements, or others, is coordinated by the network provisioning system at some point after the partial or full device credentials have been associated with the device or reserved for a particular device type or service type. In some embodiments, the network provisioning system also coordinates the information to or from the device provisioning apparatus that is described elsewhere.

(62) In view of the various embodiments described herein, it will be appreciated that many of the automated or background provisioning, activation and ambient embodiments described herein can be accomplished with network based approaches, device based approaches, or network/device combination/hybrid based approaches. For example, when the access control for the provisioning process is accomplished in the device (e.g., a device based approach), the activation server can be located anywhere on the Internet, and the device will ensure that the activation process is conducted with the activation server while blocking other traffic from occurring. As another example, some or all of the ambient provisioning programming steps become steps to program the access control, traffic control, application control, bill by account rules, and/or other aspects in the service processor or service controller as described herein.

(63) In some embodiments, the provisioning apparatus described herein can be a computer located in the user's home or business, and the user or an IT manager has access to a website that provides the provisioning information, in which the computer serves as the provisioning or software programming apparatus. In some embodiments, the network itself, possibly through an activation server **160**, website or other interface to the device, becomes the provisioning apparatus, in some cases, with the assistance of software on the device to affect the programming of provisioning information from the network or the communication of device credentials or other information to the network. For example, this software can be a background process that runs without user interaction, a portal/widget program, a web browser based program, a WAP browser based program, and/or any other program that provides a counterpart function to the network functions effecting the provisioning (e.g., activation server). In some embodiments, the activation server either initiates a specific provisioning sequence if device software is present to assist or routes to a website for manual entry if there is no software present.

(64) FIG. **10** illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments. Device credential, software and settings server **6420** provides a link to the network functions that generate or provide device credentials, and/or associate device credentials with activation profiles or pre-activation profiles in the network equipment (e.g., the billing system **123**, service controller device control system **6225**, gateways **410**, **420**, base station **125**, credential generation and association server **6410**, activation server **160**, service download control server **1660** and/or other network apparatus). For example, the link between the device credential, software and settings server **6420** to the central provider core network equipment can be over the Internet **120** (e.g., a secure link over the Internet) as shown or over another connection such as a leased line. The device credential, software and settings server **6420** obtains credentials or partial credentials from the network apparatus that generates them, illustrated by the credential generation & association server **6410**. Credential generation & association server **6410** need not be directly connected to the central provider core network **110** as shown, but can be located elsewhere (e.g., in another location connected by a secure Internet link). Credential generation & association server **6410** assigns credentials, or partial credentials, for use by device credential, software and settings server **6420**. When these credentials are assigned to a device, they are programmed, loaded or otherwise associated with the device by device credential provisioning apparatus **6430**, which is connected to the device wirelessly or via a wire line connection.

(65) In some embodiments, a device software loading and programming apparatus **6440** provides software loading or device settings functions that form a portion or all of the provisioning or pre-provisioning device configuration, or form a portion or all of the device activation profile configuration, or form the device service owner, master agent or VSP device assignment or signature, and in some embodiments, using an activation tracking service (ATS) system. As discussed herein, the ATS monitors network connections and aspects of traffic that provide insight into which networks the device **100** is gaining access to, in some embodiments, for the purpose of ensuring that an OEM, master agent, device service owner or VSP is being compensated for devices that activate on a service provider network. In some embodiments, the ATS agent connects to a server counterpart that records and, in some embodiments, also analyzes the service or network connection information to make a determination of the type of access service the device is receiving and, in some cases, determine which networks the device is activated on. In some embodiments, the ATS is installed on the device in a manner that makes it difficult to tamper with or remove so that the entity that is intended to get credit for device service activation does get credit (e.g., the ATS agent can be loaded into secure memory, it can be installed with software that makes it difficult to de-install, it can be installed on the modem possibly in secure memory, it can be installed in the BIOS, it can be installed deep in the OS kernel, it can be installed with one or more additional device agents that monitor the ATS agent and alert a network function or re-install it if tampered with). The SIM inventory **6450** is provided to illustrate that, in some embodiments, hardware elements (e.g., a SIM security module as shown) or hardware

configurations are also installed or manipulated in device **100** and these operations and the recording of the resulting associations form a portion of the provisioning or pre-provisioning process.

(66) In some embodiments, at the time the credentials or partial credentials are loaded, programmed, set, installed, read from the device or otherwise recorded, they are, in some cases, all associated together in a database that allows for later identification of the device and its appropriate provisioning and/or activation process through such associations. For example, this can involve reading device parameters such as MEID. MAC address, device type, or other information that is associated with the information being loaded or configured on the device. As discussed herein, this credential configuration and association information is stored in the network equipment responsible using it to configure the network to activate the device in one of the various embodiments disclosed herein.

(67) Some embodiments include tying some or all of the activation provisioning steps and information settings together into a database that defines a higher level activation profile for a group of users (/devices), and a server is used to perform device and equipment programming for the devices in the group, including, for example, associating the following device information into the group definition: credentials, service owner or master agent, provisioning information and/or activation profile. Some embodiments further provide for this device group information being distributed to the various network equipment components required to activate the devices as discussed elsewhere. In some embodiments, this programming and device group association is accomplished using the VSP workstation server **4910**. For example, a device can be manufactured and distributed in a manner that provides flexible assignment of the device to a group that is assigned to an activation profile or a service owner.

(68) In some embodiments, multiple activation servers **160** are provided (as shown), which illustrates that there can be multiple device activation servers **160** each with a different device activation experience and potentially controlled by a different VSP, service owner, service provider, OEM or master agent. As discussed herein, there are several ways that a device **100** can be routed to the proper activation server **160** so that the device provisioning and activation process can be completed. In some embodiments, all devices that are not activated are re-directed (or routed) to an activation server that reads one or more parameters in the device credentials. The device credential information can be determined either through the device identification information associated with the access network connection itself (e.g., MEID. IP address, phone number, security credentials, or other credentials identified for a device that gains access with the network), or with the aid of the device in a pre-arranged query-response sequence. The device can then be re-directed (or routed) to the appropriate activation server for that device, device group, device service owner or VSP. In some embodiments, the same process described above can be accomplished with a single re-direction from a service gateway **420** or **410**, or another router enable network element. In some embodiments, the gateway or network element itself decodes the device credential information as described herein and performs the correct re-direct (or route) to the appropriate activation server **160** for that device. In some embodiments, the activation server **160** can be incorporated directly into the gateway **420** or **410**, the base station **125** or other network component. In some embodiments, the activation server **160** can be incorporated into the service controller **122** or the service controller device control system **6225**.

(69) In some embodiments, apparatus other than the activation server are used to facilitate provisioning of credentials or partial credentials, or activation, during manufacturing or device distribution, and, for example, these apparatus can augment, supplement, compliment or replace the activation server function. Such apparatus include, for example, device programming equipment (e.g., device credential provisioning apparatus **6430**, device software loading and programming apparatus **6440** or SIM inventory **6450**), equipment that is networked into a central provider. MVNO or VSP database (e.g., device credential, software and settings server **6420**) to gain access to provisioning information or activation information that is programmed into a device or group of devices, or to place device credential or partial credential information in a network database for later recognition, or to receive or communicate security information such as certificates for devices or SIM modules that will later be used to complete provisioning or complete activation or gain access to a network. For example, these apparatus, or any other apparatus including the activation server, can be networked into a service provider network or device database, an MVNO network or device database or a VSP network or device database. In some embodiments, programming of the device credentials or other information associated with the service processor or device is provided, so that, for example, the device can be recognized by an activation server or similar network function at a later point in time so that provisioning or activation can be completed in an automated manner, potentially with reduced or no user involvement, that provides a provisioning or activation configuration that is in some way unique for the service provider or service provider partner, device type, user group, VSP, MVNO, master agent or other entity. In some embodiments, this programming is provided in a manner that is difficult to change without the proper authorization so that the device is properly associated with the proper “service owner” or master agent (e.g., for the purpose of activation incentive payments). For example, as discussed herein, various approaches can be applied to the device credential or other settings or software provisioning so that the settings or software are secure or protected, or so that if the software is removed, replaced or modified it is reported or replace or restored. In some embodiments, VSP control of the provisioning, partial provisioning or activation of devices is provided during manufacture or at different points in the distribution channel. As discussed herein, some of these embodiments allow the central provider to offer to service partners (e.g., VSPs, MVNOs, master agents, and/or OEMs) similar types of control for device activation experience design or device service assignment control (e.g., sometimes referred to as service provider device locking so that other service providers cannot provide primary access to the device) during the manufacturing or distribution process that are possible with devices manufactured and distributed for the central service provider.

(70) In some embodiments, the device is provisioned before the user obtains the device with permanent credentials, temporary credentials or partial credentials. In this case, the necessary credential programming of the device occurs during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of shipment. In some embodiments, provisioning of network information as discussed above is used, and the network information is provisioned at the same time, before or after the device information is provisioned. In some embodiments, the device provisioning information is programmed with dedicated apparatus that connects to the device either with wires or wirelessly. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or it can be partially or entirely networked into a database or provisioning solution located elsewhere and operated by the central provider, a VSP. OEM or other entity. For example, the apparatus to program the network portions of the provisioning information can also be networked and the operators who set up the required network programming for a device or group of devices may be in the vicinity of the servers that host the provisioning and management tools or they may network into the servers. In some embodiments, provisioning system operators have full or partial control of any device provisioning equipment associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote access via secure terminal, secure website or other techniques to network into a central provider or VSP server farm in which they control or partially control the network portion of provisioning capabilities for that subset of devices that are assigned to the entity they work for with (e.g. OEM, VSP or master agent).

(71) In some embodiments, provisioning is accomplished over the air on the mobile access network for mobile devices, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment, such as a computer to perform the programming required to complete provisioning. In the cases in which the device is provisioned at point of sale or after point of sale, the device provisioning can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, in some embodiments, partial credentials that include information such as device type, OEM or service provider are used to assist in determining how to complete the provisioning, and the information can also include secure information, certificate or signature programmed into the partial credentials that is required for the network to perform the provisioning of the remaining credential information in the device and possibly the network. In some embodiments, any network information used/required to provision the device or service is generated at the time the partial credentials are determined rather than beforehand.

(72) In some embodiments, the device is activated for service before the user obtains the device with permanent credentials, temporary credentials or partial credentials, or with a permanent service account or a temporary service account. For example, in this case, the necessary steps of provisioning

and activating service for the device can occur during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of shipment. In some embodiments, the steps for activating service include one or more of the following: provision the device (e.g., with permanent, temporary or partial credentials), provision the necessary network databases and equipment to prepare them to recognize the device and associate it with the service profile and/or service plan, create or select the service account (e.g., permanent or temporary service account), select or create the service profile and/or service plan, program any elements in the device required to activate service (e.g., account ID, device aspects of the service profile and/or service plan), and program the necessary network databases and equipment with the required associations of device credentials and service profile and/or service plan policy settings. In some embodiments, the device oriented programming portions of the service activation steps occur at the same time, before or after the network oriented programming portions of the service activation steps.

(73) In some embodiments, the device activation information is programmed with dedicated apparatus that connects to the device via a wireless or wire line connection. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or the dedicated apparatus can be partially or entirely networked into a database or service activation solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the activation information can also be networked and the operators who set up the required network programming for a device or group of devices can be in the vicinity of the servers that host the service activation and management tools or they can network into the servers. In some embodiments, activation server tools operators have full or partial control of any device activation apparatus associated with the entity they work for (e.g., OEM. VSP or master agent) but only have remote and partial access via secure terminal, secure website or other techniques to network into the network portion of the activation tools that are controlled by the central provider or VSP. The server tools operators can be restricted in some embodiments to providing network activation information or settings only for those devices or device groups that are assigned to the entity they work for with (e.g., OEM, VSP or master agent). For example, the device control group restriction can be accomplished with a secure database that has secure sub-partitions for one or more entities so that they cannot impact the control of one another's network activation settings but can control their own devices. In this way, a centralized set of activation tools resources controlled by a central provider, VSP or other entity can be partitioned so that different entities can have partial or full control of the activation service definition for devices or groups of devices without impact or risk to others who share the network and activation tools resources.

(74) In some embodiments, activation is accomplished with an over the air interface to a mobile device, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment such as a computer to perform the programming required to complete activation. In the cases in which the device is activated at point of sale or after point of sale, the final device activation process can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, some embodiments call for a temporary service account that is used to bring the device onto the network before the user has input the information necessary to create a permanent service account. In some embodiments, a temporary or permanent service account can be applied to the device at the time the device reaches the network, and the type of account, service profile and/or service plan can be influenced (e.g., partially determined or informed) or determined by information embedded in the device credentials or partial credentials, such as device type, device ID. SIM. OEM or service provider. For example, the device credentials can also include secure information, certificate or signature that can be required by the network to perform the activation steps for temporary or permanent service account status. In some embodiments, in which the device is activated in this manner before the user information is available, or before the user has selected a pay for service plan, the service profile and service plan are set up for ambient services as described herein.

(75) In some embodiments, the device is activated during the manufacturing or distribution process, and then the activated device status is suspended. Once the temporary or permanent service account is set up, with appropriate service profile and/or service plan and temporary or permanent credentials, in some networks and billing systems the service can often be more easily resumed once suspended as compared to provisioning and activating the device from scratch. The device is then later resumed (or re-activated) when some event triggers the resume process, such as when it ships to the end user or when the end user attempts to use it. This process prevents the network from needing to manage credentials and accounts for devices that have been activated but are not yet on the network.

(76) In some embodiments, provisioning is accomplished at least in part with temporary credentials in a manner which is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary credential elements replaced at a later point in time by permanent credential elements in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary credential set is pre-programmed into the device along with a temporary or permanent service account including service profile during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming is performed for the network via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, a subset of the temporary credentials is recycled once it is replaced, if a temporary service account is not activated or used after some period of time, if a permanent account is not activated or used after some period of time, or if the credentials subset is revoked from the device for some other reason.

(77) In some embodiments, more than one device is assigned one or more elements of the temporary credentials, such as the phone number, which may be limited in supply. In some embodiments, a network will accept more than one set of temporary credentials, one or more redundant elements, for two or more different devices. In some embodiments, a device that has two or more temporary credential sets, in which at least a subset of the credential elements are different for the sets, so that if one set of credentials has elements that are already being used to access the network, then one or more reserve sets can be drawn upon to gain access to the network.

(78) In some embodiments, the temporary credentials are used to log onto the network to conduct an over the air or over the network activation process in which an activation server reads at least a portion the device credentials to determine some aspect of how the device service profile. In some embodiments, the aforementioned over the air activation process is accomplished in the background without user intervention. In some embodiments, the over the air activation process is initiated when the user first attempts to use the device or when the user first attempts to access the network or upon user request or approval. In some embodiments, the over the air activation process is initiated using a temporary service account for the device and/or network to gain access to the network. In some embodiments, the over the air activation process is initiated after the user has entered the information required to create a permanent user account into the device or into the network. In some embodiments, the user is required to enter the aforementioned user information before using the device or using some aspect of the device. In some embodiments, the temporary service account is replaced by a permanent service account some time after the user has entered the necessary information to create a permanent account into the device or network. In some embodiments, the over the air activation process is initiated using a permanent service account assignment for the device and/or network to gain access to the network.

(79) In some embodiments, the service profile is assigned to the device and/or network during the aforementioned over the air activation to be a pay for service profile with a free trial period. In some embodiments, the service profile assigned to the device and/or network during the aforementioned over the air activation includes pre-pay, post-pay, session based pay or pay as you go options for service. As will be apparent to one of ordinary skill in the art, various embodiments disclosed herein are particularly well suited for control or pre-pay services. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned over the air activation is an ambient service profile providing service access before all the user information is available to assign a permanent account. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing a service upgrade selection option interface to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service

profile providing transaction services to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing bill by account functionality for the network. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing some amount of free networking or information service to entice the user to use the other ambient services. In some embodiments, the aforementioned ambient service is at least partially implemented with device based service activity control or control assistance. In some embodiments, the aforementioned ambient service is at least partially implemented by gateways, routers or switches in the network that are programmed according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account.

(80) In some embodiments, activation is accomplished at least in part with a temporary service account in a manner that is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary service account is replaced at a later point in time by permanent service account subset in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary service account settings (e.g., including the service profile settings and/or the service plan settings) are pre-programmed into the device along with a temporary or permanent credentials set during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming for the network is performed via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, the device is suspended once it is activated but before the user is using it, and then resumed before or commensurate with the point in time that the user begins to use it. In some embodiments, some subset of the temporary service account is recycled once it is replaced, if the temporary service account is not used after some period of time, if the temporary service account is not upgraded to a permanent service account after some period of time, or if the activation is revoked from the device for some other reason. In some embodiments, more than one device is assigned to the same temporary service account. In some embodiments, a network accepts more than one device on the same temporary service account. In some embodiments, a device includes or is associated with two or more temporary service accounts, in which at least a subset of the temporary service account elements are different, so that if one account is already being used to access the network then one or more reserve accounts can be drawn upon to gain access to the network. In some embodiments, the temporary service account is associated with a temporary credentials set. In some embodiments, the temporary service account is associated with a permanent credentials set.

(81) In some embodiments, un-activated devices are detected by the network muting equipment (e.g., service gateways or routers in hierarchical networks or base stations with embedded gateways in flat networks) and the device muting is programmed to re-direct un-activated devices to an activation server network destination. For example, the activation server can first inspect the information associated with the device to determine if the device belongs to the list of devices, device types or device groups that the network is programmed to provide access to. For example, the information used to determine this can include device type, service provider, phone number, device ID, SIM ID or configuration, secure information used to qualify the device. IP address. MAC address, user, user group. VSP, OEM, device distributor, service distributor (master agent), service processor presence or configuration, presence or configuration of other software or hardware. There can also be some activation definition information embedded in the credentials, or associated with some portion of the credentials, or programmed additionally on the device that informs the activation server as to the service profile and/or service plan and/or service account that should be established for the device. If activation information (the service profile, service plan and/or service account information) is found through association with the device credentials (e.g., device ID, phone number. IP address. MAC address, SIM or other security credentials) rather than being read directly from information embedded in the device or device credentials, then the pertinent aspects of the credentials can be used as a cross reference to look up the service plan and/or service profile information stored in a database networked to or within the activation server. The activation information can include information to define a wide variety of service plans and service profiles that when properly implemented on the network functions, and perhaps device if necessary, can provide for a wide range of service activity policies, service billing policies, transaction billing policies and service account types that can be associated with the device over the air or over the network.

(82) In some embodiments, once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server initiates the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up may be permanent or temporary. In some embodiments, the activation process described above is completed perhaps before the user has entered some or all of the user information necessary to set up a permanent service account, and, in these cases, a temporary service account can be set up. In some cases, the activation process can be completed in the background before the user has completed an attempt to access the network and the service profile can be set up to provide ambient services to a temporary service account. In some embodiments, the user is required to enter the information required to establish a permanent service account prior to gaining full use of the device, either on the device, on a computer or in the store, so that by the time the user begins using the device the above activation embodiments can provide for ambient services activation with permanent account status so that the user can purchase a service upgrade or any transaction without entering any more account information.

(83) In some embodiments, a device status is changed from a temporary service account to a permanent service account. If the device is activated with a temporary service account, and the user information is available to set up a permanent account, then if the billing system rules and interfaces allow for such, the user information can be changed from the mock information to the actual user information while maintaining the same account identifiers in the billing system. If the billing system will not allow for such, then the user information can be used to establish a new account, the device credentials can be re-associated with the new account, in some cases, after modifying one or more of the device credential parameters, and the network functions can be re-programmed as required, and, in some cases, the device can be re-programmed as required to accommodate the new permanent account.

(84) In some embodiments, code on the device pulls a temporary or permanent set of credentials. When the credentials are pulled, the network associates the device with an ambient service profile according to one or more of the following: embedded device information identifying device type, service owner (e.g., VSP), user group, or user, or device ID is cross referenced to a database that is populated some time from manufacturing time to post sale where the database provides information identifying device type, service owner (e.g., VSP), user group, or user. The device is then re-directed accordingly (e.g., for device based this is a matter of setting the policies or loading the software for the service processor, for the network based approach this is a matter of populating the routing tables and service profile). For example, credentials can be re-cycled after a period of time, and/or some portion of the credentials can be redundant with other devices. For example, this is essentially a dynamic service for (temporarily) assigning device credentials, and the duration of the temporary credential validity for that device ID can be time limited to give the user time to activate a real account or a free trial, session limited, or a longer duration of time that is perhaps refreshed each time the device logs on. For example, the device could also already have permanent or temporary credentials but not have a service account. The above process can be used to assign a temporary or permanent service account as well. Once the service account is assigned and the appropriate service profile is propagated to the network elements, the device can then be directed to or use the appropriate activation profile service activities or the appropriate ambient service activities.

(85) In some embodiments, the device is activated in the background in a manner that is virtually transparent to the user. For example, at some point in the distribution channel, the device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device

connects to the network and the gateways or routers re-direct the device to an activation server, as discussed above. As also described herein, the activation server either derives information from the device that informs the server what service the device should be activated with, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server causes all the necessary network settings and billing database entries to be configured/programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. For example, the provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

(86) In some embodiments, background activation is performed using the aforementioned activate/suspend process. At some point in the distribution channel, the device is programmed to seek to resume service as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device attempts to connect to the network and the gateways or routers re-direct the device to an activation server as described herein. As also described herein, the activation server either derives information from the device that informs the server that the device is ready to resume service, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the server is aware of this information, it sends a message to resume service to the billing system, or other network function that controls the suspend/resume function, and the service is resumed.

(87) In some embodiments, background activation is performed as described below. The service processor and the credentials are pre-programmed during the manufacturing or distribution process to provide the desired service profile support and/or billing profile support for the desired initial ambient service. As described herein, this programming can be accomplished with dedicated apparatus at the manufacturer or distribution depot. Furthermore, the party responsible for defining the service (e.g., typically the central provider. OEM. VSP, distributor or master agent) can network into the service processor programming apparatus to control service processor and/or credential programming for all or a subset or group of the devices or device types locally available. The service processor enabled device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. In some embodiments, the activation server is the access control server previously discussed or the access control server can act in concert with another server that performs the activation function. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to the activation server. As also described herein, the activation server can communicate with the service processor to verify the service processor security credentials, agents and configuration.

(88) In some embodiments, if the activation server determines that the pre-programmed settings stored in the service processor need to be modified to provide the latest version of the desired service, or if the service processor agent software needs to be updated, then this can be accomplished prior to completing the activation process. Once the service processor configuration and settings are confirmed, the activation server causes the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. Given that the service processor can perform some or much of the service activity control or control assistance, the service control options are generally larger than without the service processor, and there can be less configuration to perform for other networking equipment to complete the provisioning and activation process. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

(89) In some embodiments, pre-programming and pre-activation of devices with temporary credentials and a temporary service account are used to ship devices that are pre-activated. Given that the credentials are temporary and can be recycled when the permanent credentials are assigned, concerns about using up too many pre-assigned credentials are reduced. In embodiments in which a portion of credentials elements can be used for multiple devices, this concern is further reduced. If there is a concern about too many activated devices being assigned that are not actually active and generating service revenue, then the suspend/resume process discussed herein can be employed. In some embodiments, the temporary credentials and/or temporary account can be replaced with permanent credentials and/or account assignments at any time as follows. When a pre-programmed event in the device is triggered, then the device initiates a program that seeks the aforementioned activation server or another server that has the capability of fulfilling the device request to exchange the temporary credentials for permanent credentials and/or exchange the temporary account for a permanent account. The event that triggers the credential exchange can be the same or different than the event that triggers the service account exchange. The service account exchange can typically be triggered by the point in time that the user enters account information.

(90) In some embodiments, the aforementioned ambient service is partly implemented with a combination of the techniques for pre-provisioning during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy provisioning capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are pre-programmed as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the provisioning credential elements are not all pre-programmed before the device ships, but a subset of the credential elements are programmed using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service activity control settings for the gateways, routers or switches that will result in the desired ambient services activity controls.

(91) In some embodiments, the aforementioned ambient service is implemented with a combination of the techniques for pre-activation during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy control capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are programmed to recognize the pre-activated device credentials as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the device activation profile and/or service account are not pre-programmed in the network and/or the device before the device ships but the activation profile and/or service account are programmed using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service profile activity control settings for the gateways, routers or switches that results in the desired ambient services activity controls.

(92) In some embodiment, a VSP capability is enabled by providing a secure network connection to the service policy settings tools that define the device pre-provisioning settings, the device pre-activation service profile settings, the network equipment service activity control policy settings (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage), and the network billing system database. By providing server tools that enable all these settings to be controlled (or perhaps only observed in the case of the billing system) by a secure workstation or secure website interface that networks into the equipment that programs the settings, and providing for a secure partitioning of the devices that can be controlled by a given secure workstation or secure website interface, a central provider can provide VSP services to multiple entities who all have different device and service plan combinations that they desire different flavors of ambient services for. These techniques can also be extended beyond ambient to any device/service profile/service plan combo the VSP desires to create. In some embodiments, the networking equipment is implemented to secure device service group domains in which the service policies for a group of devices can be controlled. In some embodiments, the pre-provisioning and pre-activation techniques are substituted with the over the air activation server techniques discussed herein,

and a secure device group partition capability is provided in the activation server as well so that the activation server device group partition control capabilities can be added to the secure device group partition control capabilities of the network gateways, routers and/or switches, the device programming tools and the billing system to form a VSP partition solution for over the air activation of various device/service plan combinations. In some embodiments, the device groups are relatively small so that beta trials of arbitrarily large or small size can be designed and implemented by defining a service control group as described above, and after fine tuning and perfecting the beta trial settings the device group can be expanded to publish the automated provisioning and activation service settings to a larger user or device group for production services.

(93) In some embodiments, device based service activity control assistance (e.g., based on the various service processor embodiments described herein) is combined with simplified provisioning techniques described herein so that service processor enabled devices can be shipped with pre-provisioned credentials (temporary or permanent) or can obtain credentials in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain credentials and provisioning apparatus described elsewhere provide various approaches for provisioning pre-provisioned service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various approaches for over the air or over the network simplified post-sale provisioning for service processor enabled devices. For example, these embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

(94) In some embodiments, provisioning includes provisioning partial device credentials that include, for example, a secure certificate that is used to authorize full credential provisioning and/or activation by performing a process for a later look-up/validation of the full device credentials. For example, the look-up/validation of the full device credentials can be performed by a gateway, router or similar network device that re-directs to a provisioning server and/or activation server or other network components that either: (1) recognizes the partial credentials that serve as a reference to direct the device communication to a specific provisioning/activation server determined from the partial credentials; or (2) does not recognize the partial credentials, and directs the device communication to a less specific provisioning/activation server that is not necessarily associated with a reference to the partial credentials.

(95) In some embodiments, if the partial device credentials (e.g., temporary or permanent credentials) are being used for provisioning, then the partial credentials are read (e.g., and/or other credentials can be looked up based on the partial credentials as described above). The device is authorized if the proper credentials and/or secure certificate is present. The device credential provisioning is then completed (e.g., using activation server commands or settings to a device based software and/or hardware element), and the credentials are, in some cases, also communicated to the various network equipment elements.

(96) In some embodiments, if the partial device credentials are being used for activation, then partial or full device credential provisioning is performed, such as described above. A service account (e.g., temporary or permanent service account) is created or looked up based on the partial device credentials (e.g., a user account associated with the device through embedded partial or full credentials or a look up process, or based on a dynamically created/assigned temporary account associated with the device through embedded partial or full credentials). An initial service profile and, in some cases, an initial service plan (e.g., service control policy settings including a billing profile) are determined from embedded information and/or using a look up process (e.g., based on the device type and/or partial or full device credentials). The device is then programmed to enable access with the service profile and plan, and, in some cases, the various network components/elements are programmed to enable the service profile and plan, and, in some cases, proper entries in the billing system are made or confirmed, and the device credentials are, thus, activated for service.

(97) In some embodiments, the above described provisioning and/or activation processes are performed with the provisioning server(s) and/or activation server(s) in the background with reduced, minimal or no user input required, for example, after the device is sold to the user and the user turns on the device so that by the time the user attempts to access the service using the device, the provisioning and/or activation process is already completed.

(98) In some embodiments, device based service activity control assistance (e.g., based on the service processor embodiments) is combined with simplified activation techniques described herein so that service processor enabled devices can be shipped with pre-activated accounts (temporary or permanent), or can obtain activated account status in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain activation and provisioning apparatus described elsewhere provide various approaches for pre-activated service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various approaches for over the air or over the network simplified post-sale account activation for service processor enabled devices. These embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

(99) As discussed herein, in some embodiments for activation, the network AAA (or other network function) either recognizes one or more aspects of a pre-activated device credentials and routes the pre-activated device communication to an activation server that is appropriate for that device (routing information either derived through look up of the credential aspect or by obtaining the required information directly from the credential itself), or the AAA (or other network function) does not recognize the credentials and routes the device communication to an activation server for unrecognized device credentials. In either case, in some embodiments, one or more of the credential aspects can then be used to perform a secondary determination of what provisioning and/or activation sequence to perform in association with the device, or which activation server sequence the device should be directed to. For example, one or more device credential aspects can be read and used as a cross-reference to determine a routing for the device communication (or the information required for routing can be in the device credential information itself) so that the device can be routed to the appropriate activation server sequence.

(100) In some embodiments, an activation server sequence can be determined at least in part by using a browser server or a portal (e.g., http server, https server, WAP server or another standard or custom protocol server for a browser, embedded or automated browser or a portal client in the device). In some embodiments, the browser server is an http or https server. The pre-activated device communication can be routed to the https server in a manner similar to that described above, and the server can read the information embedded in the https communication to determine the device credential information required to initiate the correct provisioning completion and/or activation sequences. For example, the https header information, tokens, cookies or other secure information communicated over https from a secure embedded client on the device (or user) can either provide the activation server with the information required to perform the cross-reference to an appropriate provisioning and/or activation sequence, or the https embedded information or the embedded client (or user) information can instruct the activation server on which services the device is to be provisioned and/or activated on and any necessary device or user information (e.g., device owner and/or billing information) can be exchanged, or the device might be provisioned and/or activated first on a free ambient service with temporary or permanent credentials or account.

(101) In some embodiments, the service processor can be combined with the pre-provisioning and pre-activation techniques described above to create an ambient service solution that will work on roaming networks in which the central provider or VSP has no control or minimal control over the network elements. For example, the device includes a service processor pre-programmed for ambient service activity control as discussed herein, and the device credentials and other settings are pre-provisioned and pre-activated for the central provider network, all of which is described in numerous embodiments disclosed herein. Provided that the service provider has a roaming agreement with other service providers, or provided that the device may gain access to the roaming network, when the device is roaming it will be capable of ambient connectivity with bill by account functionality and all the other features of ambient. Furthermore, as also discussed herein, the ambient service activity control policies can be different for different roaming networks to accommodate the varying network costs and performance. Also, for example, it would be permissible to sign up for initial services or additional upgrade services with the central provider while roaming on the roaming partner network. One of ordinary skill in the art

will appreciate that this also allows for creating a VSP or MVNO for the purpose of creating a clearing house for central provider service activations according to geography or user choice. By using a global multi-mode modem module, and maintaining service agreements with a multitude of carriers, the MVNO or VSP can provide consistent ambient services across multiple carriers and multiple geographies while still maintaining a good degree of cost control. Using bill by account capabilities, it is also possible to have an activation agreement where a roaming service provider agrees to refund the cost of ambient roaming. From the ambient service platform, the VSP or MVNO can then provide service purchase options to the user based on the carrier networks available to the device, or the VSP or MVNO can broker the user off to any of the carriers by activating the device onto the carriers main central provider service.

(102) Accordingly, these embodiments provide flexible capabilities for activating a device or group of devices with a broad range of service profiles and service plans by simply programming the device with the proper credentials at some time during manufacturing or distribution, or simply programming a database associated with the network so that a portion of the device credentials can be used to look up the desired service profile and service plan. For example, various activation embodiments described herein are highly convenient for the end user and need not, in many cases, involve any human intervention.

(103) The service processor **115**, service controller **122**, policy implementation and/or profile implementation and various embodiments disclosed herein are applicable to conventional communication products as well as machine to machine applications. For example, if the machine to machine device includes a service processor **115** with an activated account, then the service profile settings can be optimized for machine communications to provide only the limited access required to support the particular machine to machine application. This allows for cost optimized access services and prevents the machine to machine device or access modem from being misappropriated and used for some other service access than that intended. For example, by programming the machine to machine communications device at time of manufacture or during distribution with credentials or partial credentials that provide for automated provisioning and activation as described herein, the device can be automatically provisioned and activated on the service network with a service account when deployed, thus eliminating the need for costly or time consuming human intervention. The various embodiments that make it simpler to design, manufacture, test and deploy devices may also be equally applied to machine to machine devices. These embodiments include the service processor **115** developers kit and the automated provisioning and activation management tools among others. Also, the service analysis and test tools and the virtual service provider embodiments can also be applied to machine to machine applications.

(104) FIG. **1** illustrates a wireless network architecture for providing device assisted services (DAS) install techniques in accordance with some embodiments. As shown. FIG. **1** includes various wireless communications devices **100** (e.g., a mobile wireless device or an intermediate networking device) in wireless communication with central provider access and core networks **210**. As shown, some of the devices **100** include service processors **115**. For example, devices **100** can include various types of mobile phones. PDAs, computing devices, laptops, netbooks, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device. In some embodiments, intermediate networking devices, as described herein, include a service processor or assist in the downloading of a service processor for one or more devices **100** to facilitate network access as described herein with respect to various embodiments. In some embodiments, a device **100** does not initially include a service processor (as shown in FIG. **1**). In some embodiments, a service processor **115** is previously installed (e.g., during manufacture or distribution), or is downloaded and installed on a device **100** (as also shown in FIG. **1**).

(105) In some embodiments, the wireless communications device is a mobile communications device, and the service includes one or more Internet based services, and the mobile communications device includes one or more of the following: a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, and a home networking system. In some embodiments, the wireless communications device includes a modem, and the processor is located in the modem. In some embodiments, an intermediate networking device includes any type of networking device capable of communicating with a device and a network, including a wireless network, example intermediate networking devices include a femto cell, or any network communication device that translates the wireless data received from the device to a network, such as an access network. In some embodiments, intermediate networking devices include 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems. DSL modems, remote access/backup routers, and other intermediate network devices.

(106) In some embodiments, there are at least two versions of a service processor. For example, a first version service processor can be a generic version of a service processor version that can be pre-installed during manufacture or distribution and used for downloading a second version service processor. For example, the first version service processor can be a generic version that is not specific to a device group while the second version is specific to a device group. As another example, the first version service processor installed during time of manufacture or during device distribution may not contain all of the functions that are available for a permanent second version service processor that is installed when the device first connects to a network. As another example, service processors can be regularly updated to change the security parameters of the software, such as software signatures, encryption, obfuscation, secure query response sequence information, and/or other parameters, so that it becomes more difficult to hack or otherwise modify the software. As another example, the second version service processor can be uniquely associated with the device **100** (e.g., wireless communications device or an intermediate networking device) and the associated service plan and/or service provider. In some embodiments, a first version service processor is installed on a device **100** (e.g., service processor **115** installed on the device **100** can be a first version service processor that was previously installed during manufacture or distribution, or downloaded and installed during initial network access, as shown in FIG. **1**). In some embodiments, a second version service processor is installed on a mobile device (e.g., service processor **115** can be a second version service processor that was previously installed during manufacture or distribution, or downloaded and installed during initial network access, as shown in FIG. **1**).

(107) In some embodiments, a new and/or updated version service processor **115** can be downloaded from, for example, a service processor download **170**, as described herein. In some embodiments, the service processor download **170** provides a function or service that is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements (e.g., the service processor download **170** can be a function/service of service control **150** and/or service policies and accounting **165**). In some embodiments, the devices **100** are in service control communication with service control **150** via central provider access and core networks **220** as shown in FIG. **1**. Service policies and accounting functions **165** are also provided in communication with the central provider access and core networks **220** as shown in FIG. **1**. In some embodiments, the service policies and accounting functions **165** provides a function or service that is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements (e.g., the service policies and accounting functions **165** can be a function/service of service control **150**).

(108) In some embodiments, the devices **100** network access is initially restricted to service control related access for service processor **115** verification and/or download(s)/update(s) (e.g., a first version service processor installed on the mobile device **100** can limit or direct network access to the service control **150**, service processor download **170**, and/or service policies and accounting function **165**), as described herein with respect to various embodiments. In some embodiments, after this initial restricted access period is completed and/or if the service processor **115** of the mobile device **100** is verified for the device and is current/updated, the device **100** can communicate via the central provider access and core networks **220** to the Internet **120** for access to various Internet sites and/or services **240** as shown in FIG. **1** (e.g., Google sites/services. Yahoo sites/services, Blackberry services, Apple iTunes and AppStore, Amazon.com, FaceBook, and/or any other Internet based sites and/or services) based on, for example, the service plan associated with the device **100**. In some embodiments, service usage information (e.g., based on network based CDRs or device generated CDRs, such as micro-CDRs generated by the service processor **115**, and/or other service usage measures) are used for service control and/or service plan billing and reporting, as described herein with respect to various embodiments.

(109) Those of ordinary skill in the art will appreciate that various other network architectures can be used for DAS install techniques, and FIG. **1** is illustrative of just another such example network architecture for which DAS install techniques described herein can be provided.

(110) In some embodiments. FIG. **1** provides a wireless network architecture that also supports partitioned device groups, in which each device group can be provided independent and secure management. In some embodiments, partitioned device groups are provided. In some embodiments, each partitioned group of devices (e.g., mobile devices **100**) can be uniquely managed with secure admin log-ins. In some embodiments, the partitioned device groups are securely managed using the service processor **115** installed on the devices **100** for that device group. In some embodiments, multi-device, multi-user accounting is provided. In some embodiments, capabilities are provided to support multi-party/multi-service reconciliation records to carriers and carrier partners. In some embodiments, service usage and profitability analytics are provided. For example, a partitioned beta test group of devices can be tested and optimized for various service usage policies and/or service plans, and then the optimized service usage policies and/or service plans can be published to an entire or larger device group. In some embodiments, a carrier can be provided a carrier branded device group, and/or a MVNO can be provided a MVNO branded device group.
(111) In some embodiments, DAS install clients (e.g., bootstrappers for devices **100**) are provided. In some embodiments, a first version service processor provides DAS install client function that facilitates a bootstrapping function for downloading and installing a second version service processor. In some embodiments, DAS install clients are provided for creating/downloading and installing a verifiable service processor for each device (e.g., a network capable device, such as a mobile wireless communications device or intermediate networking device). In some embodiments, a DAS install client downloads a uniquely secured service processer for device **100** (e.g., hashed/encrypted, such as based on device credentials, to prevent, for example, mass hacking or other security vulnerabilities, and/or a signed interface between the service processor and modem). In some embodiments, a non-advertised IP address allocated for each device group is rotated (e.g., to counter denial of service (DoS), distributed denial of service (DDS), and/or other types of attacks and/or vulnerabilities or exploits), and service processors are configured with multiple IP addresses for service control access (e.g., for secured network communication with service control **150** and/or service policies and accounting **165**).
(112) In some embodiments, DAS install techniques include one or more of the following operations. First, in some embodiments, whether a device is in a device group or list that includes an installed, up to date, and/or validated service processor is determined (e.g., verify that SIM. ESN, or other unique device identifier is registered, such as in a Home Location Register (HLR)/Network Information Repository (NIR) database or other authorized data store, as associated with service settings/policies for that device for service access and send its associated Charging Data Records (CDRs) to the service controller). Second, in some embodiments, if the device does not have an installed, up to date, and/or validated service processor, then the device is directed to, for example, an activation server to, for example, authenticate the device and/or verify a service processor for the device (e.g., ensure that a current and verified service processor version is installed and/or download a current and verified service processor version for the device).
(113) For example, a DAS install client can be downloaded and installed (e.g., using various bootstrapping techniques, in which, for example, during the installation of the service processor software it is sometimes necessary to update the installer or package manager itself, by using, for example, a small executable file, such as a bootstrapper, that updates the installer and then initiates the new/updated/second version service processor installation after the update, and, in some cases, the bootstrapper can install other prerequisites for the service processor software during the bootstrapping process as well; and using network access to a download server, and/or from a website, including, for example, service processor download function **170**) that allows for secure connection from the device (e.g., mobile device **100**) to a secure download server (e.g., service processor download **170**). In this example, support for a configuration of the device can be determined, such as through a device query or device download of client verification software can be used to verify the device hardware/software configuration). In this example, a user/device validation step can also be performed. For example, an authorization process for a user sign-up can be performed (e.g., based on a user name, MAC address, Turing machine text verification, and/or credit card verification or using other authorization/validation techniques), in which this can be performed automatically or the user/device can be required to enter certain credentials for authorization/validation.
(114) In some embodiments, the authorization process also includes various security techniques for securely associating a user's identity with the device (e.g., using public key/TLS techniques, SSH techniques for TLS, and/or identity management techniques or other security techniques). For example, a check can also be performed to determine if the device was previously and/or is currently an activated device (e.g., the device is already associated with an active service plan). For example, whether the device belongs to a registered device group can also be determined during a DAS install, and if not, then the default settings for that type of device can be applied. In some embodiments, the service processor is encrypted, hashed, and/or obfuscated based on the previous determination (e.g., device group association, default device settings, and/or any other settings/criteria).
(115) In some embodiments, if the device is not associated with a service plan (e.g., based on the device look-up using device based unique identifier(s)/credential(s) or using other techniques, as described herein), then the device can be redirected to a service portal for an activation offer for a service plan (e.g., using an activation server). In some embodiments, the portal utilizes header information to indicate that the device is a managed device (e.g., for a given service provider. MVNO, or other service partner) in the portal request to proxy to an appropriate proxy server for that service provider for the activation process.
(116) In some embodiments, the device is in probation mode after the new service processor install (e.g., restricted a restricted IP address can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS. DDS, and/or other mass or other types of attacks against publicly or other more easily accessible service controller or download servers). In some embodiments, while in probation mode, the service processor executes more robust service monitoring techniques (e.g., more frequent and/or more robust service integrity checks and/or more frequent heartbeats, for example, to monitor actual device/user behavior with the associated expected behavior, as described herein with respect to various embodiments). In some embodiments, after a probation period ends, the device is provided access based on the associated service plan, which is managed, at least in part, by the service processor (e.g., service processor **115**) in communication with, for example, a service controller (e.g., service control **150** and service policies and accounting **165**) or other authorized network elements for service control.
(117) In some embodiments, the various techniques and embodiments described herein can be readily applied to intermediate networking devices (e.g., an intermediate modem or networking device combination). In some embodiments, intermediate networking devices include, for example, WWAN/WLAN bridges, routers and gateways, cell phones with WWAN/WLAN or WWAN/Bluetooth, WWAN/LAN or WWAN/WPAN capabilities, femto cells, back up cards for wired access routers, and/or other intermediate networking devices. In some embodiments, an intermediate networking device (e.g., an intermediate modem or networking device combination) downloads and sends a service processor to one or more devices communicating via the intermediate networking device. In some embodiments, an appropriate and validated service processor is securely downloaded to the intermediate networking device, and the intermediate networking device performs the service processor functions for various wireless communication devices (e.g., mobile wireless communication devices) in communication with the intermediate networking device. In some embodiments, in which one or more wireless communication devices are in wireless communication via an intermediate networking device, some of the service processor functions are performed on the intermediate networking device (e.g., an appropriate and validated service processor is installed or securely downloaded and installed on the intermediate networking device), and some of the service processor functions are performed on the one or more wireless communication devices (e.g., an appropriate and validated service processor is installed or securely downloaded and installed on the mobile device) (e.g., stack controls can be performed on the mobile device and various other controls can be performed on the intermediate networking device). In some embodiments, the one or more wireless communication devices cannot access the network via the intermediate networking device (e.g., the devices are quarantined) unless the one or more wireless communication devices each have an installed and functioning verified service processor (e.g., using CDRs from intermediate networking device and/or network).
(118) In some embodiments, a USB WLAN stick or other similar networking device is provided (e.g., including a modem) with DAS install client software that loads onto the device **100** and installs a service processor **115** on the device **100**. In some embodiments, software on the device **100**

instructs the user to insert a properly configured memory device (e.g., a secured USB memory stick, dongle, or other secured device that can provide a DAS install client software, a service processor image, and/or device credentials for network access). In some embodiments, the USB WLAN installed software assumes control over, for example, the network stack of the device (e.g., for managing network access) and sets various service policies based on whether the service is communicated via the USB WLAN stick or via the WiFi/other (e.g., including requiring no policies, such that access is open). In some embodiments, the DAS install client software on the USB WLAN stick provides a secure client that installs itself/certain software on the device that provides a DAS install client (e.g., bootstrapper) for the device, and the DAS install client downloads an appropriate service processor onto the device and/or the USB WLAN stick (e.g., the stack can also be located and managed on the USB WLAN stick).

(119) In some embodiments. DAS install techniques include ensuring that a device's (e.g., the device modem's) credentials for the access network match the unique credentials for the service processor and the unique credentials for the device (e.g., MAC. SIM, IMSI, and/or other unique credentials for the device). In some embodiments, DAS install techniques include ensuring that multiple IP addresses are not associated with the same service processor for a particular device. In some embodiments, DAS install techniques include determining that this is the same device/modem that a service processor was previously downloaded for and whether that prior service processor is still active on the network. If so, then, in some embodiments, the user is required to type in, for example, a password to continue, for example, a reimaging of the device (or prevent the new device install or to disable the previously activated other service processor).

(120) In some embodiments, DAS install techniques include starting with a device that does not include a service processor (e.g., a device, with, for example, a SIM or EVDO ESSN, but with no service processor, attempts to connect to the network, an appropriate service processor for the device is determined, and then a uniquely associated service processor is downloaded and installed on the device, for example, using a bootstrapper, as similarly described herein). In some embodiments, unique device credentials (e.g., MAC, SIM, IMSI, and/or other unique credentials for the device) are used to create a secure connection with, for example, the service controller (e.g., service control **150**) or a secure download server (e.g., service processor download **170**), to download a (e.g., new or replacement) service processor to be securely installed on the device. Accordingly, as similarly described herein. DAS install techniques can be applied to at least one or more of the following situations: a new service processor install; and/or a replacement service processor install (e.g., the originally/previously installed service processor was wiped/reimaged, hardware failure, or otherwise corrupted or deleted, and, thus, a replacement service processor is needed). In some embodiments, when a device connects to the network without, for example, a service processor, then a look up is performed (e.g., in a data store, such as a database) to determine whether the device is a member of a device group or a new device, and an appropriate service processor (e.g., version and settings) is provided for installation on the device. In some embodiments, when the device attempts an initial access to the network, at that time an updated version of a service processor for that device can be provided based on, for example, device type, device group, master agent, user interface (UI), settings, marketing pages, and/or other features and/or settings, which, for example, can allow for a new, changed, or evolving service plan/program by the time the device logs onto the network to provide, for example, for a dynamic and scalable solution.

(121) In some embodiments, as similarly discussed above, two versions of the service processor are provided (e.g., a first version/image and a second version/image of the service processor software). In some embodiments, a first version service processor is a general purpose version used, for example, primarily for connecting to the network and loading a second version service processor software that, for example, can be one or more of the following: an updated version, a version tailored to a more specific purpose (e.g., based on a device type, device group, service type, service provider or service provider partner, or any other purpose/criteria), a version that includes additional features/functionality, an encrypted service processor version, a version that includes special service plan settings or capabilities associated with a device group, a version that includes specific branding or features/functionality for a given service provider or service provider partner associated with a device group, a version that includes special marketing materials to motivate the user to try or buy services or transactions associated with a device group, and various other versions as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

(122) In some embodiments, depending on whether the user has pre-signed up for a service plan, for example, a different version of the service processor software and/or settings is/are downloaded to the device during this initial service processor download process, including, for example, one or more of the following: a different set of options for service plan choices, marketing materials, ambient service settings and service options, service plan settings, and possibly various other features and/or settings.

(123) In some embodiments, the first version of the service processor is installed during manufacturing or in the distribution channel prior to sale of the device. In some embodiments, the first version of the service processor is installed after the time of sale of the device using various DAS install techniques as described herein with respect to various embodiments.

(124) In some embodiments, the first version of the service processor is not uniquely encrypted so that a general purpose version of the first service processor image can be distributed to multiple devices (e.g., downloadable via the Internet, such as through a website, or a software update not installed by an operable service processor or a software image that is loaded onto the device before the device credentials or device group associations are available or known). In some embodiments, a non-encrypted generic version of the service processor is used for broad distribution to many devices in which the device credentials are not known at the time of service processor software distribution (e.g., the generic version of the service processor can log onto the network to access a software update function in the service controller or service control **150**, service processor downloader or service process download **170**, and/or similar authorized network function, then the service controller can obtain the device credentials and/or user information and provide an updated version of the service processor using the various techniques or similar techniques to those described herein). In some embodiments, the second/updated version of the service processor is uniquely encrypted (e.g., based at least in part on the device credentials or device group associations).

(125) In some embodiments, a first version of the service processor need not be uninstalled and replaced by a new install of a second version of the service processor, as, in some embodiments, the second version of the service processor includes updates to the first version of the service processor, settings changes to the first version of the service processor, and/or encryption or obfuscation of the first version of the service processor to provide a second version of the service processor that is uniquely associated with the device, the device user, the device group, and/or the service plan associated with the device. In some embodiments, the second/updated version of the service processor includes one or more restricted IP addresses providing for access to the secured service control/service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks for the secured service control/service controller(s), such as DoS, DDS, and/or other mass or security attacks against publicly or other more easily accessible service control/service controller(s) and/or service processor download servers.

(126) In some embodiments, the second version of the service processor is uniquely associated with some aspect(s) of the device credentials and/or user information with a temporary user account (e.g., also sometimes referred to herein as a dummy user account) or user account. In some embodiments, the second version of the service processor and/or the settings in the service processor are chosen based on a look up of some aspect of the device credentials and/or the user information to determine which device group version of the service processor and/or settings should be loaded. In some embodiments, when there is no appropriate device group association or the user preference takes priority over device group association, the first version of the service processor software is used to log onto the network (e.g., including potentially the service controller) to select a service offer, or device group association that then determines the second version and/or settings of the service processor software that will be loaded onto the device.

(127) In some embodiments, the first version of the service processor is installed on aftermarket devices, and after installation this more general purpose version of the service processor provides for access to the service control/service controller (or similar network function). In some

embodiments, the service control/service controller determines what type of device and/or what operating system (OS) software and/or what modem and modem software is on the device, and then loads an appropriate version of the service processor for that device or facilitates an updating of the first version of the service processor to provide a second version of the service processor for that device.

(128) In some embodiments, the service processor is distributed on a peripheral device suitable for use with more than one type of device and/or more than one type of OS. Accordingly, in some embodiments, more than one version of the service processor can be shipped with the device for installation on the device once the device type and/or OS type is/are known, with each version of the software either being a first version of the service processor software as discussed above, or a second version or final version of the service processor software as similarly discussed above with respect to various embodiments.

(129) In some embodiments, the first version/second version service processor software techniques, for example, allow for installations of a new OS version that is not compatible in some way with the present version of the service processor. For example, the installation of such a new and incompatible OS version can render the currently installed service processor version incapable of connecting to the network and updating the service processor. In such an example, a rust version service processor software image that is compatible with the new OS can be used to access the network (e.g., connect to the service control/service controller or some other network element) to download and install a new, possibly uniquely encrypted and compatible second service processor image, as similarly discussed above with respect to various embodiments.

(130) In some embodiments, the first version/second version service processor software techniques, for example, can handle situations in which a device has an inadvertently wiped or damaged service processor image such that the device is no longer capable of logging onto the network with its secure credentials and/or uniquely encrypted service processor software image. In such an example, the first version software processor can then be used as similarly described above with respect to various embodiments to download and install a new/replacement second version service processor on the device.

(131) In some embodiments, there are multiple types of device log-in to the service control/service controller depending on whether a first or second version service processor is being used. For example, if a second version service processor is being used, which, in some embodiments, includes unique secure credentials, a uniquely encrypted or secure heartbeat channel, and/or a uniquely encrypted service processor software image, then the capabilities of the device and/or service processor to access the network and/or service controller elements can be as similarly described herein with respect to various embodiments. However, if the device is using a first version service processor, which, for example, does not have unique secure credentials, a uniquely encrypted heartbeat control channel, and/or a uniquely encrypted software image, then the heartbeat control channel traffic can be handled in a differential manner as compared to the traffic handling implemented for a second version service processor image. For example, the service controller heartbeat processing elements can detect that the service processor is a first version service processor and can then route the heartbeat traffic through a different set of security processes that do not rely on all the security aspects present in a second version service processor. As another example, the first version service processor can be a widely distributed software image that does not have unique encryption on the heartbeat channel and can be handled differentially, such as handled with a different server designed to handle insecure traffic and designed to not be disposed or easily exposed to mass or other security attacks (e.g., DoS, DDS attacks, and other types of security related and/or mass/large scale attacks against a network element, such as a download server or web/application server).

(132) In some embodiments, a device supports two or more operating systems (e.g., different versions of operating systems and/or different operating systems) and for each operating system includes a compatible service processor. For example, when a dual boot configured device boots in a first operating system version, then a first service processor that is compatible with that first operating system version is selected for network access, and when the dual boot configured device boots in a second operating system version, then the second service processor that is compatible with that second operating system version is selected for network access.

(133) In some embodiments, initial network access for a device is directed to a service controller (e.g., service control **150**), service processor downloader (e.g., service processor download **170**), and/or similar network element for managing service control. In some embodiments, initial network access is restricted to this initial network access to the service controller, service processor downloader, and/or similar network element for managing service control. In some embodiments, such initial network access is restricted until the device has been verified for network access, as similarly discussed herein with respect to various embodiments. In some embodiments, such initial network access is restricted until the device has been verified for network access and an appropriate service processor has been verified on the device and/or downloaded and installed on the device, as similarly discussed herein with respect to various embodiments. In some embodiments, such initial network access is restricted using various techniques, such as using a first version of a service processor on the device that restricts such initial network access. In some embodiments, such initial network access is restricted to and maintained in probation mode, as similarly described herein (e.g., a restricted IP address can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS, DDS, and/or other mass attacks against publicly or other more easily accessible service controller or download servers). For example, such initial network access can include access to a common activation server, which the device can access for determination of a supported configuration for a new or second service processor image download. As another example, such initial network access can direct the device to an initial web page including access to a service plan offer and purchase options (e.g., providing for a device credential look up for device group, provide choices of programs to user, or other service plan offer and purchase options). As another example, the initial web page can include access to a service plan offer and purchase options and a service processor verification and download/update function.

(134) In some embodiments, a network based charging data record (CDR) feed, as described herein with respect to various embodiments, is provided for monitoring service usage by managed devices. In some embodiments, the CDR feed includes device generated CDRs or micro-CDRs generated by the service processor (e.g., service processor **115** can generate CDRs for monitored service usage on the device, which can, for at least some CDRs, include unique transaction codes for uniquely identifying the monitored service usage based on service or other categorizations/criteria) on the device (e.g., a mobile device or an intermediate networking device for that mobile device). In some embodiments, the CDR feed is a real-time (e.g., near real-time) network based CDR feed provided for determining whether any devices have been compromised (e.g., a hack of a first version or second version service processor providing for unrestricted service usage for such devices, and/or any other mass or security attack or vulnerability or exploit). For example, such a CDR feed can be used to determine abnormal or unusual traffic patterns and/or service level usage activities, which, for example, can be used to identify and/or protect against a DoS/DDS attack or other types of security attacks.

(135) In some embodiments, based on various device and/or network based monitoring techniques, as described herein with respect to various embodiments, a determination is made that the service processor (e.g., service processor **115**) is not functioning properly (e.g., may have been damaged and/or compromised/tampered with and, for example, allowing network access beyond the device's associated service plan and/or not properly monitoring/billing for such service usage) and that a new/replacement service processor should be downloaded. In some embodiments, a new/replacement service processor can be downloaded and installed in such situations, using the various techniques described herein with respect to various embodiments. In some embodiments, based on various criteria (e.g., service usage monitoring, billing, and/or any other criteria) or based on proactive and/or periodic administrative/security measures, a new/replacement service processor can be downloaded and installed, using the various techniques described herein with respect to various embodiments.

(136) In some embodiments, based on, for example, service plan changes (e.g., user changes to their service plan), service provider changes (e.g., service provider changes to their services/service policies or the associated service plan), device changes (e.g., operating system version or other software platform changes or various hardware changes), a new service processor can be downloaded and installed or the installed service processor can be updated, using the various techniques described herein with respect to various embodiments.

(137) FIG. **2** illustrates another wireless network architecture for providing DAS install techniques in accordance with some embodiments. As shown, FIG. **2** includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless mobile devices **100** are in communication with base stations **125** for wireless network communication with the wireless network, and other devices **100** are in communication with Wi-Fi Access Points (APs) or Mesh **702** for wireless communication to Wi-Fi Access CPE **704** in communication with central provider access network **109**. In some embodiments, each of the mobile devices **100** includes a service processor **115** (as shown), which, for example, can be initially installed, downloaded, and/or updated service processors (e.g., first/second version service processor images) using service processor download function **170** as described herein, and each service processor **115** connects through a secure control plane link to a service controller **122**. In some embodiments, the service processor download function **170** is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements as will be apparent to one of ordinary skill in the art in view of the various embodiments disclosed herein.
(138) In some embodiments, service usage information includes network based service usage information (e.g., charging data records (CDRs)), which is obtained from one or more network elements. In some embodiments, service usage information includes micro-CDRs provided by the service processor (e.g., service processor **115**) installed on the device (e.g., mobile device **100**). In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired, as described herein with respect to various embodiments. In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor **115** is programmed to account for that activity associated with that transaction code. In some embodiments, the service processor **115** periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, the service controller **122** or some other network element. In some embodiments, the service controller **122** reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN) and then transmits it to an authorized network element for CDR mediation (e.g., CDR storage, aggregation, mediation, feed **118**, billing system **123**, and/or billing interface **127** or another authorized network element/function). In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system (e.g., billing system **123** and/or billing interface **127**) processes the mediated CDR feed from CDR storage, aggregation, mediation, feed **118**, applies the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to billing systems and/or billing infrastructure (e.g., using new transaction codes to label the new device assisted billing capabilities).
(139) As shown in FIG. **2**, a CDR storage, aggregation, mediation, feed **118** is provided. In some embodiments, the CDR storage, aggregation, mediation, feed **118** receives, stores, aggregates and mediates micro-CDRs received from mobile devices **100**. In some embodiments, the CDR storage, aggregation, mediation, feed **118** also provides a settlement platform using the mediated micro-CDRs, as described herein with respect to various embodiments. In some embodiments, another network element provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface **127** and/or another network element). In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices **100** (e.g., allocating a subset of mobile devices **100** for a distributor, an OEM, a MVNO, and/or another partner). As also shown in FIG. **2**, a MVNO core network **210** also includes a MVNO CDR storage, aggregation, mediation, feed **118**, a MVNO billing interface **127**, and a MVNO billing system **123**. In some embodiments, the MVNO CDR storage, aggregation, mediation, feed **118** receives, stores, aggregates and mediates micro-CDRs received from mobile devices **100** (e.g., MVNO group partitioned devices).
(140) Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing DAS install techniques, and FIG. **2** is illustrative of just one such example network architecture for which DAS install techniques described herein can be provided.
(141) In some embodiments, CDR storage, aggregation, mediation, feed **118** (e.g., service usage **118**, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment apparatus/systems attached to one or more of the sub-networks shown in FIG. **2** (e.g., central provider access network **109** and/or central provider core network **110**), which is in communication with the service controller **122**, and a central billing interface **127**. As shown, service usage **118** provides a function in communication with the central provider core network **110**. In some embodiments, the CDR storage, aggregation, mediation, feed **118** function is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in the AAA server **121** and/or the mobile wireless center/Home Location Register (HLR) **132** (as shown, in communication with a DNS/DHCP server **126**). In some embodiments, service usage **118** functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station **125** in FIG. **2**. In some embodiments, CDR storage, aggregation, mediation, feed **118** functionality is located or partially located in a networking component in the central provider access network **109**, a networking component in the core network **110**, the central billing system **123**, the central billing interface **127**, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed **118**) can be easily generalized as described herein and as shown in the other figures described herein as would be apparent to one of ordinary skill in the art. Also as shown in FIG. **2**, the service controller **122** is in communication with the central billing interface **127** (also sometimes referred to as the external billing management interface or billing communication interface), which is in communication with the central billing system **123**. As shown, an order management **180** and a subscriber management **182** are also in communication with the central provider core network **110** for facilitating order and subscriber management of services for the devices **100** in accordance with some embodiments, and a network provisioning system **162** is also provided in communication with the central provider core network **110** for facilitating network provisioning functions.
(142) In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) collects device generated usage information for one or more devices on the wireless network (e.g., devices **100**); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, as described herein, the CDR storage, aggregation, mediation, feed **118** collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices **100**). In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) also aggregates CDRs and/or micro-CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs and/or micro-CDRs using a rules engine (e.g., bill by account, transactional billing, revenue sharing model, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service).
(143) In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network

elements) communicates a new set of CDRs (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface **127**) or a billing system (e.g., central billing system **123**). In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller (e.g., service controller **122**) to collect the device generated usage information (e.g., micro-CDRs) for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates the device generated usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) communicates with a transport gateway (not shown) and/or a Radio Access Network (RAN) gateway (not shown) to collect the network generated usage information for the one or more devices on the wireless network. In some embodiments, the service controller **122** communicates the device generated service usage information (e.g., micro-CDRs) to the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements).

(144) In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs rules for performing a service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. In some embodiments, the service controller **122** in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed **118** (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

(145) In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed **118**. In some embodiments, the rules engine and associated functions, as discussed herein, is a separate function/device. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing interface **127**. In some embodiments, the service controller **122** performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing system **123**.

(146) In some embodiments, duplicate CDRs are sent from the network equipment to the billing system **123** that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system **123**.

(147) In some embodiments, the service controller **122** sends the device generated CDRs to the rules engine (e.g., service usage **118**), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller **122** generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface **127**. For example, for the service controller **122** to generate CDRs similar to other network elements, in some embodiments, the service controller **122** is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

(148) In some embodiments, the service controller **122** is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed **118**). In some embodiments, where the network necessary apparatus will only recognize CDRs from certain types of networking equipment (e.g. a RAN gateway or transport gateway), then the service controller **122** can provide authentication credentials to the other networking equipment that indicate it is one of the approved types of equipment. In some embodiments, the link between the service controller **122** and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted, and/or signed.

(149) In some embodiments, the CDR storage, aggregation, mediation, feed **118** discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller **122** can provide the device based service usage information (e.g., device based CDRs or micro-CDRs) to the CDR storage, aggregation, mediation, feed **118** (e.g., the CDR storage, aggregation, mediation, feed **118** can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface **127** or the central billing system **123**.

(150) In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

(151) In some embodiments, based on, for example, service plan changes (e.g., user changes to their service plan), service provider changes (e.g., service provider changes to their services/service policies or the associated service plan), micro-CDR transaction code changes, and/or any other related changes, a new service processor can be downloaded and installed or the installed service processor can be updated to allow, for example, the tracking of one or more service usage activities by the device using micro-CDRs (e.g., for new or previously unmonitored/untracked service usage activities, using, for example, new or updated micro-CDR transaction codes (uniquely) associated with such service usage activities), using the various techniques described herein with respect to various embodiments.

(152) FIG. **3** illustrates a flow diagram for DAS install techniques in accordance with some embodiments. At **302**, the process begins. At **304**, whether a device (e.g., mobile device **100**) is in a device group is determined. At **306**, whether the device includes a service processor is determined. If so, at **308**, then the installed service processor is verified (e.g., up to date and/or validated for that device, device group, and/or associated service plan) and network access is allowed (e.g., managed/monitored by the installed and verified service processor according to the associated service plan for the device). Otherwise (e.g., the device does not have an installed service processor), at **310**, then an appropriate service processor for the device is determined (e.g., based on the device type, device group, and/or version, such as hardware/software platform of the device, an associated service plan, service provider, and/or any other criteria or settings). At **312**, the service processor is downloaded and installed (e.g., using a bootstrap process or other techniques, as described herein with respect to various embodiments) and network access is allowed (e.g., managed/monitored by the installed service processor according to the associated service plan for the device).

(153) In some embodiments, the device is also directed to, for example, an activation server to, for example, authenticate the device and/or verify a service processor for the device (e.g., ensure that a current and verified service processor version is installed and/or download a current and verified service processor version for the device) prior to allowing such network access. For example, a DAS install client can be downloaded (e.g., using bootstrapping or other/similar techniques, from a download server and/or from a website) that allows for secure connection from the device (e.g., mobile device **100**) to a secure download server (e.g., service processor download **170**) (e.g., support for a configuration of the device is determined, such as through a device query or device download of client verification software can be used to verify the device hardware/software configuration). In this example, a user/device validation step can also be performed. For example, an authorization process for a user sign-up can be performed (e.g., based on a user name, MAC address. Turing machine text verification, credit card verification, and/or other authorization/validation techniques), in which this can be performed automatically or the user/device can be required to enter certain credentials for authorization/validation. In some embodiments, the authorization process also includes various techniques for associating a user's identity with the device (e.g., using public key/TLS

techniques. SSH techniques for TLS, and/or identity management techniques). In this example, a check can also be performed to determine if the device was previously and/or is currently an activated device (e.g., the device is already associated with a service plan). For example, whether the device belongs to a registered device group can be determined, and if not, then the default settings for that type of device can be applied. In some embodiments, the service processor is encrypted, hashed, and/or obfuscated based on the previous determination (e.g., device group association and/or default device settings). In some embodiments, if the device is not associated with a service plan (e.g., based on the device look-up using device based unique identifier(s)/credential(s), as described herein), then the device can be redirected to a service portal for an activation offer for a service plan (e.g., using an activation server). In some embodiments, the portal utilizes header information to indicate that the device is a managed device (e.g., for a given service provider, MVNO, or other service partner) in the portal request to proxy to an appropriate proxy server for that service provider for the activation process. At **314**, the process is completed.

(154) FIG. **4** illustrates another flow diagram for DAS install techniques in accordance with some embodiments. At **402**, the process begins. At **404**, whether a device (e.g., mobile device **100**) is in a device group is determined (e.g., or other list that indicates that this device includes an installed, up to date, and/or validated service processor, and, for example, to also verify that the SIM, ESN, or other unique device identifier is registered, such as in an HLR/NIR database, as associated with service settings/policies for that device for service access). At **406**, whether the device includes a first version service processor is determined. If not (e.g., the device does not have an installed first version service processor), at **408**, then a new service processor is downloaded (e.g., as similarly discussed above with respect to FIG. **3**) and network access is allowed (e.g., managed/monitored by the installed new service processor according to the associated service plan for the device). Otherwise (e.g., the device includes an installed first version service processor), then at **409**, an appropriate second version service processor for the device is determined (e.g., based on the device type and version, such as hardware/software platform, device group, an associated service plan, service provider, and/or any other criteria or settings). At **412**, the second version service processor (e.g., secured for the device, using various techniques, as described herein) is downloaded and installed (e.g., using bootstrapping or other/similar techniques, as described herein), or in some embodiments, the first version of the service processor is updated to provide a second version service processor uniquely associated with the device, and network access is allowed (e.g., managed/monitored by the installed second version service processor according to the associated service plan for the device). At **414**, the process is completed.

(155) FIG. **5** illustrates another flow diagram for DAS install techniques in accordance with some embodiments. At **502**, the process begins. At **504**, whether a device (e.g., mobile device **100**) is in a device group is determined (e.g., as similarly described above with respect to FIG. **3**). At **506**, whether the device includes a first version service processor is determined. If not (e.g., the device does not have an installed first version service processor), at **508**, then a new service processor is downloaded (e.g., as similarly discussed above with respect to FIG. **3**) and network access is allowed (e.g., managed/monitored by the installed new service processor according to the associated service plan for the device). Otherwise (e.g., the device includes an installed first version service processor), at **510**, then an appropriate second version service processor for the device is determined (e.g., based on the device type and version, such as hardware/software platform, device group, an associated service plan, service provider, and/or any other criteria or settings). At **512**, the second version service processor (e.g., secured using various techniques, as described herein) is downloaded and installed (e.g., using a bootstrap process or other/similar techniques, as described herein). At **514**, network access is allowed in probation mode, as described herein with respect to various embodiments. For example, the device can be managed in probation mode after the new/second version service processor install (e.g., service control communication can be limited to a particular set of probation mode IP addresses that can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS. DDS, or other mass or other security attacks against publicly or other more easily accessible service controller or download servers). In some embodiments, while in probation mode, the service processor executes more robust service monitoring techniques (e.g., more frequent and/or more robust service integrity checks and/or more frequent heartbeats, for example, to monitor actual device/user behavior with the associated expected behavior). At **516**, after the probation period is completed (e.g., based on time, monitored activities, and/or any other criteria), network access is allowed in normal mode (e.g., the device is no longer operating in the probation mode, as described herein). For example, after a probation period is completed (e.g., based on time, monitored activities, and/or any other criteria), the device is provided access based on the associated service plan, which is managed, at least in part, by the service processor in communication with, for example, a service controller or other network element for service control. At **518**, the process is completed.

(156) In some embodiments, the device OS requires a pre-registered and signed version of the service processor software in order for the OS to allow the service processor to be installed or updated. In such embodiments, a sequence of pre-registered, pre-signed service processor software versions that have differing security parameters (e.g., encryption, signature, obfuscation, differences in code sequences, information for query-response sequences, and/or other security parameters) are provided. In some embodiments, the pre-registered service processors are used to regularly update the service processor software for a portion of devices connected to the network, or for all devices connected to the network. In some embodiments, a specific version of the service processor is assigned to a given device, and other versions with other security parameters will not be allowed to obtain service from the network. For example, more than one version of the software can be registered and distributed at any one time so that a hacker cannot create code that works for all devices. A sequence of service processor versions can be held in reserve and deployed when a successful software hack version is detected in the field for one or more previous service processor versions, and the new versions that have been held in reserve can be used to update devices in the field. As the reserved versions have not yet been distributed prior to the detection of a successful hack, it is not possible for a hacker to have a hacked version of the new software, and by refreshing new versions on a frequent basis it can become impossible for a hacker to successfully hack the new versions before additional new versions are deployed. Such embodiments can buy time by keeping successful software hacks out of the devices in the field until the successful software hack can be analyzed and a systematic security solution implemented to prevent the hack from remaining effective.

(157) In some embodiments not all of the service processor software is modified into pre-registered modified security configuration versions that are regularly refreshed, but instead a portion of the service processor software that includes unique security information (e.g., security keys, signatures and/or responses to secure queries, and/or other security information, and/or the capability to analyze the integrity of the other service processor software). In this manner, when a device is suspected of being hacked the new service processor software portion with different security configuration can be updated and used to ascertain the integrity of the existing service processor configuration, which makes the update process shorter and lower bandwidth.

(158) Clause 1: A system, comprising a processor of a network device configured to: determine if a communications device in communication with a wireless network includes a service processor for assisting control of the communications device use of a service on the wireless network, wherein the service processor includes a service profile that includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service; and verify the service processor; and a memory of the network device coupled to the processor and configured to provide the processor with instructions.

(159) The system recited in clause 1, wherein the service policy settings include one or more of the following: access control settings, traffic control settings, billing system settings, user notification with acknowledgment settings, user notification with synchronized service usage information, user privacy settings, user preference settings, authentication settings, admission control settings, application access settings, content access settings, transaction settings, and network or device management communication settings.

(160) Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

INCORPORATION BY REFERENCE

(161) This application incorporates by reference the following U.S. patent applications for all purposes:

(162) Application Ser. No. 12/694,455, entitled DEVICE ASSISTED SERVICES INSTALL, filed Jan. 27, 2010; application Ser. No. 12/380,780, entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed Mar. 2, 2009; provisional Application No. 61/206,354, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed Jan. 28, 2009; provisional Application No. 61/206,944, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed Feb. 4, 2009; provisional Application No. 61/207,393, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 10, 2009; provisional Application No. 61/207,739, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed Feb. 13, 2009; and provisional Application No. 61/264,120, entitled DEVICE ASSISTED SERVICES INSTALL filed Nov. 24, 2009.

Claims

1. A system comprising: a processor of a network device configured to: determine if a wireless device in communication with a wireless network includes a service processor for assisting control of the wireless device use of a service on the wireless network, wherein the service processor includes a service profile that includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service; securely connect, via a service control device link using the wireless network, the network device to the service processor of the wireless device; receive service provider information from the wireless device; determine, based on the service provider information, that the wireless device is associated with a particular service provider, wherein the service provider information is one of a user selection indicating the particular service provider or a credential of the wireless device associated with the particular service provider; and provide, based on the determined association of the wireless device with the particular service provider, via the service control device link using the wireless network, the wireless device with a branding specific to the particular service provider, wherein the branding updates a user interface characteristic of the wireless device to be specific to the particular service provider; a memory of the network device coupled to the processor and configured to provide the processor with instructions.

2. The system of claim 1, wherein providing the wireless device with a branding specific to the particular service provider includes providing a software update or an additional software download.

3. The system of claim 2, wherein the software update or the additional software download includes: a version based on a device type, a version based on a device group, a version based on a service type, an encrypted version, a version that includes a service plan setting or capability associated with the device group, a version that includes marketing material, a version for offering a service plan option, a version with an ambient service setting, or a version with an ambient service option.

4. The system of claim 2, wherein the software update or the additional software download further includes a feature or a functionality for the particular service provider.

5. The system of claim 1, wherein the service provider information is the credential of the wireless device and includes information derived from a subscriber information module (SIM), an international mobile subscriber identity (IMSI), an electronic serial number (ESN), a media access control (MAC) address, or a unique device identifier.

6. The system of claim 1, wherein the processor of the network device is further configured to: provide the wireless device with a policy setting for assisting the wireless device in connecting to a particular wireless access network.

7. The system of claim 6, wherein the policy setting is for assisting in presenting a notification, obtaining or presenting service usage information, obtaining an acknowledgment, obtaining or implementing a user preference, or obtaining or implementing a privacy setting.

8. The system of claim 6, wherein the policy setting includes an authentication setting, an admission control setting, a network or device management communication setting, an application access setting, a content access setting, or a transaction setting.

9. The system of claim 6, wherein the policy setting assists in directing or controlling traffic or billing for a service.

10. The system of claim 1, wherein the processor of the network device is further configured to: modify the service profile of the wireless device based on association of the wireless device with one of a plurality of device groups.

11. A method for use by a processor of a network device, the method comprising: determining if a wireless device in communication with a wireless network includes a service processor for assisting control of the wireless device use of a service on the wireless network, wherein the service processor includes a service profile that includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service; securely connecting, via a service control device link using the wireless network, the network device to the service processor of the wireless device; receiving service provider information from the wireless device; determining, based on the service provider information, that the wireless device is associated with a particular service provider, wherein the service provider information is one of a user selection indicating the particular service provider or a credential of the wireless device associated with the particular service provider; and providing, based on the determined association of the wireless device with the particular service provider, via the service control device link using the wireless network, the wireless device with a branding specific to the particular service provider, wherein the branding updates a user interface characteristic of the wireless device to be specific to the particular service provider.

12. The method of claim 11, wherein providing the wireless device with a branding specific to the particular service provider includes providing a software update or an additional software download.

13. The method of claim 12, wherein the software update or the additional software download includes: a version based on a device type, a version based on a device group, a version based on a service type, an encrypted version, a version that includes a service plan setting or capability associated with the device group, a version that includes marketing material, a version for offering a service plan option, a version with an ambient service setting, or a version with an ambient service option.

14. The method of claim 12, wherein the software update or the additional software download further includes a feature or a functionality for the particular service provider.

15. The method of claim 11, wherein the service provider information is the credential of the wireless device and includes information derived from a subscriber information module (SIM), an international mobile subscriber identity (IMSI), an electronic serial number (ESN), a media access control (MAC) address, or a unique device identifier.

16. The method of claim 11, further comprising: providing the wireless device with a policy setting for assisting the wireless device in connecting to a particular wireless access network.

17. The method of claim 16, wherein the policy setting is for assisting in presenting a notification, obtaining or presenting service usage information, obtaining an acknowledgment, obtaining or implementing a user preference, or obtaining or implementing a privacy setting.

18. The method of claim 16, wherein the policy setting includes an authentication setting, an admission control setting, a network or device management communication setting, an application access setting, a content access setting, or a transaction setting.

19. The method of claim 16, wherein the policy setting assists in directing or controlling traffic or billing for a service.

20. The method of claim 11, further comprising: modifying the service profile of the wireless device based on association of the wireless device with one of a plurality of device groups.