US008792637B2

(12) **United States Patent**
Tang et al.

(10) **Patent No.: US 8,792,637 B2**
(45) **Date of Patent: Jul. 29, 2014**

(54) **DOWNLOADING OF DATA TO SECURE DEVICES**

(75) Inventors: **Lawrence W Tang**, San Diego, CA (US); **Douglas M Petty**, San Diego, CA (US); **Michael T Habrat**, San Diego, CA (US)

(73) Assignee: **Combined Conditional Access Development & Support, LLC**, Philadelphia, PA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 89 days.

(21) Appl. No.: **13/302,639**

(22) Filed: **Nov. 22, 2011**

(65) **Prior Publication Data**

US 2013/0129086 A1 May 23, 2013

(51) **Int. Cl.**

H04L 9/00	(2006.01)
H04L 29/06	(2006.01)
H04L 9/32	(2006.01)
G06F 21/00	(2013.01)
G06F 12/14	(2006.01)
H04L 9/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0891*** (2013.01); ***H04L 9/0861*** (2013.01); ***H04L 63/0435*** (2013.01); *H04L 63/0428* (2013.01); *H04L 9/3236* (2013.01)

USPC **380/44**; 380/277; 713/150; 713/168; 713/189; 713/190

(58) **Field of Classification Search**

CPC G06F 21/10; G06F 21/606; G06F 21/62; H04L 12/40104; H04L 9/0844; H04L 63/0428; H04L 9/3236

USPC 380/255, 259, 44–47, 277–286; 713/150, 168, 170, 189, 190

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

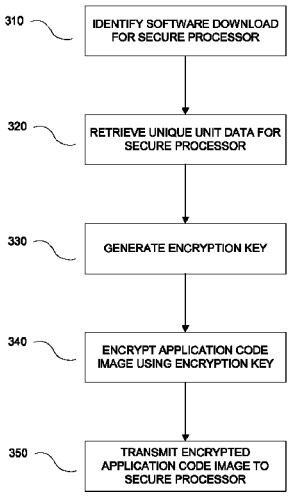
5,751,812	A *	5/1998	Anderson	713/155
5,841,871	A *	11/1998	Pinkas	713/155
6,697,945	B2 *	2/2004	Ishiguro et al.	713/171
6,831,982	B1 *	12/2004	Hughes et al.	380/281
6,934,463	B2 *	8/2005	Ishiguro et al.	386/259
7,502,467	B2 *	3/2009	Brainard et al.	380/44
7,502,933	B2 *	3/2009	Jakobsson et al.	713/172
7,929,705	B2 *	4/2011	Kim et al.	380/278
8,238,552	B2 *	8/2012	Weber	380/44
2003/0007637	A1 *	1/2003	Banks	380/51
2005/0010788	A1 *	1/2005	Craft	713/187
2006/0059571	A1 *	3/2006	Chen et al.	726/29
2006/0195402	A1 *	8/2006	Malina et al.	705/50
2006/0256961	A1 *	11/2006	Brainard et al.	380/44
2007/0067631	A1 *	3/2007	Westhoff	713/168
2007/0113083	A1 *	5/2007	Volkovs et al.	713/168

(Continued)

Primary Examiner — Tae Kim

(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

An encryption key may be generated based on personalized unit data associated with a software download recipient, for example, a secure processor. In some aspects, the secure processor may generate a decryption key based on its personalized unit data, and a software download may be performed between the software provider and the secure processor using the generated encryption keys. The secure processor may then decrypt and load the software for execution. The encryption and decryption key generation may also be based on a sequence number or other data indicating one or more previous software downloads at the secure processor. Using the sequence number or other data, sequences of multiple encryption and/or decryption keys may be generated to support multiple software downloads to a secure processor.

21 Claims, 8 Drawing Sheets