



(12) **United States Patent**
Pesonen

(10) **Patent No.:** **US 7,699,233 B2**
(45) **Date of Patent:** **Apr. 20, 2010**

(54) **METHOD FOR ISSUER AND CHIP SPECIFIC
DIVERSIFICATION**

(75) Inventor: **Lauri Pesonen**, Espoo (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 670 days.

(21) Appl. No.: **11/264,139**

(22) Filed: **Nov. 2, 2005**

(65) **Prior Publication Data**

US 2007/0095927 A1 May 3, 2007

(51) **Int. Cl.**
G06K 19/06 (2006.01)

(52) **U.S. Cl.** **235/492**; 235/472.02

(58) **Field of Classification Search** 235/492,
235/472.02, 487; 713/168, 169, 172, 173;
455/410, 411, 418, 419

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,745,571 A * 4/1998 Zuk 380/285
6,212,634 B1 * 4/2001 Geer et al. 713/156

7,246,242 B1 * 7/2007 Niemi et al. 713/181
2003/0236983 A1 * 12/2003 Mihm, Jr. 713/172
2005/0153741 A1 * 7/2005 Chen et al. 455/558

FOREIGN PATENT DOCUMENTS

GB 2389272 A * 3/2003
GB 2389272 12/2003
WO WO 04002054 12/2003
WO WO 2005036916 4/2005

OTHER PUBLICATIONS

International Search Report, PCT/IB2006/003037, Mail date Feb. 28, 2007.

* cited by examiner

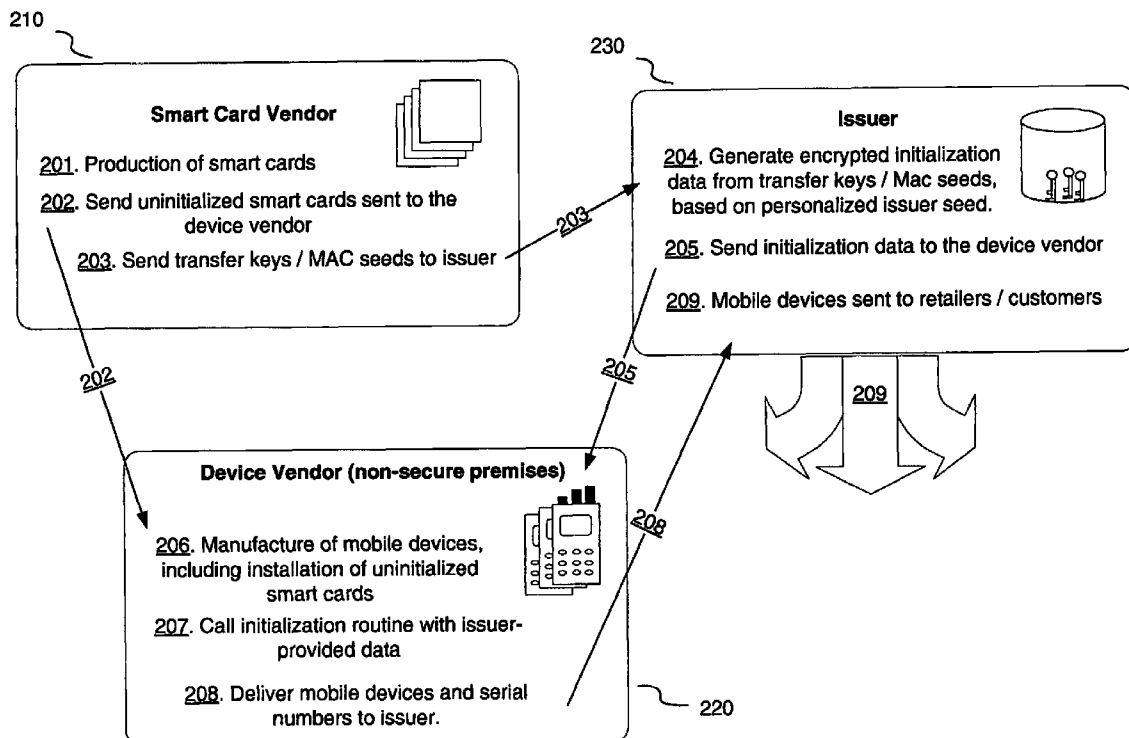
Primary Examiner—Kumiko C Koyama

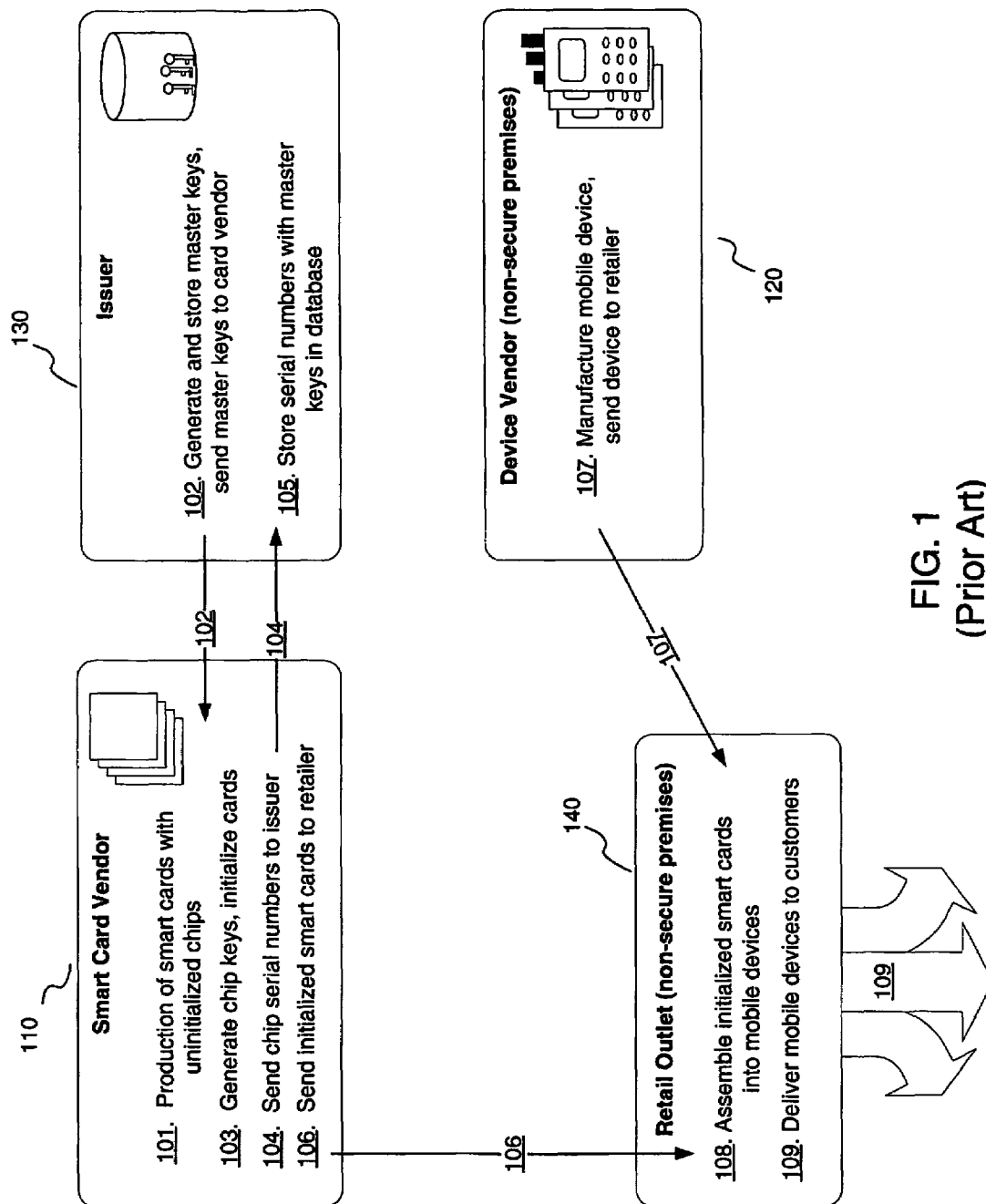
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A system and method for initializing secure elements for use in mobile devices. A mobile device manufacturer embeds uninitialized secure elements into mobile devices. An issuer-specific seed value is securely passed into an initialization routine in the operating system of the secure element. The initialization routine diversifies the initial root keys on the secure element with the issuer seed and the unique chip serial number to create master and chip keys for use in secure communications between the issuer and the mobile device user.

45 Claims, 7 Drawing Sheets



FIG. 1
(Prior Art)

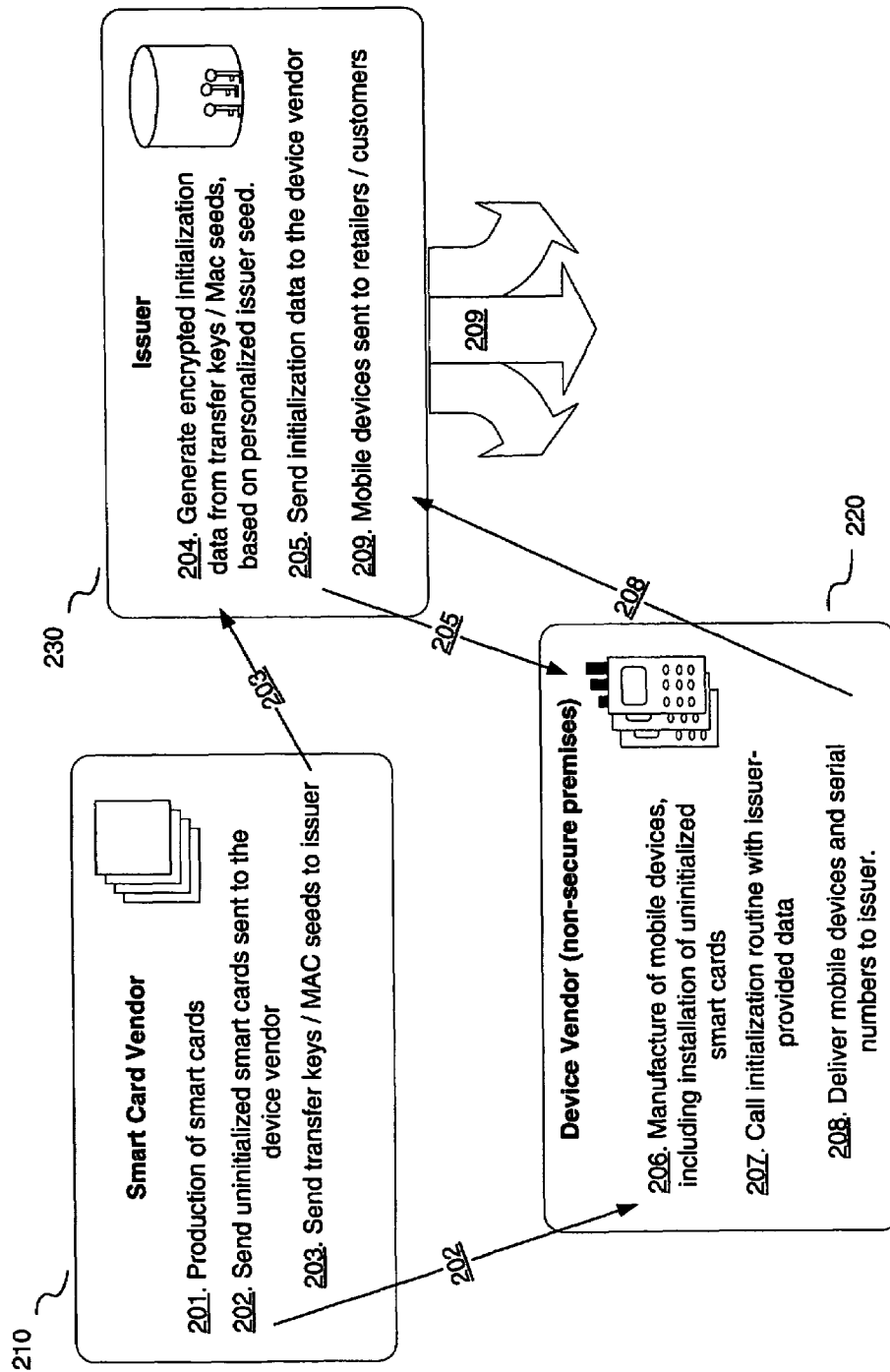


FIG. 2

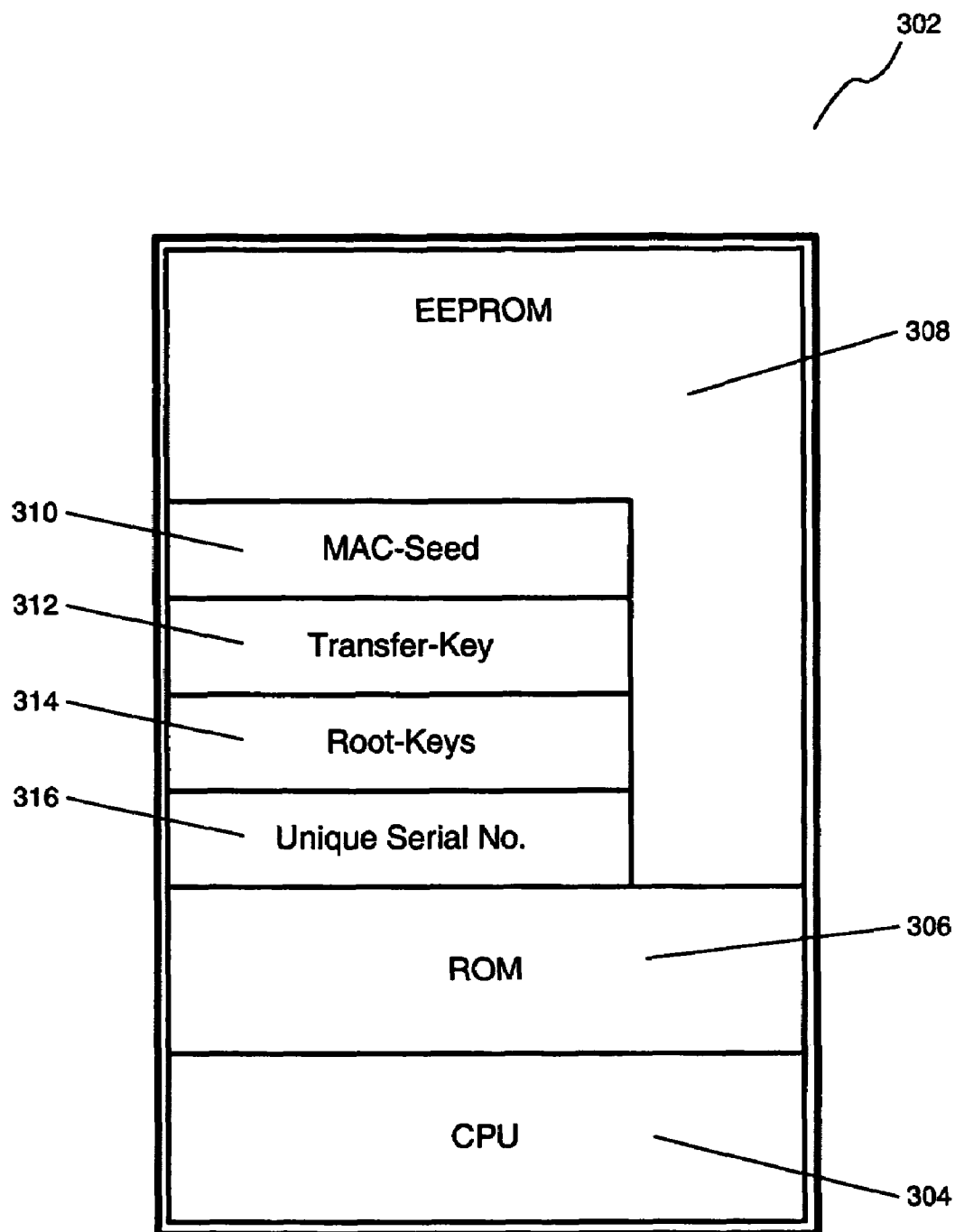


FIG. 3

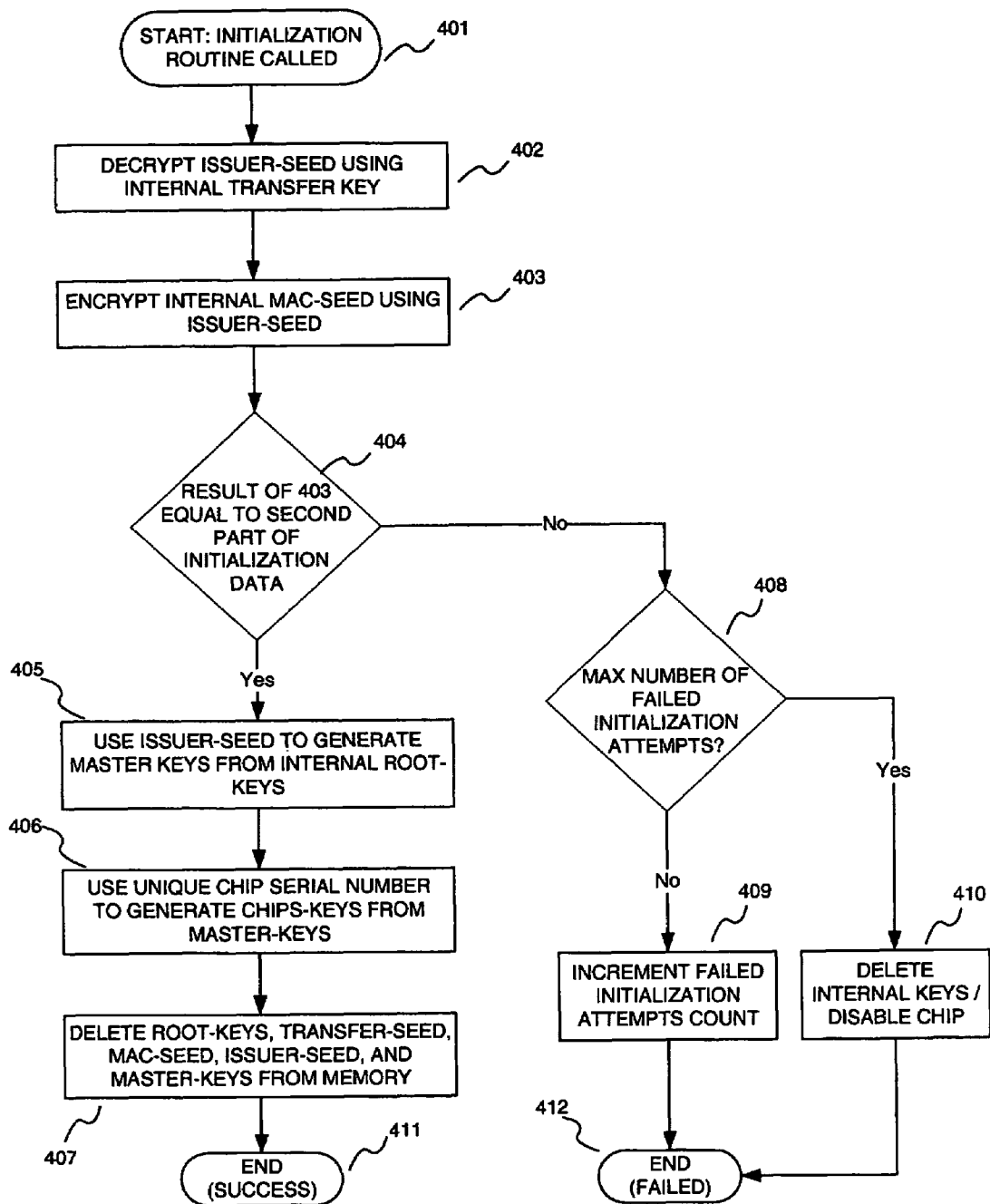


FIG. 4

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.