US006460138B1

(12) **United States Patent**
Morris

(10) **Patent No.: US 6,460,138 B1**
(45) **Date of Patent: Oct. 1, 2002**

(54) **USER AUTHENTICATION FOR PORTABLE ELECTRONIC DEVICES USING ASYMMETRICAL CRYPTOGRAPHY**

(75) Inventor: **Robert Paul Morris**, Raleigh, NC (US)

(73) Assignee: **Flashpoint Technology, Inc.**, Peterborough, NH (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/166,344**

(22) Filed: **Oct. 5, 1998**

(51) **Int. Cl.**^{7} **H04L 9/30**
(52) **U.S. Cl.** **713/184**; 713/168
(58) **Field of Search** 713/184, 168, 713/179, 170, 172, 176, 181, 193; 380/247

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,282,247 A	*	1/1994	McLean et al.	....	711/164
5,293,424 A	*	3/1994	Hotley et al.	....	713/193
5,499,294 A	*	3/1996	Friedman	....	713/179
5,552,897 A		9/1996	Mandelbaum	....	358/400
5,778,072 A		7/1998	Samar	....	380/30
5,917,913 A	*	6/1999	Wang	....	705/67
5,933,328 A	*	8/1999	Wallace et al.	....	361/737
6,003,135 A	*	12/1999	Bialick et al.	....	713/201
6,026,293 A	*	2/2000	Osborn	....	455/411
6,038,549 A	*	3/2000	Davis et al.	....	705/35
6,084,967 A	*	7/2000	Kennedy et al.	....	380/247

FOREIGN PATENT DOCUMENTS

EP	1 017 223 A2	*	7/2000

OTHER PUBLICATIONS

An Introduction to Cyptography, Entrust Technologies, Dec. 1997 http://www.entrust.com/resources/pdf/cry.

Introduction to Public–Key Cryptography, Netscape, 9/2598 http://developer.netscape.com/docs/manuals.

Smartcard Invasion Continues, Byte, Apr. 1998 http://www.byte.com/art/9804/sec19/art1.htm.

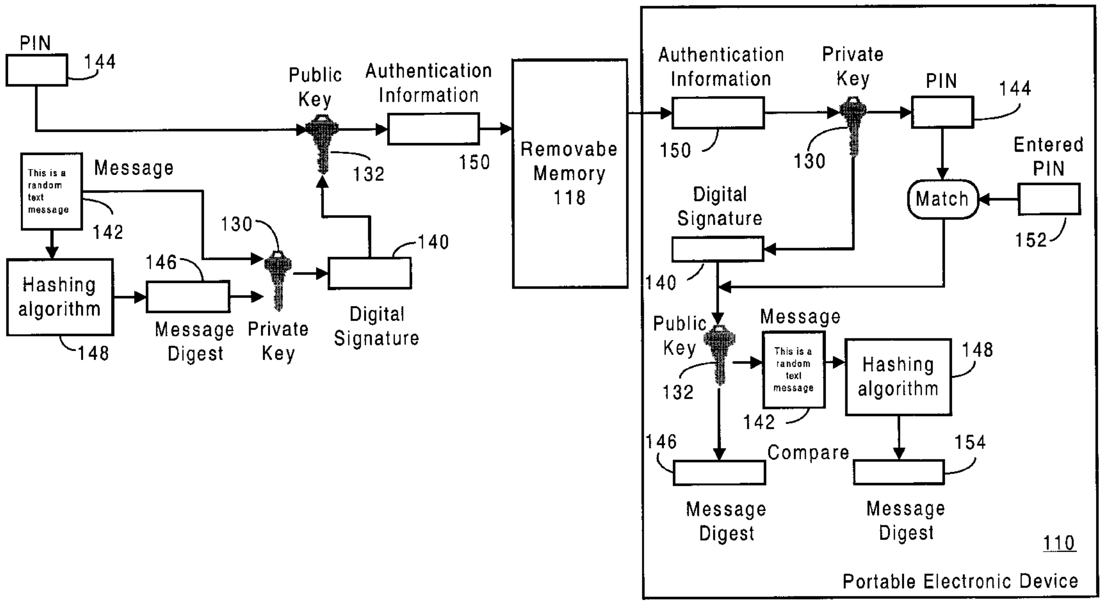
* cited by examiner

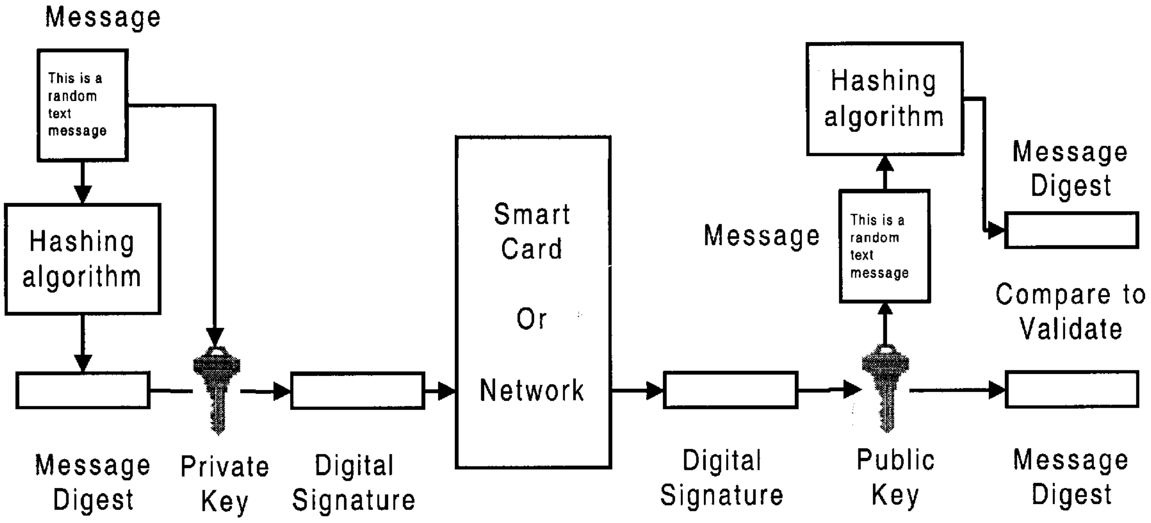
Primary Examiner—Matthew Smithers
(74) *Attorney, Agent, or Firm*—Stephen G. Sullivan; Sawyer Law Group LLP

(57) **ABSTRACT**

A system and method for authenticating a user of a portable electronic device having a removable memory using asymmetric cryptography, the asymmetric cryptography requiring the use of a user'private key and public key. The method and system include storing the user'private key and public key on the portable electronic device. Thereafter, information including the user'personal identification number (PIN) is encrypted using the user'private key and public key, respectively, to create encrypted authentication information. The encrypted authentication information is then stored on a standard removable memory, such as a flash card. When the removable memory is subsequently inserted into the portable electronic device, the portable electronic device automatically decrypts the authentication information and prompts the user for a PIN code. If the decrypted authentication information and the entered PIN are verified, the user is authenticated without the use of a smart card or card reader and the device is unlocked allowing the user to gain access.

11 Claims, 3 Drawing Sheets





PRIOR ART

FIG. 1

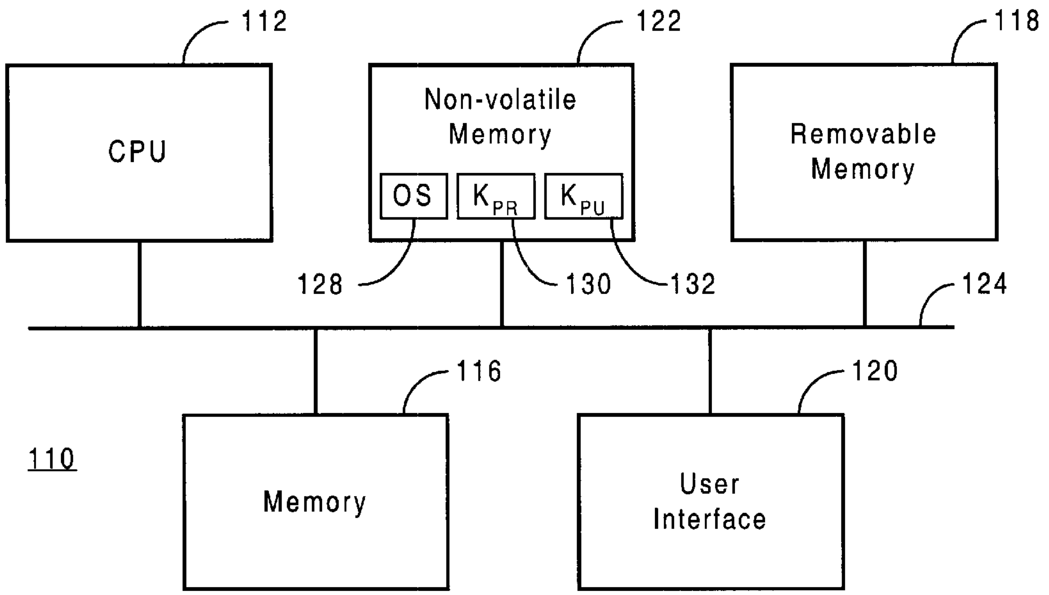
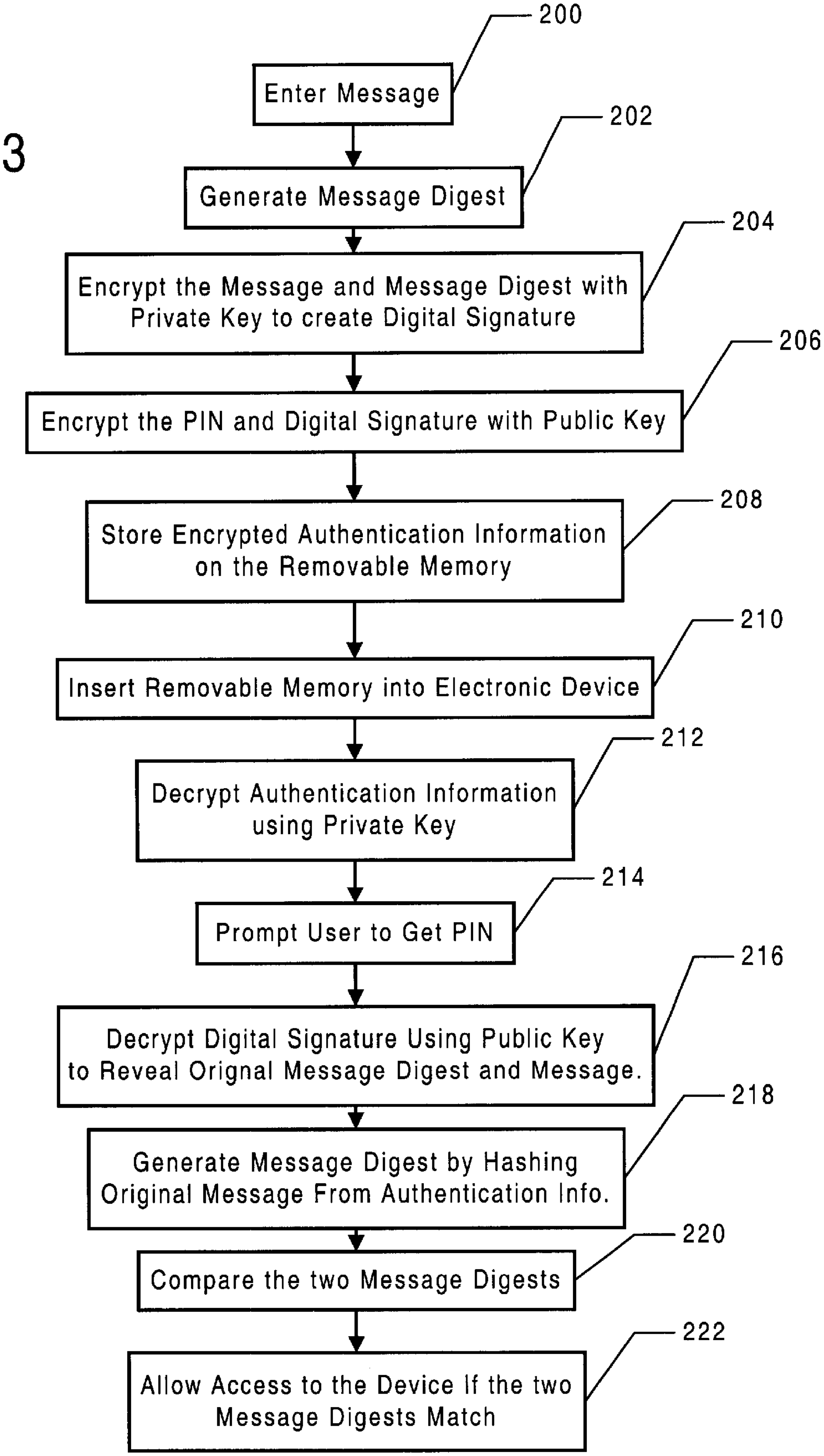


FIG. 2

FIG. 3


200
Enter Message
202
Generate Message Digest
204
Encrypt the Message and Message Digest with Private Key to create Digital Signature
206
Encrypt the PIN and Digital Signature with Public Key
208
Store Encrypted Authentication Information on the Removable Memory
210
Insert Removable Memory into Electronic Device
212
Decrypt Authentication Information using Private Key
214
Prompt User to Get PIN
216
Decrypt Digital Signature Using Public Key to Reveal Orignal Message Digest and Message.
218
Generate Message Digest by Hashing Original Message From Authentication Info.
220
Compare the two Message Digests
222
Allow Access to the Device If the two Message Digests Match

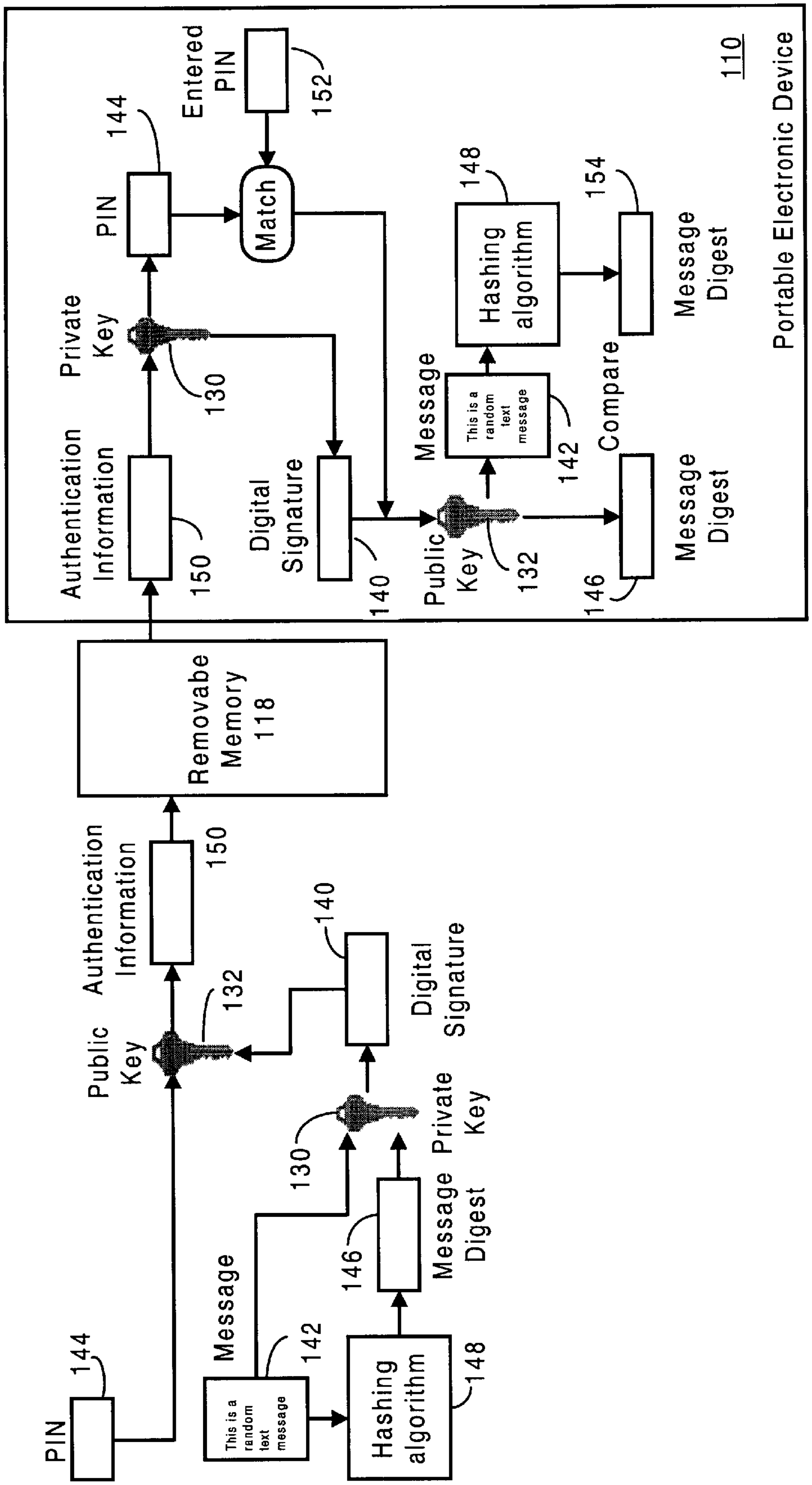

PIN
144
Message
This is a random text message
142
Hashing algorithm
148
Message Digest
146
130
Private Key
Digital Signature
140
Public Key
132
Authentication Information
150
Removabe Memory 118
Authentication Information
150
Private Key
130
PIN
144
Match
Entered PIN
152
Digital Signature
140
Public Key
132
Message
This is a random text message
142
Hashing algorithm
148
Message Digest
146
Compare
Message Digest
154
110
Portable Electronic Device

FIG. 4

USER AUTHENTICATION FOR PORTABLE ELECTRONIC DEVICES USING ASYMMETRICAL CRYPTOGRAPHY

FIELD OF THE INVENTION

The present invention relates to the security of portable electronic devices, and more particularly to a method and system for the authentication of a user of a portable electronic device using asymmetrical cryptography.

BACKGROUND OF THE INVENTION

Security for most electronic devices dealing with sensitive data utilizes one or another form of a password (PIN or access code) to prevent unauthorized access. In order to use a device the user is requested to enter a password or pin. If correct, the user is allowed to use the device, if not, well he/she is usually just prompted to try again.

Password protection, however, has not proven to be a very effective means of user authentication due to two fundamental problems with passwords. If they are relatively short and easy to memorize, they may be easily compromised either through guessing (by unauthorized users) or broken using a simple password cracking program. Stronger protection is achieved through longer, meaningless or randomly generated passwords, but they are easy to forget (by authorized users). And in many portable electronic devices, the situation is even worse in the cases where passwords are stored in storage that requires batteries to keep it stable. An unauthorized user can simply remove the batteries and wait for the password to disappear.

An improved approach to providing security for electronic devices is to create long, invincible passwords using public-key cryptography, and to then store those passwords (digital keys) on smart cards. A Smart card is a plastic credit card that carries an imbedded chip instead of a magnetic stripe.

Public-key cryptography enables two communicating parties to disguise information they send to each other through encryption and decryption. Using the digital keys stored on the smart card, the sender encrypts, or scrambles, information before storing it on a smart card. The encrypted information on the smart card is unintelligible to an intruder. When the smart card is inserted into a smart card reader attached to the device to be accessed, the smart card reader decrypts, or unscrambles, the information. Access to the device is allowed once the information is verified.

Many of today'smart cards use asymmetric cryptographic algorithms. With this method, a public key is used in combination with a private key that is only used by the owner of the smart card. Typically, the private key is stored on the smart card, while the public key is stored within the protected electronic device. A message sent using these two keys can only be decoded using the complementary keys. Thus, anonymous and secure data transmission is attained using the public key and the data can only be read by the owner of the private key.

Before a user can own a smart card, the user must first obtain a certificate from a certificate authority. A certificate issued by the certificate authority binds a particular public key to the name of the person or entity the certificate identifies (such as the name of an employee). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the person or entity identified by the certificate.

These public and private keys are used to authenticate the person by creating a digital signature for that person, which is then stored on the smart card along with the person's PIN. When the user inserts his/her smart card into a smart card reader to gain access to a particular device, the user is prompted for the PIN. If the PIN matches the PIN read from the card, the user's digital signature is then used to authenticate that the user is who he/she claims to be.

FIG. **1** is diagram illustrating a standard smart card protocol for creating and verifying a digital signature. A digital signature is created by running message text through a hashing algorithm. This yields a message digest. The message digest along with the message is then encrypted using the private key of the individual who is sending the message, turning it into a digital signature. The digital signature can only be decrypted by the public key of the same individual. The recipient of the message decrypts the digital signature to obtain the original message, and uses the original message to recalculate the message digest. The value of this newly calculated message digest is compared to the value of the message digest found from the digital signature. A match indicates that the message has not been tampered with. Since the public key of the sender was used to verify the signature, the text must have been signed with the private key owned by the sender.

This use of digital signatures is the emerging standard for user authentication and security in network environments. In theory, a person can use the same digital certificate to gain access to any number of services, rather than having to remember and manage a number of different passwords. Smart cards are not subject to tampering or forgery (provided the key is long enough). An unauthorized user would have to know the user's PIN and also have the user's digital certificate to gain access.

Unfortunately, there is problem with using smart cards to provide security for portable electronic devices because smart card readers are too bulky to be built in to such devices. For example, certain types of portable electronic devices, such as digital cameras and personal digital assistants, utilize removable memories that are even smaller than PCMCIA cards. One example of this type of memory is a compact flash card. One solution is to carry an external smart card reader around as a peripheral device and plug it into such a device when the user wishes to use the device. This, however, would be inconvenient and burdensome to the user. And simply storing a pin and a digital certificate on a removable memory compatible with the portable electronic device is not an acceptable alternative because of the risk of having the memory lost or stolen. This would allow a third party to gain access to the user's PIN and to impersonate the owner in any transaction where asymmetrical cryptography are used for authentication.

Accordingly, what is needed is a system and method for authenticating the user of a portable electronic device without the need of a smart card and reader. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The present invention provides a method and system for authenticating a user of a portable electronic device having a removable memory using asymmetric cryptography, the asymmetric cryptography requiring the use of a user's private key and public key. The method and system include storing the user's private key and public key on the portable electronic device. Thereafter, information including the user's personal identification number (PIN) is encrypted

DOCKET ALARM

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE