US005668876A

United States Patent [19]

Falk et al.

[11] Patent Number: 5,668,876

[45] Date of Patent: Sep. 16, 1997

[54] **USER AUTHENTICATION METHOD AND APPARATUS**

[75] Inventors: **Johan Per Falk**, Stockholm; **Björn Erik Rutget Jonsson**, Järfälla, both of Sweden

[73] Assignee: **Telefonaktiebolaget LM Ericsson**, Stockholm, Sweden

[21] Appl. No.: **264,939**

[22] Filed: **Jun. 24, 1994**

[51] **Int. Cl.**[6] **H04L 9/32**; H04L 9/00

[52] **U.S. Cl.** **380/25**; 380/4; 380/23; 380/49; 340/825.31; 340/825.34; 235/380

[58] **Field of Search** 380/4, 23, 24, 380/25, 28, 30, 49; 235/379, 380; 340/825.31, 825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,223,830	9/1980	Walton	235/380
4,236,068	11/1980	Walton	235/380
4,268,715	5/1981	Atalia	379/62
4,384,288	5/1983	Walton	340/825.34
4,436,957	3/1984	Mazza et al.	379/62
4,606,073	8/1986	Moore	455/89
4,654,481	3/1987	Corris et al.	379/62
4,935,962	6/1990	Austin	380/25
4,992,783	2/1991	Zdunek et al.	340/825.34
4,995,083	2/1991	Baker et al.	380/23
5,077,790	12/1991	D'Amico et al.	380/528
5,131,038	7/1992	Puhl et al.	380/23
5,153,581	10/1992	Hazard	340/825.34
5,168,520	12/1992	Weiss	380/23
5,282,250	1/1994	Dent et al. .	
5,287,545	2/1994	Kallin	455/33.1
5,390,245	2/1995	Dent et al. .	

FOREIGN PATENT DOCUMENTS

0 374 012	6/1990	European Pat. Off.	G07F 7/10
0 505 637A2	9/1992	European Pat. Off.	H04Q 7/04
0 650 307A2	4/1995	European Pat. Off.	H04Q 7/38
3 405 381	8/1985	Germany	H04Q 7/02
3 420 460	12/1985	Germany	H04Q 7/02
2 190 820	11/1987	United Kingdom	H04L 9/02
WO92/20048	11/1992	WIPO	G07F 7/08
WO93/17529	9/1993	WIPO	H04Q 7/04

OTHER PUBLICATIONS

H. Beker and F. Piper, Cipher Systems—The Protection of Communications, pp. 305–311, 320–322, published in Great Britain (1982).

"EIA Project Number 2215," Electronic Industries Association Engineering Department, published in Dec. 1989, pp. 2–72 to 2–73.

Sören Wallinder, "Implementation of UPT—Universal Personal Telecommunication," *Ericsson Review*, No. 1, 1994, pp. cover, 40–48.

EIA/TIA Interim Standard, "Cellular System Dual-Mode Mobile Station—Base Station Compatibility Standard," IS–54–B, Apr. 1991, pp. cover 86–99.

"European digital cellular telecommunications system (Phase 2); Security aspects (GSM 02.09)," *European Telecommunications Standards Institute*, Oct. 1993, pp. 1–12.

"European digital cellular telecommunications system (Phase 2); Security related network functions (GSM 03.20)," *European Telecimmunications Standards Institute*, Oct. 1993, pp. 1–53.

Primary Examiner—Bernarr E. Gregory

Attorney, Agent, or Firm—Burns, Doane, Swecker & Mathis, L.L.P.

[57] **ABSTRACT**

Authorization for a user to use a service is provided by a modified pager which calculates a unique response code to a transmitted challenge code based on the challenge code, an input personal identification number, and an internal key. The response code is input to a simple terminal, such as a telephone and if the unique response code is acceptable, the user may access the desired service, such as cashless transactions or long distance phone service.

37 Claims, 3 Drawing Sheets

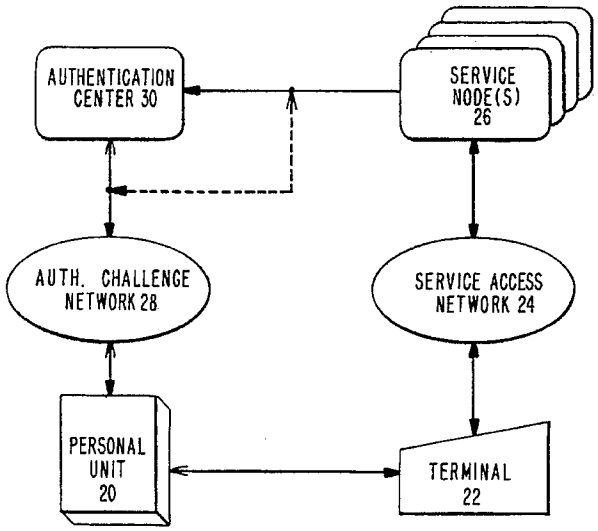


Fig. 1

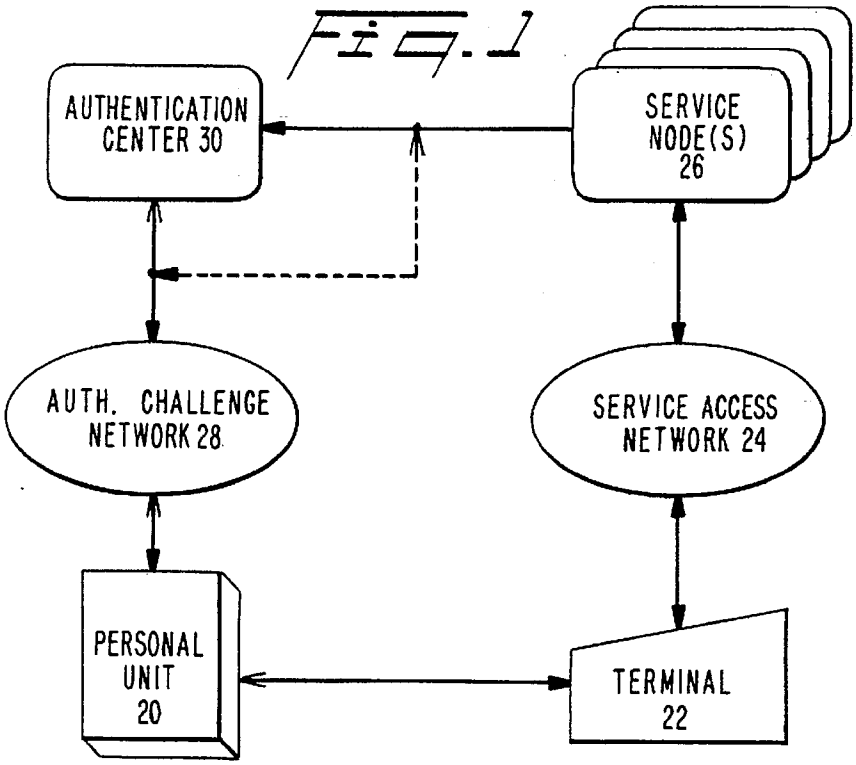


Fig. 1A

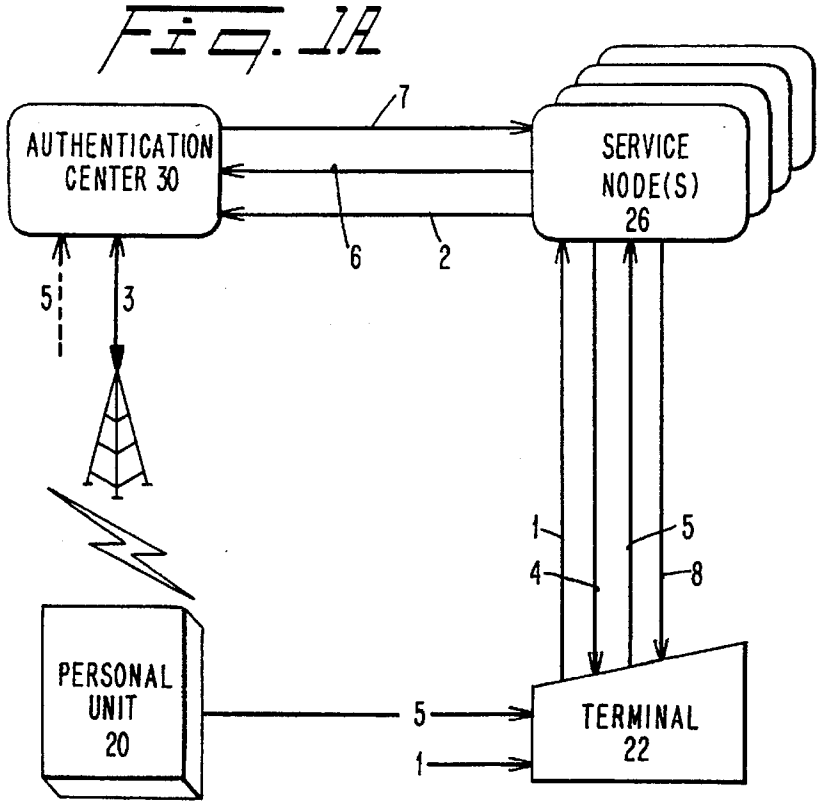


Fig. 2

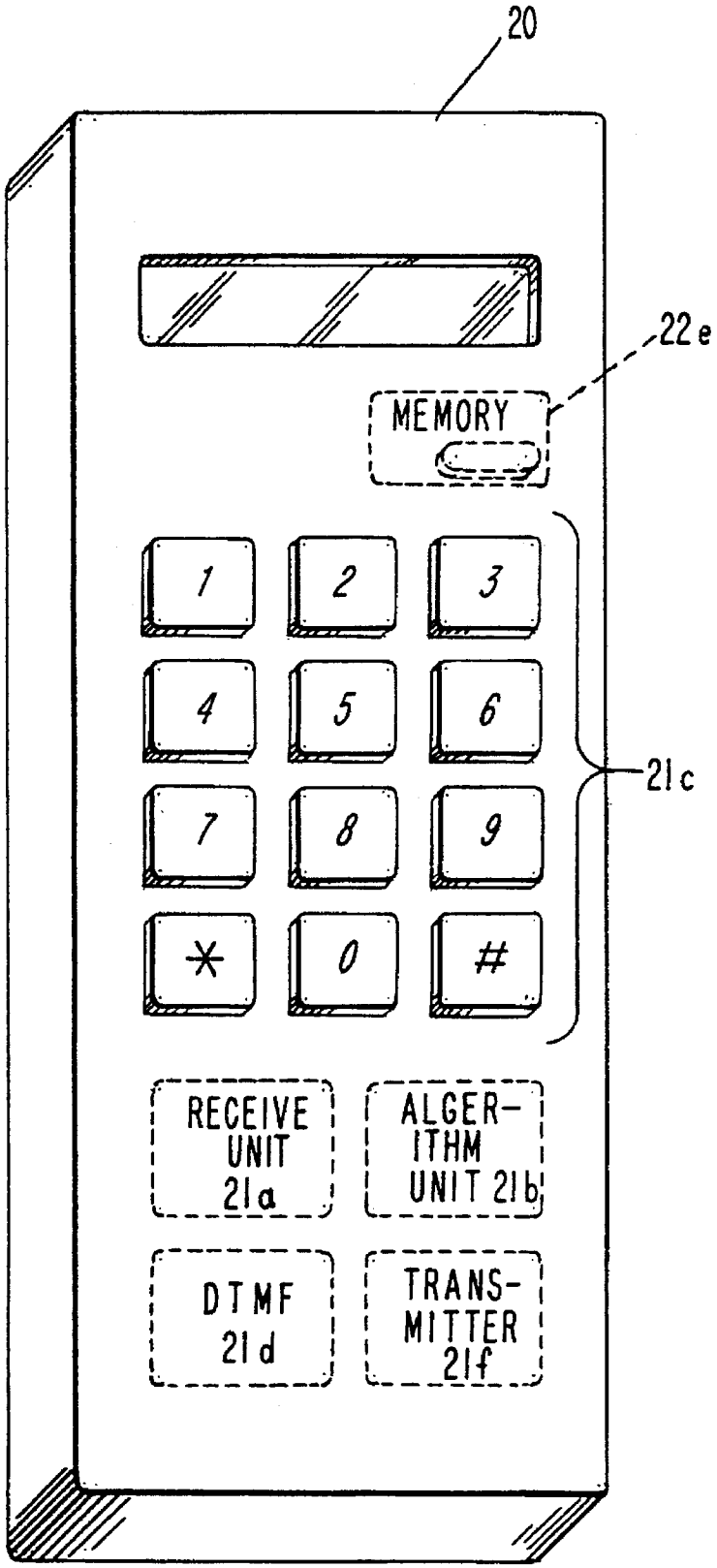
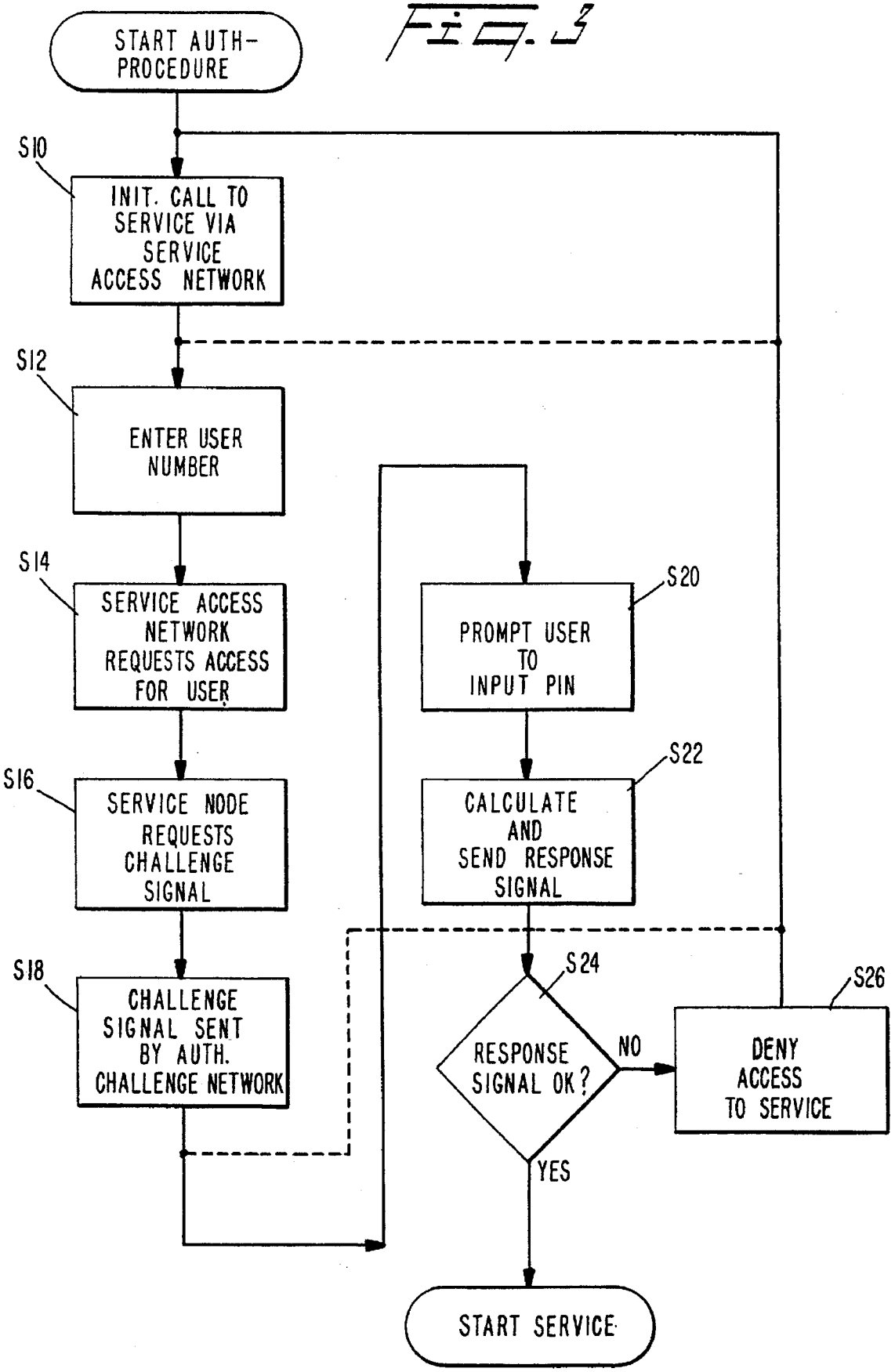


Fig. 3



USER AUTHENTICATION METHOD AND APPARATUS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention involves a method and an apparatus for authentication of a user attempting to access an electronic service, and, in particular, providing an authentication unit which is separate from preexisting systems.

2. Description of Related Art

Effective authentication methods and apparatuses have been in great demand to prevent fraud and theft of services. This demand increases with the explosion of electronic services in the current information age. Electronic services such as banking services, credit card services, automatic teller machine (ATM) services, account information services such as mortgage, savings and investment accounts, general information services such as data base services and networks, security services and long distance phone services all require that a user be accurately identified for purposes of security, proper billing and avoidance of fraud. Recently, fraud in the cellular mobile telephone industry has placed so great a demand on effective authentication methods that a protocol has been standardized for cellular mobile systems. See, GSM 03.20, European Telecommunications Standards Institute (ETSI), 1993, pp. 19–29 and U.S. Pat. No. 5,282,250, herein incorporated by reference.

However, conventional authentication systems have required specially equipped terminals with card readers such as ATMs or credit card gas station terminals, data terminals using a log-in procedure, or cellular mobile radio stations with built-in authentication capabilities. Credit cards having a magnetic snip provide only minimal security insomuch as the bearer of the card is usually permitted to conduct transactions without further authentication of the user's identification other than perhaps comparing a unauthenticated signature on the card to a signature of the user. Even in transactions when signatures are required, the certainty of the user's identification is minimal.

Other identity cards, such as ATM cards, require a log-on procedure with a password, or PIN. But the PIN, once learned by an unauthorized user, offers no security in authenticating the user if the user can duplicate the ATM card.

These methods of authentication require specially equipped, and often dedicated, terminals, which raises the cost and reduces the availability of the associated electronic service. In other words, the prior art security systems often require a dedicated or customized terminal or modification to existing terminals, which greatly restricts the use of security systems to specific sites. Also, a user may use several electronic services, each service requiring an authentication procedure and/or personal identification number (PIN) or password, each procedure or password different from the others. As a subscriber to several electronic services, a user might end up with numerous passwords to remember. Even worse, he or she may be required to change these passwords periodically, thus having to remember if a password is still valid or not.

Also, transactions requiring relatively certain authentication have been largely unavailable from relatively simple terminals like telephones. For instance, home banking by telephone has been limited to transactions involving the bank customer's own accounts or using only the customer's own telephone.

SUMMARY OF THE INVENTION

The present invention overcomes these and other problems by providing an authentication procedure wherein the user carries a personal unit not limited to use with or physically connected to a terminal of any one specific electronic service. The personal unit can be used to authenticate a user's identity through a variety of terminals associated with a variety of electronic services.

The personal unit includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm. The response code is then sent to the service node and, if it is acceptable, access to the service is authorized.

The basic method involves receiving a challenge code from a system, the user inputting a personal identification number or other recognizable input, and the personal unit generating a response code based on an internally stored algorithm. The PIN or other user input may be changed from time to time, and the challenge code and the response is unique for each transaction. The personal unit may receive and store a plurality of challenge codes for later use.

The personal unit can be used with virtually any existing terminal of an electronic service without requiring the terminal to be modified or customized. For instance, the personal unit can be used with a standard telephone, whether a radio telephone or land-line telephone. The user can input the response code displayed on the personal unit through the telephone keypad or the personal unit can include a DTMF transmitter for direct input of the response code into the microphone of the telephone. It follows that the keypad of any service terminal (e.g., a dam terminal connected to a service computer) can be used to input the response code. If some other input device is used in a terminal, such as an acoustic input, a inductively coupled input, an optical input, radio receiver (particularly if the terminal is by-passed and the response code is transmitted directly to the authentication center), etc., the personal unit can include a compatible output device. In other words, the personal unit can be modified or equipped to be compatible with existing or perspective terminals, rather than having to modify the terminals to suit the authentication procedure.

The same basic authentication procedure can be used for all services the user might wish to engage, the procedure being modifiable to suit any specific requirements of the electronic service. The user may have one personal unit for all the services he may wish to subscribe to, or several personal units, each unit being usable with one or a subset of services to which the user has subscribed.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described with reference to the attached drawing figures in which:

FIG. **1** is a schematic diagram of an authentication pager system in accordance with the present invention;

FIG. **1A** is a schematic diagram of an authentication pager system with reference to specific communications in accordance with the present invention;

FIG. **2** is a perspective view of a personal unit in accordance with the present invention; and

FIG. **3** is a flowchart outlining the authentication process in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hardware of the System

Referring to FIG. **1**, the present invention includes a personal unit **20** for generating a response code, a terminal

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.