Trials@uspto.gov
Tel: 571-272-7822

Paper 45
Entered: July 2, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EMC CORPORATION,
Petitioner,

v.

ACTIVIDENTITY, INC.,
Patent Owner, and

INTELLECTUAL VENTURES I LLC,
Exclusive Licensee.[1]

Case IPR2017-00338
Patent 9,098,685 B2

Before JAMES B. ARPIN, LYNNE E. PETTIGREW, and KEVIN C. TROCK, *Administrative Patent Judges*.

TROCK, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and
37 C.F.R. § 42.73

---

[1] Paper 13, 2–3; Paper 18, 1–2; Paper 19; *see* Paper 6, 1 ("The real parties-in-interest are ActiviDentity, Inc. and Intellectual Ventures I LLC. ActiviDentity, Inc. is the owner of U.S. Patent No. 9,098,685 ('the '685 patent'). Intellectual Ventures I LLC is the exclusive licensee of the '685 patent and has the sole and exclusive right and obligation to select and retain counsel to defend the '685 patent.").

I. INTRODUCTION

EMC Corporation, ("Petitioner") filed a request for *inter partes* review of claims 1, 3, 5, 7–9, 11, 13, 15, 16, and 19 (the "challenged claims") of U.S. Patent No. 9,098,685 B2 (Ex. 1001, "the '685 patent"). Paper 1 ("Pet."). Intellectual Ventures I LLC ("Exclusive Licensee") filed a Preliminary Response. Paper 8 ("Prelim. Resp."). We instituted an *inter partes* review of all of the challenged claims on all of the asserted grounds. Paper 9 ("Dec. Inst.").

Exclusive Licensee filed a Response (Paper 24, "Resp.") and Petitioner filed a Reply (Paper 29, "Reply"). A hearing was held on April 9, 2018, a transcript of which has been entered into the record (Paper 43, "Tr.").

We have jurisdiction under 35 U.S.C. § 6(b). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). Having reviewed the arguments of the parties and the supporting evidence, we find that Petitioner has demonstrated by a preponderance of the evidence that each of the challenged claims is unpatentable.

A. The '685 Patent

The '685 patent (the "Specification") describes methods of authorizing a user to access a workstation or secured data. Ex. 1001, 1:13–19, 2:64–3:2. The Specification recognizes that security systems based on pre-set codes, passwords, biometric identification, and "predetermined combinations" of these measures were known in the art. *Id.* at 1:22–53,

2:48–50. The Specification also acknowledges that organizations included additional security processes for remote access to their sites. *Id.* at 2:54–63. The Specification describes an approach to authorization that varies based on "computing conditions," including: (1) the type of communication link, (2) the geographical location of the workstation, and/or (3) the time of access. According to the Specification, a "security policy" is determined from a set of predetermined security policies based on previously stored policy data and computing conditions. An authorization method then is determined from this security policy and the computing conditions. *Id.* at claim 1, 3:19–34, 5:55–6:2.

Figure 3A of the Specification illustrates relevant system components.

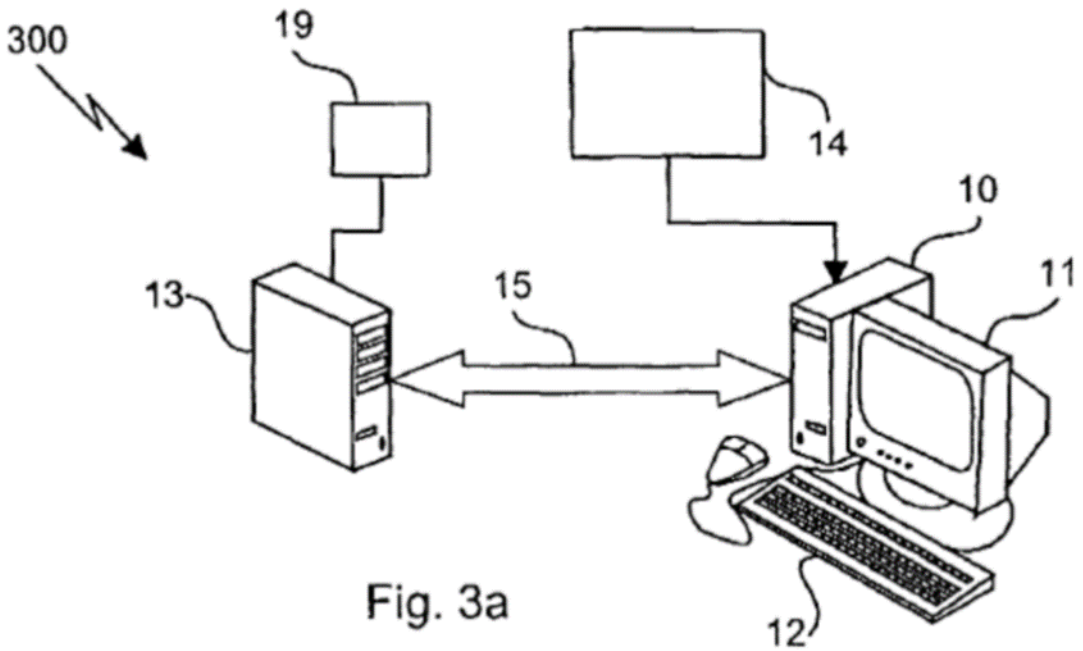

Fig. 3a

In Figure 3A, shown above, workstation 10 is connected to security server 13 though communication link 15. *Id.* at 5:18–22. Security server 13 stores policy data and also controls access to secured data on data server 19. Workstation 10 also is connected to user data input device 14 (e.g., smart

card reader or a biometric sampling device), and to keyboard 12. *Id.* at 5:22–28.

A user requesting access to secured data stored in data server 19 provides user information (e.g., a password or fingerprint scan) to user input device 14 of workstation 10, which forwards this user information to security server 13. *Id.* at 5:46–54, 7:35–46, 6:63–65. Workstation 10 also provides security server 13 with "workstation data" (also referred to as "computing conditions"), such as "the geographical location of the workstation, the time the request for access is being performed, the type of the request, and so forth." *Id.* at 7:43–46; *see also id.* at 6:3–4.

The security server determines the applicable security policy based on previously stored policy data and "computing conditions," such as the type of user data input device, the geographic location of the workstation, the type of communication link between the workstation and the security server, user ID, the data being accessed, the type of secured data being requested from the data server, and the country. *Id.* at 5:64–6:2, 6:29–33, 7:17–30.

The security server also determines an authorization method (*id.* at 5:55–58) from the determined security policy and the computing conditions (*id.* at 5:64–6:2). The Specification describes several examples of authorization methods, including methods that use a "smart card reader" (*id.* at 5:24–27), a "biometric sampling device such as a fingerprint imager, a voice recognition system, a retinal imager or the like" (*id.*), "password[s]" (*id.* at 4:63–65), and "card based user authentication" (*id.*; *see also id.* at 6:49–65).

The security server uses the determined authorization method to authorize the user's request to access the protected resource. This involves

receiving user identification data (e.g., a password or fingerprint) (*id.* at 6:63–65) and comparing the user identification data with previously stored user data (e.g., a previously stored password or fingerprint corresponding to an authorized user) (*id.* at 5:57–61). The specific type of user identification data that the security server requests and compares will depend on the determined authorization method. *Id.* at 6:40–54. If the received user identification data matches the previously stored user data, the security server identifies the user and can authorize the user to access secured data. *Id.* at 5:61–63.

B. Challenged Claims

Petitioner challenges claims 1, 3, 5, 7–9, 11, 13, 15, 16, and 19 of the '685 patent. Challenged claims 1, 9, and 19 are independent. Claim 1 is illustrative and is reproduced below.

> 1. A method of authorizing a user to access a workstation using a security server, the method comprising:
>
> receiving security data relating to computing conditions in which an authorization will be performed, wherein the security data comprises at least one indication of a type of communication link between the workstation and the security server, a geographic location of the workstation, or a time of access of the workstation;
>
> determining a security policy from a plurality of predetermined security policies based on previously stored policy data and the received indication of the type of communication link between the workstation and the security server, the geographic location of the workstation, or the time of access of the workstation;
>
> determining an authorization method for authorizing the user, wherein the authorization method is determined from the determined security policy in accordance with the received indication of the type of communication link between the

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.