

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

SMART AUTHENTICATION IP, LLC,
Patent Owner.

Case IPR2017-02047
Patent 8,082,213 B2

Before KEVIN W. CHERRY, MICHELLE N. WORMMEESTER, and
JAMES A. WORTH, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

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

I. INTRODUCTION

Unified Patents Inc. (“Petitioner”) filed a Petition (Paper 3, “Pet.”) requesting *inter partes* review of claims 1–17 of U.S. Patent No. 8,082,213 B2 (Ex. 1001, “the ’213 patent”). We initially instituted an *inter partes* review as to claims 1–10 and 12–17 based on two of the three grounds presented in the Petition. Paper 9 (“Institution Decision” or “Inst. Dec.”); *see* 35 U.S.C. § 314(a). After institution of trial, in light of the Supreme Court’s decision in *SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348 (2018), we modified our Institution Decision to include review of all the challenged claims and all the grounds presented in the Petition. Paper 14.

Smart Authentication IP, LLC (“Patent Owner”) filed a Patent Owner Response (Paper 18, “PO Resp.”), and Petitioner filed a Reply (Paper 20, “Pet. Reply”). With our authorization, Patent Owner subsequently filed a Sur-Reply (Paper 21, “PO Sur-Reply”).

On November 6, 2018, we conducted an oral hearing. A copy of the transcript (Paper 26, “Tr.”) is included in the record.

We have jurisdiction under 35 U.S.C. § 6(b). For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–10 and 12–17 of the ’213 patent are unpatentable. Petitioner has not made such a showing, however, with respect to claim 11 of the ’213 patent. This final written decision is issued pursuant to 35 U.S.C. § 318(a).

II. BACKGROUND

A. Related Proceedings

The parties identify several related district court cases. Pet. 1–2; Paper 4, 2.

B. The '213 Patent

The '213 patent relates to user authentication, where a user controls the level and complexity of an authentication process carried out by an authentication service provider (“ASP”) on behalf of both the user and an entity seeking to authenticate the user. Ex. 1001, 2:1–10.

To illustrate an example of user authentication according to the '213 patent, Figure 3 is reproduced below.

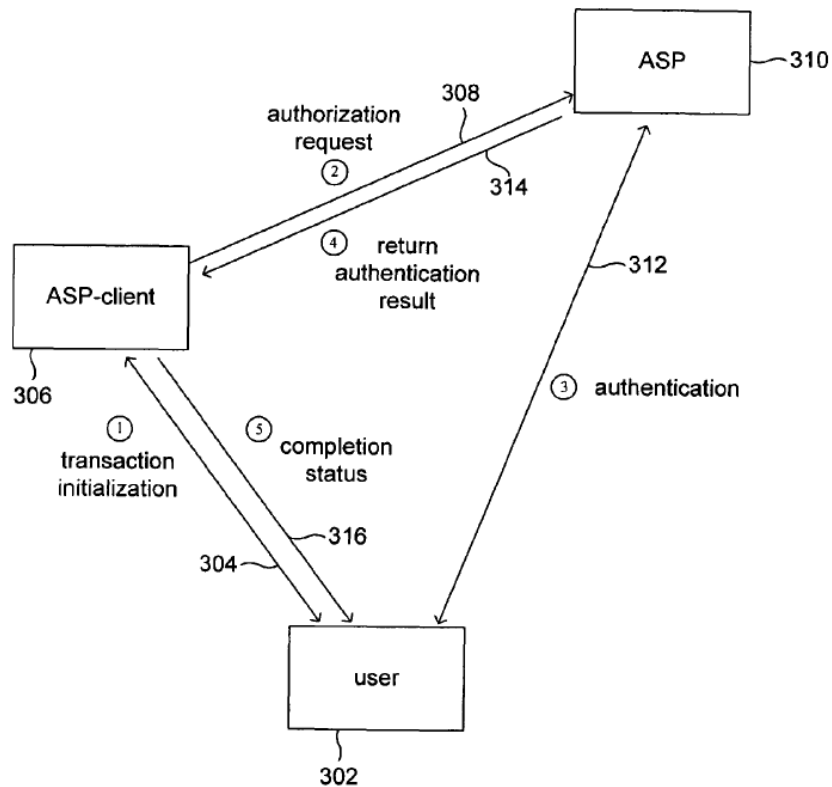


Figure 3

Figure 3 shows the interactions between a user, an ASP client, and an ASP. *Id.* at 3:47–48. First, the user starts an electronic transaction with the ASP client by requesting to log in to a commercial website or by requesting a product or service. *Id.* at 3:48–51. The ASP client obtains user information from the user. *Id.* at 3:51–55. The user information may include the user’s name, the user’s address or other contact information, the user’s billing information, the user’s employment information, or user-specified passwords. *Id.* at 4:18–27.

Next, the ASP client transmits an authentication request to the ASP to determine whether the user is authentic. *Id.* at 3:55–59. The authentication request includes the information obtained from the user. *Id.*

The ASP then carries out an authentication transaction with the user to authenticate the user according to predetermined authentication policies. *Id.* at 3:59–62. The user may specify each policy. *Id.* at 4:28–30. With respect to bank account transactions, for example, the user may specify that only transactions occurring between 1:00 pm and 4:00 pm on Monday through Friday are to be authorized, and that authorization must include variable-factor authentication using randomly generated passwords sent to the user’s cell phone and furnished by the user to the bank during the transactions. *Id.* at 4:31–40.

Once the authentication transaction is complete, the ASP returns an authentication result to the ASP client, which uses the result to complete the electronic transaction with the user. *Id.* at 3:62–67.

C. Illustrative Claim

Petitioner challenges claims 1–17 of the '213 patent. Claims 1 and 12 are independent. Claim 1 is illustrative of the claims under challenge:

1. A user-authentication service implemented as routines that execute one or more computer systems interconnected by two or more communications media with both an authentication-service client, and a user, the user-authentication service comprising:

the one or more computer systems;

stored user-authentication policies specified by the user;

stored user information;

account interface routines that implement an account interface by which the user specifies, modifies, adds, and deletes user-authentication policies; and

authentication-interface routines that implement an authentication interface by which, following initiation of a transaction by the user with the authentication service client, the authentication-service client submits an authentication request, through the first communications medium or through a second communications medium, to authenticate the user, the authentication interface routines employing a variable-factor authentication, when specified to do so by stored user-authentication policies, to authenticate the user on behalf of the authentication-service client during which the user communicates with the user-authentication service through a third communications medium different from the first and second communications media and a user device different from that employed by the user to initiate the transaction with the authentication-service client.

D. The Instituted Grounds

Petitioner asserts in its Petition three grounds based on obviousness under 35 U.S.C. § 103. Pet. 4, 12–86. Although we initially instituted *inter*

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.