

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

WILLIAM GRECIA,
Patent Owner.

Case IPR2016-00602
Patent 8,887,308 B2

Before GLENN J. PERRY, RAMA G. ELLURU, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Unified Patents Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claim 1 of U.S. Patent No. 8,887,308 B2 (Ex. 1003, “the ’308 patent”). William Grecia (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”). We have jurisdiction under 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we have decided not to institute an *inter partes* review.

I. BACKGROUND

A. The ’308 Patent

The ’308 patent is titled “Digital Cloud Access (PDMAS Part III).” Ex. 1003, at [54]. The ’308 patent describes a digital rights management system that manages access rights across a plurality of devices via digital media personalization to protect digital media subject to illegal copying. *Id.* at 1:20–27; 4:48–49.

The system includes a first receipt module, an authentication module, a connection module, a request module, a second receipt module, and a branding module. *See id.* at Fig. 1. The first receipt module receives a branding request from a user’s (content acquirer’s) device. *Id.* at 5:46–48. The branding request is a read and write request of metadata of the digital media and includes a membership verification token corresponding to the digital media. *Id.* at 5:48–51. The authentication module authenticates the membership verification token. *Id.* at 5:57–58. The connection module establishes communication with the user’s device. *Id.* at 5:59–61. The

request module requests an electronic identification reference from the user's device. *Id.* at 6:5–7. The second receipt module receives the electronic identification reference. *Id.* at 6:7–9. The branding module brands metadata of the digital media by writing the membership verification token and the electronic identification into the metadata. *Id.* at 6:9–12.

Figure 3, which is reproduced below, illustrates this process.

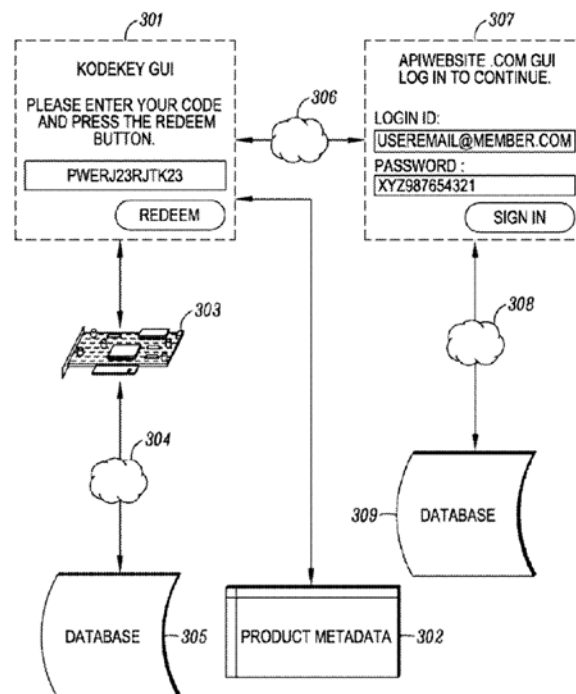


FIG. 3

In particular, Figure 3 is a flow chart of the process of digital media personalization. *Id.* at 4:24–26. A user posts a branding request via Kodekey GUI 301, which prompts the user to enter a token and press the redeem button. *Id.* at 6:66–7:4. Product metadata 302 is associated with the digital media to be acquired. *Id.* at 7:4–5. The Kodekey GUI is connected to token database 305. *Id.* at 7:7:–8. The user is then redirected to APIwebsite.com GUI 307, which prompts the user to enter a login id and password to access the digital media from database 309. *Id.* at 7:11–12, 15–

18. The APIwebsite.com GUI interfaces to a web service membership, where the user's electronic identification is collected and sent back to the Kodekey GUI. *Id.* at 7:11–15. The database containing the digital media is connected to the web service membership. *Id.* at 7:18–20.

B. Challenged Claim

Petitioner challenges claim 1 of the '308 patent, which recites:

1. A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:

a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:

a memory connected to the at least one CPU;

a storage connected to the at least one CPU; and

a database connected to the at least one CPU through the Internet; wherein

the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then

b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then

c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the APJ is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database

apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification data of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

C. Asserted Grounds of Unpatentability

Petitioner challenges claim 1 of the '308 patent on the following grounds.¹ Pet. 3, 19–52.

¹ In summarizing its asserted grounds on page 3 of the Petition, Petitioner requests cancellation of claim 1 as unpatentable under 35 U.S.C § 103, but states on page 19 of the Petition that the asserted references “anticipate and/or render obvious the claimed subject matter.” Given the substance of Petitioner’s arguments, we address claim 1 under 35 U.S.C. §§ 102 and 103.

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.