

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner

v.

VINDOLOR, LLC,
Patent Owner

IPR2019-00478
Patent 6,213,391

**PETITIONER'S REQUEST FOR REHEARING
PURSUANT TO 37 C.F.R. § 42.71(d)**

Pursuant to 37 C.F.R. § 42.71(d), Petitioner Unified Patents Inc. (“Unified” or “Petitioner”) submits this Request for Rehearing in response to the Decision on Institution entered July 3, 2019 (Paper 9) (“Decision”) by the Patent Trial and Appeal Board (“Board”) regarding U.S. Patent 6,213,391 (“the ’391 patent”).

I. STATEMENT OF RELIEF REQUESTED

Petitioner respectfully requests rehearing regarding Grounds 1 and 2 of the Petition. Ground 1 asserts that *Gullman* (Ex. 1004) anticipates Claims 1-2 under 35 U.S.C. § 102(a), (b), and (e). *See* Paper 1 (“Petition”) at 5, 26. Ground 2 asserts that *Gullman* in view of the knowledge of a person of ordinary skill in the art (“POSITA”) renders obvious Claims 1-2 under 35 U.S.C. § 103(a). *See* Petition at 5, 45.

Petitioner respectfully submits that the Decision overlooks and/or misapprehends Petitioner’s positions and supporting evidence that *Gullman* discloses the recited “access code” of the sole independent claim of the ’391 patent. Accordingly, Petitioner respectfully requests that the Board institute *inter partes* review of the ’391 patent.

II. LEGAL STANDARD

“A party dissatisfied with a decision may file a single request for rehearing” that “specifically identif[ies] all matters the party believes the Board

misapprehended or overlooked, and the place where each matter was previously addressed in a motion, an opposition, or a reply.” 37 C.F.R. § 42.71(d).

III. REASONS FOR THE REQUESTED RELIEF

In the Decision, the Board found that *Gullman*'s security token is not the claimed “access code.” Decision at 6-7. Specifically, the Decision found:

Gullman decodes the security token and ***uses what is encoded within to determine whether to grant access.*** ... Thus, the security token in *Gullman* provides transmission security, whereas ***the data contained within (the correlation factor and the code) are used to authorize access.***

Decision at 6-7 (emphasis added). The Decision misapprehends or overlooks the evidence cited in the Petition for at least the following reasons.

A. The Petition Demonstrates *Gullman*'s Security Token Provides Access.

The Petition and the accompanying Declaration establish that *Gullman* discloses a security token that “both authenticates and identifies the user,” and thus is the claimed “access code.” Petition at 43; Declaration at ¶ 134; *see also* Decision at 6 (“*Gullman* decodes the security token and uses what is encoded within to determine whether to grant access.”).

First, the Decision overlooks portions of the Petition that show *Gullman*'s security token is also an “access code,” as claimed, and can be used in a similar fashion as disclosed in the '391 patent. For example, the Petition cites to *Gullman*'s disclosure that the “[security] token is communicated to a host system *for*

determining whether access to such host is to be authorized.” See Petition at 26 (citing Ex. 1004, 1:6-13) (emphasis added); Declaration at ¶ 84 (citing same). Further, *Gullman* discloses that “[t]he security token generated ... may be input *in the same manner as PINs* or other security codes in common use.” Ex. 1004, 6:56-58; see also Petition at 29; Declaration at ¶ 89. Thus, to the extent the Decision acknowledges that a “PIN” is an “access code,”¹ the Petition also shows that *Gullman*’s security token is an “access code” for the same reasons.

Further, the Petition also demonstrates that *Gullman*’s security token is *transmitted* in the same manner as the claimed “access code.”² In the claimed

¹ Patent Owner’s Preliminary Response also acknowledges the same. See Paper 6 (“Response”) at 7 (providing a PIN as an example of a “prior art technique[] ... for providing access codes for accessing secure objectives”).

² Patent Owner mischaracterizes *Gullman*’s security token as only providing end-to-end transmission security for transmitting individual data elements between a security apparatus and a host system. Response at 21, fn. 6; see also Response at 41. However, as addressed in the Petition and supporting Declaration, *Gullman*’s security token is, in fact, used to also identify the user and determine whether access should be granted. Ex. 1004, 3:36-42, 4:3-8, 6:56-58; see also Decision at 6, Petition at 26, 29; Declaration at ¶¶ 84, 89.

subject matter, a single data structure (*i.e.*, the “access code”) is sent to a host system to determine user access. Ex. 1001, 9:1-5, 10:33-44, cl. 1; *see also* Petition at 18; Declaration at ¶ 54. Likewise, the Petition cites *Gullman*’s disclosure of transmitting a single security token to determine whether access should be granted or denied. Petition at 29 (citing Ex. 1004, 6:35-45); *see also* Decision at 6 (“[t]he security token is sent to a host computer to determine if access should be granted”); Declaration at ¶ 89. Therefore, the Petition establishes that *Gullman*’s security token is used to identify a person and determine whether access should be granted, in the same manner as a conventional “access code” (*e.g.*, a PIN or security code). *See* Petition at 29; Declaration at ¶ 89.

Second, the Decision appears not to recognize that *Gullman* advances the prior art by disclosing a security token that provides ***both*** transmission security ***and*** user identification/access. Specifically, the Decision cites:

‘[a] PIN is used to identify an individual and authorize access to a host system,’ which ‘provides user identification, while a token provides transmission security.’

Decision at 6 (citing Ex. 1004, 1:30-45). This excerpt is from *Gullman*’s “BACKGROUND OF THE INVENTION,” discussing the conventional operation of a prior art transmission token in comparison to a prior art PIN. *See* Ex. 1004, 1:28-34. By relying on this distinction between the prior art transmission token and the prior art PIN, however, the Decision overlooks that *Gullman*’s security token

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.