Trials@uspto.gov<br>571-272-7822

Paper 11
Date: February 28, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2021-01444
Patent 8,352,730 B2

Before KEVIN F. TURNER, JUSTIN T. ARBES, and
DAVID C. McKONE, *Administrative Patent Judges.*

ARBES, *Administrative Patent Judge.*

# DECISION
Denying Institution of *Inter Partes* Review
*35 U.S.C. § 314*

## I. INTRODUCTION

### *A. Background and Summary*

Petitioner Samsung Electronics America, Inc. filed a Petition (Paper 2, "Pet.") requesting *inter partes* review of claims 1–11 of U.S. Patent No. 8,352,730 B2 (Ex. 1001, "the '730 patent") pursuant to 35 U.S.C. § 311(a). Patent Owner Proxense, LLC filed a Preliminary Response (Paper 9, "Prelim. Resp.") pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." *See* 37 C.F.R. § 42.4(a) ("The Board institutes the trial on behalf of the Director."). For the reasons that follow, we do not institute an *inter partes* review.

### *B. Related Matters*

The parties indicate that the '730 patent is the subject of *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6:21-cv-00210 (W.D. Tex.) ("the district court case"). *See* Pet. 3; Paper 5, 1. Petitioner also filed petitions challenging claims of other patents asserted in the district court case in Cases IPR2021-01438, IPR2021-01439, IPR2021-01447, and IPR2021-01448.

### *C. The '730 Patent*

The '730 patent discloses systems for "authentication responsive to biometric verification of a user being authenticated," using "a biometric key [that] persistently (or permanently) stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format." Ex. 1001, col. 1, ll. 57–62. The '730 patent states that "[c]onventional user authentication techniques," such as requiring input of a password, were deficient because they "require[d] the user to memorize or otherwise keep track of the credentials" and "it can be quite difficult to keep track of them all." *Id.* at col. 1, ll. 23–32. Other techniques, such as "provid[ing] the user with an access object . . . that the user can present to obtain access," were inadequate because "authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object." *Id.* at col. 1, ll. 33–43. According to the '730 patent, there was a need in the art for a system for "verifying a user that is being authenticated that does not suffer from [such] limitations" and "ease[s] authentications by wirelessly providing an identification of the user." *Id.* at col. 1, ll. 49–53.

Figure 2 of the '730 patent is reproduced below.

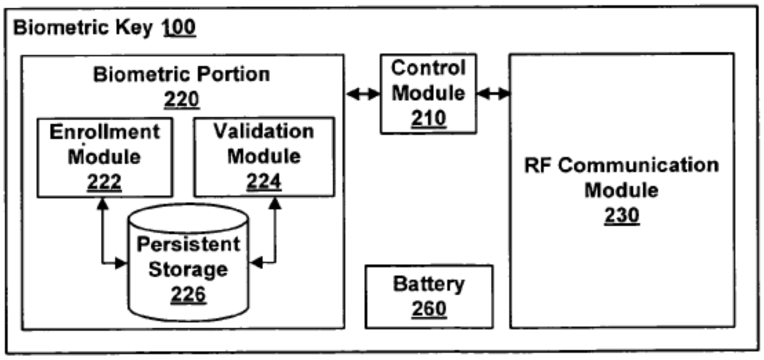

FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. *Id.* at col. 2, ll. 41–43. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at col. 4, ll. 4–28. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can provide a code to biometric key 100. *Id.* at col. 4, ll. 8–12. The code is stored in persistent storage 226. *Id.* at col. 4, ll. 43–45. "Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data." *Id.* at col. 4, ll. 36–38. "Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data).” *Id.* at col. 4, ll. 38–41. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user’s fingerprint and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at col. 4, ll. 14–23.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

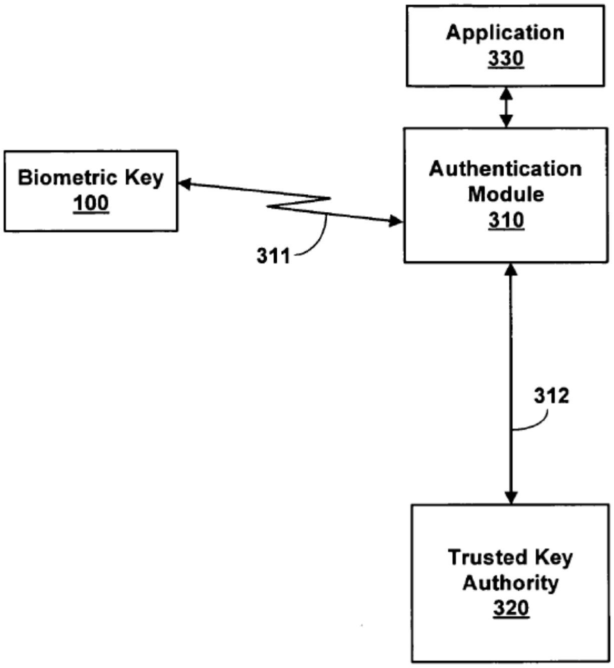

FIG. 3

Figure 3 is “a block diagram illustrating a system for providing authentication information for a biometrically verified user.” *Id.* at col. 2, ll. 44–46. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at col. 5, ll. 8–12. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at col. 5, ll. 12–19. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at col. 5, ll. 19–23; *see also id.* at col. 5, ll. 42–48 ("In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key."). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at col. 5, ll. 23–26.

"Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, and the like." *Id.* at col. 5, ll. 28–31. Trusted key authority 320 can be operated by an agent, such as "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at col. 6, ll. 35–38. "The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user." *Id.* at col. 6, ll. 38–41.

### *D. Illustrative Claim*

Challenged claims 1 and 8 of the '730 patent are independent. Claims 2–7 depend directly from claim 1 and claims 9–11 depend directly or indirectly from claim 8.

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.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.