Trials@uspto.gov
571-272-7822

Paper 9
Entered: November 29, 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

OPENTV, INC.
Petitioner

v.

CISCO TECHNOLOGY, INC.
Patent Owner

Case IPR2013-00329
Patent 6,252,964 B1

Before KALYAN K. DESHPANDE, JUSTIN T. ARBES, and PATRICK M. BOUCHER, *Administrative Patent Judges.*

ARBES, *Administrative Patent Judge.*

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

OpenTV, Inc. filed a Petition ("Pet.") to institute an *inter partes* review of claims 1-6 of U.S. Patent No. 6,252,964 B1 (Ex. 1001, "the '964 patent") pursuant to 35 U.S.C. § 311 *et seq*. Patent Owner Cisco Technology, Inc. filed a preliminary response ("Prelim. Resp.") to the Petition. We have jurisdiction under 35 U.S.C. § 314. For the reasons that follow, the Board has determined to institute an *inter partes* review.

I. BACKGROUND

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a):

> THRESHOLD—The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 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.

Petitioner challenges claims 1-4 as anticipated under 35 U.S.C. § 102(b) and claims 1-6 as unpatentable under 35 U.S.C. § 103(a). Pet. 19-60. We grant the Petition as to claims 1-4 on certain grounds of unpatentability as discussed below.

A. The '964 Patent (Ex. 1001)

The '964 patent, titled "Authorization of Services in a Conditional Access System," issued on June 26, 2001, based on Application No. 09/488,230, filed January 20, 2000.

The '964 patent relates to "systems for protecting information that is transmitted by means of a wired or wireless medium against unauthorized access." Ex. 1001, col. 1, ll. 42-45. For example, a cable television or

satellite television company may want to ensure that only designated subscribers can access certain television programs. *Id*. at col. 1, l. 48-col. 2, l. 33.

Figure 1 of the '964 patent is reproduced below:

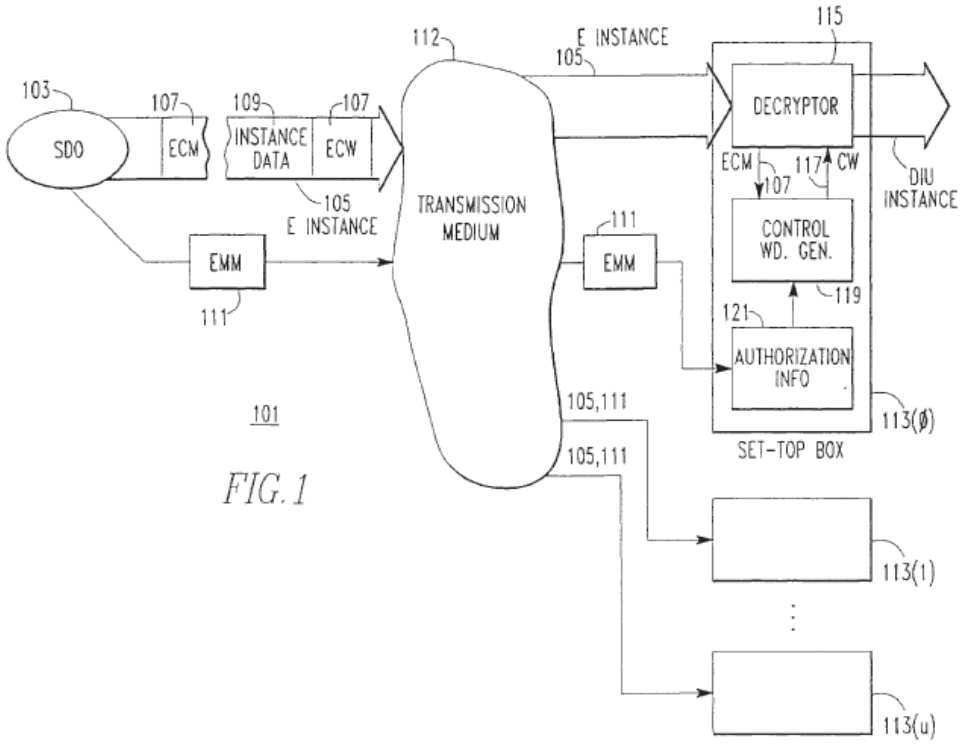

FIG. 1

Figure 1 depicts conditional access system 101 in which service distribution organization (SDO) 103 (e.g., a cable television company) provides service "instances" to set-top boxes 113 of various subscribers. *Id*. at col. 4, ll. 10-19. For example, the "History Channel" is a "service that provides television programs about history," and "[e]ach program provided by the History Channel is an 'instance' of that service." *Id*. at col. 4, ll. 16-19. Service distribution organization 103 encrypts or scrambles an instance to create encrypted instance 105, which it then broadcasts to subscribers over transmission medium 112 (e.g., cable). *Id*. at col. 4, ll. 19-22, 33-38. As shown in Figure 1 above, encrypted instance 105 includes instance data 109

(information making up the television program) and entitlement control messages (ECMs) 107 (information necessary for the receiving set-top box to decrypt the data). *Id*. at col. 4, ll. 22-27. ECMs may be sent many times per second so that the set-top box has the most current information, and ECMs may be changed every few seconds to prevent piracy. *Id*. at col. 4, ll. 27-32.

In addition to encrypted instance 105, service distribution organization 103 sends to a set-top box entitlement management messages (EMMs) 111, which may indicate, for example, what services the subscriber associated with that set-top box has purchased and include a key for a particular service. *Id*. at col. 4, ll. 47-50, 56-58. EMMs are used by the set-top box in the authorization process. *Id*. at col. 4, ll. 38-47; col. 4, l. 56-col. 5, l. 6. The set-top box stores the information contained in EMMs as authorization information 121, and uses authorization information 121 in combination with ECMs 107 to determine whether the subscriber is entitled to watch encrypted instance 105. *Id.* If the subscriber is entitled to watch the instance, the set-top box decrypts encrypted instance 105 to produce decrypted instance 123 and sends decrypted instance 123 to the television for viewing. *Id*. at col. 4, ll. 38-41.

The ’964 patent describes specifically how a set-top box, or digital home communications terminal (DHCT), is permitted to access a service instance via the operation of a number of entities, including a conditional access authority (CAA) and entitlement agents (EAs). EAs send entitlement information (e.g., in EMMs) to the DHCT. *Id*. at col. 30, ll. 48-51. The CAA “provides and removes entitlement agents,” and facilitates communication between the DHCT and EAs. *Id*. at col. 10, l. 16-48; Fig. 24

(depicting CAA 2405 and EAs 2409). DHCT 333 "receives and interprets EMMs [and] ECMs," "decrypts instances of services," and sends messages back to the CAA and EAs over a reverse path. *Id*. at col. 15, ll. 17-23. DHCT 333 includes digital home communications terminal secure element (DHCTSE) 627, which comprises (1) a secure memory for storing keys and other information, and (2) a secure microprocessor for processing incoming EMMs and ECMs and producing the return messages. *Id*. at col. 15, l. 49-col. 16, l. 9; Figs. 12 (depicting DHCTSE 627), 13 (depicting memory 1207 in DHCTSE 627).

The '964 patent also describes the encryption mechanism of the disclosed system in greater detail. Figure 3 of the '964 patent is reproduced below:

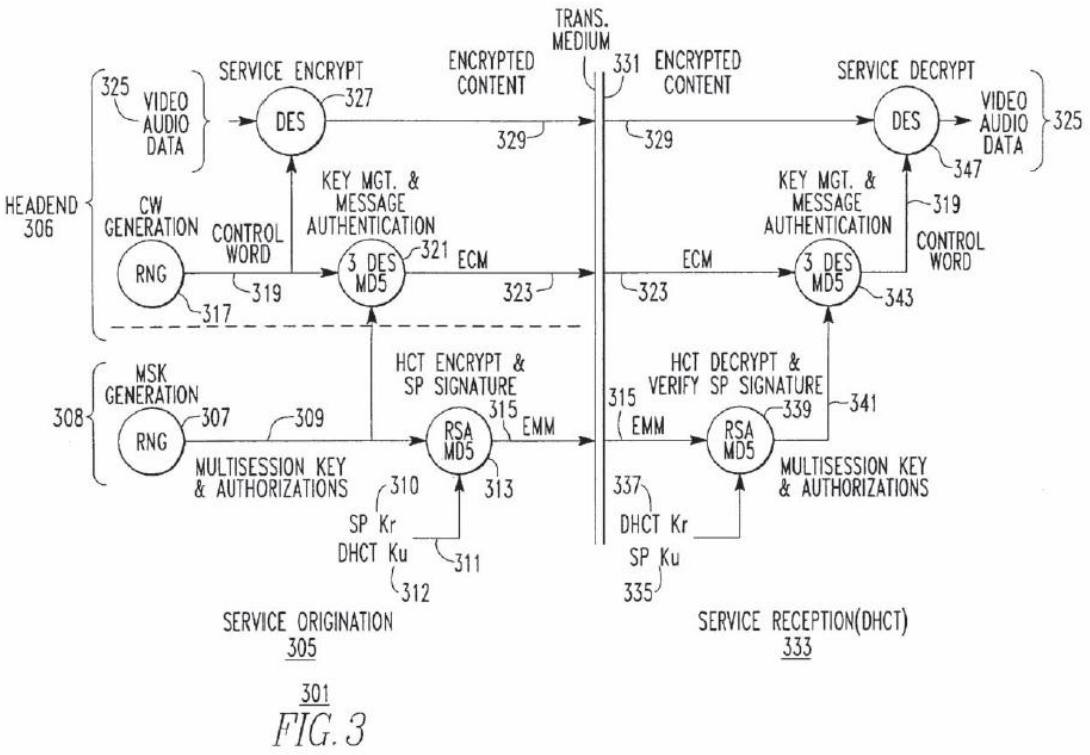

FIG. 3

Figure 3 depicts the interactions between a service origination component 305 and DHCT 333. A customer, for example, orders a service instance

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.