

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MARIA AZUA HIMMEL, HERMAN RODRIGUEZ,
NEWTON JAMES SMITH JR, and CLIFFORD JAY SPINAC

Appeal 2008-1325
Application 10/179,339
Technology Center 2100

Decided: September 30, 2008

Before ALLEN R. MACDONALD, JEAN R. HOMERE,
and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal the Examiner's final rejection of claims 1-21 under 35 U.S.C. § 134. We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

According to Appellants, the invention relates to methods, apparatus, systems, and computer program products in support of securing valid authentication and authorization for access to computer resources and other items (Spec. 1, ll. 13-16).

B. ILLUSTRATIVE CLAIM

Claim 1 is exemplary and is reproduced below:

1. A method of controlling access to a resource for a group of users, the method comprising:

creating a group security object in dependence upon one or more user-selected group security control data types, the group security object comprising security control data and at least one security method, the security control data comprising at least one security control user identification;

receiving a request for access to the resource;

receiving security request data, wherein the security request data includes at least one security request user identification; and

determining access to the resource in dependence upon the security control data and the security request data.

Appeal 2008-1325
Application 10/179,339

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Matyas	US 6,697,947 B1	Feb. 24, 2004
		(filed Jun. 17, 1999)

Claims 1-21 stand rejected under 35 U.S.C. § 102(e) over the teachings of Matyas.

We affirm.

II. ISSUES

The issue is whether Appellants have shown that the Examiner erred in finding that claims 1-21 are unpatentable under 35 U.S.C. § 102(e) over the teachings of Matyas. Particularly, the issue is whether Matyas discloses the claimed limitations of A) “creating a group security object in dependence upon one or more user-selected group security control data types, the group security object comprising security control data and at least one security method, the security control data comprising at least one security control user identification”; B) “receiving a request for access to the resource”; C) “receiving security request data, wherein the security request data includes at least one security request user identification”; and D) “determining access to the resource in dependence upon the security control data and the security request data” (Claim 1).

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Matyas

- 1A. Matyas discloses determining if a received authentication message is a valid message based on the biometric data contained in the biometric authentication message, wherein the received authentication message is considered a valid message if the comparison indicates that the received user biometric data corresponds to the stored biometric data (col. 1, l. 66 to col. 2, l. 2).
- 1B. The user biometric data and the stored biometric data comprise at least one of fingerprint, hand geometry, iris pattern, facial features, voice characteristics, handwriting dynamics, earlobe characteristics and keystroke dynamics (col. 2, ll. 23-27).
- 2A. A canonical biometric template for each user is determined by obtaining a plurality of biometric samples for the user, wherein the biometric information is stored by storing a user identification associated with the biometric information, storing each of a plurality of templates of biometric data associated with the user identification and storing an identification of at least one of the plurality of templates as a primary biometric authentication type (col. 4, ll. 50-60).
- 2B. Data 56, which represents the static and dynamic data

used by software programs that resides in the memory 36, includes user identification 70 and biometric data 72 associated with the user (col. 8, ll. 27-32; fig. 2).

- 3A. In Matyas, an authentication message is obtained from a user (block 100); the biometric information about the user is extracted from the authentication message (block 102); it is then determined if the biometric information is valid for the user (block 104); then an indication of authenticity is provided (block 112) (col. 9, ll. 15-28; fig. 3).
- 3B. User authentication is used to provide access to certain resources (col. 1, ll. 11-13).

PRINCIPLES OF LAW

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros., Inc. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987).

The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp., of America*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). “[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372

(Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)).

V. ANALYSIS

Appellants do not provide separate arguments with respect to the rejection of claims 1-21. Therefore, we select independent claim 1 as being representative of the cited claims. 37 C.F.R. § 41.37(c)(1)(vii).

Creating A Group Security Object

Appellants argue that "Matyas does not disclose creating a group security object in dependence upon one or more user-selected group security control data types, the group security object comprising security control data and at least one security method, the security control data comprising at least one security control user identification" (App. Br. 7). In particular, Appellants argue that "Matyas discloses... a very specific way of allowing for multi-party authentication by receiving a plurality of biometric authentication messages" and that "Matyas' biometric authentication messages do not disclose or suggest the security objects with user-selected group security control data types claimed in the present application" (App. Br. 9).

We begin our analysis by giving the claims their broadest reasonable interpretation. *See In re Bigio* at 1324. Furthermore, our analysis will not read limitations into the claims from the specification. *See In re Van Geuns* at 1184.

Appellants' argument that Matyas does not disclose the claimed "group security object" limitation because Matyas discloses "a very specific way" of authentication "by receiving a plurality of biometric authentication messages" where "Matyas' biometric authentication messages do not disclose or suggest the security objects with user-selected group security control data types claimed in the present invention" is not commensurate with the invention that is claimed. That is, Appellants appear to be arguing that Matyas does not disclose "biometric authentication messages" which disclose or suggest the group security object. Such *biometric authentication message disclosing or suggesting* the group security object cannot be read into the claims and such argument is not commensurate with the claimed invention. Accordingly, the issue is whether Matyas discloses the claimed limitation of "creating a group security object in dependence upon one or more user-selected group security control data types, the group security object comprising security control data and at least one security method, the security control data comprising at least one security control user identification" (Claim 1).

The term “group security object” cannot be confined to the identified specific version set forth as an exemplary embodiment in Appellants’ Specification. Appellants’ claims simply do not place any limitation on what the “group security object” is to be, to represent, or to mean, other than that it is created in dependence upon user-selected group security control data type and comprises security control data (comprising user identification) and at least one security method.

Matyas discloses creating a biometric template for each user by obtaining a plurality of biometric samples for the user, storing each of a plurality of templates of biometric data associated with the user identification and storing an identification of at least one of the plurality of templates as a primary biometric authentication type of stored biometric data, wherein the stored biometric data represents the static and dynamic data used by software programs that resides in the memory (FF 1A-2B). We find the templates created in dependence upon biometric authentication type comprising user identification and biometric data used by security software programs, as disclosed by Matyas, to be a group security object created in dependence upon security control data types, which comprises security control data (comprising security control user identification) and security method. We thus, agree with the Examiner that Matyas discloses the claimed “group security object” of the claims on appeal.

Receiving a Request for Access

Appellants argue that “Matyas does not disclose receiving a request for access to the resource” (App. Br. 11). In particular, Appellants argue “Matyas at column 4, lines 13-15, does not even mention anything resembling receiving a request for access to the resource as claimed in the present application” (App. Br. 11). Accordingly, the issue is whether Matyas discloses the claimed limitation of “receiving a request for access to the resource” (Claim 1).

Matyas discloses receiving an authentication message from a user to obtain access to certain resources (FF 3A-B). We find the received authentication message, as disclosed by Matyas, to be a request for access to resource. We thus, agree with the Examiner that, contrary to the Appellants’ assertions, Matyas discloses the claimed “receiving a request for access” of the claims on appeal.

Receiving Security Request Data

Appellants argue that Matyas does not “disclose receiving security request data, wherein the security request data includes at least one security request user identification” (App. Br. 12). In particular, Appellants argue that “Matyas’ biometric information presented to recover a secret key, which is not a resource as claimed here, does not therefore disclose, receiving security request data to determine access to the resource as claimed in the present invention” (App. Br. 12).

Matyas discloses receiving an authentication message from a user to obtain access to certain resources, wherein the authentication message contains data which includes user identification and biometric data associated with the user (FF 1A-2B). In fact, Appellants admit that Matyas discloses receiving biometric information from a user (App. Br. 12). Though Appellants argue that the biometric information is “presented to recover a secret key” (App. Br. 12), such user authentication is used to provide access to certain resources (FF 3A-B). We find the received biometric information, as disclosed by Matyas, to be a security request data which includes security request user identification. We thus agree with the Examiner that Matyas discloses the claimed “receiving security request data” of the claims on appeal.

Determining Access to the Resource

Appellants argue that “Matyas does not disclose determining access to the resource in dependence upon the security control data and the security request data” (App. Br. 13). In particular, Appellants argue that “[c]alculating security data does not disclose determining access to a resource in dependence upon security control data and security request data” (App. Br. 13).

Matyas discloses receiving an authentication message from a user to obtain access to certain resources (FF 3A-B), wherein the received authentication message is considered a valid message if the comparison

indicates that the received user biometric data contained in the message corresponds to the stored biometric data (FF 1A-B). As discussed above, we find that the stored biometric data to be security control data, and the user biometric data in the received authentication message to be security request data. We thus find determining whether a message is valid for access to the resources based on the comparison between received user biometric data and the stored biometric data, as disclosed by Matyas, to be determining access to the resource in dependence upon the security control data and the security request data. We thus agree with the Examiner that Matyas discloses the claimed “determining access to the resource” step of the claims on appeal.

Accordingly, we conclude that Matyas discloses the claimed limitations of A) “creating a group security object in dependence upon one or more user-selected group security control data types, the group security object comprising security control data and at least one security method, the security control data comprising at least one security control user identification”; B) “receiving a request for access to the resource”; C) “receiving security request data, wherein the security request data includes at least one security request user identification”; and D) “determining access to the resource in dependence upon the security control data and the security request data” (Claim 1). We thus conclude that Appellants have not shown that the Examiner erred in rejecting claim 1 and claims 2-21 falling with claim 1 under 35 U.S.C. § 102(e).

Appeal 2008-1325
Application 10/179,339

CONCLUSIONS OF LAW

- (1) Appellants have not shown that the Examiner erred in finding that claims 1-21 are unpatentable over the teachings of Matyas.
- (2) Claims 1-21 are not patentable.

DECISION

The Examiner's rejection of claims 1-21 under 35 U.S.C. §102(e) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

pgc

INTERNATIONAL CORP (BLF)
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN TX 78767-1469