

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte NAVEEN AERRABOTU, PHIEU TRAN,
and JEROME VOGEDES

Appeal 2007-4078
Application 10/267,390
Technology Center 2600

Decided: April 28, 2008

Before ROBERT E. NAPPI, JOHN A. JEFFERY,
and CARLA M. KRIVAK, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1-3, 6-8, 10-12, 14-20, and 22-24. Claims 4, 5, 9, and 21 have been indicated as containing allowable subject matter (Ans. 2-4). We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part and enter new grounds of rejection under 37 C.F.R. § 41.50(b).

STATEMENT OF THE CASE

Appellants' invention pertains to validating communications in a mobile wireless communication system. Specifically, the invention includes (1) receiving contact information with a signature from a source not on a contact list; (2) validating the signature by comparing the signature to a stored reference signature; and (3) updating the trusted contact list regarding the contact information if the signature is valid.¹ Claim 1 is illustrative:

1. A method in a wireless communication device, comprising:

receiving a session request;

rejecting the session request;

receiving a signature session request having a signature after the rejecting the session request;

validating the signature of the signature session request.

The Examiner relies on the following prior art references to show unpatentability:

Immonen	US 2002/0077993 A1	Jun. 20, 2002
Kolsky	US 2002/0142763 A1	Oct. 3, 2002

Claims 1-3, 6-8, 10-12, 14-20, and 22-24 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Kolsky and Immonen.²

¹ See generally Spec. 1:10-14; Abstract.

² We note that the Examiner's Answer does not expressly state the examiner's grounds of rejection, but instead refers us to a previous office action (Ans. 4). Such incorporations by reference, however, are improper under current practice. See MPEP § 1207.02 ("An examiner's answer should

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer for their respective details. In this decision, we have considered only those arguments actually made by Appellants.³ Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

OPINION

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966).

Discussing the question of obviousness of a patent that claims a combination of known elements, the Court in *KSR Int'l v. Teleflex, Inc.*, 127 S. Ct. 1727 (2007) explains:

When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless

not refer, either directly or indirectly, to any prior Office action without fully restating the point relied on in the answer.”).

³ Appellants acknowledge that the issues presented in the Appeal Brief filed June 29, 2006, were incorrect and can therefore be disregarded (Reply Br. 2). We therefore refer exclusively to the arguments presented in the Reply Brief.

its actual application is beyond his or her skill. *Sakraida* [v. *AG Pro, Inc.*, 425 U.S. 273 (1976)] and *Anderson's-Black Rock, Inc. v. Pavement Salvage Co.*, 396 U.S. 57 (1969)] are illustrative—a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions.

KSR, 127 S. Ct. at 1740. If the claimed subject matter cannot be fairly characterized as involving the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement, a holding of obviousness can be based on a showing that “there was an apparent reason to combine the known elements in the fashion claimed.” *Id.* at 1740-41. Such a showing requires “some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *Id.* at 1741 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

If the Examiner’s burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

Regarding the independent claims, the Examiner's rejection essentially finds that Kolsky teaches every claimed feature except for (1) receiving a signature session request having a signature after rejecting the session request, and (2) validating the signature of the signature session request as claimed. The Examiner cites Immonen as teaching these features and

concludes that the recited limitations would have been obvious to ordinarily skilled artisans in view of the collective teachings of the references (Final Rej. 4-10; Ans. 4-6).

Claims 1-3, 6-8, 10, and 11

Regarding independent claim 1, Appellants argue that there is no reason for Kolsky to validate a signature *after* rejecting a session request since validating occurs in Kolsky *before* rejecting the call (Reply Br. 3). Appellants also argue that claim 1 recites that rejection and validation occur in the *same entity*, but Immonen teaches that the user provides a digital signature in one location, and verification occurs at a different location (i.e., the Wireless Electronic Transaction server) (Reply Br. 3-4).

The issue before us, then, is whether the cited prior art teaches or suggests performing the following steps *in a wireless communication device*: (1) receiving a signature session request having a signature *after* rejecting a session request; and (2) validating the received signature. For the following reasons, we conclude that it does not.

Kolsky discloses a system for establishing a push session between a push initiator and a telephone device. In one embodiment, the push initiator 19 attempts to call a mobile phone 29 via mobile network 22. The network, in turn, sends a control message 23 encoded with the push initiator's caller ID to the mobile phone. A call processor 24 executing in the phone examines the incoming call request (control message) and retrieves the calling party ID embedded in the call request.

The retrieved ID is then checked against a database of push initiators' IDs (PIDB 26). If the calling ID matches a number in the database, the call

is rejected via connection 27. A Session Initiation Application 16 is then informed that it should establish a push session 17 with the push initiator 10 using push session mechanism 18 (Kolsky, ¶¶ 0022, 0039; Fig. 2).

Turning to the specific language of independent claim 1, we note that the claim expressly recites four method steps that, according to the preamble, are performed *in* a wireless communication device. With these limitations in mind, we agree with the Examiner that Kolsky's mobile phone 29 corresponds to the recited wireless communication device, and that such a wireless device receives and rejects a session request (i.e., the push initiator's initial call to the mobile phone). However, we do not agree that the prior art reasonably teaches or suggests performing the last two steps of claim 1 *in* the wireless communication device as claimed.

Significantly, claim 1 requires that the third step (i.e., receiving a signature session request) occurs *after* rejecting the session request and, as noted above, must occur *in* the wireless device. Kolsky's mobile phone does launch an internal Session Initiation Application to initiate the push session after rejecting the call. The communication from the phone's Session Initiation Application to the push session mechanism 18, however, is in one direction as shown in Figure 2. This unidirectional communication suggests that the phone does not receive data from the push session mechanism, let alone a signature session request from this device.

But even if we were to assume, without deciding, that Kolsky's phone could somehow receive data from the push session mechanism following rejecting a call, we find nothing on this record that would teach or suggest that this subsequently-received data would be a signature session request,

much less that validation of the signature associated with such a request would likewise occur in the phone.

The secondary reference, Immonen, does teach using digital signatures in connection with secure e-commerce communications using a mobile terminal 100 to authenticate a customer's identity and confirm payment (Immonen, ¶¶ 0040-41). Furthermore, Immonen teaches inserting a Wireless Identity Module (WIM) (e.g., a smart card) in the mobile terminal to facilitate such secure communications (Immonen, ¶ 0047). Notwithstanding these security features, however, we agree with Appellants that validating the digital signatures in Immonen is performed by an entity different from the wireless device (i.e., the phone).

As shown in Figure 6a, for example, the phone's WIM computes the digital signature (message 605a), but the signature (and certificate) is ultimately transmitted to the Wireless Electronic Transactions (WET) gateway for verification (message 606a) (Immonen, ¶¶ 0060-61; Fig. 6a). Likewise, Figure 6b depicts another embodiment with a similar remote verification function (Immonen, Fig. 6b (messages 608b and 609b); ¶ 0063)). Moreover, the Examiner's reliance on Figure 6c of Immonen (Ans. 5) is unavailing as this embodiment does not support WIM or digital signatures at all (Immonen, ¶ 0064).

Based on this functionality, Immonen does not teach or suggest validating the signature of a signature session request in the wireless device. Indeed, Immonen teaches just the opposite.⁴ Immonen therefore does not cure the deficiencies noted above with respect to the disclosure of Kolsky.

⁴ See Immonen, ¶ 0065 (“The use of digital signatures *requires* that the signature is verified on the server side.”) (emphasis added).

For the foregoing reasons, we will not sustain the Examiner's rejection of independent claim 1 or dependent claims 2, 3, 6-8, 10, and 11 for similar reasons.

Claims 12 and 14

We will, however, sustain the Examiner's rejection of independent claim 12 which calls for, in pertinent part, (1) comparing a received authenticating signature with a stored reference signature on the wireless communication device, and (2) adding a sender to a list of trusted contacts if the authenticating signature is valid. These limitations, in our view, are amply suggested by Kolsky's PIDB located in the phone and its associated set-up procedure.

As we indicated previously, the mobile phone in Kolsky includes a database of push initiators' IDs (PIDB 26). These IDs, in our view, reasonably correspond to "reference signatures" as claimed giving the term "signature" its broadest reasonable interpretation.

In interpreting the term "signature," we first turn to Appellants' Specification for guidance.⁵ According to the Specification, "[t]he signature is generally authenticating information received by the server from the network for presentation to the wireless device for the purpose of authenticating the trustworthiness of the server as a source of information for

⁵ See *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005) (en banc) ("[T]he specification is the single best guide to the meaning of a disputed term, and...acts as a dictionary when it expressly defines terms in the claims or when it defines them by implication.") (internal quotation marks and citations omitted).

at least the transaction or session with which the signature is associated.”
(Spec. 6:20-24).

Based on this description, we find that the caller IDs of the push initiators used by the mobile phone in Kolsky reasonably constitute reference and authenticating “signatures” in light of the Specification. First, these caller IDs in Kolsky are provided by a server (push initiator) and presented to the mobile phone in the form of control messages with the caller ID encoded therein (Kolsky, ¶ 0039). Second, the IDs uniquely identify the particular push initiators to which the IDs are associated. Third, the received IDs are ultimately used by the phone to verify whether a particular push initiator ID is also stored in the phone’s PIDB -- a comparison which forms a basis to reject the call and initiate the push (Kolsky, ¶ 0039).

Thus, the stored push initiator IDs in the PIDB reasonably constitute “reference signatures.” Likewise, the push initiator IDs encoded in the control messages received by the phone reasonably constitute “authenticating signatures.” Moreover, the received push initiator ID (“authenticating signature”) is validated by matching it with a corresponding push initiator ID stored in the PIDB.

Although the result of this validation process is to initiate a push, we nonetheless find that the last step of claim 12 is also amply suggested by Kolsky. Kolsky indicates that the phone can accept remote set-up or provisioning of the push initiator identification information via a provisioning message (Kolsky, ¶ 0047). During set-up, if the entry is accepted, it is inserted in the PIDB. But if the entry *already exists in the*

PIDB, the information is *updated* with or without user acknowledgment (Kolsky, ¶ 0048; emphasis added).

The ability to update previously-existing entries in the *PIDB* is most significant to the last limitation of claim 12. First, ordinarily skilled artisans would have recognized that an entry that already exists in the *PIDB* reasonably corresponds to a reference signature as noted above. Second, such a reference signature could also have been used as a basis for comparison with an incoming authenticating signature to initiate a push (i.e., determining whether the authenticating signature is valid). In this event, if the stored ID corresponding to such a valid authenticating signature were subsequently updated using the set-up procedure noted above (i.e., the entry is updated despite its existence in the *PIDB*), the sender of the message (i.e., the push initiator) would be effectively added to the list of trusted contacts (the *PIDB*) by virtue of this update.

For the foregoing reasons, we find the limitations of independent claim 12 reasonably suggested by the collective teachings of the cited prior art. Accordingly, we will sustain the Examiner's rejection of that claim.

We will also sustain the Examiner's rejection of dependent claim 14 since we find that ordinarily skilled artisans would have recognized that the IDs stored in the *PIDB* in Kolsky used as a basis for comparison would have been generated (and stored) prior to receiving an incoming control message from a particular push initiator.

Claim 15

We will not, however, sustain the Examiner's rejection of claim 15. The Examiner's reference (Ans. 7) to the cited sections of Immonen as

allegedly teaching that expiration timers are inherent to the disclosed security features is unavailing. Even assuming that such security features would be applicable in Kolsky's system, the Examiner has simply provided no evidentiary basis for concluding that this expiration feature is inherent to the disclosed system apart from a mere conclusory assertion. To conclude that this feature is inherent to the security features of the cited prior art would require us to resort to speculation.

Therefore, we will not sustain the Examiner's rejection of claim 15.

Claims 16-18

We will also not sustain the Examiner's rejection of independent claim 16. As Appellants point out (Reply Br. 11), the Examiner has not specifically indicated how Kolsky and Immonen read on the limitations of claim 16 apart from including this claim with the rejection of the other independent claims. *See, e.g.*, Ans. at 4. Although claim 16, like independent claims 1, 12, and 24, recites that the method is performed in a wireless communication device, the claim recites a significant distinction: (1) contact information with a signature is received from a source *not* on a trusted contact list; (2) the signature is validated; and (3) the trusted contact list is validated if the signature is valid.

Although skilled artisans would have recognized that the control message received by the phone in Kolsky comprises "contact information" and an associated signature (i.e., the encoded push initiator caller ID), validation nonetheless occurs if the ID matches an ID stored in the PIDB. That is, the validated signature in Kolsky would be from a source *on a trusted contact list* (PIDB) -- a requirement that runs counter to the express

limitation of claim 16 requiring the source to *not* be on a trusted contact list. Moreover, Immonen does not cure the deficiencies of Kolsky in this regard.

For the foregoing reasons, we will not sustain the Examiner's rejection of independent claim 16 or dependent claims 17 and 18 for similar reasons.

Claims 19 and 20

We will, however, sustain the Examiner's rejection of independent claim 19 which calls for, in pertinent part, a provisioning session request message comprising (1) a message header portion; (2) the header message [sic] portion including authenticating signature data; and (3) a message body portion. Appellants argue that Kolsky's control message is not a provisioning session request message (Reply Br. 14). Kolsky, however, expressly states that the phone can accept remote set-up or *provisioning* of the push initiator identification and session initiation information *via a provisioning message* (Kolsky, ¶ 0047; emphasis added).

In our view, ordinarily skilled artisans would recognize that this set-up procedure would include "authenticating signature data" at least with respect to updating the entries in the PIDB -- entries that are based, at least in part, on signature data as we noted previously. *See, e.g.*, Kolsky, ¶¶ 0047-48; *see also* Kolsky, ¶ 0042; Fig. 5 (disclosing an alternative set-up procedure involving sending a provisioning message to the mobile phone).

Formatting such a message to include a header and body portion with the header portion containing such signature data as recited in claim 19 is merely a function of a given messaging protocol. Such a format, in our view, is tantamount to the predictable use of prior art elements according to

their established functions -- an obvious improvement. *See KSR*, 127 S. Ct. at 1740. Moreover, we find that formatting this provisioning message to conform to the specific type of message recited in claim 20 likewise merely constitutes a predictable use of prior art elements according to their established functions. *See id.*

For the foregoing reasons, we will sustain the Examiner's rejection of claims 19 and 20.

Claim 22

We will sustain the Examiner's rejection of independent claim 22 that, unlike independent claims 1, 12, 16, and 24, calls for the method to be performed in a server. Nevertheless, we find the prior art amply suggests these limitations essentially for the reasons previously indicated with respect to independent claim 1, and we therefore incorporate that discussion here by reference.

We add that nothing in the claim precludes the functionality of an intermediate server within the mobile network 22 of Kolsky -- a predictable wireless network capability well within the level of ordinarily skilled artisans. By establishing communications with an upstream push initiator, such an intermediate server would effectively request a signature from the wireless communications network -- a signature that ultimately originates from the push initiator. Moreover, in its intermediary role, the server would also subsequently send a session request including the authenticating signature (i.e., the control message) to the downstream mobile phone.

For the foregoing reasons, we will sustain the Examiner's rejection of independent claim 22.

Claim 23

We will not, however, sustain the Examiner's rejection of claim 23. We find the Examiner's reliance on the cited passages to Immonen along with the Examiner's rationale pertaining to receiving data from "an alternate, trusted source" (Ans. 7) unavailing. While we can envision an intermediate server on the mobile network 22 of Kolsky functioning as an intermediary between the push initiator and the mobile phone as noted above, we find nothing in the record before us that reasonably teaches or suggests *generating the session request* based upon the information received from the wireless communication network as claimed.

At best, an intermediary server could *send* such a session request (i.e., transmitting the received control message to the phone), but we fail to see how such a server would *generate* such a request as claimed. Nor do we find anything in the cited prior art that reasonably suggests such a feature.

Accordingly, we will not sustain the Examiner's rejection of claim 23.

Claim 24

We will also sustain the Examiner's rejection of independent claim 24 essentially for the reasons we indicated previously with respect to independent claims 12 and 19. We therefore incorporate that discussion here by reference. For the previously stated reasons, the Examiner's rejection is therefore sustained.

New Grounds of Rejection Under 37 C.F.R. § 41.50(b)

Claims 19-21 are rejected under 35 U.S.C. 101 as reciting non-statutory subject matter. Claim 19 calls for, in pertinent part, a provisioning

session request message comprising: (1) a message header portion; (2) the header message [sic] portion including authenticating signature data; and (3) a message body portion.

Independent claim 19 and the claims dependent thereon, in effect, recite data per se arranged in the form of a message with the recited format. Such mere arrangements of data, however, constitute non-functional descriptive material -- material which does not fall within any category of statutory subject matter under § 101. *See* MPEP § 2106.01(II), Rev. 6, Sept. 2007 (“Certain types of descriptive material, such as...mere arrangements or compilations of facts or data, without any functional relationship is not a process, machine, manufacture, or composition of matter.”).

But even if the recited message data could be considered functional descriptive material, it too would be non-statutory in the manner recited. Mere recitations of descriptive material, without more, do not constitute statutory subject matter. *See id.* at § 2106.01 (noting that both functional and non-functional descriptive material is non-statutory subject matter when claimed as descriptive material per se).

DECISION

We have sustained the Examiner's rejection with respect to claims 12, 14, 19, 20, 22, and 24. We have not, however, sustained the Examiner's rejection with respect to claims 1-3, 6-8, 10, 11, 15-18, and 23. Therefore, the Examiner's decision rejecting claims 1-3, 6-8, 10-12, 14-20, and 22-24 is affirmed-in-part. We have also entered a new grounds of rejection under 37 C.F.R. § 41.50(b) for claims 19-21 under 35 U.S.C. § 101.

Appeal 2007-4078
Application 10/267,390

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b). This section provides that “[a] new ground of rejection... shall not be considered final for judicial review.”

Section 41.50(b) also provides that the Appellants, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

(1) Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner. . . .

(2) Request that the proceeding be reheard under § 41.52 by the Board upon the same record. . . .

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-IN-PART
37 C.F.R. § 41.50(b)

KIS

MOTOROLA INC
600 NORTH US HIGHWAY 45
W4 - 39Q
LIBERTYVILLE, IL 60048-5343