Citation: Dresser, Inc. (Re), 2023 CACP 3
Commissioner's Decision 1636
Décision du commissaire nº1636
Date: 2023-01-17

TOPIC:	O00	Obviousness
	D00	Division
SUJET:	O00	Évidence
	D00	Division

Application No. : 3,081,876
Demande nº 3 081 876

IN THE CANADIAN PATENT OFFICE

DECISION OF THE COMMISSIONER OF PATENTS

Patent application number 3,081,876 having been rejected under subsection 199(1) of the *Patent Rules* (SOR/2019-251), has consequently been reviewed in accordance with paragraph 86(7)(c) of the *Patent Rules*. The recommendation of the Patent Appeal Board and the decision of the Commissioner are to refuse the application.

Agent for the Applicant:

KIRBY EADES GALE BAKER
100 Murray St., Suite 500
Ottawa, Ontario
K1N 0A1

INTRODUCTION

[1] This recommendation concerns the review of rejected Canadian patent application number 3,081,876 which is entitled “System and Method for Secure Communication in a Retail Environment” and is owned by DRESSER, INC. (“Dresser”). A Panel of The Patent Appeal Board (“we”) reviewed the application pursuant to paragraph 86(7)(c) of the *Patent Rules* (SOR/2019-251). We recommend that the Commissioner of Patents refuse the application for the reasons given below.

BACKGROUND

The Application

[2] The application relates generally to systems for secure communications in a retail environment. The application was a divisional filing of application CA 2,702,833 and inherits the parent’s filing date of October 7, 2008. The parent case was the subject of Commissioner’s Decision no. 1503. The Commissioner of Patents refused to issue a patent for that application, which is now dead. The instant application has 3 claims on file, received in the Patent Office on July 20, 2020.

Prosecution History

[3] On May 18, 2021, the Examiner issued a Final Action pursuant to subsection 86(5) of the *Patent Rules* (SOR/2019-251). The Final Action found the claims on file to be obvious, contrary to section 28.3 of the *Patent Act*. The Final Action also found the application to be an improper divisional, contrary to subsection 36(2) of the *Patent Act*.

[4] Dresser submitted a Response to the Final Action on September 15, 2021, including a set of 10 proposed claims.

[5] The Examiner was not persuaded by Dresser’s arguments in the Response to the Final Action and did not consider the proposed claims to overcome the defects. Therefore, the application was forwarded to the Patent Appeal Board for review on February 17, 2022 along with an explanation outlined in a Summary of Reasons.

[6] We reviewed the application on behalf of the Board under paragraph 86(7)(c) of

the *Patent Rules*. In a Preliminary Review letter ("PR letter") dated November 18, 2022, we analyzed the issues with respect to the application on file. We also invited Dresser to make oral and/or written submissions. In a letter received on December 6, 2022, Dresser declined the opportunity of a hearing or to make written submissions.

ISSUES

[7] The issues to be addressed in this review are the two identified in the Final Action:

- are the claims non-obvious and compliant with section 28.3 of the *Patent Act*? and

- as a divisional application, are the claims directed to an "other" invention compared to the parent application, as required by subsection 36(2) of the *Patent Act*?

[8] We also consider the proposed claims.

ALL CLAIMED ELEMENTS ARE PRESUMED TO BE ESSENTIAL

[9] The starting point for the analysis of both issues is purposive construction of the claims.

[10] In accordance with *Free World Trust v Électro Santé Inc*, 2000 SCC 66 and *Whirlpool Corp v Camco Inc*, 2000 SCC 67, purposive construction is performed from the point of view of the skilled person in light of the relevant common general knowledge, considering the whole of the disclosure including the specification and drawings. In addition to interpreting the meaning of the terms of a claim, purposive construction distinguishes the essential elements of the claim from the non-essential elements. Whether or not an element is essential depends on the intent expressed in or inferred from the claim, and on whether it would have been obvious to the skilled person that a variant has a material effect upon the way the invention works.

[11] Purposive construction begins by defining the notional skilled person and their common general knowledge.

[12] Our view of the skilled person remains as we wrote in the PR letter:

> Based on the background of the invention (pages 1-2 of the description), and consistent with the characterization in the Final Action, in our preliminary view, the skilled person or team has experience designing secure data communications systems to be used in the retail environment.

[13] The Final Action cited the following:

> D1: Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., Handbook of Applied Cryptography (Boca Raton: CRC Press, 1997) at pages 169-172, 506-507, 512-514, 559 and 560.
>
> D2: US 2005/0147250 Tang July 7, 2005

[14] Our view of the common general knowledge remains as we wrote in the PR letter:

> We also cite D1 to exemplify the common general knowledge. In our preliminary view, D1--a well-known reference book in the field of applied cryptography--demonstrates that the skilled person would have knowledge of cryptographic concepts such as trusted authorities, key certificates, public and private keys, signing of keys, symmetric and asymmetric encryption, key exchange protocols and random number generation. From the background of the instant description, the skilled person would also be familiar with point of sale (POS) systems in retail environments such as fueling stations, card readers, secure payment modules and data communication links between devices.

[15] Dresser did not submit any comments with respect to our characterization of the skilled person and common general knowledge.

[16] Claim 1 reads:

> A system for secure communication in a fueling environment, comprising:
>
> a first card reader configured to be disposed in a fuel dispenser;
>
> a first secure payment module (SPM) configured to be disposed in the fuel dispenser, the first SPM being communicably coupled to the first card reader, the first SPM including at least one processor configured to receive data from the first card reader, the first SPM storing a first public key certificate uniquely identifying the first SPM, the first public key certificate issued by a trusted certificate authority system, and a first private key associated with the first public key certificate; and
>
> a point-of-sale (POS) system, the POS system comprising at least one POS server storing a second public key certificate issued by the trusted certificate

> authority system, the POS system including at least one processor, wherein the at least one processor of the POS system is configured to:
>
> retrieve the first public key certificate from the first SPM, wherein the first public key certificate contains a first public key associated with the first SPM;
>
> verify an identity of the first SPM by authenticating the first public key certificate with the second public key certificate;
>
> generate a random first session key;
>
> wherein generating the first session key comprises using, at least in part, pseudorandom POS system entropy data;
>
> encrypt the first session key using, at least in part, the first public key; and
>
> transmit the encrypted first session key to the first SPM;
>
> wherein the at least one processor of the first SPM is configured to execute instructions stored at the first SPM, the instructions stored at the first SPM operable, when executed, to:
>
> receive the encrypted first session key from the POS system;
>
> decrypt the first session key using, at least in part, the first private key;
>
> receive a first set of sensitive data from the first card reader;
>
> encrypt the first set of sensitive data using, at least in part, the first session key; and
>
> transmit the encrypted first set of sensitive data to the POS system.

[17] In the PR letter we found all claim elements to be essential:

> Considering the whole of the specification, the skilled person would understand that there is no use of language in claim 1 indicating that any of the elements are optional or one of a list of alternatives. Therefore, in our preliminary view, all elements recited in the claim are essential. All elements of claims 2 and 3 are similarly essential.

IS THE CLAIMED INVENTION NON-OBVIOUS?

[18] In our view, the claimed invention is obvious according to the following analysis, which remains as expressed in the PR letter.

[19] Section 28.3 of the *Patent Act* requires claimed subject matter not to be obvious:

> The subject matter defined by a claim in an application for a patent in Canada must be subject matter that would not have been obvious on the claim date to a person skilled in the art or science to which it pertains, having regard to

> (a) information disclosed before the one-year period immediately preceding the filing date or, if the claim date is before that period, before the claim date by the applicant, or by a person who obtained knowledge, directly or indirectly, from the applicant in such a manner that the information became available to the public in Canada or elsewhere; and
>
> (b) information disclosed before the claim date by a person not mentioned in paragraph (*a*) in such a manner that the information became available to the public in Canada or elsewhere.

[20] In *Apotex Inc v Sanofi–Synthelabo Canada Inc*, 2008 SCC 61 at para 67, the Supreme Court of Canada stated that it is useful in an obviousness inquiry to follow the following four-step approach:

> (1)(a) Identify the notional "person skilled in the art";
>
> (b) Identify the relevant common general knowledge of that person;
>
> (2) Identify the inventive concept of the claim in question or if that cannot readily be done, construe it;
>
> (3) Identify what, if any, differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claim or the claim as construed;
>
> (4) Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention?

Identify the notional person skilled in the art and the relevant common general knowledge

[21] We identified these above for purposive construction.

Identify the inventive concept of the claim in question or if that cannot readily be done, construe it

[22] In our view, the inventive concept of representative claim 1 is expressed by the language of the claim itself.

Identify what, if any, differences exist between the matter cited as forming part of the "state of the art" and the inventive concept of the claim or the claim as construed

[23] In our view, D2 is the closest prior art. D2 discloses the application of secure communications in a fueling environment between an SPM and POS system.

[24] Below we requote claim 1, note which elements are disclosed in D2 through references to D2 in brackets, and underline those elements which are not disclosed in D2. This is unchanged from the PR letter:

> A system for secure communication in a fueling environment [abstract], comprising:
>
> a first card reader configured to be disposed in a fuel dispenser [Figure 5, also para 0067 and Figure 11; a card reader is implicit as the paragraph recites reporting card information from this node];
>
> a first secure payment module (SPM) configured to be disposed in the fuel dispenser [para 0071 and Figure 11, element 1105], the first SPM being communicably coupled to the first card reader, the first SPM including at least one processor configured to receive data from the first card reader [para 0047 and Figure 5, element 510], the first SPM storing a first public key certificate uniquely identifying the first SPM, the first public key certificate issued by a trusted certificate authority system, and a first private key associated with the first public key certificate [para 0073]; and
>
> a point-of-sale (POS) system [para 0071 and Figure 11, element 1120], the POS system comprising at least one POS server [paras 0071 and 0073-0074], <u>storing a second public key certificate issued by the trusted certificate authority system</u>, the POS system including at least one processor, wherein the at least one processor of the POS system is configured to:
>
> retrieve the first public key certificate from the controller, wherein the first public key certificate contains a first public key associated with the first SPM [para 0071];
>
> verify an identity of the first SPM by authenticating the first public key certificate [para 0071 recites authentication] <u>with the second public key certificate</u>;
>
> generate a random first session key;
>
> wherein generating the first session key comprises using, at least in part, pseudorandom POS system entropy data;

encrypt the first session key using, at least in part, the first public key; and

transmit the encrypted first session key to the first SPM;

wherein at least one processor of the first SPM is configured to execute instructions stored at the first SPM, the instructions stored at the first SPM operable when executed to:

receive the first encrypted first session key from the POS system;

decrypt the first session key using, at least in part, the first private key;

receive a first set of sensitive data from the first card reader [para 0053 and Figure 6, step 605];

encrypt the first set of sensitive data using, at least in part, the first session key [para 0053 and Figure 6, step 610 using symmetric key encryption as disclosed in para 0074 and Figure 12, step 1220]; and

transmit the encrypted first set of sensitive data to the POS system [para 0074].

[25] In the PR letter, we wrote (note that references to “you” in this and other quotations from the PR letter mean Dresser) :

> In our preliminary view, the differences between the inventive concept of claim 1 and D2 are:
>
> > ● the POS system storing a second public key certificate used for authenticating the first public key certificate; and
> >
> > ● the POS system generating a random first session key using at least in part, pseudorandom entropy data; encrypting the first session key using, at least in part, the first public key of the SPM; and transmitting the encrypted first session key to the first SPM; the first SPM receiving the first encrypted first session key from the POS system; and the SPM decrypting the first session key using, at least in part, the first private key.
>
> D2 does not recite the POS system authenticating the SPM’s public key certificate using a second certificate at the POS. Rather, in D2, the symmetric session key is generated at each of the SPM and POS independently by using the same key generation algorithms, whereas in claim 1, the symmetric session key is generated at the POS, using at least in part, pseudorandom system entropy data, encrypted with a public key of the SPM, and sent to the SPM, where it is decrypted, using the corresponding private key. We will discuss each of these differences.

> In the Response to the Final Action, you pointed out (page 3) that D1 pertains to general encryption and does not disclose various details of the components recited in claim 1. We have based our analysis on D2 as the primary citation with D1 providing some elements of common general knowledge.

Viewed without any knowledge of the alleged invention as claimed, do those differences constitute steps which would have been obvious to the person skilled in the art or do they require any degree of invention

[26] In the PR letter, we wrote:

> Regarding the first difference, D2 teaches the use of a signed certificate by a trusted source [para 0071] but teaches the use of the enclosed public key to verify the SPM's identify through transfer of an encrypted random number. Claim 1 instead recites verifying the SPM's identity by authenticating the first public key certificate with the second public key certificate. In our preliminary view, the skilled person familiar with trusted authorities and public key certificates would understand that the specific authentication embodiment of D2 is optional and but one of several possible methods [para 0072]. If there is a high degree of trust in the certificate authority, then a verification of the first public key certificate, such as by comparison with the second public key certificate, is sufficient to authenticate the SPM. In our preliminary view, this difference is obvious.
>
> Regarding the second difference, in D2 both the SPM and the POS independently generate the same symmetric session key by running the same agreed algorithm, whereas in the system of claim 1, the POS generates a random symmetric session key and sends it to the SPM using public/private key encryption. D2 [para 0072] notes that the recited key generation technique is but one possible method. In our preliminary view, the skilled person knowing the common general knowledge would be led to consider modifying the system of D2 to avoid the need to generate session keys at the SPM or to avoid storing potentially discoverable session key generation algorithm(s) at the SPM.
>
> The skilled person would then consider the various secure key exchange techniques of the common general knowledge. As D2 describes a fueling environment with a public key infrastructure, the skilled person would be motivated to consider using one of the well-known public key transport protocols. It was well known in the art to distribute a randomly-generated session key to an entity using the entity's public key. In particular, the "one-pass key transport by public-key encryption" scheme of D1, section 12.5.1, provides an example of encrypting a session key with a public key for transport with a minimal number of messages needed to be exchanged. Therefore, in our preliminary view, this difference between D2 and claim 1 is obvious.

Regarding the aspect of using pseudorandom system entropy data, D2 discloses random number generation [para 0064]. In D2, pseudorandom entropy system data relates to a random number used in authentication, not as a session key. In our preliminary view, the cited passage in D2 exemplifies that the use of pseudorandom system entropy data in generating random or pseudorandom numbers for various purposes is common general knowledge. This is further exemplified specifically for cryptographic keys in D1 [pages 169-172].

In the Response to the Final Action, you asserted that neither DI nor D2 mentions pseudorandom POS system entropy data at all, much less in generating a random session key. In our preliminary view, D1 and D2 show this to be common general knowledge.

Independent claims 2 and 3 do not recite the pseudorandom system entropy aspect. Omission of this element broadens the scope of these claims and does not render them inventive.

Claim 2 additionally recites that the coupling between the first SPM and first card reader is physically secured in a tamper-resistant enclosure. D2 discloses a card reader in a tamper-resistant enclosure [para 0004] but does not disclose the coupling to the card reader being in such an enclosure. In our preliminary view, the choice of which elements to physically secure in a tamper-resistant enclosure is a design decision which is part of the common general knowledge and non-inventive.

You asserted in the Response to the Final Action (page 3) that D2 fails to recognize the importance of secure communication between the card reader and an SPM. As we noted above, D2 does disclose a tamper-proof enclosure for the card reader, indicating a concern for security locally at the pump. We did not consider the choice to also include the SPM within the tamper-proof enclosure to be inventive.

Independent claim 3 additionally recites that the first SPM receives the encrypted first session key from the POS and decrypts it *before* the first SPM receives the first set of sensitive data from the card reader. In our preliminary view, the skilled person would understand that the decrypted first session key is necessary to encrypt and transmit the first sensitive data, and whether that first data is received before or after the first session key is immaterial, as encryption and transmission must wait until there is a decrypted first session key available. We therefore do not consider the additional restriction of claim 3 to be inventive.

You further asserted in the Response to the Final Action (page 4) that D2 indicates that its symmetric key is generated at "run-time", and therefore not before the SPM receives the first set of sensitive data. As we stated above, the skilled person would understand that the session key is necessary before any

> received data from the card reader can be encrypted and transmitted. We do not consider D2 to teach away from this principle.

[27] Dresser did not submit any comment on our analysis.

Conclusion on obviousness

[28] In our view, claims 1 - 3 are obvious having regard to D2 in view of the common general knowledge and do not comply with section 28.3 of the *Patent Act*.

IS THE APPLICATION A PROPER DIVISIONAL?

[29] Subsection 36(2) of the Patent Act sets out the conditions in which an applicant may properly file a divisional application:

> Where an application (the “original application”) describes more than one invention, the applicant may limit the claims to one invention only, and any other invention disclosed may be made the subject of a divisional application, if the divisional application is filed before the issue of a patent on the original application.

[30] The question is whether the claims of the instant application define an “other” invention.

[31] As we stated in the PR letter, in *Bayer Schering Pharma AG v Canada (Attorney General)*, 2009 FC 1249, the Court stated (at paragraph 54):

> The prohibition against double patenting involves a comparison of the claims rather than the disclosure, because the claims define the monopoly. There are two approaches as to determining whether there has been a double patenting: one is to consider whether the claims are identical or conterminous, an approach which is sometimes called the “same invention”; a second branch of the test is to consider whether the second patent is “obvious” or not “particularly distinct” from the first, based on the common knowledge of an ordinary workman as of the date of publication of the patent.

[32] To be clear, there is no issue of double patenting in the instant case. The parent case is now dead. However, the approach used in the second branch of double patenting analysis can also be used to determine if the instant claims define an “other” invention relative to the claims of the parent case.

[33] In the PR letter, we wrote:

> Comparing independent claim 1 of the instant application to claim 7 of CA 2702833, received in the Patent Office on March 31, 2015, (the latest set of claims on file) the only difference is that instant claim 1 does not recite a controller between the SPM and POS system. The controller in CA 2702833 merely forwards information; all processing of the information occurs in the SPM and POS. The skilled person with common general knowledge of data communications would appreciate that data communications transmit and receive functions could be implemented within the SPM and POS elements.
>
> Comparing independent claim 2 of the instant application to claim 13 of CA 2702833, the only difference is the absence of a controller as discussed above.
>
> Comparing independent claim 3 of the instant application to claim 1 of CA 2702833, the only difference is that the first SPM receives the encrypted first session key from the POS and decrypts it before the first SPM receives the first set of sensitive data from the card reader. As discussed above for obviousness, the skilled person would understand that the decrypted first session key is necessary to encrypt and transmit the first sensitive data, and whether that first data is received before or after the first session key is immaterial. We preliminarily do not consider this an inventive feature.

[34] Dresser did not submit any comment on our analysis.

[35] We conclude that the instant claims do not define an “other” invention relative to CA 2702833, and do not comply with subsection 36(2) of the *Patent Act*.

DO THE PROPOSED CLAIMS CURE THE DEFECTS?

[36] In brief, as we expressed in the PR letter, proposed independent claims 1 and 6 are similar to claim 1 on file, but proposed independent claims 1 and 6 additionally recite:

- there are two SPMs in communication with the POS environment, and a common third public key certificate issued by the trusted certificate authority is used to authenticate both first and second public key certificates for the first and second SPMs respectively; and

- each SPM and card reader authenticate each other prior to exchanging information.

Would the proposed claims be non-obvious?

[37] In the PR letter, we wrote:

> We need only examine the incremental differences of the proposed claims with respect to those on file, having already determined that those on file are obvious.
>
> In our preliminary view, the proposed claims are also obvious.
>
> Regarding proposed independent claims 1 and 6, directed to a secure fuel payment system and a secure fuel dispensing system respectively, the skilled person would know that a plurality of fuel payment or dispensing systems at a fueling station is common. The extension of the system to multiple SPMs does not require inventive ingenuity. The skilled person would appreciate that a public key certificate can be used to authenticate multiple public keys and would naturally consider using a common public key certificate to authenticate the keys associated with multiple SPMs. We also note that D2 alludes to a multiplicity of SPMs when it recites “at least one dispenser node” [para 0068.]
>
> Regarding the mutual authentication of SPMs and respective card readers, in our preliminary view, applying the well-known concept of mutual authentication to two nodes within the fuel dispenser (SPM and card reader) is a design option within the common general knowledge of the skilled person and would not require inventive ingenuity.
>
> Proposed claims 2 and 7 recite receiving and decrypting the first session keys at the POS. This is common general knowledge.
>
> Proposed claims 3 and 8 recite the POS server sending the payment data to a first authorization network. This is common general knowledge. We also note that D2 discloses this [para 0041 and Figure 2, element 220.].
>
> Proposed claims 4, 5, 9 and 10 recite the detailed steps of authenticating the first and second SPMs using public key certificates. These are common general knowledge.
>
> In our preliminary view, proposed claims 1 - 10 would be obvious having regard to D2 in view of the common general knowledge and would not comply with section 28.3 of the Patent Act.

[38] Dresser did not submit any comment on our analysis.

[39] We conclude that in our view, the proposed claims would be obvious, contrary to subsection 28.3 of the *Patent Act*.

Would the proposed claims render the application a proper divisional?

[40] In the PR letter we wrote:

> In our preliminary view, the proposed claims do not define an “other” invention compared to the parent application. In our analysis of the proposed claims for obviousness above, we preliminarily found the differences of those claims with respect to the claims on file to be obvious in view of common general knowledge alone, although some passages of D2 were additionally cited for emphasis. Since we also found the instant claims on file not to define an “other” invention from those of the parent application CA 2702833, it follows that the proposed claims differ from those of parent application CA 2702833 only with respect to non-inventive features of common general knowledge.
>
> We also note that claim 10 of parent case CA 2702833 claimed the feature of there being two SPMs in communication with the POS environment.

[41] Dresser did not submit any comment on our analysis.

[42] Therefore, we conclude that the proposed claims would not define an “other” invention according to subsection 36(2) of the *Patent Act*.

RECOMMENDATION OF THE BOARD

[43] We recommend that the Commissioner of Patents refuse to issue a patent for this application on the grounds that:

- the claims on file are obvious and therefore non-compliant with section 28.3(b) of the *Patent Act*; and

- the application on file is an improper divisional and does not comply with subsection 36(2.1) of the *Patent Act*.

[44] The proposed claims do not cure the defects and therefore do not constitute "necessary amendments" according to subsection 86(11) of the *Patent Act*.

Howard Sandler	Michael Ott	Lewis Robart
Member	Member	Member

DECISION OF THE COMMISSIONER

[45] I concur with the recommendation of the Board that the application be refused on the grounds that:

- the claims on file are obvious and therefore non-compliant with section 28.3(b) of the *Patent Act*; and

- the application on file is an improper divisional and does not comply with subsection 36(2.1) of the *Patent Act*.

[46] Therefore, in accordance with section 40 of the *Patent Act*, I refuse to grant a patent on this application.

[47] Under section 41 of the *Patent Act*, the Applicant (Dresser) has six months within which to appeal my decision to the Federal Court of Canada.

Konstantinos Georgaras

Commissioner of Patents

Dated at Gatineau, Quebec

this 17th day of January, 2023