Commissioner’s Decision No. 1503

Décision du commissaire n^{o} 1503

TOPICS: O00 Obviousness

SUJETS: O00 Évidence

Application No. 2,702,833

Demande n^{o} 2 702 833

IN THE CANADIAN PATENT OFFICE

DECISION OF THE COMMISSIONER OF PATENTS

Patent application number 2,702,833, having been rejected under subsection 30(3) of the *Patent Rules* (SOR/96-423) as they read immediately before October 30, 2019 (the *former Patent Rules*), has consequently been reviewed in accordance with paragraph 199(3)(*c*) of the *Patent Rules* (SOR/2019-251). 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 2,702,833, which is entitled “System and Method for Secure Communication in a Retail Environment” and is owned by Dresser Inc. (the Applicant). A review of the rejected application has been conducted by the Patent Appeal Board (the Board) pursuant to paragraph 199(3)(*c*) of the *Patent Rules*.

[2] As explained in more detail below, our recommendation is that the Commissioner of Patents refuse to issue a patent for this application.

BACKGROUND

The Application

[3] The application, based on a previously filed Patent Cooperation Treaty application, is considered to have been filed in Canada on October 7, 2008 and was laid open to the public on April 23, 2009.

[4] The application relates generally to systems for secure communications in a retail environment.

Prosecution History

[5] On January 12, 2017, a Final Action (FA) was issued pursuant to subsection 30(4) of the *former Patent Rules*. The FA stated that the instant application was defective as all of the 19 claims on file were directed to obvious subject matter and therefore did not comply with section 28.3 of the *Patent Act*.

[6] In a response to the FA (RFA) received on July 4, 2017, the Applicant submitted arguments in favour of the claims being allowable.

[7] The Examiner considered the application not to comply with the *Patent Act* despite the arguments submitted with the RFA. Therefore, pursuant to paragraph 30(6)(*c*) of the *former Patent Rules*, the application was forwarded to the Board for review along with an explanation outlined in a Summary of Reasons (SOR). The SOR set out the position that the claims on file were still considered to be defective. In a letter dated August 23, 2017, the Board forwarded a copy of the SOR to the Applicant.

[8] In a response to the SOR (RSOR) received on March 5, 2019, the Applicant submitted further arguments in favour of the claims being allowable.

[9] The present panel (the Panel) was formed to review the application under paragraph 30(6)(*c*) of the *former Patent Rules*. The Panel sent a Preliminary Review letter (the PR letter) to the Applicant on July 17, 2019 wherein we set out our preliminary analysis and rationale as to why, based on the record before us, the claims on file are obvious.

[10] The Applicant declined the opportunity for a hearing. On August 15, 2019, the Applicant provided written submissions in response to the PR letter (the RPR) arguing in favour of the claims being allowable and also submitted a proposed amended set of 18 claims (the proposed claims).

ISSUES

[11] The issue to be addressed by the present review is whether the claims on file are directed to obvious subject matter according to section 28.3 of *the Patent Act*. In the event that the claims on file are found to be defective, we also consider the proposed claims.

LEGAL PRINCIPLES AND OFFICE PRACTICE

Purposive construction

[12] In accordance with *Free World Trust v Électro Santé Inc*, 2000 SCC 66, essential elements are identified through a purposive construction of the claims done by considering the whole of the disclosure, including the specification and drawings (see

also *Whirlpool Corp v Camco Inc*, 2000 SCC 67 at paras 49(f) and (g) and 52). Patent Office practice to construe claims according to a purposive construction is specified in the *Manual of Patent Office Practice* (CIPO) at §12.02, revised June 2015 [*MOPOP*].

Obviousness

[13] 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 more than one year before the filing 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.

[14] In *Apotex Inc v Sanofi-Synthelabo Canada Inc*, 2008 SCC 61 [*Sanofi*] 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?

ANALYSIS

Purposive Construction

[15] In the RFA as well as the RSOR, the Applicant disagreed with the purposive construction used in the FA in which some recited elements of claim 1, notably the fueling environment, were not considered to be essential. In our obviousness analysis below, we have considered all the features of the claims as essential, thus rendering this issue moot. Additionally, we found no issues regarding the meaning of terms used in the claims. Therefore, a detailed purposive construction analysis of the claims is not necessary.

Obviousness

(1)(a) Identify the notional "person skilled in the art" (PSA)

[16] Consistent with the PR letter, based on the background of the invention (pages 1-2 of the description), in our view, the PSA is a person or team designing secure data communications systems to be used in the retail environment. In the RPR, the Applicant did not dispute this definition and we adopt it here.

(1)(b) Identify the relevant common general knowledge of that person

[17] The FA 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.
D3: US 2005/0147250 Tang July 7, 2005

[18] We cite D1 to exemplify CGK. In our view, D1--a well-known reference book in the field of applied cryptography--demonstrates that the PSA 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 PSA

would also be familiar with point of sale (POS) systems in retail environments, card readers, secure payment modules and data communication links between devices.

[19] With the exception of random number generation, which we add due to the emphasis on this issue given by the Applicant in the RPR and in the proposed claims, we noted the above CGK in the PR letter, and the Applicant did not dispute this in the RPR.

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

[20] In our view, the combination of all features of independent claim 1 represents the inventive concept. In the RPR, the Applicant did not dispute this.

(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

[21] In our view, D3 is the closest prior art. Below we quote claim 1, note which elements are disclosed in D3 through references to D3 in brackets, and *italicize* elements which are not disclosed in D3:

> 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 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; also para 0071 discloses a controller for GUI 1116], 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];
>
> *a controller configured to receive the first public key certificate from the at least one processor of the first SPM, a first communication line*

coupling the controller and the at least one processor of the first SPM; 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], *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 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] *with the second public key certificate*;

generate a random first session key;

encrypt the first session key using, at least in part, the first public key; and transmit the encrypted first session key to the controller;

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 controller;

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 controller [para 0074]; and

wherein the controller is configured to receive the encrypted first set of sensitive data from the first SPM and to transmit the received encrypted first set of sensitive data to the POS system [para 0053 and Figure 6, step 615 using symmetric key encryption as disclosed in para 0074 and Figure 12, step 1222].

[22] In our view, the differences between the inventive concept of claim 1 and D3 are:

- a controller configured to receive the first public key certificate from the at least one processor of the first SPM, a first communication line coupling the controller and the at least one processor of the first SPM;
- the POS authenticating the first public key certificate using the second public key certificate;
- the POS generating a random first session key; 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 controller; the SPM receiving the first encrypted first session key from the controller; and the SPM decrypting the first session key using, at least in part, the first private key.

[23] To summarize, claim 1 differs from the closest prior art D3 in three respects. First, D3 does not explicitly recite a controller at the SPM. Second, D3 does not recite the POS authenticating the SPM's public key certificate using a second certificate at the POS. Third, in D3 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, encrypted with a public key of the SPM, and sent to the SPM, where it is decrypted, using the corresponding private key. These differences generally correspond to those identified as differences (A) – (E) by the Applicant in the RPR. We will discuss each of these differences below in detail in step 4.

[24] Independent claim 14 recites the same essential elements as claim 1. Independent claim 15 is similar to claim 1 but does not recite the encryption of data. Our analysis with respect to the differences between D3 and claim 1 apply also to claims 14 and 15.

[25] Dependent claim 2 recites using digital signatures to authenticate components. D3 further discloses this aspect [para 0067].

[26] Dependent claim 3 recites the POS receiving and decrypting the data using the session key. D3 further discloses decrypting data at the POS using the session key [para 0053 and Figure 6, step 620].

[27] Dependent claims 4-6 recite generating and sending a second session key which is used to encrypt a second set of data. D3 further discloses second session keys [para 0040].

[28] Dependent claim 7 recites generating the first session key using pseudo-random system entropy data. In the PR letter, we noted that D3 discloses using system entropy data to generate random or pseudo-random data [para 0064]. In the RPR, the Applicant pointed out in difference (F) that the random or pseudo-random number thus generated in D3 is not used as a session key, but is used as part of an authentication protocol. We discuss this difference below in step 4.

[29] Dependent claim 8 recites the trusted certificate authority being associated with an operator of the SPM. D3 further discloses a trusted authority associated with a node [para 0067].

[30] Dependent claim 9 recites the data comprising magnetic card data. D3 further discloses encrypting magnetic card data [para 0041].

[31] Dependent claims 10-12 recite a second SPM and associated keys, certificates, and session key exchanges. D3 further discloses a multiplicity of SPMs and associated keys and certificates [para 0039 "…each PIN pad module…" and para 0068 "…at least one dispenser node…"].

[32] Dependent claim 13 recites the coupling between the first SPM and first card reader being physically secured in a tamper-resistant enclosure. D3 discloses a card reader in a tamper-resistant enclosure [para 0004] but does not disclose the coupling to the card reader in such an enclosure. Therefore, this difference is discussed below in step 4.

[33] Dependent claims 16-17 recite the limitations of the encryption or decryption performed at the SPM or POS respectively, not the controller. D3 further discloses encryption performed at the SPM and decryption at the POS [para 0053 and Figure 6, steps 610 and 620], but does not recite an explicit controller in the SPM which does not perform encryption or decryption. Therefore, this difference is discussed below in step 4.

[34] Dependent claim 18 recites the encryption of the data using the session key, as per claim 1, as well as the decryption at the POS using the session key, as previously considered with respect to claim 1.

[35] Dependent claim 19 recites that the first SPM, the controller and the POS systems are standalone. D3 does not recite a standalone controller.

[36] In summary, in our view, most additional elements recited by the dependent claims are disclosed by D3 except some elements of claims 7, 13, 16-17 and 19, which we will consider in our step (4) analysis.

(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?

Claim 1: The Controller

[37] While not explicitly recited in D3, the controller, defined as the means at the SPM to relay data physically over the link to and from the SPM and POS (see instant description at page 13, lines 8-26), is implicitly present in the system of D3. There is a requirement for data communications between the dispenser system and POS in D3 [para 0047 and Figure 5, element 506]. Thus, there exists some means associated with providing this communication function within the dispenser system (as well as in the POS). The data communication means within the SPM corresponds to at least part of the controller as defined in the instant description.

[38] In the RPR, the Applicant pointed out in difference (A) that the controller recited in claim 1 also acts to control electronic components of the fuel dispenser and may control other components. The Applicant also noted that D3 already recites a pump controller [Figure 5, element 515] and a dispenser control library for maintaining public keys [para 0048 and Figure 5, element 512] and therefore the PSA would not think to add an additional controller component.

[39] In our view, the collection of processing components in D3 such as pump controller 515, dispenser control library 512 and communications link 506 constitute an implementation of the controller recited in claim 1. The difference between a distributed implementation of these functions in several components within the SPM as claimed or within a single component implicit in D3 is merely a design implementation choice, which is CGK. It would be well-known to the PSA to design the controller element as either a combination of an input/output circuit working in conjunction with a general purpose processor in the SPM (such as in a processor with integrated input/output ports), or as a standalone device (such as a modem connected to a computer). In our view, this difference is obvious.

Claim 1: Authenticating the first public key certificate with the second public key certificate

[40] D3 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. As the Applicant pointed out in the RPR difference (B), claim 1 instead recites verifying the SPM's identity by authenticating the first public key certificate with the second public key certificate. In our view, the PSA familiar with trusted authorities and public key certificates would understand that the specific authentication embodiment of D3 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 view, this difference is obvious.

Claim 1: Session key generation at the POS, sent encrypted to the SPM

[41] As the Applicant pointed out in RPR differences (C), (D) and (E), in D3 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. The Applicant argued that D3 teaches the security advantage of its scheme in that the session key is not sent over the communication link, even in encrypted form, and that the PSA

would not be motivated to consider another scheme which involves key transfer over the communication link due to security concerns highlighted in D3. The Applicant highlighted that the system of D3 creates a problem in that special session key generation algorithms need to be resident on and executable by both the POS and SPM. However, the Applicant argued that D3 does not acknowledge this problem and thus does not provide a motivation to look for a solution to this problem.

[42] D3 [para 0072] notes that the recited key generation technique is but one possible method. In our view, the PSA knowing the CGK would be led to consider modifying the system of D3 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.

[43] The PSA would then consider the various secure key exchange techniques of the CGK. As D3 describes a fueling environment with a public key infrastructure, the PSA 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 view, this difference between D3 and claim 1 is obvious.

Differences in other claims

[44] Regarding dependent claim 7, in the PR letter, we stated that D3 discloses the aspect of random number generation [para 0064]. In the RPR, the Applicant pointed out in difference (F) that the cited passage in D3 relates to a random number used in authentication, not as a session key. In our view, the cited passage in D3 exemplifies that the use of system entropy data in generating random or pseudo-random numbers for various purposes is CGK. This is further exemplified specifically for cryptographic keys in D1 [pages 169-172].

[45] Regarding dependent claim 13, in our view, the choice of which elements to secure in a tamper-resistant enclosure is CGK.

[46] Regarding claims 16-17, as we noted above, data communications is within the CGK of the PSA. It would be well-known to the PSA to design the controller element as either a combination of an input/output circuit working in conjunction with a general purpose processor in the SPM, or as a standalone device. In our view, performing the encryption outside of the controller is a design choice which would be an obvious alternative considered by the PSA. For example, in standalone modems, the modem simply modulates and transmits the data it is given; any encryption would normally be performed prior to relaying data to the modem.

[47] Regarding dependent claim 19, the term "standalone" was not in the originally-filed specification and is not described. In our view, the term has ordinary meaning to the PSA as a physically separate component and is within the CGK.

[48] Therefore, in our view, claims 1 to 19 are obvious and do not comply with section 28.3 of the *Patent Act* having regard to D3 in view of CGK.

PROPOSED CLAIMS

[49] In the RPR, the Applicant proposed a set of amended claims. The proposed claims incorporate claim 7 on file into the independent claims. This is the element of generating the first session key using, at least in part, pseudo-random POS system entropy data.

[50] As mentioned above with respect to claim 7, this aspect is considered CGK.

[51] In our view, therefore, the proposed claims would not overcome the obviousness defect.

RECOMMENDATION OF THE BOARD

[52] For the reasons set out above, we recommend that the Commissioner of Patents refuse this application as the claims on file are directed to obvious subject matter and are therefore non-compliant with section 28.3 of the *Patent Act.*

[53] For the reasons set out above, we do not consider the proposed claims to constitute specific amendments necessary to comply with the *Patent Act* and *Patent Rules*. Accordingly, we decline to recommend that the Applicant be notified under subsection 199(5) of the *Patent Rules* that said proposed claims are necessary.

Howard Sandler Member	Claude Plante Member	Lewis Robart Member

DECISION

[54] I concur with the conclusions and recommendation of the Board that the application be refused on the ground that the claims on file are directed to obvious subject matter and are therefore non-compliant with section 28.3 of the *Patent Act*.

[55] Therefore, in accordance with section 40 of the *Patent Act*, I refuse to grant a patent on this application. Under section 41 of the *Patent Act*, the Applicant has six months within which to appeal my decision to the Federal Court of Canada.

Johanne Bélisle
Commissioner of Patents

Dated at Gatineau, Quebec,

This 5th day of December, 2019