Intellectual Property Office

BL O/0097/23

01 February 2023

PATENTS ACT 1977

APPLICANT	Avaya Inc.
ISSUE	Whether patent application GB1900670.9 complies with section 1(1)(b) and section 1(2) of the Patents Act 1977
HEARING OFFICER	Phil Thorpe

DECISION

Introduction

1 Patent application GB1900670.9 was filed on 17 January 2019 claiming a priority date of 22nd January 2018 from US application number 15/877,140. The application was published as GB2573187 A on 30th October 2019.

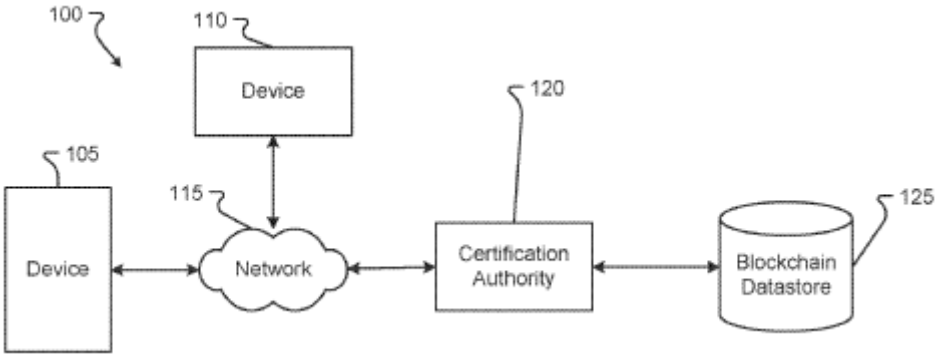
2 Despite numerous rounds of correspondence between the examiner and the applicant's attorney, the applicant has been unable to satisfy the examiner that the application meets the requirements of the Act. An initial hearing was offered on the 30th March 2022 primarily based on sections 14(3) and 14(5) of the Act regarding issues of sufficiency, clarity and support. However, the agent addressed these issues through amended claims filed on the 31st August 2022 and the hearing was postponed.

3 Following a further round of examination and amendments the examiner remained of the opinion that the application did not meet the requirements of the Act. In particular, he considered the claims to lack and inventive step and also relate to excluded subject matter as a method of doing business as such. A hearing was again offered based on these issues and took place on the 23rd November 2023. At the hearing the applicant was represented by Mr David Williams of Page, White and Farrer Limited. In advance of the hearing Mr Williams provided a skeleton argument for which I am grateful, and an amended set of claims.

The invention

4 In secure interactions, such as those in which entities utilise a trusted third party to complete a blockchain operation, some protocols used to facilitate the interaction are subject to hacking attacks by a malicious entity. One such attack is a denial of service ("DoS") attack in which the malicious entity overloads the trusted third party with a large number of requests for assistance with a secure transaction.

5 The invention relates to a method, device and system which aims to prevent DoS attacks. In particular, a trusted third party in the form of a certification authority ("CA") 120 receives a request to facilitate a blockchain operation between one device 110 and another device 105, sends a message back to the requesting device that includes a prompt for the requesting device to meet one or more conditions. The CA 120 completes the requested blockchain operation when the one or more conditions are met and denies the request if they are not met. Therefore, for example where the condition is a payment of a fee, requests of entities that have not paid the fee are ignored to prevent DoS attacks.



6 Furthermore, the first and second devices 110,105 are associated with entities that belong to or are members of the CA 120. Therefore, even if the device owners 110,105 are members of the trusted third party 120, a prompt is still sent to the devices requiring them to satisfy the condition(s). This ensures that a prompt is issued if a member device has been 'hijacked'.

7 The claims under consideration were filed on the 16th November 2022. Method claim 1 is reproduced below:

> A method comprising:
>
> receiving a request from a first device to initiate a blockchain operation on behalf of the first device and a second device wherein the request is received by a certificate authority (CA) different from the first and second devices, the CA being a trusted third-party that facilitates secure interactions for the first and second devices, the first and second devices being associated with entities that belong to or are members of the CA;
>
> generating, by the CA and in response to receiving the request, a prompt including at least one condition that is associated with the blockchain operation
>
> sending a first message that acknowledges the request to the first device, the first message including the prompt;
>
> receiving a second message from the first device, the second message including an indication of whether the at least one condition of the prompt in the first message has been satisfied;

determining if the at least one condition of the prompt has been satisfied or is authorised to be satisfied, and either:

denying the request upon determining that the at least one condition of the prompt has not been satisfied or is not authorised to be satisfied; or

approving the request upon determining that the at least one condition of the prompt has been satisfied or is authorised to be satisfied; and initiating the blockchain operation.

8 There are also independent claims to a device (claim 9) and system (claim 18). I am satisfied that these claims stand or fall with claim 1.

The Law

9 The examiner has raised an objection that the invention does not involve an inventive step. Section 1(1) states (with added emphasis): A patent may be granted only for an invention in respect of which the following conditions are satisfied, that is to say –

(a) the invention is new;

(b) it involves an inventive step;

(c) it is capable of industrial application;

(d) the grant of a patent for it is not excluded by subsections (2) and (3) or section 4A below;

10 Section 3 then sets out how the presence of an inventive step is determined. It says:

An invention shall be taken to involve an inventive step if it is not obvious to a person skilled in the art, having regard to any matter which forms part of the state of the art by virtue only of section 2(2) above (and disregarding section 2(3) above).

11 It is well-established that the approach to adopt when assessing whether an invention involves an inventive step is to work through the steps set out by the Court of Appeal in *Windsurfing*[1] and restated by that Court in *Pozzoli*[2]. These steps are:

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

(1) (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;

[1] *Windsurfing International Inc. v Tabur Marine (Great Britain) Ltd*, [1985] RPC 59
[2] *Pozzoli SPA v BDMO SA* [2007] EWCA Civ 588

(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?

12 The examiner has also raised an objection under section 1(2) of the Patents Act 1977 that the invention is not patentable because it relates a category of excluded matter. The relevant provisions of this section of the Act are shown with added emphasis below:

> *1(2) It is hereby declared that the following (amongst other things) are not inventions for the purpose of the Act, that is to say, anything which consists of...*
>
> *(c) …**a scheme, rule or method for…doing business**;*
>
> *but the foregoing provisions shall prevent anything from being treated as an invention for the purposes of the Act only to the extent that a patent or application for a patent relates to that thing as such.*

13 As explained in the notice published by the IPO on the 8th December 2008[3], the starting point for determining whether an invention falls within the exclusions of section 1(2) is the judgment of the Court of Appeal in *Aerotel/Macrossan*[4].

14 The interpretation of section 1(2) has been considered by the Court of Appeal in *Symbian*[5]. *Symbian* arose under the computer program exclusion, but as with its previous decision in *Aerotel* the Court gave general guidance on section 1(2). Although the Court approached the question of excluded matter primarily on the basis of whether there was a technical contribution, it nevertheless (at paragraph 59) considered its conclusion in the light of the *Aerotel* approach. The Court was quite clear (see paragraphs 8-15) that the structured four-step approach to the question in *Aerotel* was never intended to be a new departure in domestic law; that it remained bound by its previous decisions, particularly *Merrill Lynch*[6] which rested on whether the contribution was technical; and that any differences in the two approaches should affect neither the applicable principles nor the outcome in any particular case.

15 Subject to the clarification provided by *Symbian*, it is therefore appropriate to proceed on the basis of the four-step approach explained at paragraphs 40–48 of *Aerotel* namely:

(1) Properly construe the claim.

(2) Identify the actual contribution (although at the application stage this might have to be the alleged contribution).

(3) Ask whether it falls solely within the excluded matter.

(4) If the third step has not covered it, check whether the actual or alleged contribution is actually technical

---

[3] http://www.ipo.gov.uk/pro-types/pro-patent/p-law/p-pn/p-pn-computer.htm
[4] *Aerotel Ltd v Telco Holdings Ltd and Macrossan's Application* [2006] EWCA Civ 1371; [2007] RPC 7
[5] *Symbian Ltd v Comptroller-General of Patents*, [2009] RPC 1
[6] *Merrill Lynch's Appn*. [1989] RPC 561

Claim Construction

16 Before considering the issues of inventive step and excluded matter, I think it is prudent to construe the claim, that is to say I must interpret claim 1 in the light of the description and drawings as instructed by Section 125(1). In doing so I must interpret the claims in context through the eyes of the person skilled in the art. Ultimately the question is what the person skilled in the art would have understood the patentee to be using the language of the claims to mean. This approach has been confirmed in the decisions of the High Court in *Mylan v Yeda*[7] and the Court of Appeal in *Actavis v ICOS*[8].

17 In order to interpret the claims through the eyes of the skilled person, they must first be identified. The examiner has identified the person skilled in the art as a network security engineer, and Mr Williams did not disagree with this interpretation.

18 A passage in claim 1 that I believe requires construing is:

> "…the request is received by a certificate authority (CA) different from the first and second device, the CA being a trusted third-party that facilitates secure interactions for the first and second devices, the first and second devices being associated with entities that belong to or are members of the CA"

19 Firstly, how would the term "certificate authority (CA)" be interpreted by the person skilled in the art? The examiner has asserted that, as claim 1 does not provide any functions of a CA and does not require a CA, the term CA should be construed in broad terms as a "server".

20 Looking at the description, in particular at paragraphs 3-5, 7 and 50, it is discussed that that a certificate authority issues/generates certificates, after local verification, using a protocol - PKCS#12 (which involves using keys). However, paragraph 4 also discusses generating forms or documents in more general terms (by way of an analogy with a passport office).

21 I do not agree with the examiner that a certificate authority (CA) is simply a server or third party which provides the functionality of the method defined in claim 1. In particular, the term certificate authority has meaning and is more than just a server. I consider that the person skilled in the art would construe the term CA in light of the description as a server which verifies or authenticates an entity and consequently provides a certificate, document, signature or the like.

22 Claim 1 also defines that the first and second devices are "associated with entities that belong to or are members of the CA" and that the CA is a "trusted third party that facilitates secure interactions for the first and second devices". With regard to the entities associated with the devices which "belong to or are members of the CA", it was accepted by Mr Williams that the application does not discuss how a device or entity is a member of the CA. Mr Williams discussed that this feature in claim 1 conveys that the devices are known to the CA and thus, as a CA knows the devices making the request, they are effectively trusted devices. Mr Williams submitted that

---

[7] Generics UK Ltd (t/a Mylan) v Yeda Research and Development Co. Ltd & Anor [2017] EWHC 2629 (Pat)

[8] Actavis Group & Ors v ICOS Corp & Eli Lilly & Co. [2017] EWCA Civ 1671

the skilled person would construe claim 1 to mean that the devices are trusted by the CA and vice versa. In particular, he stated that:

> "The devices being associated with respective entities that belong to or are members of the certificate authority combined with the feature of the certificate authority (CA) being a trusted third party that facilitates secure interactions between the first and second devices conveys a meaning and a limitation that they are known and trusted devices to the certificate authority when it receives the request."
>
> "By having that limitation to the devices being associated or with entities which belong to the certificate authority or are members of the certificate authority, and the intention is to convey a limitation there that the devices are actually known to the certificate authorities…..The certificate authority knows the devices which are making their request, and therefore they are effectively trusted devices."

23 However, he accepted that there was no particular part of the application to form a basis for this reasoning – other than page 4 which corresponds to the wording of claim 1. It is my opinion that the term "trusted third party" would be construed by the person skilled in the art as a party trusted by the provider of the (blockchain) operation. For example, paragraph 16 of the description states that the blockchain may be "accessible/maintained by a trusted third-party or Certification Authority (CA)". Consequently, it follows that the entities associated with the devices that belong to or are members of the CA do not necessarily have to be trusted by the CA.

24 Furthermore, as there is no detail or further discussion in the application with regard to the first and second devices being "associated with entities that belong to or are members of the CA", I consider that the person skilled in the art would construe this to mean that the devices are associated with entities that are known to the CA.

Inventive Step

25 The examiner has objected that claim 1 (and corresponding claims 9 and18) does not involve an inventive step. He notes that, whilst there are differences between claim 1 and the prior art, these differences are obvious. I shall assess claim 1 based on the approach set out in Windsurfing as restated by the Court in *Pozzoli*.

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

26 As discussed above in paragraph 17, the person skilled in the art is considered to be a network security engineer.

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

27 The examiner has submitted that protecting networks against attacks such as DoS attacks by providing a user a prompt or challenge would form part of the common general knowledge ("CGK") of the skilled person. In doing so the examiner provided six example patent documents (US2016173526, US2018007085, US2012174196, EP2723035, US2007157300 and WO2004006115) to demonstrate this CGK. At the hearing Mr Williams accepted that the provision of prompt or challenge was part of the skilled person's CGK. I also think it reasonable to conclude that the person skilled in the art would be at least aware of blockchains and of operations performed by them.

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

28 In his skeleton argument, Mr Williams submitted that the inventive concept resides in:

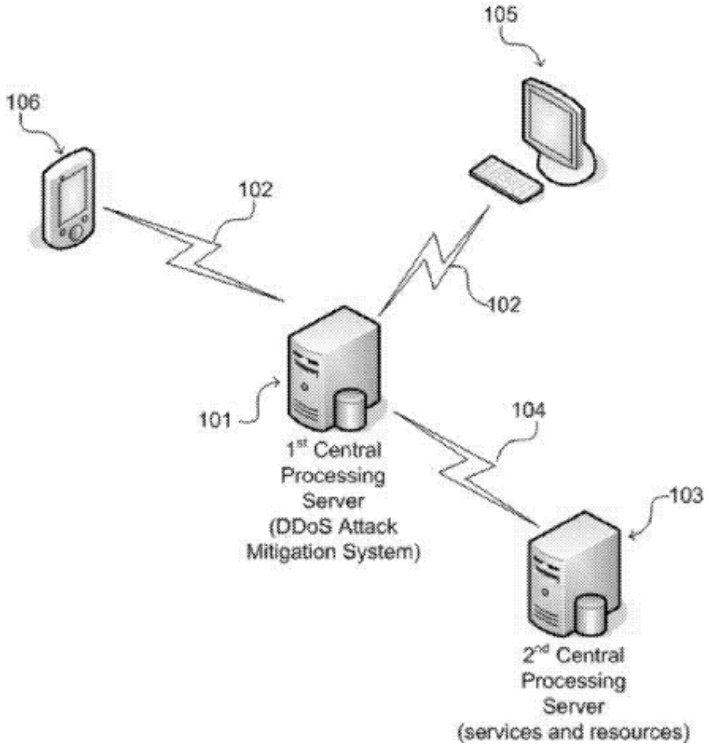
> "…the independent claims define a relationship between the first and second devices and the certificate authority, with the certificate authority being a trusted third-party that facilitates secure interactions for the first and second devices, and the first and second devices being associated with entities that belong to or are members of the certificate authority. According to claim 1, with this established relationship between the first and second devices and the certificate authority, a prompt is generated when a request is received."

29 I am happy to accept this assessment of the inventive concept, with the caveat that the secure interactions are a request to initiate a blockchain operation.

(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

30 The examiner has cited two documents: US 2016/0173526 (US'526) and US 2016/0173527 (US'527) which are said to each form the state of the art. I would note that the arguments submitted by the examiner and Mr Williams were based on an assessment of US'526, as US'527 does not appear to offer any additional disclosure beyond that disclosed in US'526 (US'527 incorporates US'526 by reference). Therefore, I will assess the state of the art based on US'526.

31 US'526 discloses a method for network attack mitigation on a network resource 103. The attack mitigation system 101 acts as an intermediary between the client users' devices 105 and 106, and the services and/or resources provided by the second central processing server 103 in their data communication paths. The system 101 intercepts requests for services and/or resources originated from a client user's device 105,106, and forwards the requests to the second central processing server 103 if deemed safe. As part of the process to determine if the requests are safe, the central processing server 101 responds to client's resource access requests with a challenge. The challenge is a prompt for user action. If the user action suffices the device is authenticated and the request is forwarded to the network resource. Figure 1 from US'526 is reproduced below.



32 The attack mitigation system 101 maintains a list of IP addresses of known and suspected attackers, and unauthenticated (or unverified) client users' devices (untrusted list). The system 101 also maintains a list of IP addresses of legitimate and authenticated (or verified) client users' devices (trusted list) – in particular the system 101 stores data records of the one or more lists of IP addresses of legitimate and authenticated (or verified) client users' devices.

33 Furthermore, the system 101 continuously records a data access frequency originated from every client users' device, the Internet Protocol (IP) address of every data-originating client users' device, and the particular services and/or resources being requested/accessed by every data-originating client users' device. The data access frequency is the number of individual data message received from a data-originating client users' device within a set period of time. For unauthenticated (or unverified) client users' devices, the system utilises a blocking threshold value of data access frequency above which a DDoS attack is considered detected, and a triggering threshold value of data access frequency above which a DDoS attack is considered suspected.

34 Based on the lists, the data access frequency and the thresholds a number of actions can be performed for a request by the system 101. At the hearing Mr Williams helpfully provided a table which summarises the processes performed by the system 101 and actions taken based on certain conditions (see also paragraphs 33-45 of US’526), which I have reproduced below. Mr Williams emphasised (see row highlighted in blue) that, according to the system 101 of US’526, when the IP address of the requesting device is on the trusted list no mitigation challenge is issued. He also noted that a challenge was only issued (see point highlighted in yellow) when the requesting device was not on the trusted list and the frequency of requests was greater than a threshold.

	Request Condition	Data Access Frequency Consideration	DDoS Attack Status	Mitigation Challenge Issued	Mitigation Challenge Result	Request Handled
1	IP address of requesting device on trusted list.	NA	No DDoS attack suspected or detected. **[Step 5)a)]**	No mitigation challenge issued	NA	Request always forwarded. **[Step 6)]**
2	IP address of requesting device not on trusted or untrusted list.	It is determined that data access frequency is within triggering threshold.	No DDoS attack suspected or detected. **[Step 5)b)]**	No mitigation challenge issued	NA	Request always forwarded. **[Step 6)]**
3	IP address of requesting device is not on trusted or untrusted list.	It is determined that data access frequency of requesting device exceeds the triggering threshold, but is less than the blocking threshold.	DDoS attack suspected. **[Step 5)c)]**	Mitigation challenge issued. **[Step 7)]**	Challenge successful	Request then forwarded
					Consecutively fails a number of times exceeding a retry limit. **[Step 5)d)]**	Request then denied.
4	IP address of requesting device is not on trusted list or untrusted list.	The data access frequency of requesting device exceeds the blocking threshold.	DDoS attack detected. **[Step 5)d)]**	NA	NA	Request then denied.
5	IP address of requesting device is on untrusted list.	NA	DDoS attack detected. **[Step 5)d)]**	NA	NA	Request always denied.

35 So what are the differences between the state of the art (US'526) and the inventive concept? Mr Williams and the examiner are in agreement that US'526 does not disclose the request being to initiate a blockchain operation. However, Mr Williams alleges that there are further differences. In particular, Mr Williams argues that the invention of claim 1 requires that a prompt be issued when the devices are members of the CA, and therefore inherently trusted, thus ensuring that a prompt is issued if a known and trusted device has been 'highjacked'. Mr Williams agreed that US'526 disclosed entities or devices being members of the CA – i.e. devices on the trusted list – see row 1 in Mr William's table. However, Mr Williams argued that these members were never issued a mitigation challenge.

36 However, on the basis of claim 1 as correctly construed, I consider that the features and conditions in US'526 discloses the further alleged differences submitted by Mr Williams. In particular, as US'526 discloses a third party system 101 which stores *data records* of IP addresses (i.e. provides a certificate, document, signature or the like) of *legitimate and authenticated* client users' devices. Therefore system 101 is a CA. Furthermore, as the system 101 forwards device requests to the second central processing server 103 *if it is deemed safe*, it is consequently a "trusted third party".

37 The system 101 also keeps a record(s) with regard to a particular device and the frequency of the requests from that device. As the server has a record of the device it is *known* to the system 101, and therefore belongs to or is a member of the system 101. Devices which are known to the system 101, as per the records, and which exceed a triggering threshold for the requests are issued with a prompt or challenge – as per row three of Mr Williams table. Therefore, US'526 discloses a prompt being issued by a CA to devices that belong to or are members of a CA. Whilst US'526 may or may not issue prompts to devices which are members – see e.g. rows two and three of Mr Williams table – *always* issuing prompts to devices which are members is not a limitation of claim 1.

38 Therefore, the only difference between US'526 and the inventive concept is the request being to initiate a blockchain transaction.

(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?

39 At the hearing Mr Williams agreed that the particular application of processing a blockchain operation request to a method of prompting or challenging a known user did not impose any additional constraints on the checking process.

40 When presented with US'526 the person skilled in the art would understand that US'526 discusses a general methodology for protecting any suitable resource from DDoS attacks. Consequently, applying or implementing this general methodology to a particular resource would be no more than a "workshop development" for the skilled person. Based on their CGK the person skilled in the art would know that providing prompts or challenges is ubiquitous and they would readily appreciate that blockchains are simply one of number of resources suitable for the method of US'526. In particular, the system of US'526 would require no adaptation to be used with blockchains – it is merely an application of the method of US'526 to a known resource which requires no degree of invention. Consequently, claim 1 does not involve an inventive step. Similarly claims 9 and 21 also do not contain an inventive step.

41 I note that the examiner also considered, following the reasoning in *SABAF*[9], claim 1 to relate to a collocation of known features which do not contain an inventive step. This was not discussed in any detail at the hearing and having already found that the independent claims are not inventive, I do not need to decide that point.

42 Whilst the focus at the hearing was on the independent claims, I have nevertheless also considered dependent claims 2-8,10-17,19 and 20 to try and identify anything that might provide the necessary inventive step. The dependent claims however relate to conventional features in the art of network security - such as the use of certificates, keys and/or payments - which do not appear to introduce any inventive step.

Excluded Matter

43 The examiner has raised an objection that the claims are excluded under section 1(2)(c) of the Act as a method of doing business as such.

Applying the Aerotel test

Step 1 – Properly construe the claim

44 This has been done above in paragraphs 16-24. I would also note that the focus of the application is where the condition is a nominal payment. It is clear that the prompt being for a payment falls within the scope of the claims, and Mr Williams accepted as much at the hearing.

Step 2 – Identify the actual or alleged contribution

[9] SABAF v MFI [2004] UKHL 45

45 Jacob LJ addressed this step in *Aerotel/Macrossan* where he noted:

> *"43. The second step — identify the contribution — is said to be more problematical. How do you assess the contribution? Mr Birss submits the test is workable — it is an exercise in judgment probably involving the problem said to be solved, how the invention works, what its advantages are. What has the inventor really added to human knowledge perhaps best sums up the exercise."*

46 Jacob LJ also added in paragraph 44:

> *" Mr Birss added the words "or alleged contribution" in his formulation of the second step. That will do at the application stage – where the Office must generally perforce accept what the inventor says is his contribution"*

47 At the hearing and in the skeleton arguments, Mr Williams assessed the contribution on the basis of US'526 and concluded that the contribution resides in:

> "A trusted relationship between the device making the request and the CA which generates the prompt….The limitation in claim one is now of the prompt being generated when there is a relationship between the device which is generating the request (and the CA)."
>
> "The features of the independent claims which are not disclosed in the prior art result in a system which uses less resources and performs better than the prior art, being that it (at least) allows a "denial of service" attack to be identified by issuing a prompt, even when a request has been received from a trusted device."

48 I will proceed on the basis of Mr Williams assessment of the contribution.

Steps 3 and 4 - Ask whether it falls solely within the excluded matter and check whether the actual or alleged contribution is actually technical

49 I will consider steps 3 and 4 together.

50 Mr Williams submitted that the contribution did not lie solely in the membership or relationship between the device and the CA, but also in the technical process that occurs, i.e. the generation of a prompt, according to whether or not that relationship exists. In particular, he emphasised that, for a member or device trusted to the CA, a prompt is generated following a request – compared to the prior art where requests from trusted devices are always forwarded and no challenge is issued. This is also said to provide a technical benefit as it ensures a prompt is issued even when the devices are known to each other, and this will ensure that a prompt is issued if a known and trusted device has been "highjacked". Therefore, this will prevent system resources being consumed even when a trusted device sends a request, if that trusted device fails to respond correctly to a prompt.

51 It is my opinion that the contribution lies in the administrative decision to challenge or prompt user devices which are members or belong to the CA. Whilst such an administrative decision may result in less resources being used in the particular scenario of processing requests from a 'highjacked' member device, this is no more than a better business method. I would add that the invention does not 'detect' any 'high jacking' of devices, rather the invention lies in a policy decision to challenge member devices with a prompt – in case they have been 'highjacked'. Furthermore, the invention does not necessarily prevent DoS attacks through prompting (known) devices with a condition, such as requiring payment, rather it mitigates or deters

such attacks. The invention at best circumvents any problems with DoS attacks by providing the administrative solution of requiring a known device to satisfy a condition. Therefore, I do not see how providing a challenge to devices which are members of the CA provides a technical contribution. The contribution relates solely to a business method.

52 Claim 1 is therefore excluded as a business method as such. Similar reasoning can be applied to independent claims 9 and18. Nor do the dependent claims appear to escape the business method exclusion – in particular using conventional payments, certificates and/or keys in the administrative method does not provide a technical contribution

Conclusion

53 Having carefully considered the arguments, I am of the view that the invention as defined in claims 1-20 is not inventive in light of US 2016/0173526 (and US 2016/0173527). Furthermore, the invention relates to matter excluded under section 1(2) of the Act as a method of doing business as such. I therefore refuse this application under section 18(3).

Appeal

54 Any appeal must be lodged within 28 days after the date of this decision.

PHIL THORPE

Divisional Director, acting for the Comptroller