Intellectual Property Office

BL O/554/20

09 November 2020

PATENTS ACT 1977

APPLICANT	Barclays Execution Services Limited
ISSUE	The Patents Act 1977: whether patent application GB1510315.3 complies with section 1(2) of the Act
HEARING OFFICER	Dr L Cullen

DECISION

Introduction

1 This decision concerns patent application GB1510315.3 entitled "*Generation, configuration and authentication of a temporary code"* and whether the invention as claimed in this application relates to excluded matter as defined in Section 1(2) of the Patents Act 1977 (hereafter the Act).

2 The application was filed 12 June 2015, with no earlier priority date and was published as GB2539266 A on 14 December 2016.

3 The matter came before me at an oral hearing (by video link) on 5 December 2019. Present at the hearing were the agent representing the applicant, Simon Kahn and his assistant on the case, Rhodri Kendrick, from Boult Wade Tennant LLP. In addition, Eleanor Wade as assistant to the hearing officer and an observer for training purposes were also present.

4 In advance of the hearing, on 28 November 2019, the agent provided a written skeleton argument, which was very helpful. In addition, they enclosed a possible amendment to the claims for discussion at the hearing.

5 I note that in March 2020, the agent responsible for dealing with this application on behalf of the applicant has changed.

The Invention

6 The invention finds utility in the authorisation of transactions, payments or secure log ins, for example, to a virtual private network (VPN). A user device, which may be a payment card or authentication device, produces a code. The code is transmitted

across a network and authenticated by a device at the authentication end producing the same code. The codes are generated in response to a signal produced at regular intervals by a periodic oscillator, also referred to as a clock, which generates a signal at predetermined frequency. A clock provided at the authorisation device is synchronised to change the code at the same frequency as the clock provided in the user device so that when a code is generated from the clock at the authorisation device it will match the code generated at the user device at the same time. Authorisations under such systems rely on being able to match both of these codes. However, a discrepancy in the frequency between a pair of initially synchronised clocks will accumulate over time so that the clocks gradually drift, i.e., go out of synchronisation. This clock drift means that the user device and the authorisation device are no longer generating the same code at the same time. Lower quality clocks may drift more quickly.

7 The time interval it takes to transmit the code between the remote user device and the authentication device will be dependent on conditions in the network – at periods of high traffic or poor connectivity this will be slower than at other times when this is not the case. If transmission of the code from the user device across the network is too slow then the clock at the authorisation device may have stepped-on to generate a new code before the code from the user device is received. In both cases, setting the clocks to change code at a lower frequency will reduce the effect. So, reliably matching codes through this synchronisation depends on the quality of clocks used, the frequency that the clocks have been set to and the speed of transmission of the code across network.

8 Clock drift is an unavoidable reality inherent in even high-quality clocks and network propagation is not directly controllable, so synchronisation is an inevitable problem. Where the authentication code changes at intervals there is a trade-off in that frequent change reduces the risk of fraud but increases the likelihood of authentication failure due to the synchronisation problem.

9 The invention combines two values to set the period or frequency with which the user device changes the temporary code, the first value is set by the periodic oscillator associated with the user device and the second value is an adjustment value received by the user device via the network from a remote network terminal, for example, from a point-of-sale terminal. The adjustment factor is variable and its transmission to, and use by, the user device results in the code being generated more or less frequently.

Application History

10 The application was subject to a combined search and examination report dated 08 December 2015, with objections raised against plurality and excluded subject matter. Following a request and necessary fee from the applicant, a further search was conducted on 17 June 2016. Through subsequent rounds of amendment, most recently 11 February 2019, the plurality objection has been overcome but the examiner has maintained the excluded matter objection. No objection to lack of novelty or inventive step has been raised and excluded matter is the only issue outstanding.

11 The applicant filed written arguments ahead of the hearing, including a proposal for amending claim 1. As this latter proposal for amendment has not been filed formally my decision below is based on the latest set of amended claims currently on file, dated 11 February 2019.

The Claims

12 There is one independent claim, claim 1, which reads as follows:

> *A method for an electronic payment device comprising a periodic oscillator to generate a temporary code and for an authorisation system, comprising an internal clock to authenticate the temporary code generated by the electronic payment device, wherein the electronic payment device is configured to interface with a payment network terminal;*
>
> *wherein generating the temporary code comprises:*
>
> *obtaining a first value that changes periodically with a first period at least in part from an output of the periodic oscillator;*
>
> *receiving, via the payment network terminal, an adjustment indicator for setting a second period;*
>
> *generating, using at least the adjustment indicator and the first value, a second value that changes periodically with the second period, wherein the second period is greater than or equal to the first period, and wherein the first value continues to change periodically with the first period; and*
>
> *generating the temporary code based at least in part on the second value;*
>
> *and*
>
> *wherein authenticating the temporary code comprises;*
>
> *generating an authentication code in an analogous manner to the temporary code, by the authorisation system; and*
>
> *performing an authentication process on the temporary code using the authentication code, thereby reducing the effect of: a time drift between the electronic payment device oscillator and the authorisation system clock; and/or an amount of time difference between generation of the temporary code and generation of the authentication code.*

The Issues to be decided

13 The issue to be decided is whether the invention as claimed relates to matter excluded under Section 1(2) of the Act.

14 If I find that the amended claims, dated 11 February 2019, do not comply with the requirements of the Act, I will then go on to consider whether the proposal included with the written arguments filed before the hearing might provide a fruitful way forward.

15 If I find that the application does not relate to matter excluded under Section 1(2), I will remit the case to the examiner for completion of the examination process. In this regard, I note that there are no further outstanding objections and no substantive matters have been deferred.

Excluded Matter – Section 1(2)

The Law

16 Section 1(2) of the Act sets out certain categories of invention that are not patentable as follows (my emphasis added):

> *"It is hereby declared that **the following** (among other things) **are not inventions for the purposes of this Act**, that is to say, anything which consists of –*
>
> *(a) …..;*
>
> *(b) …..;*
>
> *(c) **a** scheme, rule or **method for** performing a mental act, playing a game or **doing business**, **or a program for a computer**;*
>
> *(d) the presentation of information;*
>
> *but the foregoing provision shall prevent anything from being treated as an invention for the purposes of this Act only to the extent that a patent or application for a patent relates to that thing as such."*

17 Current IPO examination practice is to use the structured approach set out by the Court of Appeal in its judgment in *Aerotel/Macrossan [2006] EWCA 1371* (hereafter *Aerotel*) for deciding whether an invention is patentable. The test comprises four steps as follows:

(1) Properly construe the claim;
(2) Identify the actual contribution;
(3) Ask whether it falls solely within the excluded matter;
(4) Check whether the contribution is actually technical in nature.

Operation of this test is explained in paragraphs 40-48 of the *Aerotel* judgment. Paragraph 43 confirms that identification of the contribution is essentially a matter of determining what it is that the inventor has really added to human knowledge and involves looking at the substance of the invention claimed, rather than the form of the claim. Paragraph 46 explains that the fourth step of checking whether the contribution is technical may not be necessary because the third step – asking whether the contribution is solely of excluded matter - should have covered that point already.

18 More recently, the Court of Appeal in the case of *Symbian [2009] RPC 1* (hereafter *Symbian*) confirmed that this structured approach is one means of answering the question whether or not the invention reveals a technical contribution to the state of the art. In other words, *Symbian* confirmed that the four-step test is equivalent to the prior case law test of '*technical contribution'*, as discussed in *Merrill Lynch*[1], *Gale*[2] and *Fujitsu*[3]. The key question is what does the '*technical contribution*' amount to, not whether it happens to be implemented by a computer.

Program for a computer

19 Lewison J (as he then was) in *AT&T/CVON Innovations* [2009] EWHC 343 (hereafter *AT&T*) set out five factors or signposts that he considered to be helpful when considering whether a computer program makes a technical contribution. These signposts were modified slightly in *HTC Europe Co Ltd V Apple Inc* [2012] EWHC 1789. The five signposts are:

(i) Whether the claimed technical effect has a technical effect on a process which is carried on outside of the computer.

(ii) Whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run.

(iii) Whether the claimed technical effect results in the computer being made to operate in a new way.

(iv) Whether the program makes the computer a better computer in the sense of running more efficiently and effectively as a computer.

(v) Whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

Method for doing business

20 The Court of Appeal in *Aerotel* made clear that this exclusion is to be interpreted as encompassing tools or steps having administrative or financial character, noting (at para 68) that "*whether as an abstract or generalised activity or as a very specific activity, if it is a method of doing business as such it is excluded*".

The business method exclusion is generic, as discussed in *Merrill Lynch*[1], and providing a better way of conducting business, as confirmed in *Halliburton*[4], will not confer patentability.

---

[1] Merrill Lynch's application [1989] RPC 561.
[2] Gale's application [1991] RPC 305.
[3] Fujitsu Limited's application [1997] RPC 608.
[4] Halliburton Energy Services Inc's Applications [2012] RPC 129

Analysis

21 As noted above, I will follow the four-step test outlined in the Court of Appeal judgement in *Aerotel* when considering if this application relates to matter excluded under section 1(2) of the Act.

Step (1): Properly construe the claim;

22 The steps of the method set down in independent claim 1 are clear except in relation to following points:

a) This adjustment indicator is received from a source external to the electronic device that generates the temporary code and to the authorisation system that authenticates the temporary code. This adjustment indicator is combined with the first value to set a second value that changes when a second period of time elapses ("the second period"). This second value can be zero so that the adjustment indicator, at its lowest value, is equal to the first value. Thus, the temporary code will always correspond at least to the first value that changes with the first period. The first value and the second value in combination are used to set the period of time that elapses between code changes. The change in the second value – the adjustment indicator – can be upwards and downwards.

b) authenticating the temporary code is defined as comprising "*generating an authentication code in an analogous manner to the temporary code by the authorisation system*". It is implicit in my view that the authentication system uses its internal clock to generate a first periodically changing value in a manner analogous to the periodic oscillator associated with the payment device and uses the same adjustment indicator as the payment device to produce an authentication code with the same adjusted periodicity.

c) the final part of the claim includes the expression "*and/or*" when referring to the fact that the invention reduces the effect of (i) time drift between the electronic payment device oscillator and the authorisation system clock; or (ii) the time difference between generation of the temporary code and generation of the authentication code, i.e. the network latency effect, or (iii) a combination of (i) and (ii) together. While I accept that the effect of each may alter in the course of the operation of the system, both clock drift and network latency have to be accounted for to some degree all the time. I consider that it is the combination of (i) and (ii) that is covered by the claim not just (i) or (ii) alone.

Step (2): Identify the actual contribution.

23 There has been a lot of discussion between the agent and the examiner regarding the nature of the contribution of this invention. In their letter of 11 February 2019, the applicant has characterised the technical contribution encapsulated by the claims currently on file as follows:

> *"[A] method of generating, on an electronic payment device, a temporary code that changes periodically with a period that may be adjusted using an adjustment indicator communicated to the electronic payment device via a payment network terminal; and performing an analogous process at an*

authentication system that uses the same adjustment indicator to generate an authentication code and authenticate the temporary code. The effects of drift between the electronic payment device oscillator and/or the authorisation system clock or a delay between generation and authentication of a temporary code are reduced by these technical means. Moreover, the period of the temporary code may be adjusted depending on the particular requirements of a given transaction or entity using the electronic payment device, or if it is known that network congestion may lead to a significant delay between temporary code generation and authentication for any individual transaction. Hence, the claimed methods provide secure and reliable generation and authentication of temporary codes, leading to a more secure and efficient payment network."

24 The examiner was mostly in agreement with this assessment of the contribution but noted that the provision of a more reliable method of authentication is achieved by balancing against the level of security as set out on page 2 of the application as filed. As a result, he considered that the contribution is not to provide '*a more secure and efficient payment network'* but rather to provide a more reliable authentication method for a payment network, i.e. a method wherein fewer payments are declined. By increasing the adjustment factor, fewer transactions fail authentication but this is reducing security because the frequency with which the code changes has been reduced. In support of this view, the examiner, referring again to the disclosure on page 2 of the description, notes that there is clear acknowledgement that time intervals may be set, either higher or lower, during manufacture of the clock. As a consequence, any variation from the shortest time interval – that where the temporary code corresponds to the first value and the adjustment indicator is zero - can only provide decreased security. Thus, he was of the view that the contribution in this instance does not include enhanced security.

25 In correspondence and at the hearing, the attorney argued that the contribution identified by the examiner only represents part of the invention. He submits that the invention lies in the fact that the temporary code increases and decreases as the adjustment factor is increased or decreased based on the information it is receiving from the payment network terminal. This is a dynamic trade-off; it is not simply increased reliability at the expense of security. The invention is providing a dynamically adjustable balance between authentication reliability and security through the use of the adjustment indicator to set the periodicity of the temporary and the authentication code. The agent also argued that the examiner's assessment of the contribution fails to recognise the temporary code as 'technical data' and so failed to recognise that the communication of this data to a device to modify the generation of such technical data provides a technical contribution.

26 Addressing the examiner's assertion that any variation from the shortest possible time interval can only provide decreased security, the attorney submits that this is not the correct comparison; he says the correct comparison is with the prior art where the periodicity has had to be fixed at a level that consistently provides sufficient reliability.

27 The prior art identified by the examiner in his report dated 8 December 2015, and which was also referred to by the agent at the hearing, shows that dynamic code generation for a payment card is known, where the period at which the code generates changes and where the code is generated at least in part from a count of said period:

US-2013/0297503A1 (McGowan) discloses payment cards that have verification codes that change at defined intervals, the frequency of change can be selected when the card is manufactured. However, the frequency of change cannot be adjusted in use, it is fixed and is not variable. Similarly, US-2008/0035738A1 (Mullen) describes a payment card wherein the frequency of change of a dynamic number can be changed "*if the dynamic credit card detects tampering*". Any adjustment is performed internally on the card and is carried out in order to prevent validation by causing the number generated by the card to become out of synch with those generated at an authorisation facility. Such an adjustment can be carried out after manufacture of the card as necessary.

28 Neither document suggests the reconfiguring of the frequency – both up and down -at which a temporary code changes by communicating data to a payment card via a communications interface as provided by the adjustment indicator of this invention.

29 The temporary code of the invention comprises two elements – the first element is the value generated by the device reflecting the state of the oscillator in the device and the second element – which is the adjustment indicator – is set depending on data received from a device external to the payment device, i.e. from the payment network terminal. In my view, it is this second element which allows an adjustment to take place to account for clock drift between the user device and the authentication device and for any delays arising from network latency when communicating the request for payment and the associated request for the authentication code to confirm a transaction.

30 The view of the examiner was that the adjustment indicator is still a time interval and that changing the time interval to higher values reduces security even though it increases approval. The shorter the time interval between changes in code on the user device and the authentication device, the more secure the transaction, the longer this interval becomes, the less secure it is and the greater the chance that the process can be interfered with and compromised. The examiner considers that the dynamic change which the attorney for the applicant considers the key feature of the invention leads to a reduction in security when the temporary code including the adjustment factor is increased and that this security is only restored when the temporary code including the adjustment factor is decreasing. The agent considers that both aspects are part of the contribution because this reflects the dynamic nature of the change in the adjustment factor to take account of the prevailing conditions in the payment network and ensure that transactions continue to be approved.

31 At the hearing, the attorney for the applicant argued that contrary to the above view expressed by the examiner, the invention as claimed does not state or otherwise imply that the adjustment indicator is ever set so as to cause a payment system to be less secure than any conventional system. He pointed out that the invention could be implemented with a threshold value of the adjustment indicator that corresponds to the frequency of a conventional periodic payment device. He set it out thus in his skeleton argument:

> "For instance, the temporary code could be set to vary with a higher frequency (and hence a higher level of security) than a conventional system when it is known that there is low network latency, and then to vary at the same frequency as a conventional system when there is known to be high

> latency or if clock drift has occurred. This would provide the claimed feature of "*reducing the effect of […] an amount of time difference between generation of the temporary code and generation of the authentication code*" in a way that did not make the payment system any less secure than any known device."

He further argued that the invention as implemented would be more secure than a conventional device due to its ability to increase security when the network is not congested, and no less secure than a conventional device when the security is relaxed to conventional levels when the network is congested or clock drift has occurred. In other words, the current claims encompass an implementation that would be at least as secure as a conventional device in a worst-case scenario, and more secure in all other cases.

32 I consider that that the examiner is correct in so far as use of the adjustment factor will lead to an increase in time between changes in code, this will increase reliability but reduce security – in the manner that the examiner has referred. Thus, I consider that the invention is as secure as a known system when the adjustment factor is zero (i.e. when the second period is equal to the first period") and, as the adjustment indicator, increases it is in effect less secure but more reliable, i.e. it will approve more transactions. However, as the attorney indicates, the adjustment indicator can also reduce when the network congestion is reduced, this will increase security but maintain reliability because, for example, the network latency will not have as strong an impact. Thus, I consider that there is a balance being achieved between reliability and security that has the overall impact of providing a more reliable authentication method for a payment network. While, it allows for ongoing adjustment of the balance between reliability and security because the adjustment factor can be increased or decreased depending on conditions, I do consider that improving the reliability comes in effect by reducing the security because it is achieved by using the adjustment indicator to increase the period between code changes.

33 I consider the contribution to be:

> A method of generating, on an electronic payment device, a temporary code that changes periodically with a period that is adjusted using an adjustment indicator communicated to the electronic payment device via a payment network terminal; and performing an analogous process at an authentication system that uses the same adjustment indicator to generate an authentication code and authenticate the temporary code, wherein the change in the adjustment indicator is determined by the impact of clock drift and network congestion. This provides a more reliable authentication method for a payment network, i.e. a method wherein fewer payments are declined. By increasing and decreasing the adjustment factor to take account of the impact of clock drift and network congestion, fewer transactions fail authentication.

Step (3): Ask whether the contribution falls solely within the excluded matter;

Program for a Computer

34 I am satisfied that the contribution, as I have identified it, requires a computer programme for its implementation. However, just because it is given effect in software, this is not sufficient for the invention to be considered excluded, what is key is whether the programme provides a contribution that is technical. As noted above, in answering whether a contribution is technical, the five signposts identified in *AT&T* can be helpful.

35 The attorney suggested in correspondence that the first and third signposts, and at the hearing, that the fifth signpost are helpful in determining that the contribution made by the invention as claimed is a technical one. The examiner maintained in his pre-hearing report that none of the signposts are helpful in identifying that the contribution, as he has assessed it, is a technical one.

36 I will consider the signposts based on my assessment of the contribution set out above.

37 The first signpost asks whether the claimed technical effect has a technical effect on a process which is carried on outside of the computer. The attorney proposes that there is a technical effect in making the authentication process at an authentication server, external to an electronic device, more secure and reliable by the process of generating a temporary code performed by the electronic device. In this instance, the computer can be considered to be the server that performs the authentication, and which is networked to the payment terminal. Such a computer does not have a link to or exert an effect on anything outside the computer arrangement on which the authentication is being run. Thus, I do not find this signpost helpful.

38 The second signpost asks whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run. The claimed method relates to data derived from periodic oscillator and not from the computer as a whole. The contribution identified does not relate to the architecture of the computer but rather to the data generated by clock (periodic oscillator). The data being generated by the computer does not alter the architecture of the computer or of the oscillator. Thus, I can find no assistance from the second signpost.

39 The third signpost asks whether the claimed technical effect results in the computer being made to operate in a new way. The invention results in a device producing an initial code which is then modified by communication of the adjustment indicator resulting in the frequency of change of the temporary code used for authentication being controlled so that the balance between reliability and security can be changed during use. Payment devices do not conventionally communicate in the claimed way. While I accept that the contribution identified relates to a new method for operating an electronic payment device, it does not relate to a new way to operate the computer itself. Communication of data is a common property of servers and computers and this invention does not describe a new means for doing so. Thus, I can find no assistance form the third signpost

40 The fourth signpost asks whether the program makes the computer a better computer in the sense of running more efficiently and effectively as a computer. While, it is

accepted that the contribution provides a more reliable authentication method for a payment network, this does not extend to the computer carrying out this method. Being able to authenticate a greater number of transactions or reduce the number of such transactions that fail, does not change the computer itself. It still has to authenticate the same number of transactions and it still has to carry out the same steps to do so. The outcome is that fewer transactions fail but there is no change in how efficient the computer is. Thus, I can find no assistance from this signpost.

41 The fifth signpost asks whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented. The attorney's submission is that the linked problems of authentication reliability, due to clock drift and network latency, and transaction security are inherent to authentication processes. These constrain authentication systems in balancing reliability and security. The invention does not circumvent the problem but addresses it directly by allowing the balance to be adjusted within those constraints in accordance with conditions. It does not simply work around the problem by, for example, using a different channel to remove the problem of latency.

42 The examiner considered that the problem identified in the application with clock draft and network latency have not been solved, they have been accepted and are accounted for by calculating an adjustment factor, i.e. using data derived for data processing. Thus, the problem identified is not overcome, it is circumvented.

43 I find that I am in agreement with the examiner on this point. In my view, the issues being addressed by the invention as claimed – clock drift and network latency – are not changed or eliminated by the invention, instead they are being accepted and used by the computer to calculate the adjustment indicator – which is in effect a time factor – to ensure that the process for authentication will continue to work because the clock drift and network congestion cannot be eliminated.

Method for doing business

44 The examiner has also objected that the contribution falls within the business method exclusion because it comprises a business policy to allow more payments to be approved at the expense of security.

45 I have identified the contribution above. In my view, the invention as claimed relates to a business policy to allow more payments by increasing the interval between code changes using the adjustment indictor and that as a result this will reduce the security of the process. I accept that if the adjustment factor increases, the code changes less frequently, but when the adjustment factor decreases, the code will change more frequently. These changes are not fixed or stationary and only in one direction, the change depends on the information from the payment network terminal which reflects the nature of the transaction and takes account of the conditions in the network. Thus, the contribution results in more payments being approved because the method takes better account of the factors which result in failed authentication such as time to transmit data in network, condition of periodic oscillators and associated drift, and nature of transaction being authenticated. This results in the more transactions being approved, i.e. more payments being made.

Step (4) Check whether the contribution is actually technical in nature

46 Given my answer under Step 3 above, I do not need to go on and consider this fourth step of the Aerotel test.

Other matters

47 A point made by the agent at the hearing is that the invention does not have to be carried out using a computer, it can also be implemented using digital logic. In support of this he directed me to the embodiment set out on page 16, lines 4 to 13 of the application as filed. While I accept this point, as far as it goes, this does not change the question that needs to be answered, does the invention provide a contribution that is technical. As I have discussed above, the invention relates to a method for doing business and so does not deliver a technical contribution. Also, I note that the agent acknowledged that the invention was most likely to be implemented using a computer.

Possible Amendment

48 As part of the materials submitted by the agent in advance of the hearing, there was a proposal to amend claim 1 as follows (*changes highlighted in **red** below*):

> *A method for an electronic payment device comprising a periodic oscillator to generate a temporary code and for an authorisation system, comprising an internal clock to authenticate the temporary code generated by the electronic payment device, wherein the electronic payment device is configured to interface with a payment network terminal;*
>
> *wherein generating the temporary code comprises:*
>
> *obtaining a first value that changes periodically with a first period at least in part from an output of the periodic oscillator;*
>
> *receiving, via the payment network terminal, an adjustment indicator for setting a second period;*
>
> *generating, using at least the adjustment indicator and the first value, a second value that changes periodically with the second period, wherein the second period is greater than or equal to the first period, and wherein the first value continues to change periodically with the first period; and*
>
> *generating the temporary code based at least in part of the second value* **wherein the adjustment indicator causes the electronic device to be reconfigured such that the temporary code changes more frequently*;***
>
> *and*
>
> *wherein authenticating the temporary code comprises;*

generating an authentication code in an analogous manner to the temporary code, by the authorisation system; and

performing an authentication process on the temporary code using the authentication code~~, thereby reducing the effect of: a time drift between the electronic payment device oscillator and the authorisation system clock; and/or an amount of time difference between generation of the temporary code and generation of the authentication code.~~

49 These claims have not been filed formally, hence my analysis above and conclusion below relates to set of claims on file (dated 11 February 2019). However, in this instance I do think that it is helpful for me to give an initial view. Given my analysis above in relation to the contribution and the interplay between reliability and security discussed above, the proposed amendment would appear to relate only to part of the situation, i.e. where the adjustment indicator results in a decrease in the second value so that the temporary code changes more frequently. This would appear to suggest that the temporary code would only be able to increase in frequency. Albeit on this initial assessment, such an amendment would not appear to be a fruitful direction to pursue in that it does not appear to allow for situation where the network latency is significant so that there is a delay in transmitting the authentication code for approval of the payment. Such a situation would appear to be addressed in the application as filed by reducing the frequency of the change of temporary code.

Period for putting the application in order (the compliance period) and impact of period of interruption

50 The period for putting this application in order under Section 20 of the Act, the compliance period, has been extended, firstly, as of right under rule 108(2) of the Patents Rules 2007 (as amended, hereafter 'The Rules') until 12 February 2020 and, secondly, through exercise of discretion under rule 108(3) of the Rules until 12 April 2020.

51 However, as a consequence of the COVID-19 coronavirus pandemic, the Comptroller declared 24 March 2020 and subsequent days up to and including 29 July 2020 to be "interrupted days" under Rule 110 of the Rules. This means that the end of the compliance period is not in fact 12 April 2020 but that it is 30 July 2020, the first day after the end of this period of interruption.

52 A further request for extension of the compliance period under rule 108(3) was received on 12 June 2020. This request for a discretionary extension was agreed but it took effect from the first day after the end of the period of interruption (i.e., 30 July 2020), and thus the period for putting this application in order was extended to 30 September 2020.

53 A further request to extend the compliance date under rule 108(3) was received on 12 October 2020. I have considered this request for a discretionary extension and find that it is acceptable. Thus, the compliance period for putting this application in order will expire on 30 November 2020.

Conclusion

54 I find that the invention, as claimed in claim 1, is excluded under Section 1(2) of the Act as relating to a program for a computer.

55 I find also that the invention, as claimed in claim 1, is excluded under Section 1(2) of Act as relating to a method of doing business.

56 As a result, I refuse this application for failure to meet the requirement under Section 18(3) of the Act.

Appeal

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

Dr L Cullen
Deputy Director, acting for the Comptroller