Intellectual Property Office

BL O/566/14

23 December 2014

PATENTS ACT 1977

APPLICANT Recipero Ltd

ISSUE Whether patent application number GB1312146.2 complies with section 1(2)

HEARING OFFICER Mr Peter Slater

DECISION

1 Patent application GB1312146.2 entitled "System for generating a security document" was filed on the 5th July 2013 by Recipero Ltd.

2 Following several rounds of examination and amendment, the examiner remained of the view that the claimed invention was excluded from patentability under section 1(2). With the situation unresolved the applicant asked to be heard and the matter came before me at a hearing on the 21st October 2014. The applicant was represented by Mr Freddie Noble and Mr Marc Maidment of Albright Patents LLP. The examiner Sally Vinall was also present.

3 The examiner also raised objections in relation to clarity, consistency and support. However, these matters have been deferred pending the outcome of the hearing.

The Invention

4 The invention relates to a system for generating electronic security documents on a computing system, where the security documents can be used by third parties to certify that certain articles of value, such as a mobile phone, have not been the subject of an insurance claim, reported stolen, or blocked by mobile phone networks etc. Such security documents or certificates issued by a trusted authority can increase the resale value of articles such as mobile phones. These certificates can be tied to a particular article by using the device serial number as a certificate or security document identifier and authentication can be provided by an online database that can allow the retrieval of the original certificate and thus verify the authenticity of the issued certificate. Fraudulent traders can however exploit such verification systems by changing the serial number of a stolen article to match the serial number shown in a genuine certificate or by obtaining certificates that have serial numbers that differ only slightly to the serial number of the stolen article.

5 Known large scale systems for generating and storing security documents that can handle large volumes of authentication requests typically comprise a plurality of

computing nodes working in parallel. For document retrieval it is possible to generate a central index of document identifiers which can be queried, and which points to the storage location of a particular individual document. This however, adds to the complexity of the system and is therefore more vulnerable to failure.

6 In systems without a central index there is a risk that different computers in the same cluster will generate document identifiers that are the same. This situation is known as a collision, which can be avoided by checking documents between clusters. However, such checking creates additional network and database load, thereby reducing performance, and also imposes a practical limit on the scalability of the cluster. Such systems are also vulnerable to race conditions where two nodes check for collisions at the same time, determine that there is no collision, and then store two documents with identical identifiers.

7 The invention provides a computing system comprising a cluster of computing nodes for generating document identification codes derived using a process node identifier, a process identifier, a subject identifier such as a device serial number that uniquely identifies a device, random numbers, and a cryptographic hash function. The cryptographic hash function is applied to a concatenation of random number values and the subject identifier to provide a message digest value. The message digest value is truncated and concatenated with a node identifier, a process identifier, a random value and delimiters to generate a document identifier.

8 With this system inter node collisions and race conditions are not possible within the cluster because a part of the document identification code comprises a unique node identifier. Advantageously, therefore it is only necessary to check for document identifier collisions on individual nodes rather than on all of the computing nodes. Due to the use of random values to generate the document identifier the chances of collisions occurring within a node are very low and are easy to detect and correct if they do occur. Therefore, the network and computing resources necessary are reduced compared with previously known systems for generating security documents. The reduction in inter-node communications increases the scalability of the computer system. Also, the use of the cryptographic hash function and random values makes it difficult to guess valid document identifiers using a known device serial number, thereby limiting the opportunities for fraud.

9 The most recent set of claims was filed on the 13 June 2014. Whilst there are eight claims in total, Mr Noble in his submissions chose to focus primarily upon claims 1-3 which read as follows:

> *1. A system for generating a security document,the system including a plurality of computing nodes forming a computing cluster, each computing node having a node identifier for uniquely identifying the node within the cluster, each node being capable of running multiple concurrent processes, and each process having a process identifier for uniquely identifying the process within the node, at least some of the processes on at least some of the nodes being adapted to perform the steps of:*
>
> *a. collecting information for inclusion in the document, the information including at least a subject identifier for uniquely identifying a subject of the document;*
>
> *b. generating a first random value and a second random value;*

c. concatenating the subject identifier and the second random value;

d. applying a cryptographic hash function to the concatenation of the subject identifier and the second random value, resulting in a message digest value;

e. truncating the message digest value;

f. generating a document identifier comprising a concatenation of the node identifier, first delimiter, the process identifier, the first delimiter, the first random value, a second delimiter, and the truncated message digest value;

g. generating the security document, and applying the document identifier visibly to the document; and

h. storing the document and the document identifier in a database, the document being retrievable from the database by means of the document identifier.

2. A system for generating a security document as claimed in claim 1, in which the document and document identifier are stored in a database on the same computing node which generated the document.

3. A system for generating a security document as claimed in claim 1 or claim 2, in which the generated document identifier is checked for identity against document identifiers previously generated by the same process on the same node, the process returning to step b) if identity is detected, and continuing to step g) if identity is not detected.

The Law

10 The examiner has raised an objection under section 1(2)(c) of the Patents Act 1977 that the invention is not patentable because it relates to a program for a computer as such; the relevant provisions of this section of the Act are shown in bold 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-***
>
> *(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) …..*
>
> *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.*

11 As explained in the notice published by the UK Intellectual Property Office on 8 December 2008[1], the starting point for determining whether an invention falls within

[1] http://www.ipo.gov.uk/pro-types/pro-patent/p-law/p-pn/p-pn-computer.htm

the exclusions of section 1(2) is the judgment of the Court of Appeal in *Aerotel/Macrossan*[2].

12 The interpretation of section 1(2) has been considered by the Court of Appeal in *Symbian Ltd's Application*[3]. *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*[4] 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. But the *Symbian* judgment does make it clear, that in deciding whether an invention is excluded, one must ask does it make a technical contribution? If it does then it is not excluded.

13 Subject to the clarification provided by *Symbian*, it is therefore still appropriate for me, to proceed on the basis of the four-step approach explained at paragraphs 40-48 of *Aerotel/Macrossan* 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, which (see paragraph 45) is merely an expression of the "as such" qualification of section 1(2).
>
> 4) If the third step has not covered it, check whether the actual or alleged contribution is actually technical.

14 The operation of this test is explained at paragraphs 40-48 of the decision. Paragraph 43 confirms that identification of the contribution is essentially a matter of determining what it is the inventor has really added to human knowledge, and involves looking at substance, not form. Paragraph 46 explains that the fourth step of checking whether the contribution is technical may not be necessary because the third step should have covered the point.

15 Mr Noble agreed that this was the correct approach to take.

Arguments and Analysis

16 The examiner maintains that the invention as claimed is excluded under section 1(2)(c) of the Act as it relates to a program for a computer and a business method as such. Her position is set-out most recently in the official letter dated 21 August 2014. The applicant's arguments to the contrary are contained in their letters of 11th February 2014 and 13th June 2014 respectively. I am also grateful to Mr Noble for having supplied me with a copy of his "skeleton arguments" prior to the hearing

---

[2] *Aerotel Ltd v Telco Holdings Ltd* and *Macrossan's Application* [2006] EWCA Civ 1371; [2007] RPC 7
[3] *Symbian Ltd v Comptroller-General of Patents*, [2009] RPC 1
[4] *Merrill Lynch's Application* [1989] RPC 561

which provide a useful summary of the main points which were discussed during the hearing. I do not intend to repeat all the arguments here in full but will summarise them appropriately in the paragraphs which follow.

Claim construction

17 The first step of the test is to construe the claims. I do not think this presents any real problems since both the applicant and the examiner appear to agree as to the meaning of the claims.

Identifying the actual contribution

18 For the second step, it is necessary to identify the contribution made by the invention. Paragraph 43 of *Aerotel/Macrossan* explains that this is to be determined by asking what it is - as a matter of substance not form - that the invention has really added to the stock of human knowledge having regard to the problem to be solved, how the invention works and what its advantages are.

19 The examiner in her letter of 21 August 2014 identified the actual contribution of claim 1 to be the selection of the specific elements for inclusion in a document identifier so that two identical document identifiers cannot be generated by processes running on different nodes. The specific elements specified in claim 1 are the truncated message digest value, node identifier, process identifier, a first delimiter, and a random value which are concatenated to form the document identifier.

20 Mr Noble argued that the examiner in identifying the actual contribution had merely stripped out all of the features of the claim that are known and that further features were also necessary to place the invention in its proper context. Therefore, it was necessary for the actual contribution to include *storing a document and using the document identifier as a retrieval key*. Mr Noble also argued that the technical context requires that the contribution includes *a system for generating a security document which includes multiple nodes*.

21 Having considered the correspondence in some detail, I think there is a certain degree of agreement between the applicant and the examiner in so far as the contribution includes the selection and arrangement of the specific elements for inclusion in the document identifier. However, I agree with Mr Noble's argument that the contribution is broader than the mere generation of the document identifier and must include, as a matter of substance, some aspects of the system in which the document identifier is to be used. In my opinion, the contribution resides in a new method for generating and storing a security document in a multi-node network in which the document is assigned a unique document identifier including amongst other things a process identifier, and a node identifier providing an indication of the node where the security document was created. This has the effect of reducing the amount of inter-node traffic as it is no longer necessary to check for the creation of duplicate document identifiers on different nodes.

22 In addition, claim 2 requires the security document and document identifier to be stored in a database on the same computing node which generated the document. The document identifier thereby providing, by way of the node identifier, an indication of the location in which the document has been stored. This is said to improve the

speed with which the document is retrieved as there is no longer a need for centralised indexing.

23 Claim 3 introduces a localised "collision" detection step whereby the generated document identifier is checked for identity against document identifiers previously generated by the same process on the same node thereby further reducing the need for inter-node queries and additional network traffic.

Does the contribution fall solely within excluded subject matter? Is the contribution technical in nature?

Computer program

24 There is no doubt in my mind that the contribution requires a computer program for its implementation. However, the fact that the invention is effected in software does not mean that it is automatically excluded from patentability as a computer program as such. What matters is whether or not the program provides a technical contribution.

25 The task of determining whether the invention provides a technical contribution is a difficult one, as is evident from the plethora of case law in this area. However, I note that both the examiner and Mr Noble have made reference to the 'signposts' set out by Lewison J in *AT&T/CVON*[5], which I consider to be a useful guide in determining whether the contribution is technical in nature. The signposts were modified slightly by Lewison J in *HTC v Apple*[6] and now read as follows:

> *i) Whether the claimed technical effect has a technical effect on a process which is carried on outside 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 application 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.*

26 The examiner does not consider the contribution to be technical in nature as it does not, in her opinion satisfy, any of the above "signposts" and concludes that the invention relates to a computer program which provides no technical contribution and as such is excluded. In her letter of 21 August 2014, she makes reference to the judgement in *Lantana v Comptroller General of Patents*[7] which supports her view that the "computer" in this instance is the system as a whole and not an individual node of the cluster. Therefore, it follows that there is no technical effect outside of the computer arising from the reduction in inter node communications. She was also of the opinion that there is no change in how the computer works at the architectural level or any increase in the reliability of the computer because the underlying

[5] AT&T Knowledge Ventures/Cvon Innovations v Comptroller General of Patents [2009] EWHC 343 (Pat)
[6] HTC Europe Co Ltd v Apple Inc [2012] EWHC 1789 (Pat)
[7] *Lantana Ltd's Application* [2013] EWHC 2673 (Pat)

computer system remains unchanged. Moreover, she was of the view that the invention merely circumvents the problems of generating duplicate document identifiers on different nodes.

27 Mr Noble maintains that the contribution lies in the cluster of computing nodes, with each node generating and storing security documents with identifiers including node and process identifiers, and that this contribution is clearly outside of the statutory exclusions.

28 Determining what is "the relevant computer" is an important consideration and Mr Noble made reference to the judgement in *Protecting Kids the World Over (PKTWO) Limited v Comptroller General of Patents*[8] to support his view that the relevant "computer" is a single node and that there is a clear technical effect outside of that node because of the reduced need for inter-node communication and inter-node control.

29 Mr Noble also set out the alternative argument that if the "computer" was the whole cluster then the technical effect is a better cluster, which has substantially unbounded scalability and is resistant to failure of individual nodes because of the way in which the generation, storage and retrieval of security documents is carried out, mean that each node can be autonomous.

30 I will deal with "signposts" (i)-(iv) first. In substance, the claims relate to computer software for generating and storing a security document running on a cluster of interconnected nodes formed by conventional computers connected by a conventional network. In my opinion there is no technical effect going on outside of the computer which would save the invention from exclusion, any effect such as the apparent reduction in network traffic, results from the way in which the document identifiers are generated and structured. The computers themselves are entirely conventional not only in their architecture, but in the way they operate. Furthermore, I can see no inherent improvement in the reliability or speed of the computer which would suggest it was a better computer as required by the fourth of the signposts. I therefore do not think the invention as claimed satisfies any of signposts (i)-(iv).

31 In relation to signpost (v), the applicant acknowledges that one of the problems associated with the prior art, is the need to avoid "collisions". i.e. situations where different nodes create identical document identifiers. Whilst this can be avoided, for example, by checking each node for the creation of duplicate document identifiers it tends to result in an increase in network traffic. In the invention as claimed, inter-node collisions are not possible because the document identifier includes a unique node identifier corresponding to the node which created the document. Advantageously, therefore it is only necessary to check for document identifier collisions on individual nodes rather than on all of the nodes in the network. Again, the problem has been addressed by including within the document identifier, a node identifier thereby circumventing the problem and not solving it in any technical way.

32 What the applicant has done is to create a new computer program, albeit a very clever one, which is capable of generating security documents with unique document identifiers with the purpose of eliminating the possibility of generating the same identifier on different nodes of a multi node network without the need for implementing duplicate checking methods across the nodes and thereby reduce

[8] *Protecting Kids The World Over (PKTWO) Limited* [2011] EWHC 2720 (Pat)

network traffic between nodes when the program is running. In essence, the applicant has created new and better software implemented using conventional computing hardware that does not provide a relevant technical contribution and as such the invention as claimed in claim 1 falls within the computer program exclusion of section 1(2)(c).

33 Regarding the additional contribution as defined in claim 2, it is true to say that by storing the security document locally in a database associated with the node that generated the document and including the node identifier, and thereby the location of the document within the document identifier, it is possible to improve the speed with which the document is retrieved as there is no longer a need to provide centralised indexing. However, I do not think this provides the necessary technical contribution to avoid exclusion as a computer program. Claim 3 introduces the concept of locallised “collision” detection which again would appear to reduce network traffic but I am not convinced that this provides any additional contribution beyond that already provided by the invention as claimed in claim 1 for much the same reasons.

Business method

34 The examiner has also found that the invention is excluded under section 1(2) as a method of doing business. However, having found that the invention is excluded as a computer program I have no need to decide that issue.

Conclusion

35 In the light of my findings above, I conclude that the invention as claimed is excluded under section 1(2) because it relates to a computer program as such. Having read the specification I do not think that any saving amendment is possible. I therefore refuse the application under section 18(3).

Appeal

36 Any appeal must be lodged within 28 days

PETER SLATER

Deputy Director, acting for the Comptroller