Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 24 October 2018

Case Number: T 1372/11 - 3.5.01

Application Number: 06011945.0

Publication Number: 1734472

IPC: G06Q30/00

Language of the proceedings: EN

Title of invention:
Issuing machine and issuing system

Applicant:
Sato, Michihiro

Headword:
Issuing machine and issuing system/SATO

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - server-side authentication of hardcopy certificates based on combination of random pattern and cryptographic checksum (yes - non-obvious combination)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1372/11 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 24 October 2018

Appellant: (Applicant)	Sato, Michihiro 12-7-2-082, Gobancho, Chiyoda-ku Tokyo 102-0076 (JP)
Representative:	Bockhorni & Brüntjen Partnerschaft Patentanwälte mbB Elsenheimerstraße 49 80687 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 9 February 2011 refusing European patent application No. 06011945.0 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Chandler
Members:	N. Glaser
	Y. Podbielski

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the European patent application No. 06 011 945.0 pursuant to Article 97(2) EPC on the ground of lack of inventive step (Article 56 EPC) over EP-A-1 039 420 (D1).

II. In the statement setting out the grounds of appeal, dated 9 June 2011, the appellant requested that the examining division's decision to refuse the application be set aside and that a patent be granted on the basis of a main request, or one of a first to third auxiliary requests, all filed therewith.

III. In a communication, the Board set out its preliminary opinion that the invention did not involve an inventive step (Article 56 EPC). The Board introduced the following documents:

US 6 575 362 (D2), and
WO 01/91007 (D3)

IV. In a reply, dated 18 August 2017, the appellant filed fourth to sixth auxiliary requests, together with arguments in favour of inventive step.

V. In the communication accompanying the summons to oral proceedings, the Board confirmed its preliminary opinion about inventive step and questioned the admissibility of the fourth to sixth auxiliary requests.

VI. In a reply dated 10 September 2018, the appellant filed a new third and fourth auxiliary request and upheld

previous third to sixth auxiliary requests as fifth to eighth auxiliary requests.

VII. At the beginning of the oral proceedings, the appellant confirmed the above requests. At the end of the oral proceedings, the appellant requested that the decision under appeal be set aside and a patent be granted on the basis of:

Claims 1-15 of the main request, filed at 16:00h on the day of the oral proceedings before the Board,

A description and drawing sheet 12/13 filed on the same date,

Drawing sheets 1/13 to 11/13 and 13/13 as originally filed.

VIII. Independent claim 1 of the main request reads as follows:

"A method of transacting a security or a fixed rate financing instrument, wherein the security or fixed rate financing instrument is transacted as a hardcopy certificate (107) by means of an issuing system including a securities issuing institution (101) and at least one issuing machine (105) for transacting the hardcopy certificate (107) connected to the securities issuing institution (101), the issuing system comprising receiving means of the issuing machine (105), information retrieving means of the issuing machine (105), input means (105a) of the issuing machine (105), transaction processing means of the issuing machine (105), computing means in the securities issuing institution (101), printing means of

the issuing machine (105), scanning means of the issuing machine (105), conveying means of the issuing machine (105) and determining means in the securities issuing institution (101), wherein

the receiving means receives a recording medium (106) provided by a potential purchaser;

the information retrieving means retrieves identification recoded in the received recording medium (106);

in the input means (105a) the potential purchaser input request for a transaction of the security or the fixed rate financing instrument;

the transaction processing means processes the requested transaction by retrieving information via a network from a server of the issuing institution (101);

the computing means computes a cryptographic checksum by applying a cryptographic algorithm to information to be printed on the hardcopy certificate (107), the information including at least one of a face value, a serial number, an issuer identification, an issue date, an expiry date, and an owner name, the cryptographic checksum enabling to verify that the information contained in the hardcopy certificate (107) has not been changed;

the printing means prints out said hardcopy certificate (107) as purchased by the potential purchaser and the computed cryptographic checksum thereon;

wherein said hardcopy certificate (107) further includes a random pattern and said scanning means scans

said hardcopy certificate (107) with the random pattern prior to providing said hardcopy certificate (107) to the purchaser;

wherein the conveying means conveys the result of the scan of the scanning means to the securities issuing institution (101) for storage;

wherein said scanning means scans the hardcopy certificate (107) inserted by a holder, the conveying means conveys the result of the subsequent scan of the scanning means to the securities issuing institution (101); and

the determining means determines whether the hardcopy certificate (107) is valid by checking that

a) the subsequently scanned cryptographic checksum scanned by the issuing machine (105) matches the computed cryptographic checksum in the securities issuing institution (101) and

b) the subsequently scanned hardcopy certificate (107) contains the random pattern."

IX. The appellant's arguments can be summarized as follows :

D1 is concerned with a method for issuing test certificates for vehicles, so-called MOT certificates, and their authentication. These certificates are different in nature and are subject to less stringent restrictions against modification and/or forgery than the hardcopy certificates of financial instruments of the present invention.

While an MOT certificate includes an authentication code, generated at a central authentication authority using its cryptographic key, it does not comprise additional security elements printed on it in a random pattern and/or micro printing font.

The check of the MOT certificate occurs locally at a user terminal, without involvement of the central authentication authority. There is no check whether or not the scanned cryptographic checksum matches the computed cryptographic checksum in the central authentication authority. Forged MOT certificates are not recognizable and may also be duplicated.

Reasons for the Decision

1. Background

1.1 The invention concerns an issuing system including a plurality of issuing machines for locally and cost-effectively selling, generating, and printing hardcopy certificates for newly-issued securities which are unmodifiable and unforgeable. Each of the issuing machines can also redeem hardcopy certificates and identify whether it is one which was previously issued by an issuing machine of the system.

1.2 Looking at Figure 1 and paragraph [124], a customer uses an issuing machine (ASD) 105 to specify a purchase transaction and identify himself, e.g. by an ID read from a recording medium 106, see paragraphs [94, 97], such as a payment or credit card, see paragraph [68]. The issuing machine sends these details to the issuing institution (ASD host) 101, which computes and returns a cryptographic checksum. The issuing machine then

prints out a hardcopy certificate 107 (Figure 15) with details of the transaction and the checksum, see paragraph [124]. The hardcopy certificate is printed on paper with an embedded random pattern, which is recorded by scanning the certificate before issuing it to the purchaser. This scan is sent to the issuing institution for storage, see paragraph [143].

1.3 The terminal can check the validity of the hardcopy certificate by scanning it and comparing the checksum and the random pattern with the stored versions, see paragraph [147]. Such a check occurs when a customer inserts a hardcopy certificate to "sell" or to redeem it. The checksum makes the certificate "unmodifiable" because any change to the information on the printed certificate can be easily detected, see paragraph [73], while scanning the random pattern makes it "unforgeable" because the printed certificate cannot be easily duplicated with conventional means, see paragraph [74]

2. Article 56 EPC

2.1 Despite the above-mentioned clearly technical aspects of the invention and associated means in the securities issuing machine of the claims, the Search Division issued what was in the Board's opinion a questionable no-search declaration under Rule 45 EPC. After amendment, the division introduced document D1, which concerns printing unforgeable MOT certificates for tested cars.

2.2 In D1, the government Vehicle Inspectorate Data Centre 101 with a central server 104 and a database 105 is connected to a vehicle testing centre issuing machine 102 with a terminal 106 and printing means 108 which

includes a barcode scanner. A MOT certificate is a hardcopy certificate with a printed message authentication code (MAC) in the form of a barcode. The MAC is generated by the central server 104 by encrypting with a secret key the vehicle and test data and a unique serial number read from the barcode of the blank MOT certificate. The authenticity of the certificate can be checked at a Post Office by reading the barcode and checking that the MAC corresponds to a MAC generated locally using the vehicle and test information encrypted with the secret key, which is known to the Post Offices [29].

2.3 Claim 1 as amended before the Board differs from D1 by the printing of the random pattern on the hardcopy certificate, and the storage of the random pattern and checksum on the server. Furthermore, there is a centralised verification of the certificates by the issuing institution rather than a local check at the terminal 112 of the Post Office, which is not connected to the issuing institution of the certificate. The subject-matter of claim 1 is therefore novel over D1 (Article 54 EPC).

2.4 While it could be argued that a more efficient way of checking the MAC of a certificate would be achieved by connecting the terminal 112 to the central server 104 in order to realise a centralised verification of the MAC, based on common general knowledge, there is no incentive to print a random pattern on an MOT certificate, to store this random pattern at the server and to implement a centralised check based on checksum and random pattern. These two features represent additional steps which are not obvious to the person skilled in the art. The Board therefore judges that the

subject-matter of claim 1 involves an inventive step over D1 (Article 56 EPC).

3. D2 and D3 were introduced by the Board under Article 114(1) EPC in reaction to the argument of the appellant that the MOT certificates of D1 do not correspond to the claimed hardcopy certificates (grounds of appeal, page 9, first paragraph).

3.1 D2 was cited in the search report of the USPTO available on 5 July 2006, prior to the date when the European (no-)search report was drawn up. D2 concerns the printing of unforgeable and unmodifiable certificates for money orders at an ATM or POS terminal, as well as their redemption. It represents therefore the closest prior art. Each certificate comprises a security label in the form of a printed 2D barcode provided by a service centre.

3.2 In detail, D2 discloses an issuing institution 16, 18 which is connected to an issuing machine, comprising a receiving means and an information retrieving means as well as an input means as part of an input/output section 10 (column 4, lines 9 to 34; column 5, lines 18 to 38), a transaction processing means 12, 14, a computing means 12 and a printing means 20 to print out a hardcopy certificate 22 and a computed cryptographic checksum 24 (column 4, lines 23 to 55), as well as a scanning means 70 as part of the input/output section 10 and determining means to determine whether the hardcopy certificate was issued "by" the securities issuing institution (column 4, line 56, to column 5, line 5). For redeeming certificates, they are scanned and visually verified and thereafter destroyed (column 9, lines 17 to 41, and column 10, lines 18ff.).

3.3 The method of claim 1 differs in that:

(random pattern) "*the hardcopy certificate further includes a random pattern*";

(combined check) "*said scanning means scans said hardcopy certificate with the random pattern prior to providing said hardcopy certificate to the purchaser, wherein said scanning means scans the hardcopy certificate inserted by a holder, wherein the determining means determines whether the hardcopy certificate is valid by checking that the subsequently scanned cryptographic checksum scanned by the issuing machine matches the computed cryptographic checksum computed in the securities issuing institution, and the subsequently scanned hardcopy certificate contains the random pattern*."

(remote check on a server) "*wherein the conveying means conveys the result of the scan of the scanning means to the securities issuing institution for storage, the conveying means conveys the result of the subsequent scan of the scanning means to the securities issuing institution, wherein the computing means and the determining means is in the securities issuing institution*."

3.4 The first difference (pattern) defines an additional security element for a hardcopy certificate. It leads to an improved certificate as an additional security characteristic to protect it against forgery. It may be self-identifying for a visual check, for example.

The second difference (automatic combined check) defines an automated check of a certificate where a checksum is validated, but also the random pattern.

This improves the accuracy of validation checks.

The third difference (remote check on server) defines a centralised storage of information and a centralised validation check which leads to a more efficient system where certificates can be redeemed at various locations different from the location where they were bought.

3.5 The objective technical problem stemming from these three differentiating features can be formulated as how to provide unforgeable and unmodifiable documents which can be redeemed with an improved validation at various locations different from the location where they were bought.

3.6 D3 also addresses the problem of providing unforgeable and unmodifiable documents, including stock and bond certificates (page 1, third paragraph, paragraph bridging pages 3 and 4). It is also a sort of reservoir of a variety of prior art techniques that have been used to address these aims in different ways, mostly presented as single solutions in isolation from the other approaches. It discloses, page 44, second last and last paragraph, pages 45 and 46, bridging paragraph, pages 46 and 47, bridging paragraph, various kinds of security measures against counterfeiting, such as, serial number encoding in machine readable form as magnetic ink, barcodes, 2D barcodes, random patterns of magnetic toner, codes having multiplicity of complexity levels and invisible security features.

3.7 Thus D3 proposes an additional security element (pattern) and the person skilled in the art would adapt the generation of the print image of D2, column 8, lines 31 to 43, to include a random pattern, and adapt

the validation check, D2, column 9, lines 17 to 34, to include the random pattern in the authentication check.

3.8 In D2 the decoded cryptographic information is displayed, column 9, lines 17 to 23, for a visual check, presumably by a human, as disclosed further down in line 38. There is no disclosure in D2 that the decoded information is checked with previously stored information (automatic combined check). D2 goes rather in the other direction: a service center 16 acts as an independent third party, column 4, lines 28 to 34, to generate the security identification to be printed on the certificate, but it is not involved in the authentication and verification of a certificate, which would imply that the security information is stored and provided to the issuing machine for the validation check. Similarly, although D3 discusses checks of patterns, checks of checksums, e.g. the passage bridging pages 35 and 36, it does not clearly disclose all of these in combination with scanning of the hardcopy on production at the terminal.

3.9 Concerning a remote check on server, there is no incentive to move away from a local authentication in D2, see column 9, lines 17 to 23, line 38 and 54, where a representation of an encoded image is displayed at the kiosk and compared to the money order itself. Furthermore, while D3 discloses an online authentication, page 46, second and third paragraph, pages 50 and 51, bridging paragraph, the disclosure remains too general and refers to the logging of security risks. The on-line technique, disclosed in the bridging paragraph of pages 35 and 36, works on remotely stored information of a whole document, such as a hash code. A stored image pattern is not transmitted (e.g. conveyed) for security reasons.

3.10 The claimed combination of the above features goes a step further by explicitly combining two specific security characteristics and a server-based authentication, namely during issuing, the printing of a hardcopy certificate, the scanning of it to retrieve security information (cryptographic checksum and random pattern) and the storage of this information on a server, and then during redemption a subsequent scan to authenticate it based on a cryptographic checksum and random pattern.

3.11 Although the person skilled in the art may retrieve some of these features from D3, the Board judges that this is not a straightforward case of partial solutions to partial problems because the solutions are not clearly disclosed individually or in the claimed combination. The Board therefore judges that such a combination would only be possible with hindsight.

3.12 Accordingly, claim 1 involves an inventive step over D2, in combination with D3 (Article 56 EPC).

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the Examining Division with the order to grant a patent in the following version:

- Claims 1-15 according to the main request filed during the oral proceedings before the Board

- Description: pages 1-32 filed during the oral proceedings before the Board

- Drawings: sheets 1/13 to 11/13 and 13/13 as originally filed and sheet 12/13 as filed during the oral proceedings before the Board.

The Registrar: The Chairman:

T. Buschek W. Chandler

Decision electronically authenticated