

Internal distribution code:

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

**Datasheet for the decision
of 23 April 2013**

Case Number: T 1941/09 - 3.4.03

Application Number: 02749306.3

Publication Number: 1431891

IPC: G06F 17/60

Language of the proceedings: EN

Title of invention:

IC card and IC card operation method

Applicant:

Sony Corporation

Headword:

-

Relevant legal provisions (EPC 1973):

EPC Art. 56

Keyword:

"Inventive step (no)"

Decisions cited:

-

Catchword:

-



Case Number: T 1941/09 - 3.4.03

D E C I S I O N
of the Technical Board of Appeal 3.4.03
of 23 April 2013

Appellant: Sony Corporation
(Applicant) 7-35, Kitashinagawa 6-chome
Shinagawa-ku
Tokyo 141-0001 (JP)

Representative: Robinson, Nigel Alexander Julian
D Young & Co LLP
120 Holborn
London EC1N 2DY (GB)

Decision under appeal: Decision of the Examining Division of the
European Patent Office posted 18 May 2009
refusing European patent application
No. 02749306.3 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: G. Eliasson
Members: T. M. Häusser
T. Bokor

Summary of Facts and Submissions

- I. The appeal concerns the decision of the examining division to refuse European patent application No. 02 749 306 for lack of inventive step within the meaning of Article 56 EPC 1973 (main and auxiliary request).
- II. During the oral proceedings before the board the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of Claims 1-6 filed with the letter dated 14 March 2013 under the title of Main Request, as sole request.
- III. The following document is referred to in this decision:

D1: EP 0 933 717 A2.
- IV. The wording of independent claim 1 reads as follows (labelling (1), (2), ..., (7) by the board):

"(1) An IC card operation system (1) comprising:
a plurality of IC cards,
(2) each IC card (5) having:
(a) a public area (32) including:
(i) a plurality of proprietary files providing an issuer-specific point area (34) for storing cumulative amounts of points issued by respective point issuers (8), the issued points being accumulated in a manner specifying each of said cumulative points for the corresponding point issuer, and each proprietary file corresponding to a respective point issuer having access thereto controlled by a respective proprietary

file key to permit each point issuer to access its proprietary file only among said plurality of proprietary files; and

(ii) a common point area (36) for storing a cumulative amount of said points issued by said point issuers, the issued points being accumulated in a manner mingling all point issuers; and

(b) a private area (31) including a payable amount area (37) for storing a payable amount that may be paid so as to acquire either a product or a service offered by a specific business operator (6), said private area also storing private area key information for use in encryption and decryption;

- (3) a plurality of point issuing apparatuses (21) for issuing points to be stored into said issuer-specific point area and said common point area,
- (4) each point issuing apparatus using a proprietary file key to access a proprietary file among said plurality of proprietary files providing said issuer-specific point area for said point issuing apparatus;
- (5) an adjusting apparatus (15, 16) for allowing said business operator to adjust an amount to be paid using at least one of said points accumulated in said common point area and said payable amount stored in said payable amount area,
- (6) wherein said cumulative amount of said points in said common point area is convertible into said payable amount at a predetermined rate; and
- (7) a center apparatus (10) for acquiring the number of points issued by respective point issuing apparatus for storage into said common point

area, said center apparatus further calculating the amount of points to be adjusted by said point issuers in payment for said business operator by use of the acquired number of issued points."

V. The appellant argued essentially as follows in relation to inventive step:

Document D1 could be considered to be the closest prior art. There was no disclosure in document D1 of a plurality of proprietary files. A 'file' was a complete collection of data manipulated as a unit. In particular, access rights could be assigned to the collection of data. On the other hand, a 'register' was regarded to be an authoritative record. The merchant loyalty registers described in document D1 could therefore not be regarded as proprietary files within the meaning of the expression in claim 1.

Furthermore, in document D1 it was merely described that a single loyalty key allowed access to the smart card as a whole. There was thus no disclosure that each proprietary file had access controlled by a respective proprietary file key.

Moreover, there was no disclosure of a common point area. Rather, it was described in D1, paragraph [0008], that loyalty points could be shared by merchants.

The objective technical problem could be considered to be the prevention of merchant-merchant abuse of the system. One merchant might want to interfere with the records of another merchant. An example of such abuse would be one merchant increasing the points of another

merchant. This could be done by means of a fictitious transaction. The proprietary files allowed fraudulent behaviour to be tracked. Even though the fraud example and the abuse problem was not explicitly described in the description of the application, the aim to prevent fraud could be derived from the description, in particular page 16, paragraph 4.

Starting from the system of D1, an obvious solution of that problem would be to record transactions. Even if this involved electronic signatures, that solution could be easily performed.

Providing files which were protected by keys led to a "hack-proof" solution which went beyond any business considerations. Such a solution was not obvious for the skilled person, especially at the priority date of the application.

Therefore, the subject-matter of claim 1 involved an inventive step.

Reasons for the Decision

1. Admissibility

The appeal is admissible.

2. Inventive step

2.1 Closest state of the art

2.1.1 The appellant regards document D1 as the closest prior art.

Indeed, document D1 is conceived for the same purpose as the invention, namely to provide a chip card operation system, and has the most relevant technical features in common with it. Document D1 is therefore regarded as the closest state of the art.

2.1.2 In particular, document D1 discloses (see paragraphs [0019]-[0025], [0029] and [0034]-[0036]; Figures 1-8 and 10) a smart card 4, such as a VISA Cash Smart Card, with a microcomputer 6 having memory in which a transaction log 20 is stored. The first part 22 of the transaction log 20 is used for storing a purse value and the second part 24 comprises a purchase log 26 and a loyalty program application 28. The loyalty program 28 is initiated by inserting the smart card 4 into a stand alone terminal 2, which then loads one or more merchant loyalty registers 40 within an area of the memory of the smart card 4. Each merchant loyalty register 40 is identified by a merchant number 42 to allow transactions, which are identified by transaction numbers 44, with a particular merchant to be matched with the loyalty register 40 for that merchant.

For making a purchase at a merchant the smart card 4 is inserted into a merchant terminal, which authenticates that the smart card 4 can be used for the particular transaction. The merchant terminal then loads or unloads value from the smart card 4 and writes information about the transaction to the purchase log 26.

One alternative to update the merchant loyalty register 40 is by use of a stand alone terminal 2. The customer inserts the smart card 4 into the stand alone terminal 2, which uses a loyalty key residing in it in order to authenticate the smart card 4. The stand alone terminal 2 compares information in the purchase log 26 to information in the merchant loyalty register 40 and then adjusts the loyalty register 40 to account for any unrecorded transactions with the corresponding merchant thus accumulating the loyalty points for that merchant.

In another alternative the merchant loyalty register 40 is updated automatically. In this case, when a transaction is performed at the merchant terminal, the loyalty application on the smart card 4 automatically reads information in the transaction log 26 and in the merchant loyalty register 40 and performs a comparison. The loyalty application then automatically updates the merchant loyalty register in order to account for each transaction. The merchant terminal reports the data back to a central system.

In order to inquire about a particular merchant loyalty register 40 or to redeem loyalty points the customer inserts the smart card 4 into the stand alone terminal 2. The customer can choose options to display the balance for a specific loyalty register 40 or to show the number of loyalty points required to obtain specific merchant products. The customer can also choose to exchange loyalty points for a particular product. In that case the stand alone terminal 2 updates the specific merchant loyalty register 40 and prints out a coupon for use by the consumer.

It is also disclosed in D1 (see paragraphs [0008] and [0026]) that the invention of D1 permits one merchant to join with another merchant so that loyalty points may be exchanged at each other's businesses. Moreover, smart card purchases made at the store of a particular merchant or at an associated chain of stores is credited only to the loyalty register 40 for the particular merchant.

2.1.3 Consequently, document D1 discloses, using the wording of claim 1:

- (1) an IC card (chip card) operation system comprising:
 - a plurality of IC cards (chip cards),
- (2) ' each IC card (chip card) having:
 - (a) a public area including:
 - (ii) a common point area (merchant loyalty register 40) for storing a cumulative amount of said points issued by said point issuers (cooperating merchants whose loyalty points may be exchanged at each other's businesses), the issued points being accumulated in a manner mingling all point issuers (cooperating merchants); and
 - (b) a private area (first part 22 of transaction log 20) including a payable amount area for storing a payable amount (purse value) that may be paid so as to acquire either a product or a service offered by a specific business operator (merchant), said private area also storing private area key information for use in encryption and decryption (implicit - the purse value is necessarily stored in an encrypted fashion on the smart card as it could otherwise

- be manipulated);
- (3) ' a plurality of point issuing apparatuses (merchant terminals) for issuing points to be stored into said common point area,
 - (5) an adjusting apparatus (merchant terminal) for allowing said business operator (merchant) to adjust an amount to be paid using at least one of said points accumulated in said common point area and said payable amount (purse value) stored in said payable amount area,
 - (6) wherein said cumulative amount of said points in said common point area is convertible into said payable amount at a predetermined rate (ratio of price of redeemable product to number of required loyalty points); and
 - (7) a center apparatus (stand alone terminal 2) for acquiring the number of points issued by respective point issuing apparatus for storage into said common point area (merchant loyalty register 40), said center apparatus further calculating the amount of points to be adjusted by said point issuers in payment for said business operator by use of the acquired number of issued points (new point balance after redeeming loyalty points).

2.1.4 Document D1 does not disclose the following features of claim 1:

- (2) '' each IC card (chip card) having:
 - (a) a public area including:
 - (i) a plurality of proprietary files providing an issuer-specific point area for storing cumulative amounts of points issued by respective point issuers, the issued points being

accumulated in a manner specifying each of said cumulative points for the corresponding point issuer, and each proprietary file corresponding to a respective point issuer having access thereto controlled by a respective proprietary file key to permit each point issuer to access its proprietary file only among said plurality of proprietary files; and

- (3) '' a plurality of point issuing apparatuses for issuing points to be stored into said issuer-specific point area,
- (4) each point issuing apparatus using a proprietary file key to access a proprietary file among said plurality of proprietary files providing said issuer-specific point area for said point issuing apparatus.

2.2 Objective technical problem

- 2.2.1 According to the appellant the objective technical problem could be considered to be the prevention of merchant-merchant abuse of the system.

However, even the claimed system does not prevent a customer to spend points which were awarded in a fraudulent manner. Rather, according to claim 1 the points are accumulated in the common point area and may be spent at an adjusting apparatus of the business operator. Furthermore, according to the claim 1 each point issuer has access to his proprietary file via the proprietary file key. Therefore the proprietary files do not necessarily provide an impartial record of the issue of the points. Rather a point issuer who wanted to award fraudulent points could also manipulate his

proprietary file in order to erase any trace of the fraud. The claimed system therefore does not allow objective tracking of system abuse. Hence such abuse cannot even realistically be considered to be prevented by the concern that it may be revealed.

Moreover, in the system of document D1 a merchant does not have access via the merchant terminal to the merchant loyalty register 40 and therefore cannot manipulate the number of loyalty points stored in it. Rather, as described above under point 2.1.2, the content of the merchant loyalty register 40 is updated automatically or by use of the stand alone terminal 2. Manipulating the number of loyalty points by means of fake transactions by the merchant, as suggested by the appellant, is not regarded to be realistic as those fraudulent transactions would then be part of the merchant's accounts. The problem as formulated by the appellant does therefore not arise in the system of the closest prior art document D1.

Finally, the object to prevent merchant-merchant abuse of the system is not mentioned anywhere in the description of the application.

- 2.2.2 On the other hand, the description of the application does explicitly mention (see page 13, paragraphs 2 and 3; page 16, paragraph 4) that each shop can check the sum total of points issued by the shop in question in order to see how important the customer is for the shop. Furthermore, no proprietary file is accessible by anyone not in possession of the appropriate access key.

It is evident that these statements are related to the difference features (2)'', (3)'' and (4) (see point 2.1.4 above) since the points issued by a point issuer are accumulated - using the relevant point issuing apparatus - to provide the desired sum total of points issued by the corresponding shop and the access of each proprietary file is controlled by a respective proprietary file key.

- 2.2.3 In the decision under appeal the examining division held that it was the objective technical problem of the invention to implement the business administrative procedure related to the IC chip's public and private area as defined in claim 1 then on file.

Indeed, allowing each shop to check in a confidential manner the sum of points issued by it, while at the same time allowing a plurality of shops to have common loyalty points, is considered to be a business aim and thus to be achieved in a non-technical field. That aim may therefore legitimately appear in the formulation of the objective technical problem as part of its framework (see "Case Law of the Boards of Appeal of the EPO", 6th edition 2010, I.D.8.1.5).

Technical aspects come into play when such a scheme is implemented into the known smart card system.

- 2.2.4 In view of the above it is regarded to be the objective technical problem of the invention to implement the smart card system in such a way as to allow each shop to check in a confidential manner the sum of points issued by it, while at the same time allowing a plurality of shops to have common loyalty points.

2.3 Obviousness

2.3.1 The appellant argued that the claimed subject-matter provided a "hack-proof" solution which went beyond any business considerations. Furthermore, the loyalty key of document D1 allowed access to the smart card as a whole and there was no disclosure that each proprietary file had access controlled by a respective proprietary file key.

2.3.2 The smart card 4 of document D1 is in the possession of the consumer while having value in the form of electronic money (purse value) and merchant loyalty points which can be exchanged for merchant products. It is therefore natural that security mechanisms are built into the smart card 4 in order to avoid any manipulation of it. Indeed, as mentioned under points 2.1.2 and 2.1.3 above, a private area key is used for storing the purse value on the smart card and a loyalty key is used for authentication of the smart card 4 when updating the merchant loyalty register 40 using the stand alone terminal 2. It is also described in document D1 (see paragraph [0040]) to use a purchase key for the redemption of loyalty points.

Furthermore, it is envisaged in the system of D1 (see paragraph [0023]) to have several loyalty programs installed on the smart card 4. An identification of each installed loyalty program 28 can be placed on the outside of the card. Moreover, the loyalty programs 28 are separate from the other functionality of the smart card of providing electronic money (purse value). On the other hand, the loyalty key is merely described to

allow secure update of the loyalty register 40. Under these circumstances the loyalty key cannot be expected to give access to the smart card as a whole, but rather to provide only access to the parts of the memory of the smart card 4 which are relevant for the update, i.e. the purchase log 26 and the loyalty registers 40.

- 2.3.3 In order to achieve the given aim of allowing each shop to check the sum of points issued by it, it would be obvious for the person skilled in the art of smart card systems to create on the smart card 4 further records for storing the accumulated points of each single merchant. This would be analogous to and in addition to the merchant loyalty register 40 in which cooperating merchants store their loyalty points. Organizing the data in the memory of the smart card 4 in a file structure is common practice of the skilled person.
- 2.3.4 In view of the above it would also be obvious for the skilled person to implement the desired confidentiality by means of a further security mechanism. In particular, in a manner similar to the use of the loyalty key, the skilled person would restrict the access to the parts of the memory of the smart card in which the points issued by a particular merchant are stored by means of a further key assigned to that merchant ("merchant key").

The easiest way to update and to read the accumulated points issued by a single merchant would be to take advantage of the structure of the system of D1 already in place and to adjust the merchant terminal of D1 in such a way as to allow it to access the relevant parts of the memory of the smart card 4 by means of the

corresponding merchant key. The skilled person would therefore consider such a solution.

2.3.5 For these reasons it would be obvious for the skilled person to solve the posed objective technical problem by means of the difference features (2)', (3)' and (4). Therefore, the subject-matter of claim 1 does not involve an inventive step (Article 52(1) EPC and Article 56 EPC 1973).

3. Conclusion

In view of the above the sole request is not allowable. Consequently, the appeal must fail.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:

The Chairman:

S. Sánchez Chiquero

G. Eliasson