# Appeal decision

Appeal No. 2018-10270

| | |
|---|---|
| Appellant | SONY CORPORATION |
| Patent Attorney | Sakai International Patent Office |

The case of appeal against the examiner's decision of refusal of Japanese Patent Application No. 2017-86951, entitled "ELECTRONIC SETTLEMENT SYSTEM, INFORMATION PROCESSING DEVICE, AND ELECTRONIC SETTLEMENT MANAGEMENT DEVICE" (the application published on July 20, 2017, Japanese Unexamined Patent Application Publication No. 2017-126386) has resulted in the following appeal decision.

## Conclusion

The appeal of the case was groundless.

## Reason

### No. 1 History of the procedures

Regarding the present application,

Japanese Patent Application No. 2001-139164 was filed on May 9, 2001 (Priority date: May 10, 2000, February 23, 2001),

a part thereof was filed on May 9, 2011 as Japanese Patent Application No. 2011-104326,

a part thereof was filed on May 24, 2013 as Japanese Patent Application No. 2013-109556,

a part thereof was filed on November 29, 2013 as Japanese Patent Application No. 2013-247649,

a part thereof was filed on June 10, 2015 as Japanese Patent Application No. 2015-117432, and

a part thereof was filed on April 26, 2017 as Japanese Patent Application No. 2017-086951. Subsequent procedures are as follows.

| | |
|---|---|
| dated January 30, 2018: | Notice of reasons for refusal |
| April 4, 2018: | Submission of Written opinion and Written amendment |

dated May 9, 2018: Examiner's decision of refusal

July 27, 2018: Submission of Written appeal and Written amendment

dated July 12, 2019: Notice of reasons for refusal of the body

September 13, 2019: Submission of Written opinion and Written amendment

No. 2 The Invention

Claims 1 to 4 of the scope of claims amended by the written amendment submitted on September 13, 2019 include the following descriptions (hereinafter referred to as "Invention 1", "Invention 2", ... "Invention 4", which are collectively referred to as "the Invention").

"[Claim 1]

An electronic settlement system comprising:

an information processing device; and

an electronic settlement management device, wherein

the information processing device includes:

a determination unit which determines one payment method from among a plurality of payment methods including payment by credit card, payment by debit card, and electronic payment, on the basis of an input from a user;

a transmission unit which transmits settlement request information including information on the amount of money to the electronic settlement management device in response to a determination of the electronic payment when the electronic payment is determined; and

a processing unit which causes a data storage device to acquire settlement information including balance information read from a tamper-resistant memory in the data storage device, through processing in accordance with the settlement information including a balance read request received from the electronic settlement management device, and transmits the acquired settlement information to the electronic settlement management device,

the electronic settlement management device includes:

a receiving unit which receives the settlement request information;

a generation unit which generates settlement information including a balance read request on the basis of the settlement request information; and

a transmission unit which transmits the settlement information including the balance read request to the information processing device.

[Claim 2]

The electronic settlement system described in Claim 1, wherein

the electronic settlement management device

generates a settlement processing request including log write information for writing log information generated from settlement information including balance information received from the information processing device into the data storage device and subtraction information for subtracting the amount demanded from the amount indicated by the balance information, encrypts the generated settlement processing request with a session key, and transmits the encrypted settlement processing request with a signature based on a secret key to the information processing device,

in the information processing device, the signature added to the settlement request information is checked by using a public key corresponding to the secret key is valid, and when the result of checking is valid, balance information stored in the data storage device is updated.

[Claim 3]

The electronic settlement system described in Claim 2, wherein

when the result of checking is valid, in the data storage device, the settlement request information is decrypted by a common key, and balance information stored in the data storage device is updated on the basis of subtraction information included in the decrypted settlement request information.

[Claim 4]

An information processing device including:

a determination unit which determines one payment method from among a plurality of payment methods including payment by credit card, payment by debit card, and electronic payment, on the basis of an input from a user;

a transmission unit which transmits settlement request information including information on the amount of money to the electronic settlement management device in response to a determination of the electronic payment when the electronic payment is determined; and

a processing unit which causes a data storage device to acquire settlement information including balance information read from a tamper-resistant memory in the data storage device, through processing in accordance with the settlement information including a balance read request received from the electronic settlement management device, and transmits the acquired settlement information to the electronic settlement management device."

No. 3 Outline of notice of reasons for refusal of the body

The reasons in the notice of reasons for refusal dated July 12, 2019, which are the reasons for refusal of the body, are outlined as follows.

The description of the Scope of Claims of the present application does not satisfy the requirements stipulated in Article 36(6)(i) of the Patent Act, in the following points.

Notes

1. Regarding whether the invention described in the Scope of Claims is the invention described in the Detailed Description of the Invention

(Omitted)

2. Regarding whether the invention described in the Scope of Claims falls within a scope where the problem of the invention can be solved by a person skilled in the art based on the description of the Detailed Description of the Invention (or whether the invention falls within a scope where a person skilled in the art can recognize that the problem of the invention can be solved in light of the common general technical knowledge at the time of the priority date without description or indication in the Detailed Description of the Invention)

It is acknowledged, in the Detailed Description of the Invention in the Specification, regarding the technical field of the Invention, background art, and the problem to be solved by the invention, according to [0001] to [0010], that the problem of the invention is to conduct e-commerce transactions safely over a network using a data storage device, such as an IC card with a common key.

In order to solve the problem, it is necessary that a session key KSES is generated from a common key KC, in a security server 31 in a settlement management device 3 and a data storage device 20, such as an IC card, and that by using the session key KSES information to be transmitted and received between the settlement management device 3 and an information processing device 22, e.g., settlement information or balance information BI including a balance readout request BRC, includes a matter to be encrypted / decrypted.

The inventions according to Claims 1 to 5, which are the inventions described in the Scope of Claims, do not include the above technical matters, and it is not recognized that there is a matter of common general technical knowledge where a person skilled in the art can acknowledge that the problem of the invention can be solved from the inventions according to Claims 1 to 5. Thus, it is not acknowledged that the means for solving the problem of the invention is reflected.

The Detailed Description of the Invention in the Specification does not describe the problem of the invention other than the above matters. Even in light of the common general technical knowledge at the time of the priority date, according to the Detailed Description of the Invention in the Specification, it is not recognized that the problem to be solved by the invention is acknowledged.

Accordingly, it is not acknowledged that the invention described in the Scope of Claims falls within a scope where the problem of the invention can be solved by a person skilled in the art based on the description of the Detailed Description of the Invention, or that the invention falls within a scope where a person skilled in the art recognizes that the problem of the invention can be solved in light of the common general technical knowledge at the time of the priority date without description or indication in the Detailed Description of the Invention.

Thus, the inventions according to Claims 1 to 5 are not described in the Detailed Description of the Invention.

No. 4 Description of the Detailed Description of the Invention

The Detailed Description of the Invention includes the following descriptions.

(1) "[Technical field]

[0001]

The present invention relates to an electronic settlement system in which settlement processing, using a network or the like, can be safely carried out by using a data storage device holding a common key, such as an IC card, as well as a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium.

[Background Art]

[0002]

In order to safely carry out electronic commercial transactions through an open network such as the Internet, a PKI (Public Key Infrastructure) protocol has been adopted.

[0003]

In the PKI protocol, a transmission source creates signature information by using a secret key, and the transmission source transmits the signature information together with transmission information to a transmission destination. At the transmission destination, by checking the signature information by using a public key corresponding to the secret key, it is judged whether or not the received transmission information has been created by a proper transmission source.

[0004]

In recent years, attempts have been made to carry out electronic commercial transactions through a network by using an IC (Integrated Circuit) card. Here, in general, the data storage device, such as an IC card, holds a common key, and carries out input/output of secret information using a common key encryption system. In this sort of data storage device, such as an IC card, since the common key cannot become a key for creating signature information, there is merit in that, even in the case where the data storage device such as an IC card is lost, the damage can be kept at a low level.

[Summary of Invention]

[Problem to be solved by the invention]

[0005]

However, in order to safely carry out the electronic commercial transactions through the network, it is necessary to create signature information by using a secret key. However, in the conventional method, since the data storage device such as the IC card does not hold (store) the secret key, there is a problem that the signature information cannot be created. In this case, although it is also conceivable to adopt a method in which the data storage device such as the IC card holds the secret key, as described above, since the secret key can create the signature information, it has the same effect as certificate of a seal impression, and there is a problem that the level of damage is too high when the data storage device is lost and is used for an illicit purpose.

[0006]

In addition, if the electronic commercial transactions are carried out through the network by using only the common key encryption system adopted by the data storage device, such as an IC card, as described above, since numerous opposite partner server devices or the like of the transactions have the common key, there is also a problem that such a probability becomes high that the common key is stolen or is used for an illicit purpose.

[0007]

In the present electronic settlement system, SSL (Secure Socket Layer) or SET (Secure Electronic Transaction) is often adopted. However, in SSL, although safety of a communication path between a client device and a store device is assured, there is a problem that dishonesty at the store side cannot be detected.

[0008]

Although SET has both the merit of SSL and the merit that falsification cannot be done by the client device, the store device, and the settlement management device, since the respective devices must have certificates of the PKI, there are problems that it is troublesome and expensive. Further, signature and signature check must be performed many times, which is redundant.

[0009]

Moreover, the current electronic commercial transaction system does not include means of confirmation as to whether value information confirmed by the user on the client device is identical to value information actually written in the data storage device, such as the IC card.

[0010]

The present invention has been made in view of the problems of the prior art, and an object thereof is to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out by using a data storage device, such as an IC card, holding a common key, as well as a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium."

(2) "[0058]

The "electronic settlement system" is a system in which, in the case where a commodity or service is sold through an online communication system such as the Internet, payment settlement is electrically done through the online communication system. As a method of making the settlement through the online communication system, payment by a credit card, a cash card, or a debit card, or payment by electronic money such as a prepaid card is possible."

(3) "[0085]

The data storage device 20, such as an IC card, is such that for example, an IC chip is embedded in a card of plastic or the like. The data storage device 20 such as the IC card includes a tamper-resistant IC module 50 as shown in FIG. 2(A), and has a built-in processing circuit 51 and a built-in memory 52 in the IC module 50 as shown in FIG. 2(B)."

(4) "[0114]

The "settlement information" is created by the settlement management device 3 on the basis of the settlement request information transmitted from the store device 4 to the settlement management device 3, and includes various types of information for performing settlement by increasing or decreasing value information stored in the data storage device 20, such as an IC card, from the settlement management device 3 through the personal computer 22 as the client device and the reader/writer 21. The security of the settlement information is secured by the common key shared by the settlement management device 3 and the data storage device 20, such as an IC card. Further, the validity of the settlement information is secured in such a manner that a second signature created by using a secret key of the settlement management device 3 is affixed, and the personal computer 22 serving as the client device checks the second signature by using a public key corresponding to the secret key of the settlement management device 3."

(5) "[0136]

Next, a commodity information transmission sequence and a value information transmission sequence in the electronic settlement system of the embodiment using the common key, the public key, and the electronic signature and having high security will be described in detail with reference to FIGS. 9 to 11.

(Omitted)

[0141]

Step ST1:

Server authentication or mutual authentication using SSL (Secure Socket Layer) is performed between the personal computer 22 and the network server 40, and a secure communication path is established.

[0142]

Step ST2:

On a commodity selection screen as shown in FIG. 12, when the user 2 operates a keyboard, a mouse or the like of the personal computer 22 to determine a commodity which the user desires to purchase, commodity determination information corresponding to that is transmitted from the personal computer 22 to the network server 40.

[0143]

Step ST3:

When receiving the commodity determination information from the personal computer 22, the network server 40 transmits estimation information to the personal computer 22.

[0144]

Step ST4:

As shown in FIG. 13, the personal computer 22 displays on the display the estimation information received from the network server 40. In the case where the user 2 agrees to the estimation, a payment method is selected on the screen shown in FIG. 14. When the user 2 selects a settlement using electronic money by operating the keyboard or the like of the personal computer 22, a bill request is transmitted to the network server 40.

[0145]

Step ST5:

When receiving the bill request from the personal computer 22, the network server 40 transmits to the personal computer 22 settlement request information indicating the sum which the store device 4 charges the user 2, first signature information SIG1 created by using a secret key KSHOP,S of the store device 4 with respect to the settlement request information, and the interface program 24.

[0146]

Step ST6:

As shown in FIG. 15, the personal computer 22 displays on the display the sum indicated by the settlement request information received from the network server 40 in step ST5.

[0147]

Step ST7:

When the user 2 who agrees to the sum displayed on the display in step ST6 issues a predetermined instruction by using the keyboard or the like of the personal computer 22, the interface program 24 received from the network server 40 in step ST5 is started.

[0148]

When the user 2 puts the data storage device 20 such as the IC card to the reader/writer 21 in accordance with a screen display as shown in FIG. 16, the personal computer 22 uses the started interface program 24 to perform server authentication or mutual authentication using the SSL to the application server 30 of the settlement management device 3, and establishes a secure communication path.

[0149]

In the settlement system of this embodiment, when the settlement processing is performed, a screen to urge the user to wait as shown in FIG. 17 is displayed on the display of the personal computer 22.

[0150]

Step ST8:

The personal computer 22 transmits the settlement request information received from the network server 40 of the store device 4 in step ST5, and the settlement request information including the first signature information SIG1 with respect to the settlement request information to the application server 30 of the settlement management device 3.

[0151]

Step ST9:

When the application server 30 checks the first signature information SIG1 received in step ST8 by using, for example, a public key KSHOP,P read out from the information management server 32 and corresponding to the secret key of the store device 4, and judges that the first signature information SIG1 is valid information affixed in the network server 40 of the store device 4, the processing of step ST10 is performed.

[0152]

In the case where the application server 30 judges that the first signature information SIG1 is false, the application server ends the processing after, for example, it notifies the personal computer 22 thereof.

[0153]

Step ST10:

Next, the application server 30 of the settlement management device 3 transmits, for example, settlement request information to the security server 31.

[0154]

Step ST11:

When receiving the settlement request information from the data storage device 20, such as an IC card, the security server 31 performs mutual authentication with the application server 30, and creates a session key KSES from a common key KC shared by the data storage device 20, such as an IC card. Similarly, the data storage device 20, such as an IC card, also creates the session key KSES from the common key KC.

[0155]

Step ST12:

The security server 31 creates settlement information, encrypts this by the session key KSES, and outputs it to the application server 30. At that time, the security server 31 affixes a second signature created by using the secret key of the settlement management device.

[0156]

The application server 30 transmits to the personal computer 22 the settlement information including balance readout request (BRC) inputted from the security server 31.

[0157]

The personal computer 22 outputs the settlement information including the balance readout request BRC received from the application server 30 to the data storage device 20, such as an IC card, through the reader/writer 21.

[0158]

Step ST13:

When the settlement information including the balance readout request BRC from the personal computer 22 is inputted, the data storage device 20 decrypts this by using the session key KSES created in step ST11.

[0159]

The data storage device 20 reads out the settlement information including balance information BI from the tamper-resistant memory 52 in the data storage device 20, such as an IC card, by processing of the processing circuit 51 in accordance with the settlement information including the balance readout request BRC, and after encrypting this by using the session key KSES, the data storage device outputs it to the personal computer 22.

[0160]

The personal computer 22 transmits to the application server 30 the settlement information including the balance information BI from the data storage device 20, such as an IC card.

[0161]

The application server 30 outputs to the security server 31 the settlement information including the balance information BI received from the personal computer 22.

[0162]

The security server 31 decrypts the settlement information including the balance information BI inputted from the application server 30 by using the session key KSES and creates log information."

## No. 5 Judgment

According to the matters described in No. 4 (1), the technical field of the Invention

"relates to an electronic settlement system in which settlement processing, using a network or the like, can be safely carried out by using a data storage device holding a common key, such as an IC card, as well as to a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium".

The problems to be solved by the invention are as follows:

(A) "in the conventional method, since the data storage device such as the IC card does not hold (store) the secret key, there is a problem that the signature information cannot be created";

(B) in "a method in which the data storage device such as the IC card holds the secret key", "since the secret key can create the signature information, it has the same effect as certificate of a seal impression, and there is a problem that the level of damage is too high when the data storage device is lost and is used for an illicit purpose";

(C) "if the electronic commercial transactions are carried out through the network by using only the common key encryption system adopted by the data storage device, such as an IC card, as described above, since numerous opposite partner server devices or the like of the transactions have the common key, there is also a problem that such a probability becomes high that the common key is stolen or is used for an illicit purpose";

(D) in the SSL often adopted in electronic settlement, "there is a problem that dishonesty at the store side cannot be detected";

(E) in the SET often adopted in electronic settlement, "since the respective devices must have certificates of the PKI, there are problems that it is troublesome and expensive. Further, signature and signature check must be performed many times, which is redundant"; and

(F) "the current electronic commercial transaction system does not include means of confirmation as to whether value information confirmed by the user on the client device is identical to value information actually written in the data storage device, such as the IC card".

According to the above problems, an object of the invention is "to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out by using a data storage device, such as an IC card, holding a common key, as well as a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium".

The object of the invention in the present application, "to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out by using a data storage device, such as an IC card, holding a common key, as well as a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium", can be literally interpreted as an object "to use a data storage device, such as an IC card, holding a common key" in order "to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out, a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium", or can be interpreted as an object "to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out, a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium" on the assumption of "using a data storage device, such as an IC card, holding a common key".

However, as indicated in (B), even when "using a data storage device, such as an IC card, holding a common key", there is a problem in "providing an electronic settlement system in which electronic commercial transactions using a network can be safely carried out, a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium". Thus, the former interpretation is impossible. It is reasonable to consider that an object of the Invention is "to provide an electronic settlement system in which electronic commercial transactions using a network can be safely carried out, a settlement management device, a store device, a client device, a data storage device, such as an IC card, a computer program, and a storage medium" on the assumption of "using a data storage device, such as an IC card, holding a common key".

As matters corresponding to the above problems and object, the following matters are described in the Detailed Description of the Invention, as indicated in No. 4 (5):

A A secure communication path is established by server authentication or mutual authentication using SSL between the personal computer 22 and the settlement management device 3;

B "The personal computer 22" transmits "the settlement request information including the settlement request information and the first signature information SIG1 with respect to the settlement request information to the settlement management device 3";

C "The settlement management device" "encrypts information by the session key KSES" created "from a common key KC shared by the data storage device 20, such as an IC card", and

"transmits the settlement information including balance readout request (BRC)" "with a second signature created by using the secret key of the settlement management device"

"to the personal computer 22";
D "The personal computer 22" "decrypts" "the settlement information including balance readout request (BRC)" "using the session key KSES", and "reads out the settlement information including balance information BI from the tamper-resistant memory 52 in the data storage device 20, such as an IC card, by processing of the processing circuit 51 in accordance with the settlement information including the balance readout request BRC";
E "The personal computer 22" encrypts "the settlement information including balance information BI" read out from the tamper-resistant memory 52 in the data storage device 20, such as an IC card, by the session key KSES, and transmits "the settlement information including balance information BI" to the settlement management device.

According to the matters indicated in No. 2, the Invention specifies that "a data storage device acquires settlement information including balance information read from a tamper-resistant memory in the data storage device, through processing in accordance with the settlement information including a balance readout request received from the data storage device, and transmits the acquired settlement information to the electronic settlement management device", which corresponds to Matter D described in the Detailed Description of the Invention, but does not specify Matters A to C and E.

Considering that the memory holding a secret key or a common key inside is a "tamper-resistant memory", Matter D corresponds to prior arts which are problems to be solved by the Invention, and inherently includes the problems (B) and (C). Thus, it is not acknowledged that the problem of the Invention can be solved by Matter D.

Furthermore, the problem of the Invention other than the above problems is not described in the Detailed Description of the Invention in the Specification. Even in light of the common general technical knowledge at the time of the priority date, according to the Detailed Description of the Invention in the Specification, it is not recognized that the problem to be solved by the Invention is acknowledged.

Accordingly, it is not acknowledged that the Invention falls within a scope where the problem of the invention can be solved by a person skilled in the art based on the description of the Detailed Description of the Invention, or that the Invention falls within a scope where a person skilled in the art recognizes that the problem of the invention can be solved in light of the common general technical knowledge at the time of the priority date without description or indication in the Detailed Description of the

Invention.

Therefore, the Invention exceeds, in the Detailed Description of the Invention, a scope described so that a person skilled in the art recognizes that the problem of the invention can be solved, and does not satisfy the provisions of Article 36(6)(i) of the Patent Act.

No. 6 Examination on Appellant's allegation

1 Appellant's allegation

The appellant alleges in the written opinion submitted on September 13, 2019 that

"[4] Opinion on the reasons for refusal

(Omitted)

The amendment may produce an effect of the Invention, based on the description of the Detailed Description of the Invention, at least that convenience of users is improved by 'being selected from among a plurality of payment methods (0058)', and an effect that 'security is enhanced by using a tamper-resistant IC module 50 (0085)'. We consider that problems in convenience of users and security can be solved."

2 Examination

The matters described in [0058] and [0085] in the Specification of the present application, which are matters described in No. 4 (2) and (3), include the description, "as a method of making the settlement through the online communication system, payment by a credit card, a cash card, or a debit card, or payment by electronic money such as a prepaid card is possible", and the description, "the data storage device 20 such as the IC card includes a tamper-resistant IC module 50 as shown in FIG. 2(A)".

However, the Specification of the present application does not describe that a prior electronic settlement system has a problem in "convenience of users" or that an IC card used in an electronic settlement system has a problem in "security", and also does not include descriptions about an effect of improving convenience of users by allowing "payment by a credit card, a cash card, or a debit card, or payment by electronic money such as a prepaid card" in the Invention, and an effect of enhancing security by using an IC card "including a tamper-resistant IC module 50".

Therefore, the above appellant's allegation is not based on the Invention and the description of the Specification of the present application. Thus, the allegation cannot be accepted.

## No. 7 Closing

As described above, regarding this application, the description of the Scope of Claims does not satisfy the requirements stipulated in Article 36(6)(i) of the Patent Act.

Therefore, the appeal decision shall be made as described in the conclusion.

October 29, 2019

Chief administrative judge: WATANABE, Satoshi
Administrative judge: SATO, Satoshi
Administrative judge: ISHIKAWA, Shoji