Advisory opinion

Advisory opinion No. 2018-600018

Demandant	Quard Co., Ltd.
Patent Attorney	ICHIHARA, Masaki
Demandee	NTT DATA CORPORATION
Attorney	MASUNAGA, Hidetoshi
Patent Attorney	SATO, Mutsumi

The advisory opinion on the technical scope of a patent invention for Patent No. 3796528 between the parties above is stated and concluded as follows:

Conclusion

"CECSIGN (certification authority)" that is Article A does not fall within the technical scope of the invention of Japanese Patent No. 3796528.

Reason

No. 1 Object of the demand and History of the procedures

The object of the demand for the advisory opinion regarding the subject case is to demand the advisory opinion that Article A falls within the technical scope of Patent No. 3796528 (hereinafter, referred to as "the Patent").

The history of the procedures of the case is as follows.

Dec. 28, 1999	Patent application concerning the patent of the case
Apr. 28, 2006	Registration of the patent of the case
May 25, 2018	Request for Advisory Opinion of the case
Aug. 6, 2018	Written reply (Demandee)
Sep. 21, 2018	Written refutation (Demandant)
Jan. 21, 2019	Questioning (date of dispatch: Jan. 23, 2019)

Feb. 22, 2019 Written reply (Demandant)
Mar. 18, 2019 Written statement (Demandee)

No. 2 The patent invention

Since Demandant calls Claim 8 of the scope of claims of the patent of the case "the Patent", the patent invention is as follows, as viewed from the descriptions of the patent specification, as described in Claim 8 of the Scope of Claims.

"[Claim 8]

H A contents certification site device

A to perform certification that transmission information transmitted from a device of a sender in an encrypted state has been received and decoded by a device of a receiver via a network, the contents certification site device comprising:

B first reception means for receiving, from the sender device, sender signature data created by the sender performing electronic signature to data by which similarity of the contents of the transmission information transmitted by the sender device can be confirmed;

C second reception means for receiving, from the receiver device, receiver signature data created by the receiver performing electronic signature to data by which similarity of the contents of the transmission information received and decoded by the receiver device can be confirmed;

D storing means for storing the sender signature data received from the sender device and the receiver signature data received from the receiver device so as to perform contents certification; and

E means for collating, as part of the content certification, the data by which similarity of the contents of the transmission information transmitted by the sender device can be confirmed from among the sender signature data and the data by which similarity of the contents of the transmission information received and decoded by the receiver device can be confirmed from among the receiver signature data, wherein

F the data by which similarity of the contents of the transmission information transmitted by the sender device can be confirmed is limited to a digest of the transmission information transmitted by the sender device or a digest of the encryption information created by encrypting the transmission information, wherein

G the data by which similarity of the contents of the transmission information received and decoded by the receiver device can be confirmed is limited to a digest of transmission information received and decoded by the receiver device or a digest of

encryption information created by encrypting the transmission information."

Although the reference characters "A"-"H" are symbols assigned by Demandant of the advisory opinion for the purpose of separate descriptions, for the sake of convenience, these are utilized without change.

No. 3 Article A

Regarding "Article A", from the matter that Demandant of the advisory opinion alleges in the written request for an advisory opinion as of May 25, 2018 (hereinafter, referred to as "The Written Request") that:

"'Article A' is a third party organization (Evidence A No. 1, page 100, line 18, page 139, lines 10-11, and line 19) that is 'CECSIGN (certification authority)' (Evidence A No. 1, page 101, FIG. 5.1, and page 105, FIG. 5.4, and Evidence A No. 2): for which Demandee (hereinafter, also called 'NTT Data') is performing operation of the system in a manner faithfully following the guideline (Evidence A No. 1, pp. 138-139) concerning the Construction Industry Act (Evidence A No. 1, pp. 100-101 and 104-105); and which proves in 'securing originality' as a measure for a problem that there is no trace even if a contract matter is falsified, originality that is an index indicating conformance to intention of contractors (contract matter) supported by mutual electronic signatures of the contractors, as a certification action in 'third party organization' (Evidence A No. 1, page 100, line 18, and page 139, lines 19-20)." (page 5, lines 3-11), and,

from the description of Evidence A No. 2 of

"CECSIGN certification service verifier utilization rule

(Application of the present rule)

Article 1 'CECSIGN certification service verifier utilization rule' (hereinafter, referred to as 'the Rule') is a rule to define a contract relation between Construction-ec.com Co., Ltd. (hereinafter, referred to as 'the Company') and a person (hereinafter, referred to as 'verifier') who has received an electronic certificate (hereinafter, referred to as 'the Electronic certificate') issued by the Company in 'CECSIGN certification service' (hereinafter, referred to as 'the Service') from a party other than the Company." (page 1, lines 1-7),

also from the description of Evidence A No. 2 that

"Article 4 A verifier can, after confirming authenticity and validity of the Electronic certificate by a predetermined method designated by the Company, confirm, by confirming authenticity of the electronic signature of the user that has been carried out regarding digital data related to a designated transaction using a user public key

(hereinafter, referred to as 'User validation key') described in the Electronic certificate, whether the relevant digital data is created by the user in question, and whether or not the relevant digital data has not been changed or not." (page 2, lines 4-9),

also from the description of Evidence A No. 2 that

"4. As shown in the figure below, out of the information described in the Electronic certificate, the name of a user described in the item of 'CommonName' is a subject of certification in the certification system of Electronic Signature Act, and true/false confirmation thereof is performed by a method specified by CPS., and, although the information other than that is not a subject of certification of the same Act, the Company is performing true/false confirmation thereof by the method specified by CPS.

	識別情報項目	当社による真偽の確認	電子署名法の認定対象
1	氏名（CommonName）	CPS 所定の方法で確認 （住民票の写し、及び、印鑑登録証明書との照合）	対象
2	所属法人名 （organizationalUnitName）	CPS 所定の方法で確認 （利用法人の届出内容との照合）	対象外
3	所属部署名 （organizationalUnitName）	CPS 所定の方法で確認 （利用法人の届出内容との照合）	対象外
4	役職（Title）	CPS 所定の方法で確認 （利用法人の届出内容との照合）	対象外

識別情報項目　Identification information items
当社による真偽の確認　True/false confirmation by the Company
電子署名法の認定対象　Subject of certification in Electronic Signature Act
ＣＰＳ所定の方法で確認 Confirmation by a method specified by CPS
（住民票の写し、及び、印鑑登録証明書との照合）　(Comparison with Copy of residence certificate and Seal registration certificate)
（利用法人の届出内容との照合） (Comparison with notification contents by a user corporation)
対象　Subject
対象外　Not subject

" (page 2, lines 17-26),

also from the description of Evidence A No. 2 that

"(Confirmation of authenticity and validity of the Electronic certificate)
Article 5　In order to confirm authenticity of the Electronic certificate, a verifier shall confirm by a method specified by the Company, after having acquired a link certificate when an electronic certificate and a valid link certificate of the Company are being published from the repository, that an electronic signature of the Company has been

performed in relation to the Electronic certificate.

2. After having performed confirmation of the previous item, the verifier shall confirm each of the following matters by a method specified by the Company in order to confirm validity of the Electronic certificate.
(1) At the time of receiving the Electronic certificate, the term of validity of the Electronic certificate has not elapsed.
(2) At the time of receiving the Electronic certificate, the Electronic certificate has not lapsed.

3. The term of validity of the Electronic certificate is described in the item of 'Validity' of the Electronic certificate, and a verifier shall confirm, at the time of receiving the Electronic certificate, that the term of validity has not elapsed based on the relevant item. In this connection, the term of validity of the Electronic certificate shall be 366 days or 761 days. The term of validity of an electronic certificate signed by a CA signature key that corresponds to a former CA electronic certificate (the period of validity: Mar. 26, 2002 to Mar. 26, 2007) shall be 366 days or 396 days.
4. The Electronic certificate lapses at the time point that the Company registers revocation information of the Electronic certificate in an electronic certificate revocation list (Certificate Revocation List: hereinafter, referred to as 'CRL') specified by the Company, and the CRL after completion of the registration is published on the repository. A verifier shall confirm, after referring to CRL at the time of receiving the Electronic certificate and confirming that CRL is updated to the latest information, that the Electronic certificate has not lapsed. Note that, the Company updates CRL every 24 hours with the exception when the Service is stopped.)" (page 3, lines 1-24),

from the description in "Recommendation of Introduction of Electronic Contract -For Inter-enterprise E-commerce-, edited and written by NTT DATA Corporation and NTT Data Institute of Management Consulting, Inc., published by Software Research Center Co., Ltd., Apr. 10, 2004, the first print issue" which was cited in the questioning as of Jan. 21, 2019 (hereinafter, this is referred to as "Questioning") by the body, and a part of which was cited as Evidence A No. 1 by Demandant of the advisory opinion that

"4.4.2 Electronic registered seal and seal registration card

In performing electronic signature and verification of whether or not that signature is correct, a private key that corresponds to a registered personal seal in the real world, and a public key certificate that corresponds to a seal registration card are

required. A pair consisting of a private key and a public key are created by a person personally, and a public key certificate that proves that the public key has been created definitely by that person is issued from a reliable third party organization (certification authority).

This private key is very important for identifying a signatory, and thus it is necessary to manage this strictly. Although it is also possible to store a private key in a hard disk of a PC, there is a risk that the private key disappears by a failure or mis-operation of the hard disk, and also there is inconvenience that signature cannot be performed in a device other than the PC storing the key. For that reason, it is preferred to use an IC card or a token device that can be managed in a manner physically separated from a PC. If it is an IC card or a token device, access to a private key can be protected by biometrics such as a password and a fingerprint. Since, also when signature is carried out, signature data is created within an IC card or a token device, also there is no risk of outflow of a private key outward.

By enforcement of the Act on Electronic Signatures and Certification Business (hereinafter, Electronic Signature Act), in certificate issuing operations, a certification authority that satisfies a certain level such as in identity verification and operation rules can receive national authorization as a specified certification authority. In an electronic contract, it is also possible to use a certificate for which such authorization has not been given. However, when the admissibility of evidence regarding the certificate is questioned in a suit and the like, management of the certification authority will be also checked. For that reason, it is important to select a specified certification authority in which business operations such as operation rules and an identity verification method are specified securely.

CECTRUST supports 'CECSIGN certification service' for which Construction-ec.com Co., Ltd. performs issuing operations and 'TDB electronic certification service Type-A' for which Teikoku Databank, Ltd. performs issuing operations. The above certification authorities have acquired authorization of specified certification operations together." (page 83, line 1-the last line),

from the disclosure matter, which was cited in Questioning similarly and which is in the website of "Electronic Certification Authority Meeting", that

"In the specified certification operations, how to certify that 'electronic signature has been performed by a specific person'?

In the Electronic Signature Act, an operation to certificate whether or not an electronic signature is given by a very person is regarded as 'certification business', and certification business that is performed about ones, among electronic signatures, that

conform to the criteria prescribed by ordinance of the competent ministry as ones capable of being performed only by a specific person are defined as 'specified certification business'.(Article 2(3))

Note that, currently, the certification technology adopted in the standards of the 'specified certification business' is PKI technology using public key cryptography. (Ordinance for Enforcement of Act on Electronic Signatures and Certification Business, Article 2: Mar. 27, 2001, Item 2 of Ordinance of the Ministry of Internal Affairs and Communications/the Ministry of Justice/the Ministry of Economy, Trade and Industry)

In other words, business operations to issue an electronic certificate (public key certificate) for proving that an electronic signature is made by a specific person are 'specified certification business', and a third party organization that performs such business operations is called an 'electronic certification authority'.

Accredited certification business

In addition, in the Electronic Signature Act, a qualification system that is given to ones that clear stricter standards among 'specified certification business' is defined.

Certification business for which the following are recognized can receive qualification as 'specified certification business' by the competent minister (Minister of Internal Affairs and Communications, Minister of Justice, or Minister of Economy, Trade and Industry).

(I) Facilities provided for use in certification business conforms to the criteria, as provided by Ordinance of the Competent Ministry,

(II) The confirmation of identity of the user in the certification business is implemented by a method, as provided by Ordinance of the Competent Ministry, and

(III) certification business is performed by a method conforms to the criteria, as provided by Ordinance of the Competent Ministry. Usually, 'specified certification business' that receives the qualification is called 'accredited certification business'. In order to receive qualification of 'specified certification business', on-site investigation by the national government (and by a designated investigative body that conducts on-site investigation) regarding whether or not the above requirements are satisfied is needed. The term of validity of the qualification is defined by Cabinet Order.

In order to receive qualification continuously, it is necessary to undergo, before the term of validity of the qualification is ended, on-site investigation for receiving updated qualification by the national government and a designated investigative body. In the Electronic Signature Act, a business operator that performs

'accredited certification business' is referred to as an 'accredited certification business operator', and, generally, it is called 'accredited certification authority'.

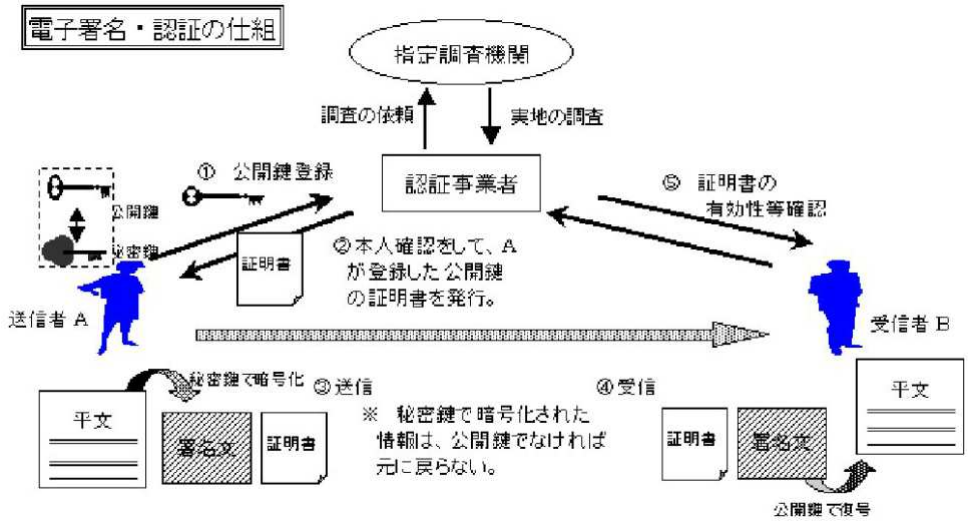
By receiving qualification, it can be said that it is confirmed by national government that an 'accredited certification authority' is operating in a manner satisfying strict standards." (http://www.c-a-c.jp/about/law.html), and

from the disclosure matter on the website of Ministry of Justice similarly cited in Questioning that

"2 Introduction of arbitrary certification system related to certification operations

Regarding certification business (business to certify that an electronic signature is made by a very person and the like), it is made in such a way that ones that satisfy a certain level (identity verification method and the like) may receive qualification of the national government, and can indicate the operations to which the qualification has been given to that effect, and, in addition, requirements for qualification, duty of an entity that receives qualification, and the like are determined.

--> To provide an indication for judging reliability of such as identity verification in certification business.



電子署名・認証の仕組　Mechanism of electronic signature and certification
指定調査機関　Designated investigative body
調査の依頼　Request for investigation
実地の調査　On-site investigation
認証事業者　Certification operator
公開鍵　Public key

秘密鍵　Private key
公開鍵登録　　Public key registration
証明書　Certificate
送信者　Sender
受信者　Receiver
本人確認をして、Ａが登録した公開鍵の証明書を発行。　　Perform identity verification to issue certificate of public key registered by A
平文　Plaintext
署名文　Signed text
秘密鍵で暗号化　Encryption by private key
送信　Transmission
受信　Reception
証明書の有効性等確認　　Confirmation of validity and the like of certificate
公開鍵で復号　　Decryption by public key
秘密鍵で暗号化された情報は、公開鍵でなければ元に戻らない。Information encrypted by private key is not restored without public key

" (http://www.moj.go.jp/MINJI/minji32-1.html),
Article A is recognized as having the following constitutions (hereinafter, referred to as 'Constitution a' and the like).

'a　A CECSIGN (certification authority) that is an accredited certification authority that issues an electronic certificate describing at least a name of a user and a public key (user validation key) of the user,

b　the CECSIGN (certification authority) comprising: a registration reception means for receiving a public-key registration request from the user;

c　identity verification means for performing identity verification of the user with respect to the request; and

d　issuance means for issuing, after the identity verification, to the user an electronic certificate in which at least the name of the user and the public key of the user are described, and to which an electronic signature of the CECSIGN certification (certification authority) is added, wherein

e　the user signs digital data concerning a designated transaction with a verifier using a private key of the user that forms a pair with the public key, and transmits the signed digital data together with the electronic certificate, wherein,

on the occasion that the verifier inspects the signature of the signed digital data having been received,

the verifier publicizes, so as to confirm authenticity of the electronic certificate, a link certificate to be used for inspecting the electronic signature of the CECSIGN (certification authority) added to the electronic certificate, and wherein

f the user updates an electronic certificate revocation list (CRL) to be used for confirming validity of the electronic certificate."

No. 4 Allegations of the parties

1. Demandant's allegation

(1) Demandant of the advisory opinion states in detail that, regarding each of the constituent components, Article A satisfies each of the constituent components, and the outline of the allegation is as follows.

A. Article A is a third party organization described and advertised, in an extract of a book "Recommendation of Introduction of Electronic Contract For Inter-enterprise E-commerce" (Evidence A No. 1) written by Demandee itself, that Demandee is performing operation of the system based on the guideline (Evidence A No. 1, pp. 138-139) (hereinafter, referred to as "the Guideline") related to the Construction Industry Act.

B. Therefore, Article A satisfies each of the constituent components including the constituent component E so long as it is faithfully following the Guideline.

2. The Demandee's allegation

(1) Article A does not satisfy the constituent component E.

A. Demandant of the advisory opinion alleges, after having alleged that, based on existence of Article 4(1) of CECSIGN certification service verifier utilization rule (Evidence A No. 2), the acts being performed by Article A include not only a service to issue an electronic certificate, but also performing each of the confirmation operations described in the provision in question, further that the constituent component E is satisfied because description of the provision in question and Article A are faithfully following the guideline concerning Construction Industry Act.

B. However, the subject of the provision is a "verifier", and "verifier" indicates "Construction-ec.com Co., Ltd. (hereinafter, referred to as 'the Company') and a person (hereinafter, referred to as 'verifier') who has received an electronic certificate

(hereinafter, referred to as 'the Electronic certificate') issued by the Company in 'CECSIGN certification service' (hereinafter, referred to as 'the Service') from a party other than the Company" (Article 1(1) of the same rule).

Accordingly, "CECSIGN (certification authority)" does not perform a confirmation operation described in Article 4(1) of the same rule. Furthermore, it does not inquire a verification value of a written contract proved by a signature of a sender and a verification value of a written contract proved by a signature of a receiver, and does not have means for the verification in question, and, therefore, it does not satisfy the constituent component E.

C. Meanwhile, although Demandee does not dispute expressly about sufficiency of the constituent components other than that, in the light of the gist of the whole allegation of the written reply and the written statement as of Mar. 18, 2019, it is understood that Demandee is alleging to dispute also regarding sufficiency of the other constituent components.

No. 5 Judgment by the body

1. Regarding sufficiency of each of the constituent components of the Patent Invention

(1) Regarding the constituent component A and the constituent component H

Article A is an "accredited certification authority", and is one that issues an "electronic certificate" that is used by a "verifier" (this corresponds to "receiver" in the patent invention) to inspect a "signature" added to "digital data to which a signature has been added" (this corresponds to "transmission information" in the patent invention) received from a "user" (this corresponds to "sender" in the patent invention), and that is transmitted to a "verifier" together with the "digital data", and

does not prove that the "digital data" have been decoded.

Therefore, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component A and the constituent component H.

(2) Regarding the constituent component B

Article A is one as pointed out in the above (1), and, thus, does not receive "the user signature data (this corresponds to 'sender signature data' in the patent invention)" made by the "user" performing an electronic signature to data by which similarity of the contents of "digital data" transmitted from the "user" can be confirmed.

Therefore, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component B.

(3) Regarding the constituent component C

Similarly, since Article A is one as has been examined in the above (1), it does not receive "verifier signature data" (this corresponds to "receiver signature data" in the patent invention) made by the "receiver" performing electronic signature to data by which similarity of the contents of "digital data" received by "receiver" can be confirmed.

Therefore, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component C.

(4) Regarding the constituent component D

As has been examined in the above (2) and (3), since Article A does not receive "the user signature data" and "verifier signature data", it does not store such data, either.

Therefore, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component D.

(5) Regarding the constituent component E

In Article A, although inspection of "signature" is carried out by the "verifier", confirmation of "similarity" of "digital data" is not performed.

Furthermore, the "verifier" indicates a person (hereinafter, referred to as 'verifier') who has received an electronic certificate (hereinafter, referred to as 'the Electronic certificate') issued by "Construction-ec.com Co., Ltd. (hereinafter, referred to as 'the Company') in 'CECSIGN certification service' (hereinafter, referred to as 'the Service') from a party other than the Company" (Article 1(1) of the same rule), and thus it does not mean "CECSIGN (certification authority)".

Therefore, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component E.

(6) Regarding the constituent components F and G

Since, in Article A, confirmation of "similarity" of "digital data" is not carried out as has been examined in the above (5), a "digest" of "digital data" to be used for the confirmation in question or a "digest" of data made by encrypting "digital data" is not used.

Accordingly, "CECSIGN (certification authority)" that is Article A does not satisfy the constituent component F and the constituent component G.

(7) Summary

As has been examined in the above (1)-(6), Article A does not satisfy any of the constituent components A to G.

2. Regarding Demandant's allegation

Although, as has been examined in the above 1., it is recognized that Article A does not satisfy any of the constituent components A to G, Demandant of the advisory opinion alleges repeatedly to the effect that, so long as it is faithfully following the Guideline, Article A satisfies the constituent components, and, therefore, the relevant allegation is examined hereinafter.

(1) A. In The Written Request, Demandant of the advisory opinion alleges as in 1) and 2) below.

"1) All of the following descriptions [1], [2], and [3] regarding data to be inspected ('original copy' described in FIG. 5.1 on page 101 of Evidence A No. 1, and FIG. 5.4 on page 105 of the same) which is managed (including utilization of a storing service) by the user (hereinafter, these [1], [2], and [3] are referred to as 'Confirmation actions') are descriptions about a third party organization that is CECSIGN (certification authority) that certificates, at any time after a transaction, originality that is an index to indicate conformance to mutual intention (contract matter) of contractors proved by mutual electronic signatures by the contractors (Evidence A No. 1, pp. 100-101, 104-105, and Evidence A No. 2) as a measure against a problem that there is no trace even if a contract matter is falsified (Evidence A No. 1, page 138, lines 33-34).

[1] A description (Evidence A No. 1, page 100-101) that 'since certification of originality even requires acquisition of certification from a third party organization', 'when certification of originality is needed to be acquired', 'it is certified in a rapid manner, by providing information on an original copy, that it has not been falsified' (Evidence A No. 1, page 100, line 17-line 22)

[2] A description (Evidence A No. 1, pp. 104-105, and 138-139) concerning a third party organization that performs an action that, in a manner faithfully following the guideline concerning Construction Industry Act that has an advantage of stamp duty reduction (Evidence A No. 1, page 104, lines 13-17), and as a certification action in a third party organization for securing originality (Evidence A No. 1, page 139, lines 19-20) that is a measure against the problem that there is no trace even if a contract matter is falsified (Evidence A No. 1, page 138, lines 32-34), regarding data made by '(2)

attaching an electronic certificate' to '(1) an electronic signature according to the public key encryption method' concerning a transaction, 'a record related to the record in question is stored in a third party organization, and certification of originality thereof can be given'

[3] Descriptions of A2, such as the description of Article 4(1) that 'using a public key of a user described in the certificate, it can be confirmed, by confirming authenticity of an electronic signature of the user that has been carried out regarding digital data concerning a designated transaction, whether the relevant digital data have been created by the very user, or whether alteration of the relevant digital data has not been performed'

2) The above 1) is supported by: the matter that CECSIGN (certification authority) is illustrated together with SecureSeal (originality assurance) (hereinafter, referred to as 'SecureSeal (originality assurance) server') and 'CECTRUST (delivery confirmation) or CECTRUST (original copy storing)' (hereinafter, referred to as 'CEC server') (Evidence A No. 1, page 101, FIG. 5.1, and page 105, FIG. 5.4); and the matter that, in any of: an example where the SecureSeal (originality assurance) server is a 'device nothing but one that issues a timestamp and inspects whether the issued timestamp has been issued by itself' (explanation of Demandee), the CEC server is a 'device nothing but one that inspects a timestamp issued at the time when a written contract is stored in the CEC server' after having performed 'delivery confirmation' (Evidence A No. 1, page 101, FIG. 5.1, 'CECTRUST (delivery confirmation)') before a contract is completed (explanation by Demandee), and the SecureSeal (originality assurance) server is illustrated together with the CEC server which is not used after the completion of the contract (Evidence A No. 1, page 100, line 17, 'original copy is stored in the company itself") (Evidence A No. 1, page 100-101); and an example where the SecureSeal (originality assurance) server is illustrated together with a CEC server that is a 'device nothing but one that inspects a timestamp issued at the time when a written contract is stored in the CEC server' after contract completion (Evidence A No. 1, page 104-105), at any time after contract completion, the confirmation action is performed (Evidence A No. 1, page 100, lines 17-22 of 'since certification of originality even requires acquisition of certification from a third party organization', 'when certification of originality needs to be acquired', 'it is certified in a rapid manner, by providing information on an original copy, that it is not being falsified', and Evidence A No. 1, page 104, lines 13-17 of '... it is faithfully following the Guideline'). Furthermore, the above 1) is supported from any of a matter that neither SecureSeal (originality assurance) server nor CEC server is a third party organization, and a matter that these are not ones that are faithfully following the

guideline." (page 5, line 13-page 7, line 6).

B. Demandant's allegation cited in the above will be discussed below.
(A) In Evidence A No. 1, there are the following statements.
"In TAISEI CORPORATION, a written order and an order acknowledgment in construction operations are computerized, and computerization is realized from procurement business operations to contract and billing operations. At the moment, 12 TAISEI CORPORATION branch offices and 800 or more cooperative companies all over the country are carrying out electronic contracts, and an electronic contract service is used for transmission of written orders and reception of order acknowledgments that number 17,000 times annually. Although a person in charge of each branch office issues an average of 120 written orders per month, for confirmation and reception of order acknowledgments to these written orders, the person will perform processing to a degree of 250 items per month. If these items are processed one by one using a web browser, this does not lead to improvement of business operations in computerization. For this reason, there has been established an original copy storing system incorporating an API that applies electronic signature to a plurality of electron documents in a lump and an API that performs transmission and reception to/from an electronic contract service in a lump (refer to FIG. 5.1).

The original copy storing system that satisfies visual readability and securing of originality indicated in the guideline by Ministry of Land, Infrastructure, Transport and Tourism has been developed by the company itself, and original copies are being stored in the company itself without using the electronic contract service. Since, regarding certification of originality, it is necessary to receive certification from a third party organization, an original copy is registered to the originality certification service using the electronic contract service, and only a certificate of originality assurance is being entrusted to the electronic contract service. Then, when receipt of originality certification is desired, a certificate of original copy certification that corresponds to an original copy is searched using the electronic contract service, and it is arranged so as to enable to prove that an original copy has not been falsified in a rapid manner by submitting information on the original copy stored in the company itself." (page 100, line 7-the last line), and,

in addition, in page 101 of Evidence A No. 1, there is disclosed, as "FIG. 5 .1 Utilization image of services between TAISEI CORPORATION and subcontractors", an image of utilizing "services" constituted of "CECSIGN (certification authority)", "CECTRUST (delivery confirmation)", and "SecureSeal (originality assurance)"

between "TAISEI CORPORATION" and "cooperative companies".

Furthermore, in Evidence A No. 1, there are the following statements.

"Since Daimei Co., Ltd. had determined to introduce electronic contracts, it started utilization of the electronic contract service CECTRUST in October 2003.

... (Omitted) ...

(2) Reason for selecting the realization method

The reason is that it is an ASP service faithfully following the guideline concerning "technical standards" stipulated in Article 13-2(2) of Ordinance for Enforcement of Construction Industry Act by Ministry of Land, Infrastructure, Transport and Tourism. A service that deals with a written contract needs to continue the service for a long term due to long storage years thereof, and therefore it is necessary to prepare for imperilment of an encryption method, and to change its function while making it conform to the needs and laws at that time. In addition, when essential functions are specified by a law or a guideline, and if it becomes a situation such as a situation where re-establishment of the service is needed fundamentally, investment for establishment is required once again. Therefore, if it is a service that faithfully follows a guideline specified by national government, there is no reason to worry about deviation from the measures of national government, and, by utilizing a service performed by a specialist of security, it is possible to reduce a risk of in-house development.

As another reason for the selection, a sense of trust that NTT Data is performing system operation is cited. NTT Data is a group member of NTT that is the largest customer of Daimei Co., Ltd., and they were in an order-taking and -placing relationship from the past, and, thus, it is said that there was a judgment by Daimei Co., Ltd. that, if it is a system operated by NTT Data, important written contracts can be entrusted thereto." (page 104, line 2-the last line)

In addition, on page 105 of Evidence A No. 1, there is disclosed, as "FIG. 5.4 Utilization image of the service between Daimei Co., Ltd. and the group companies", a drawing similar to that of "FIG. 5 .1" indicated above.

(B) In the statement contents of Evidence A No. 1 cited above, it is not described that "CECSIGN (certification authority)" that is Article A receives "digital data with signature" from both of "user" and "verifier", the relevant "digital data" are stored therein, and inspection is performed using "digest" of the relevant "digital data", and, in addition, such matter cannot be read from the description of Evidence A No. 1.

(2) A. When the response to the questioning by the body is taken in a good construction, it is understood that it is an allegation to the effect that CECSIGN (certification authority) has a function as "device [1]" described in "1" and "device [2]" in "2" of page 2 of the response, in addition to [3] that is a function as a accredited certification authority.

As a ground for allegation indicated above, Demandant of the advisory opinion alleges as follows.

"(A) According to a book (Evidence A No. 1) created by Demandee, Demandee is faithfully following the guideline concerning the Construction Industry Act cited above.

(B) According to the image diagrams on page 101 and page 105 of Evidence A No. 1, the system of Demandee based on the guideline includes three systems of 'CECSIGN (certification authority)', CEC server, and SecureSeal (originality assurance). However, according to the previous allegation of Demandee (Evidence A No. 4, Evidence A No. 6), the SecureSeal (originality assurance) server is a 'device nothing but one that issues a timestamp and inspects whether the issued timestamp has been issued by itself', and the CEC server is a 'device nothing but one that inspects a timestamp issued at the time a written contract is stored in the CEC server' after having performed 'delivery confirmation' (Evidence A No. 1, page 101, FIG. 5.1, 'CECTRUST (delivery confirmation)') 'before a contract is completed', and, therefore, if Demandee is following the guideline, it is only 'CECSIGN (certification authority)' that can take a role of a confirmation means for such as originality certification and the like described in the guideline.

(C) Then, if 'CECSIGN (certification authority)' is faithfully following the Guideline, the constituent components are satisfied as a matter of course."

B. Demandant of the advisory opinion has the burden of proof about CECSIGN (certification authority) having a function as "device [1]" and "device [2]".

However, even if reference is made to any of the written request for an advisory opinion, the written refutation, and the written reply to the questioning, it is not recognized as it is proved that CECSIGN (certification authority) has a function as "device [1]" and "device [2]".

In the guideline described in Evidence A No. 1 (this is referred to as "the Guideline" by Demandant of the advisory opinion), there exist descriptions to the effect

that a construction company should have a system to perform certification operations by attaching an electronic certificate issued by a "third party organization" to the other party of a contract (Evidence A No. 1, page 139, the part of (2)) and that it is effective to take a measure to enable receipt of certification of originality by a trusted "third party organization" (Evidence A No. 1, page 139, the part of (3)). However, there is no word existing to require that a "third party organization" that performs certification operations and a "third party organization" that performs certification of originality should be identical, and thus the Guideline is not one that excludes the constitution in which a third party organization that performs certification operations and a third party organization that performs certification of originality are of different bodies.

In addition, the description of the Guideline (3) (Evidence A No. 1, page 139, (3)) is only saying that "it is considered to be effective" for a construction company to store a record related to the record in question in a third party organization that is trusted, and take a measure to enable receipt of certification of originality, and thus it is not one that makes it mandatory to establish a system for taking the relevant measure.

Besides, Demandant of the advisory opinion has not shown an evidence that is worthy of judging that, if faithfully following the description of the Guideline, a third party organization for issuing an electronic certificate inevitably needs to take a constitution to assume confirmation means for, for example, certification of originality and the like.

Therefore, when interpreting from the described words of the Guideline, just because a party is faithfully following the Guideline, it cannot be necessarily said that "CECSIGN (certification authority)" needs to take a constitution to assume issuance of an electronic certificate and confirmation means for originality certification and the like.

Then, according to the description of "CECTRUST (original copy storing)" of FIG. 5.4 on page 105 of Evidence A No. 1, it is understood that "CECTRUST" can be configured in a manner having a function of "original copy storing" in addition to "CECTRUST (delivery confirmation)" described in FIG. 5.1 of page 101 of Evidence A No. 1, and therefore

it is interpreted that, in Evidence A No. 1, "original copy storing" is conducted, not in "CECSIGN", but in "CECTRUST", and

from the above examination, it cannot be read, from Evidence A No. 1, that CECSIGN (certification authority) has a function as "device [1]".

Therefore, although it is recognized that there is a description in the portion of "(3) Preservation of electromagnetic records and the like" of the guideline on page 139 of Evidence A No. 1 that "In addition, as needed, it is also effective to store a record

related to the relevant record in a trusted third party organization, and to take a measure to enable receipt of certification of originality", even based on the all the evidence (Evidence A No. 1 to No. 8-2) submitted by Demandant of the advisory opinion, it is not recognized that, as previously explained in the above "No. 3 Article A", CECSIGN (certification authority) has a function as "device [1]" and "device [2]".

No. 6 Closing

As described above, "CECSIGN (certification authority)" that is Article A does not belong to the technical scope of the Patent Invention.
Therefore, the advisory opinion shall be made as described in the conclusion.

May 16, 2019

Chief administrative judge: NAKAMA, Akira
Administrative judge: ISHII, Shigekazu
Administrative judge: SUDA, Katsumi