DocuSign®

Whitepaper

Court Support for Electronic Signatures in Japan

Table of contents

1/ Introduction

An Electronic Signature—a signature added by electronic means—is an important and critical tool to effectively execute documents, including commercial contracts, especially in today's business environment where companies need to communicate and transact more quickly and often remotely. Even though an Electronic Signature is not a mandatory requirement to execute a document, including an agreement, Japanese laws reaffirms the acceptability of Electronic Signature pursuant to the Act on Electronic Signatures and Certification Business (E-Signature Act, Act No.201 of May 31, 2000). Specifically, documents signed by an Electronic Signature can be submitted to a court as evidence of a party's assent to be bound by an agreement. Unless the valid formation of the document is in dispute between the plaintiff and the defendant, the court accepts the document with an Electronic Signature as acceptable evidence.

Further, the E-Signature Act provides an optional variation of an Electronic Signature, which has a heightened identity presumption for the signer, which is called a Digital Signature. In this type of Electronic Signature, a civil court presumes that the specific identified party that relied upon a Digital Signature validly executed the document.

To further encourage the use of Electronic Signatures in Japan, the Japanese government recently publicized announcements reconfirming and further encouraging the use of cloud-based Electronic Signature, such as DocuSign eSignature, as an acceptable method of generating Electronic Signatures.

This document provides detailed information on Electronic Signatures (including Digital Signatures) and how courts have supported such Electronic Signatures.

2/ Electronic Signature and Digital Signature

2.1/ Definitions of Electronic Signature and Digital Signature

The E-Signature Act has the following provisions:

Article 1
Statement of purpose of the Act—"smooth utilization of Electronic Signature"

Article 2
Definitions

Section 1: Definition of Electronic Signature—two factors to satisfy

Section 2: Definition of Certification Business—certification of the identity of the signer (a service that, in response to either a request of any person who uses the business [hereinafter referred to as the "User"] with respect to the Electronic Signature that he/she himself/herself performs or a request of another person, certifies that an item used to confirm that such User performed the Electronic Signature pertains to such User)

Section 3: Definition of Specified Certification Business—Certification Business that satisfy specific technical standards (performed with respect to an Electronic Signature that conforms to the criteria prescribed by ordinance of the competent minister as an Electronic Signature that can be performed by that person in response to the method)

Article 3
Assumption of validity of electronic records when an Electronic Signature satisfies a heightened identity requirement

Articles 4 to 47
Other provisions concerning Certification Business and miscellaneous provisions

2.1.1/ Electronic Signature overview

The "**E-Signature Act**" defines an Electronic Signature as a measure taken with respect to information that can be recorded in an electromagnetic record, a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers. An Electronic Signature further must satisfy both of the following requirements (Article 2(i)):

a. It must indicate that the information was created by the person who has applied the measure; and

b. It must be possible to detect whether any alteration has been made to the information or document (being tamper evident).

The E-Signature Act also provides, in Article 3, that electronic records, to which a heightened Electronic Signature with identity is affixed (a Digital Signature), will be assumed to be "validly created" by the signer associated with the Digital Signature, so long as it is assured that the Digital Signature is affixed by that signer through proper management of "codes and items." The term "codes and items" typically refers to electronic signing encryption key information, such as a digital certificate, that is issued to the specific individual desiring to sign with a Digital Signature, such as by the issuance of an identification card that includes an embedded digital certificate associated with that individual. Though courts provide a heightened identity assumption for such Digital Signatures, most companies still use a standard Electronic Signature because they are easier to implement and are similarly enforceable in court.

Note that, for documents created by public officers in the course of their duties, the assumption relating to Digital Signatures does not apply. Rather, a separate provision in the Code of Civil Procedures addresses the treatment of electronic documents with Electronic Signatures created by public officers.

To help further understand the difference between an Electronic Signature and a Digital Signature, the below table is provided.

Electronic Signature	**Digital Signature**
a. It must indicate that the information was created by the person who has applied the measure (e.g., login & password). b. It must be possible to detect whether any alteration has been made to the information (e.g., tamper evident).	a. It must indicate that the information was created by the person who has applied the measure (e.g., login & password). b. It must be possible to detect whether any alteration has been made to the information (e.g., tamper evident). c. It is assured that the Digital Signature is affixed only by that individual through proper management of codes and items (e.g., digital certificate is issued to the individual to use to generate the Digital Signature).
Documents can be submitted to courts as evidence.	Documents can be submitted to courts as evidence. Should a dispute occur as to the identity of the signer, documents are "assumed" to be validly created by that signer of the Electronic Signature, who used a digital certificate to generate the Digital Signature.

2.1.2/ Electronic Signatures

This definition of Electronic Signature is intended to ensure technical neutrality, without referring to any specific type or format of technology that must be used for the Electronic Signature. This typical approach to defining Electronic Signatures ensures that new forms of Electronic Signature may be used in the future. So long as both requirements are satisfied (e.g., ability to identify the user and the document is tamper evident), it is deemed an Electronic Signature. A good example of such a technological development is a cloud-based Electronic Signature service, such as DocuSign eSignature, where users upload documents to the service provider's cloud service and the service provider allows the user to affix the Electronic Signature within that service. Please note that the E-Signature Act and its relevant Ministerial Order does separately refer to the need to use specific types of technology, such as RSA, when the more specific use case of a "Specified Certification Business" is involved.

In furtherance of the continuing promotion by the Japanese government of broad use of Electronic Signatures in Japan, on 17 July 2020, the Ministry of Justice (MOJ) publicized an announcement[1] reaffirming the current interpretation of the E-Signature Act that use of a cloud-based service, such as DocuSign eSignature, is considered a valid use of an Electronic Signature. The MOJ specifically stated in the announcement that even if the service provider's signing key is used for cloud-based Electronic Signatures for documents, so long as the signing key is added automatically based on the signer's request to the service provider (e.g., on the website) without any interference by the service provider, such signature is deemed to be added by the signer, not by the service provider, and therefore deemed acceptable as the signer's use of the Electronic Signature. The MOJ further stated that if the service makes it possible to confirm the document signer and date of uploading as additional information, the entire process, including information added to the document, can be considered a "measure" to "indicate that the information was created by the person who has applied the measure." (Article 2(i)(a))

This MOJ announcement also reaffirmed that "there are variations of the level of identification and defense against misuse in each electronic signature service" and "it is appropriate to choose suitable services considering the nature of the agreement or necessary level of identification of the signer for the parties." Therefore, a cloud-based Electronic Signature service, such as DocuSign eSignature, is effectively considered a use of an Electronic Signature and is suitable as a valid mechanism for electronically signing documents. If the service also satisfies the heightened identity requirement as set out above (e.g., ability to allow the user to associate a digital certificate with the Electronic Signature to link the signer's identity with the Electronic Signature), such an Electronic Signature also will be attributed the heightened Digital Signature status.

Cloud-based Electronic Signature services, such as DocuSign eSignature, also partner with and support third party services, such as a certification authority, to streamline the generation of a Digital Signature. In particular, a signer using such a cloud-based Electronic Signature service can obtain a digital certificate from the certification authority, which may be integrated with the Electronic Signature service, and the signer uses the obtained digital certificate to generate a Digital Signature within the cloud-based Electronic Signature service.

Furthermore, the Ministry of Justice (MOJ) publicized on September 4, 2020 a question and answer (Q&A) resource regarding Article 3 of the Electronic Signature Act including on the topic of electronic contract services that are encrypted with the service provider's own signature key based on the user's instructions. (https://www.meti.go.jp/covid-19/denshishomei3_qa.html Japanese only) In this Q&A, MOJ clearly reiterated (1) what an electronic signature by the person in question is, (2) the relationship between electronic contracting services and Article 3, (4) what is required to properly manage the sign and property, and (5) what to keep in mind for choosing an electronic contracting service.

2.1.3/ Digital Signatures

Article 3 of the Electronic Signature Act states that when an electronic document (digital information) is presumed to be digitally signed by a person (e.g., the owner of the electronic document) through proper management of the signatures and objects necessary to sign the document, it shall be presumed that the owner of the electronic document has created the document. If it is found that the document has been electronically signed by the person (e.g., the person in whose name the document was created) by properly managing the signatures and the property, the document is presumed to have been created by the person in whose name the document was created.

The reason why Article 3 of the Electronic Signature Act is more stringent than Article 2 is that Article 3 creates a presumption of authenticity of the formation of an electronic document. In other words, in order to create such a presumption, it is necessary, as a precondition, that it is recognized that others cannot easily create the same Electronic Signature. For that purpose, it is believed that a reasonable technical level is required for the electronic signature in question. Therefore, the presumption rule of the Article would apply, for example, to digital signatures with sufficient cryptographic strength that others cannot easily create the same digital signature key. In order for an electronic contract service that encrypts electronic documents created by the user based on the user's instructions using the service provider's own digital signature key to fall under Article 3, it is necessary to ensure that the provision of the service does not leave room for the service provider's intentions to intervene technically and functionally. The user's intentions cannot be interfered with. The information must be encrypted based on the information provided by the service provider. The measures also taken by the service provider in the electronic document, including the accompanying information, must be considered to be a single measure, which makes clear that the measures are based on the user's intentions. MOJ reiterated that the service must meet an adequate level of indigenousness based on (1) the process that takes place between the user and the service provider and (2) the process that takes place within the service provider following the user's actions in (1).

Whether a sufficient level of inherent security is met will be judged by evaluating the security of the system or service as a whole, but for example, for the process in (1), if the system is equipped with a mechanism that requires users to be authenticated by two factors to take measures, then two-factor authentication could be considered to meet a sufficient level of uniqueness. In addition to entering a pre-registered email address and login password, users could also use their email address to send an SMS to their smartphone or use a token in their possession, etc. For example, a one-time password is authenticated by entering a one-time password obtained by a method.

With respect to the process (2), if a service provider encrypts an electronic document using the service provider's own digital signature key, it is considered to satisfy the requirement of uniqueness if it is evaluated as satisfying a sufficient level of uniqueness as a measure to show that the electronic document is created by the user in light of the strength of the encryption and a mechanism to ensure individuality of each user (e.g., the system processing is appropriately linked to the user), etc.

2.2/ Third party Digital Signature service—certification authority

The E-Signature Act also has provisions concerning certification authorities. However, the use of a certification authority is not a legal requirement for an Electronic Signature to become effective. Rather, a certification authority is a third-party service to assist in issuing digital certificates in order to assist a signer to generate a Digital Signature within a cloud-based Electronic Service Provider like DocuSign eSignature. In particular, a certification authority certifies the identity of the user of the Digital Signature by confirming that the signature key is linked to the signer, by which the Digital Signature then can satisfy the heightened identity requirement. Specifically, the certification authority verifies the specific identity of the signer and issues that signer a specific digital certificate tied to that signer, which then is used by the signer with the Electronic Signature service, like DocuSign eSignature, to generate a Digital Signature that is tied to the signer's identity.

The E-Signature Act defines the following three types of entities as certification authorities:

a. Certification Business;

b. Specified Certification Business; and

c. Specified Certification Business accredited by the government.

A Certification Business is a service to certify that an item used to confirm that a User affixed the Electronic Signature (e.g., a signature key), actually pertains to that User. The Specified Certification Business is a Certification Business that ensures a certain security level provided by the relevant regulation. One of the technological requirements for the Specified Certification Business is to use a public key cryptosystem that meets the standard provided in the Regulation (i.e., RSA, RSA-PSS, ECDSA or DSA). Such an entity/organization, however, is not required to apply for accreditation with the government. The Specified Certification Business that does obtain accreditation by the government will be afforded special legal status (e.g., automatic presumption of authenticity).

3/ The legal effect of an Electronic Signature

Under the Japanese Civil Code, contracts are validly formed if legally competent parties reach an agreement, whether they agree verbally, electronically or in a writing (i.e., on physical paper document). In other words, affixing a seal or signature (including Electronic Signature) on an agreement is not a legal requirement for the execution of an agreement.

However, to prove the formation of a valid contract in court where a legal dispute as to formation arises, parties may need to present evidence that they actually entered into the agreement. Verbal contracts or electronic contracts formed by email or simple click-through arrangements are more difficult to prove. The Code of Civil Procedures for courts does provide that a document signed by an individual, or to which an individual seal is affixed, is assumed to be executed and validly created by the individual.

An Electronic Signature service, such as DocuSign eSignature, is an effective tool to help establish the formation of an agreement. Further, as mentioned above, the E-Signature Act confirms that electronic documents, where a heightened Electronic Signature (Digital Signature) is used, results in an assumption that adequate evidence exists as to there being a validly created signature by the signer. That being said, in Japan, the principle of free evaluation of evidence applies to any civil procedure and the court can examine any type of evidence under this fundamental principle. The court may, at its discretion, accept and admit evidence which does not bear an Electronic Signature.

On 19 June 2020, the Japanese government published a document[2] summarizing questions relating to the execution of agreements under the COVID-19 situations and legal answers. In reaffirming the interpretation concerning formation of a contract and Electronic Signature, the document states the following:

- Agreements can be executed without a seal or written/electronic signature. However, if a seal or electronic signature is affixed to an agreement, the agreement is assumed to be created by the individual to which the seal or electronic signature belongs. That being said, in actual court cases, the court may reach a different conclusion if evidence that shows contrary to the assumption is submitted.
- Therefore, it is recommended that companies try to secure the means to prove the execution of agreements, including record of email exchanges, materials concerning the identity of the other party and use of an Electronic Signature service, like DocuSign eSignature, which includes an audit trail.

Further, should a heightened Electronic Signature be used to further link the identity of the signer with the Electronic Signature, that Digital Signature will have a higher level of deference in a court of law. As mentioned above, though this heightened assumption in certain circumstances may be desired, most users still rely upon standard Electronic Signatures and do not proceed with seeking to electronically sign with a heightened Digital Signature.

4/ What documents can be executed using an Electronic Signature

An Electronic Signature can be used not only for agreements, but also for other documents where a seal or signature is required. For example, the Companies Act provides that directors and company auditors must sign or affix a seal to the minutes of the board of directors meetings and meetings of company auditors. The Companies Act explicitly provides that an Electronic Signature can be used for that purpose.

On 29 May, 2020, the Ministry of Justice reaffirmed this point by issuing a notice stating that not only can an Electronic Signature be used where users use a physical item to assure that the electronic signature is affixed only by the individual (such as IC cards), but also that cloud-based Electronic Signature, such as DocuSign eSignature, can be used for the minutes of board of directors meetings and meetings of company auditors.

There are certain documents, however, for which an Electronic Signature cannot be used due to specific legal requirements for the notarization of those documents. Such documents include, among others:

a. Certain fixed term real estate lease agreements (Act on Land and Building Leases)

b. Voluntary guardianship contracts (Act on Voluntary Guardianship Contract)

c. Notarized testaments (Civil Code)

5/ Court decisions that support documents electronically signed

Although there are only a limited number of court decisions in Japan where the validity of an electronic document with an Electronic Signature was specifically questioned, Japanese courts generally have recognized the validity of electronic documents with Electronic Signatures and have provided the industry with a satisfactory level of confidence that Electronic Signatures are generally acceptable. Below are some examples of court decisions which specifically referred to evidence to which an Electronic Signature is used. Because the parties of these cases did not specifically argue the validity of documents, the court did not specifically examine whether the electronic signature is an Electronic Signature or a Digital Signature, but rather reaffirmed its validity by simply accepting the electronic documents as validly signed and proper evidence.

Tokyo District Court decision on 10 July 2019 (Hei 29 (wa) 11641)

The plaintiff of this case filed a lawsuit against the defendant and demanded payment of money based on a loan agreement executed between the parties. The Electronic Signature of both the plaintiff and the defendant was affixed to the agreement. However, the defendant in this case argued that the Electronic Signature was affixed by someone else and therefore was not executed by the defendant. The court found that the agreement was indeed executed by the defendant because there were no facts contrary to the assumption that the Electronic Signature was affixed by the defendant. The court accepted the plaintiff's claim and ordered payment under the loan agreement.

Tokyo High Court decision on 17 July 2018 (Hei 30 (Ne) 1766)

The plaintiff in this case filed this lawsuit to obtain a court order confirming that the plaintiff is the representative of the defendant. However, the defendant submitted as evidence an electronic version of the articles of incorporation to which an Electronic Signature of a public notary was affixed. The court found that a different person, not the plaintiff, was the representative of the defendant based on the electronic version of the articles of incorporation, and therefore dismissed the plaintiff's claim. Since the case turned on an issue unrelated to the Electronic Signature, the validity of the Electronic Signature was not specifically argued between the parties.

Disclaimer

The information in this White Paper is for general information purposes only and is not intended to serve as legal advice. It is limited to the laws of Japan. Laws governing Electronic Signature may change quickly, so DocuSign cannot guarantee that all the information in this White Paper is current or correct. Should you have specific legal questions about any of the information in this White Paper, you should consult a suitably qualified legal practitioner.

September, 2020

Notes

1 http://www.moj.go.jp/content/001323974.pdf
2 http://www.moj.go.jp/content/001322410.pdf

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040