Introduction
The COVID-19 pandemic has highlighted the necessity of digital transformation, and an increasing number of companies are using electronic contracts rather than contracts written on paper. However, the use of electronic contracts requires various considerations, including how to address the increased risk of using external vendors to successfully execute such contracts.

Background
In principal, under the Civil Code, agreements do not need to be in writing but may be verbal as well. However, once a dispute arises, the party alleging the existence of an agreement has the burden of proof in showing that an agreement exists. Failure to do so will result in a judgment that is favorable to the other party who denies that such an agreement exists.

Accordingly, for ease of proof and in order to prevent unnecessary disputes, agreements should be in writing and confirmed by both parties by affixing their seals to the agreement. For contracts on paper, the parties must physically affix their seals by signing the written contract. For electronic contracts, the parties must use an electronic signature to affix their seals.

Electronic signatures
According to the Act on Electronic Signatures and Certification Business (Electronic Signature Act), "electronic signature" means:

- A measure to be taken with respect to information that can be recorded in an electromagnetic record (a record that is prepared in an electronic form, a magnetic form, or any other form not perceivable by human senses and used for information processing by computers), which measure satisfies both of the following requirements:
  - The measure must indicate that such information was created by the person who took such measure; and
  - The measure must be able to confirm that such information has not been altered.

A comparison of physical seals and electronic signatures is set forth below:

<table>
<thead>
<tr>
<th>Parties</th>
<th>Physical seals</th>
<th>Electronic signatures</th>
</tr>
</thead>
</table>
| Affixing (signature) side | Placing a seal impression created in vermilion ink to a target paper document. | Adding:
- data called hash value that is converted from the target electronic data; and
- data of the electronic certificate to the target electronic data. |
Receiving side | Verifying by human eyes (of the receiving side) whether the placed seal impression is the same as that of the party who affixes the seal. | Verifying by software whether the electronic signature is that of the signer and has not been tampered with since the time of signature, via added hash value and/or data of the electronic certificate.

### Importance of Signer Identification

Verifying that the seal or signature is in fact that of the party to the contract itself is critically important when the situation enters the stage of disputes. According to Article 228, Paragraph 4 of the Code of Civil Procedure (CCP), a private document that is signed by, or bears the seal of, a principal or an agent, is presumed to have been duly executed. This is part of the so-called “dual presumption” theory that has been used to establish proof regarding the valid execution of a contract.

For example, in cases where a contract has been concluded between two companies, with both companies using physical corporate seals, the dual presumption is as follows:

(i) regarding a contract with a corporate seal impression, that seal is presumed to be affixed by the party to the contract (first de-facto presumption – established by court precedent); and

(ii) a contract with a seal affixed by the party to the contract is presumed to be duly executed (second presumption – provided for in Article 228, Paragraph 4 of the CCP).

As the dual presumption theory heavily relies upon the placement of the seal, it has become the standard for companies to use in important cases their corporate seal, which is registered with the Legal Affairs Bureau. Each party should be able to confirm that the seal used is registered with the Legal Affairs Bureau (i.e., by providing a certified copy of the authenticated corporate seal).

As for the electronic signature, however, the first de-facto presumption does not apply. In addition, Article 3 of the Electronic Signature Act provides for a presumption rule similar to the above second presumption although without the ability to provide authentication by the Legal Affairs Bureau. The first alternative is to issue electronic certificates for electronic signatures by third-party certification authorities. When certification authorities are involved, the function to identify the actor of an electronic signature is equivalent to that of a registered seal in the case of physically affixing a seal. However, the lengthy process to obtain such electronic certificates from a certification authority is one of the reasons why electronic signatures have not become widespread.

As a solution to this problem, businesses serve as certification authorities for electronic signatures, where a business issues an electronic certificate for its customer and stores it in a secure location (referred to as “remote signature style”). This practice is rapidly increasing. Based on the customer’s instruction, the business enters the electronic signature for its customer. Remote signatures are sometimes provided with an email certification (described below).

With regard to a risk of replication without permission, set forth below is a comparison between physical seals and electronic signatures:

<table>
<thead>
<tr>
<th>Physical Seals</th>
<th>Electronic Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seals produced in volume, such as a cheap seal or saturation seal.</td>
<td>Electronic signature using an algorithm with low cryptographic strength.</td>
</tr>
<tr>
<td>A hand-carved seal by a craftsmen.</td>
<td>Electronic signature using an algorithm with sufficient cryptographic strength.</td>
</tr>
</tbody>
</table>

### Tampering

When physically signing a contract written on paper, there is no function to detect whether the contents of the contract have been tampered with. However, it is relatively easy to determine if the contract was tampered with since it is on paper, and, in cases where multiple parties each have their own copy, the original may be compared with such copies to determine whether tampering exists.
On the other hand, it is not easy to detect traces of tampering in electronic contracts due to the nature of electronic data. In addition, when multiple parties each have their own electronic copy, it is difficult to distinguish which, if any, have been tampered with.

Email certification

In addition to electronic signatures, email certification also is used as a form of affixing of a seal.

Email certification focuses on the fact that an email address has a corresponding relationship with the person who uses the email address. For example, if an electronic contract is sent (or accepted) via email from the email address of party A, the transmission is presumed to have been made by party A, and the content of the contract is presumed to be based on party A’s intention.

Types of electronic contracts

Electronic contracts may be classified into the following types:

<table>
<thead>
<tr>
<th>Types</th>
<th>Contents</th>
<th>Points</th>
</tr>
</thead>
</table>
| Electronic exchange of a contract between the parties. | Party A sends data of a contract (e.g., PDF) to party B by email and makes an offer.  
Party B replies with the acceptance by email. | Low cost; easy to tamper with.                                           |
| Electronic contract with email certification by an electronic contract vendor. | Data of a contract and party’s A’s offer of the contract are sent to party B via the vendor.  
When party B sends its acceptance to the vendor, data of the contract is stored by the vendor. | Slightly difficult to tamper with.                                      |
| Electronic contract vendor uses email certification and remote electronic signature. | When the vendor stores data of the executed contract, the vendor affixes the electronic signature to the data according to the parties’ instructions. | More difficult to tamper with.                                      |
| Electronic contract to which local electronic signatures only are affixed. | When parties A and B exchange data of a contract, local electronic signatures are affixed to the data. | Similar to the business flow of a paper contract.  
More difficult to tamper with.  
Local electronic signature is not widely used, and the counterparty may not be able to affix an electronic signature. |
Deloitte Japan’s View

With telework becoming common due to the COVID-19 pandemic, there is a growing interest in using electronic contracts and electronic signatures to eliminate in-person meetings to sign contracts. However, it is essential to understand the legal issues before selecting an electronic verification vendor or setting up an internal system to verify electronic signatures.

Specifically, the following should be considered:

- A contract does not need to be written on paper under the Civil Code, and there is no specific requirement for using electronic contracts; as such, companies may choose an electronic contract platform that is compatible with their operations.

- Affixing a seal is not a requirement to conclude a contract, but a means to prove that the contract exists. As a result, companies may choose from various alternatives to affix seals, including electronic signatures and email certification.

Furthermore, with respect to electronic contracts, it is important to confirm that the requirements under the law concerning the preservation of electronic books are met, because if a tool provided by an electronic contract vendor does not meet the requirements, the company may need to take additional measures in order to comply.
Newsletter Archives

To see past newsletters, please visit our website at www.deloitte.com/jp/tax-legal-inbound-newsletter.

Subscribe to Japan Tax & Legal Inbound Newsletter and tax@hand

To automatically receive future newsletters, please email japan_taxlegal_inbound@tohmatsu.co.jp and register by providing your name, company, position, and email address.

Please visit www.taxathand.com or click here to download our tax@hand app to view newsletters and other content.

Contacts

Deloitte Tohmatsu Tax & Legal Inbound Client Services Team

Not all facts and circumstances are covered in this newsletter. If you have any questions regarding your specific situation, please contact one of the tax professionals at our Deloitte office in Tokyo or visit our website at www.deloitte.com/jp/tax-legal-inbound-services.

Jun Sawada, Inbound Client Services Leader

| Business Tax Services         | Sunie Oue, Partner |
| Indirect Tax Services         | Fumiko Mizoguchi, Partner |
| Global Employer Services      | Russell Bird, Partner |
| Transfer Pricing              | Samuel Gordon, Partner |
| Tax Management Consulting     | Sreeni Menon, Director |
| International Tax and M&A     | Masato Iwajima, Partner |
| Financial Service Industry    | Yang Ho Kim, Partner |
| Tax Controversy               | Kai Hielsher, Partner |
| Legal                        | Kaori Oka, Partner |
| Immigration                  | Kumiko Kawai, Partner |
| Payroll and Social Benefits Processing | John Dorff, Partner |
| Family Consulting            | Michael Tabart, Partner |

email to japan_taxlegal_inbound@tohmatsu.co.jp

Issued by

Deloitte Tohmatsu Tax Co.
Marunouchi-Nijubashi Building, 3-2-3 Marunouchi, Chiyoda-ku, Tokyo 100-8362, Japan
Tel: +81 3 6213 3800 email: tax.cs@tohmatsu.co.jp
Corporate Info: www.deloitte.com/jp/en/tax

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte network”). DTTL refers to the “Deloitte global network,” each member firm of which (and their related entities) is a legally separate and independent entity.

Deloitte Touche Tohmatsu Limited (DTTL), a member of the Deloitte network, is a global leader in providing audit and assurance, tax, legal, consulting, financial advisory, and risk advisory services.

Deloitte Touche Tohmatsu Limited is a global organization that offers a range of services designed to help clients achieve their business objectives and improve their performance.

The Deloitte network is made up of over 345,000 professionals in more than 150 countries and territories, providing audit and assurance, tax, legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500®.

These materials are copyright of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities, and may not be reprinted, duplicated, etc., without the prior written permission of the Deloitte network under relevant copyright laws.

Deloitte Touche Tohmatsu Limited

© 2022. For information, contact Deloitte Touche Tohmatsu Group.