AN OVERVIEW: ELECTRONIC SIGNING AND THE NEW "SIGN WITH SINGPASS" SERVICE IN SINGAPORE

Date: 30 April 2021

Singapore Corporate Alert

By: Christopher Tan, Charlotte Kouo, Nicholas Wee

This publication is issued by K&L Gates Straits Law LLC, a Singapore law firm with full Singapore law and representation capacity, and to whom any Singapore law queries should be addressed. K&L Gates Straits Law is the Singapore office of K&L Gates, a fully integrated global law firm with lawyers located in five continents.

With the COVID-19 pandemic accelerating the global shift toward digital transformation, the use of electronic signatures in place of traditional “wet ink” signatures has become more common. In Singapore, the enforceability of electronic signatures is governed by the Electronic Transactions Act (Chapter 88) (the ETA), which draws a distinction between electronic signatures, secure electronic signatures, and digital signatures. Further, as part of its National Digital Identity Smart Nation strategic project, the Singapore Government has introduced a new “Sign with SingPass” digital signing service which enables SingPass users to electronically sign contracts, agreements, and other legal documentation.

This article will explore the various methods of electronic signing and associated concerns.

ELECTRONIC SIGNATURES

The ETA clarifies that information documented in an electronic record is not to be denied effect, validity, or enforceability solely because it is an electronic record. In relation to the execution of documents, while the ETA does not expressly define “electronic signatures,” it does afford recognition to signatures made electronically as long as there is an appropriate and reliable method in which the signatory's identity and “intention in respect of the information contained in the electronic record” can be ascertained. Practically speaking, this means that as long as the aforesaid verification can be satisfied, execution by way of an electronic signature could be as simple as doing a copy and paste of an electronic image of a handwritten signature, creating a signature using a computer trackpad, or even typing one's name into the soft copy contract.

SECURE ELECTRONIC SIGNATURES: OVERVIEW

The challenge in relation to the above is of course the means to verify the appropriate and reliable method to ascertain the signatory's identity and intention in respect of the information contained in the electronic record.

Aside from recognizing electronic signatures, the ETA also recognizes a more enhanced type of signature applied using technological means: the “secure electronic signature.” An electronic signature will be regarded as a “secure electronic signature” for the purposes of the ETA if, through the application of a specified security

procedure or a commercially reasonable security procedure agreed to by the parties, it can be verified that it was, at the time it was made:

- Unique to the person using it.
- Capable of identifying such person.
- Created in a manner or using a means under the sole control of the person using it.
- Linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.

Whether or not a security procedure is commercially reasonable is dependent on the purposes of the procedure and the commercial circumstances at the time the procedure was used. In evaluating this, the relevant considerations include:

- The nature of the transaction.
- The sophistication of the parties.
- The volume of similar transactions engaged in by either or all parties.
- The availability of alternatives offered to but rejected by any party.
- The cost of alternative procedures.
- The procedures in general use for similar types of transactions.

Requiring the use of secure electronic signatures by the counterparty to a contract is beneficial as there is a statutory presumption under the ETA that (i) the secure electronic signature is the signature of the person to whom it correlates, and (ii) it was affixed by that person with the intention of signing or approving the electronic record. Such a legal presumption assists with alleviating certain risks associated with the use of electronic signatures in contracting (e.g., ascertaining the identity of the signing party and whether the electronic record/contract has been altered or tampered with). In contrast, electronic signatures (which are not secure electronic signatures) do not have the benefit of any similar presumption.

Nevertheless, it should be noted that the application of a secure electronic signature by one party does not automatically grant the same status to all other signatures in the same document. This is because each signature is evaluated on its own facts.

DIGITAL SIGNATURES

A digital signature, which is regulated as a specified security procedure, is defined in the ETA as:

> [A]n electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine: a. Whether the transformation was created using the private key that corresponds to the signer's public key; and b. Whether the initial electronic record has

> been altered since the transformation was made.

To better understand these requirements, we set out an illustrative example below:

- Party A and Party B wish to enter into a contract using their digital signatures. This means that there will be two digital signatures involved in the process. For the purposes of this illustration, we will focus on Party A signing the contract.
- Party A generates a private key for himself/herself and a public key to be shared with Party B. The public key will enable Party B to verify a signature subsequently created by Party A's private key. Taken together, the private key and the public key constitute a key pair.
- In respect of the contract, Party A then produces an algorithm mapping or translating one sequence of bits into another, generally smaller but unique set such that it would be computationally infeasible to be reproduced by any other algorithm (a hash or hashing) and encrypts the algorithm with the private key. Once Party A's hash has been encrypted, it becomes his/her signature to the contract.
- Party A will then send the contract and the signature to Party B.
- Upon receipt, Party B will commence his/her own hashing process, and Party B will use the public key to decrypt Party A's signature.
- To verify whether the contract has been altered since Party A's digital signature, Party B may compare his/her hash with the hash created by Party A. If they are the same, then Party B may rely on Party A's signature as a digital signature.

While a digital signature goes through layers of encryption and works to facilitate the safe sending of the signature, the relevant digital signature's authenticity cannot be verified. This is an issue that goes to the root of the digital signature's creation, and it is where the digital certification by a third-party authority is of importance.

A valid digital signature certificate refers to a record issued by an accredited or recognized authority for the purpose of supporting digital signatures that purport to confirm the identity or other significant characteristics of the individual who created a particular key pair. In our illustrative example above, a valid digital signature certificate for Party A would identify both Party A's information as well as his/her public key (which would have been sent to Party B). Digital signature certificates usually have validity periods and/or expiry dates, and they may also be revoked or suspended where necessary (e.g., if the person's private key is compromised). Further, the ETA provides that unless evidence to the contrary is adduced, the information (except for information identified as subscriber information that has not been verified) listed in a certificate issued by an accredited or recognized certification authority, or in a recognized certificate, is presumed to be correct if the certificate was accepted by the subscriber.

In this regard, it should be noted that a digital signature can achieve secure electronic signature status and, if so, will consequently trigger the advantageous legal presumptions under the ETA relating to secure electronic signatures, if:

- It was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate.

- The certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity, because one of the following apply:
  - The certificate was issued by an accredited certification authority.
  - The certificate was issued by a recognized certification authority.
  - The certificate was issued by a public agency approved by Singapore's Minister for Communications and Information to act as a certification authority on such conditions as he may by regulations impose or specify.
  - The parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

SIGN WITH SINGPASS

In 2003, the Singapore Government commenced the implementation of its digital identity system for Singapore residents and businesses registered in Singapore to conclude transactions digitally. As part of this initiative, the Government Technology Agency of Singapore (GovTech) launched the “Sign with SingPass” digital signing service on 5 November 2020. The service enables SingPass users to electronically sign contracts, agreements, and other legal documentation and is being introduced by Assurity Trusted Solutions Pte Ltd (Assurity), Singapore's National Certification Authority, in collaboration with DocuSign, iText, Netrust, Adobe, OneSpan, Dedoco, Tessaract.io, Kofax, and Modus Consulting.

Sign with SingPass is presently only available for specific documents and with certain government agencies (such as the Singapore Land Authority) and private sector businesses. Other businesses in the private sector may still register their interest to use the “Sign with SingPass” service.

GovTech has explained that Sign with SingPass allows SingPass users to use the SingPass mobile application to sign an electronic document by scanning a QR code specifically generated for that electronic document and applying a digital signature that is unique and cryptographically linked to the signer. It has also explained that digital signatures generated by Sign with SingPass will be issued certificates by Assurity and that, once signed, a cryptographically random, unintelligible, and irreversible code representing the electronic document will be transferred to the receiving party.

It would appear that a signature made via Sign with SingPass qualifies as a digital signature. However, as Assurity is presently neither an accredited certification authority nor a recognized certification authority, a Sign with SingPass digital signature is currently not recognized as a secure electronic signature for the purposes of the ETA. Nevertheless, GovTech's media releases appear to suggest that Assurity's accreditation under the ETA is in the works. Upon such accreditation, signatures made using Sign with SingPass will be regarded as secure electronic signatures.

EXCLUDED MATTERS AND OTHER CONSIDERATIONS

There are categories of transactions and documents to which certain provisions of the ETA do not apply. These are as follows:

- The creation or execution of a will.
- The creation, performance, or enforcement of an indenture, a declaration of trust, or a power of attorney, with the exception of implied, constructive, and resulting trusts.
- Any contract for the sale or other disposition of immovable property or any interest in such property.
- The conveyance of immovable property or the transfer of any interest in immovable property.

Depending on the relevant laws and legal requirements that govern the transaction/document, it may still be possible to execute such transactions/documents electronically. However, it will not be possible to benefit from the various statutory presumptions under the ETA.

On a concluding note, while the rise of electronic signatures affords parties greater convenience when transacting, parties should nonetheless be cognizant of the varying degrees of technological risks that can be associated with their use, as well as differences between the laws of different countries when contracting with an international counterparty or where the governing law of the contract is not specified to be Singapore law.

KEY CONTACTS

CHRISTOPHER TAN
PARTNER
K&L GATES STRAITS LAW LLC
SINGAPORE
+65.6507.8110
CHRISTOPHER.TAN@KLGATES.COM

CHARLOTTE KOUO
ASSOCIATE
K&L GATES STRAITS LAW LLC
SINGAPORE
+65.6713.0247
CHARLOTTE.KOUO@KLGATES.COM