ALLEN & OVERY

Covid-19 coronavirus: electronic signatures in the UAE

April 2020

IN BRIEF

As the impact of the Covid-19 coronavirus pandemic deepens there are clear impediments to a traditional signing process. Thankfully the use of electronic signatures can offer parties flexibility and efficiency in executing documents.

Electronic signatures are valid in the UAE, subject to certain conditions, and have been recognised since 2006. The use and admissibility of electronic records, documents and signatures in the UAE are governed by Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce (the E-Commerce Law).

This note looks at the essential requirements for using electronic signatures in the UAE and also considers a number of the practical questions which are likely to arise.

OVERVIEW OF ELECTRONIC SIGNATURES UNDER UAE LAW

Electronic signatures are broadly defined and include 'any letters, numbers, symbols, voice or processing system in electronic form applied to, incorporated in, or logically associated with an electronic message with the intention of authenticating or proving the same.'

A key principle of the E-Commerce Law is that a person can use any form of electronic authentication, as long as a specific law does not provide otherwise. If a signature is required on a document by law, this requirement will be satisfied by a reliable electronic signature.

Reliance on electronic signatures must be reasonable. Reasonableness will generally be based on the following:

– the nature of the underlying transaction and its value or importance to the parties (if known);

– the steps taken by the party relying on the electronic signature to verify its reliability;

– whether the party relying on the electronic signature took reasonable steps to verify if it is supported by a certificate, or if it should be expected to be so supported;

– whether the party relying on the electronic signature knew or ought to have known that it had been compromised or revoked;

– any agreement or course of dealings between the parties which relied on electronic signatures; and

– any other relevant factors.

WHAT EVIDENTIAL WEIGHT DOES AN ELECTRONIC SIGNATURE CARRY?

The E-Commerce Law provides that a signature in electronic form is admissible in evidence in legal proceedings. A range of factors will be considered when assessing its evidential weight.

This position is reinforced by Federal Law No. 36 of 2006 amending certain provisions of the Evidence Law in Civil and Commercial Transactions which provides that, 'electronic signatures shall have the same evidential weight as the signatures referred to in this law if they comply with the provisions prescribed in the E-Commerce Law'.

CA2003075

EXCLUSIONS FROM THE E-COMMERCE LAW

The E-Commerce Law does not apply to all transactions however, and the following are expressly excluded:

– transactions and issues relating to personal law such as marriage, divorce and wills;

– documents of title to immovable property;

– negotiable instruments;

– transactions concerning the sale and purchase of immovable property, and leases for over ten years (and the registration of any related rights);

– any document the law requires to be notarised by a notary public; and

– any other documents or transactions excluded by a special provision of law.

PROTECTED ELECTRONIC SIGNATURES

If an electronic signature process meets certain criteria, it will be deemed a 'Protected Electronic Signature'. A statutory presumption then applies that: reliance on the signature is reasonable; it is the signature of the person to whom it relates; and it was affixed by that person with the intention of signing or approving the electronic message to which it is affixed or associated. In such a case, the burden of proof will fall on the party seeking to disprove the electronic signature's validity, if the security of the signature can be established.

A document is executed by a Protected Electronic Signature where it is shown that an agreed prescribed or commercially reasonable 'Secure Authentication Procedure' is applied. As a result of that procedure it can be verified that, at the time the electronic signature was made, the signature was:

– unique to the person using it;

– capable of verifying the identity of that person;

– under the signatory's full control, whether in relation to its creation or the means of using it at the time of signing; and

– linked to the electronic message to which it relates, in a manner which provides reliable assurance as to the integrity of the signature so that if the record is changed, the electronic signature will become unprotected.

An example of a secure authentication procedure could be SMS authentication. This works by sending the relevant documents to the individual's email address, and requiring the person accessing the email to input an automatically generated, unique pin, which would be sent to the signatory's mobile phone. This further limits the risk that someone other than the signatory will access and sign the document. These additional safeguards should be recorded in the audit trail which will assist in disputing any claim that the document was not signed by the person purporting to have signed it. This method also provides an added layer of protection for confidential documents.

Reliance on a Protected Electronic Signature is deemed to be reasonable if there is no proof to the contrary.

CAN SOME PARTIES SIGN ELECTRONICALLY WHILST OTHERS SIGN BY HAND?

We are not aware of any prohibition under UAE law on using a combination of different methods of signature, ie, signing by hand (a 'wet ink' signature) and with an electronic signature.

If an electronic signing platform (such as DocuSign, a market leader in this field) is used, it is advisable for wet ink signatures to be uploaded to the system and therefore included within the audit trail and become part of the tamper-proof electronic original circulated to all parties. The other option is to create a composite original between the printed electronically signed document and the wet ink signed signature pages.

WHAT STEPS SHOULD BE TAKEN PRIOR TO USING ELECTRONIC SIGNATURES?

Consider if any of the parties are prevented from using electronic signatures

Each party contemplating signing electronically must have the necessary corporate capacity and authority to do so. In particular, it should be confirmed that there are no express exclusions relating to the use of electronic signatures in articles, board resolutions or other constitutional documents.

Internal policies should be considered, including those relating to document storage and whether there is a requirement for wet ink originals.

If the document needs to be filed with an authority or regulator, it should be confirmed that the relevant body will accept electronic signatures.

Confirm the counterparty's agreement

The E-Commerce Law does not require parties to accept information in electronic form, but it does state that a person's agreement to do so may be inferred from their affirmative conduct. With that in mind, a counterparty's agreement to the use of electronic signatures should be obtained. Since electronic signatures are not the market norm in the UAE, it is good practice to ensure that all parties are made aware that there will be an electronic signature. Always keep in mind what is practical and make sure the method is fully understood by all the parties well in advance of signing.

Where a counterparty to a transaction is a government body, the express consent of that body to use electronic signatures should be obtained. This is because the E-Commerce Law requires government bodies to give express consent to deal 'electronically' in transactions. Although it is not clear if this is intended to extend to the use of electronic signatures, our recommendation is that the express consent of a government counterparty is always obtained.

Should specific references to electronic signatures be incorporated in the document itself to ensure valid execution?

Whilst not strictly necessary, it is good practice to include language to this effect in any document that is to be signed electronically. This would be particularly the case for government entities.

What is the governing law of the document?

The analysis set out in this note applies to UAE law governed documents, and, subject to the exclusions and requirements noted, parties can be confident about the validity of using electronic signatures.

If the document in question is not governed by UAE law, then whether or not electronic signatures may be used is a question of the relevant local law, so the advice of local counsel should be sought on this. If the position is unclear, it is unlikely to be cost-effective to use electronic signing. Electronic signing is therefore only likely to be possible if the jurisdiction has legislation that explicitly permits the use of electronic signatures or there is consensus in the jurisdiction that electronic signatures are valid.

If the document is governed by English law, as may often be the case in the UAE, the key point is generally to ensure that it is executed in a way which is valid in the relevant company's jurisdiction of incorporation. If the provisions of the E-Commerce Law have been followed therefore, English law will consider it to have been validly executed by a UAE counterparty.

What about enforcing the document outside the UAE?

The next step is to consider where the assets crucial to the transaction are located and where parties might therefore wish to enforce the document. If this includes a jurisdiction other than the UAE, local counsel should be asked to confirm whether signing the document electronically may raise any issues (such as on enforcement).

Recognition of foreign certificates and electronic signatures

Provided the laws of foreign jurisdictions require the same level of approval as the E-Commerce Law, electronic signatures meeting those legal requirements will be recognised and treated in the same way as electronic signatures issued in accordance with the E-Commerce Law.

Local counsel should be consulted on the approval process for electronic signatures outside the UAE however and it should be confirmed that a foreign counterparty has the requisite authority to use an electronic signature to sign a UAE law document. Authority is determined by the relevant local law. The authority of a signatory under local law may depend on them signing in a certain way or following certain formalities which may affect their ability to sign electronically.

Consider information security risks

If an electronic signing platform is to be used to manage electronic signings, parties should consider whether the relevant platform meets any information security requirements they may have. Some entities (such as financial institutions) require the highest standards of encryption when confidential information is being uploaded to third party sites. The default configuration offered by many electronic signing platforms does not meet these requirements.

Are there any additional evidential requirements?

To reduce the risk that a signatory is not who they purport to be, an electronic signing platform which offers functionality to create an evidential trail that records when documents are signed and the IP addresses that

access them should be used. In addition, the system should be capable of recording any changes to the signing process such as a change of signatory after the documents have been sent out or an amendment to a recipient's details. Additional evidence could be required if the validity of a document were ever disputed.

WHAT HAPPENS AFTER SIGNING?

What constitutes an original following an electronic signing?

The distinction between original and copy documents is important for document retention, for evidential purposes and for certification, filing and registration purposes.

Whilst the E-Commerce Law does not expressly address what constitutes an original signature, our view is that:

– when using an electronic signing platform where the documents are held and signed in electronic form, the electronic document within the electronic signing system should be considered as an original; and

– if the parties intend to create multiple originals in electronic and/or hard copy form, then it should be possible to have multiple originals of a document (in the same way as parties may sign multiple physical originals to enable each party to have their own). There should be clarity regarding the parties' intentions to create multiple originals when agreeing the signing procedure. All parties to the transaction should confirm in the relevant transaction documentation that each signed, dated document shared with the other parties will constitute an electronic original.

Storage and record keeping

The general position under the E-Commerce Law is that records can be retained solely in electronic form, subject to certain minimum requirements.

If an electronic signing platform is used, for document security and data protection reasons our recommendation is that once fully signed, original executed documents should be downloaded and removed (ie, deleted) from the signing platform.

Where a document has been executed electronically, can amendments be made to it electronically?

The E-Commerce Law is silent on its application to amendments to documents. However, the principles for electronic amendments should be the same as the principles for electronic documents and signatures in the first instance ie, electronic signatures are only enforceable in the event that the principles of the E-Commerce Law are complied with. Provided then that the E-Commerce Law is complied with, amendments to documents in the form of an amendment agreement signed electronically should be valid and enforceable in the UAE.

This note is for general guidance only and does not constitute definitive advice. If you would like to discuss this in further detail, or if you have any related queries, Tom Butcher or Rachael Ashley would be happy to speak with you.

KEY CONTACTS

Tom Butcher
Partner – UAE
Tel +971 2 418 0414
tom.butcher@allenovery.com

Rachael Ashley
Senior Associate – UAE
Tel +971 4 426 7189
rachael.ashley@allenovery.com