Digital Signature Regulations in the UAE

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

Fadi Kilani
F.Kilani@tamimi.com - Sharjah, UAE

What is a digital signature? How is it different from an electronic one? In a world where new technological solutions materialise on a daily basis, users often find themselves confused by the number of options at their disposal, also confused about whether those solutions are regulated by domestic laws or not, understanding the difference between a digital signature and an electric signature is important to know as well as how regulated they are.

History of signatures

Taking a look back at the changing face of the signature from the distant past right through to present-day, the following explores how have signatures evolved throughout history?

1. Ancient signature

- The first known use of signatures was by the Romans around 400 AD.
- In 1677, the State of Frauds act was passed by the English Parliament which made signature the marker of everyday as tell today. This law stated that contracts must be signed. One hundred years later, around the world, signatures became a requirement in order to make contractsbinding. .

2. Modern signature

- Stepping into the 1980s, the role of the signature changed as a result of the rapid changes in technology. The rise of the fax machine meant more contracts were being scanned and sent electronically, and legislation in both the United States and United Kingdom changed to adopt the different use in such technology;
- in 1996 the United Nations Commission on International Trade Law (‘UNCITRAL’) adopted the Model Law on Electronic Commerce, which was the first legislative text to adopt the fundamental principles of non-discrimination, technical neutrality and functional equivalence which are considered to be founding elements of modern electronic law.
- the EU regulation on Electronic Identification, Authentication and Trust Services (‘eIDAS’) which oversees electronic identification and trust services for electronic transactions in the EU’s internal market entered into force in 2014 (and became effective from 1 July 2016). EIDAS has created standards for which electronic signatures, qualified digital certificates and other proof of authentication mechanisms offer electronic signatures the same legal standing as a transaction that is documented in a hard copy.

3. UAE Regulations

- in 2002, the Emirate of Dubai issued the Electronic Transactions and Commerce Dubai Law No. (2) of 2002;
- in 2006, The United Arab Emirates issued the Federal Law No. (1) of 2006 Concerning E-transactions and e-commerce;
- Federal Law No. (36) of 2006 was issued to amend Federal Law No. (10) of 1992 The Law of Evidence in Civil and Commercial Transactions by adding Article (17-bis), which gives the electronic signature the

same probative force given to the original signature.

Is there a difference between electronic signature and digital signature?

Very generally, “electronic signature” is a broad term referring to any electronic process that indicates acceptance or approval of an agreement or a record. An electronic signature would encompass a simple digital scan of a ‘wet signature’ through to a much more sophisticated authentication mechanism. A “digital signature” is one specific type electronic signature.

Typical electronic signature solutions use common electronic authentication methods to verify signer identity (e.g. as an email address, a corporate ID, or a phone PIN). If increased security is needed, multifactor authentication may be used.

Digital signatures use certificate-based digital identifiers (generated and authenticated by public key encryption) to authenticate signer identity and demonstrate proof of signing by binding each signature to the document with encryption. Validation occurs through trusted certificate authorities or trust service providers.

Digital signatures, like handwritten signatures, are unique to each signer. Digital signature solution providers currently follow a specific protocol, called PKI (Public Key Infrastructure). PKI requires the provider to use a mathematical algorithm to generate two long numbers, called keys. One key is public, and one key is private.

When a signer electronically signs a document, the signature is created using the signer’s private key, which is always securely kept by the signer. The mathematical algorithm acts like a cipher, creating data matching the signed document, called a hash, and encrypting that data. The resulting encrypted data is the digital signature. The signature is also marked with the time that the document was signed. If the document changes after signing, the digital signature is invalidated.

Digital Signatures have sophisticated and complex encryptions which do not allow for any kind of manipulation of the signed documents.

In brief, all digital signatures are electronic, but not all electronic signatures are digital.

The UAE Regulations

Back to regulation developments in the UAE concerning electronic signatures:

Federal Law No. (1) of 2006 Concerning E-transactions and E-commerce (‘ETL’), defines Electronic Signature as

> “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 approving the same.”
> Under the ETL a person may rely on an Electronic Signature to the extent that such reliance is

reasonable. In determining whether it is reasonable for a person to have relied on an Electronic Signature, regard must be had, if appropriate, to the following (see Article 18 of ETL):

(a) the nature of the underlying transaction which was intended to be supported by the Electronic Signature;

(b) the value or importance of the underlying transaction, if this is known;

(c) whether the reliant party, in respect of the Electronic Signature, has taken appropriate steps to determine the reliability of the Electronic Signature;

(d) whether the reliant party, in respect of the Electronic Signature, took reasonable steps to verify if the Electronic Signature was supported by an Electronic Attestation Certificate, or if it should be expected to be so supported;

(e) whether the reliant party, in respect of the Electronic Signature, knew or ought to have known that the Electronic Signature had been compromised or revoked;

(f) any agreement or course of dealing between the originator (i.e. the person by whom, or on whose behalf, the data message containing the Electronic Signature is sent) and the reliant party, or any trade usage which may be applicable; and

(g) any other relevant factors.

In practical terms, when considering how best to implement electronic signatures it is recommended to use a solution that is likely to meet as many of the Article 18 criteria as possible.

The ETL expressly contemplates the use of digital signatures.

An Electronic Attestation Certificate is defined under the ETL as “a certificate issued by a Certification Services Provider confirming the identity of the person or entity holding an Electronic Signature creation tool”.

A Certification Service Provider (‘CSP’) is defined as “an accredited or authorised person or organisation that issues Electronic Attestation Certificates, or provides other services in this regard”. A CSP is required to be licensed by or registered with the Telecom Regulatory Authority (‘TRA’), and the current process contemplates a licensing system for local entities wishing to be recognised as CSPs under the Electronic Transactions Law, and a registration system for foreign entities wishing to be recognised by the law.

Presently, CSPs registered with the TRA include: Adobe, Lleida, Palaxo, Ascertia, First Abu Dhabi Bank, Digital Trust and Docusign.

Accordingly, using a CSP’s electronic signature and digital certification solution will enhance the reliability of an electronic signature under the ETL

The ETL also provides for a “Secure Electronic Signature”. An Electronic Signature will be treated as a Secure Electronic Signature, if, through the application of prescribed or commercially reasonable Secure Authentication Procedures agreed to by the parties, it can be verified that an Electronic Signature was, at the time it was made:

(a) limited to the person using it;

(b) capable of verifying the identity of that person;

(c) under that person's full control, whether in relation to its creation or the means of using it at the time of signing; and

(d) linked to the electronic message to which it relates, in a manner which provides reliable provides reliable assurance as to the integrity of the Electronic Signature.

In the absence of proof to the contrary, reliance on a Secure Electronic Signature Electronic Signature is presumed to be reasonable under the Electronic Transaction Law (and that the Secure Electronic Signature is the signature of the person to whom it relates).

"Secure Authentication Procedures" are procedures aimed at verifying that an electronic message is that of a specific person and detecting an error or alteration in the message, content or storage of an electronic message or Electronic Record from a specific point in time may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgement procedures, or similar information security devices.

In order to determine whether Secure Authentication Procedures are commercially reasonable, such procedures shall be considered in the commercial circumstances at the time of use thereof, including:

(a) the nature of the transaction;

(b) the experience and skill of the parties;

(c) the scope of similar transactions conducted by either or both parties;

(d) the presence and cost of alternative procedures; as well as

(e) generally used procedures in similar types of transactions.

It is important to understand that the ETL does not expressly deem that having an Electronic Signature supported by an Electronic Attestation Certificate issued by CSP to be a Secure Electronic Signature.

While it may well be that having an Electronic Attestation Certificate issued by CSP will be a Secure Authentication Procedure, it remains open under the ETL for it to be determined in individual cases if it is a commercially reasonable Secure Authentication Procedure.

It is also important to understand that not all the electronic signature solutions offered by licensed CSPs in the UAE are supported by qualified digital certificates that would mean that they would be considered the equivalent of handwritten signatures under the EU eIDAS regulations Accordingly, due diligence on what CSP, and more particularly, what solution is to be used, is recommended in order to get the maximum benefit of the UAE law.

Enhancing the reliability of the electronic signature solution is critical, as in assessing the evidential weight of electronic information, due regard will be paid by the Court (under Article 10 of the ETL) to the following:

(a) the extent of the reliability of the manner in which one or more of the operations of executing, entering, generating, processing, storing, presenting or communicating was carried out;

(b) the reliability of the manner in which the integrity of the information was maintained;

(c) the extent of reliability of the source of information, if identifiable;

> (d) the extent of reliability of the manner in which the identity of the originator, if relevant, was ascertained; and
>
> (e) any other relevant factor(s).

Finally, it is important to recognise that Article 6 of the Electronic Transactions Law provides that nothing in the ETL requires a person to use or accept information in electronic form, but a person's agreement to do so may be inferred from the person's affirmative conduct.

Consequently, it is recommended that a contracting party wishing to rely on an electronic signature incorporates specific reference to the use of a particular electronic signature solution in the contract documentation, so that there will be less likelihood that another party can challenge the use and reliability of the electronic signature. A court should also recognise that the parties' agreement that the use of electronic signatures, and that a particular electronic signature solution provider is considered reliable.

Conclusion

While the ETL refers to electronic signatures only, the provisions in the law for Electronic Signatures to be supported by electronic attestation certificates issued by CSPs and secure Electronic Signatures that use secure authentication procedures actually contemplates what have become more colloquially known as "digital signatures". Further the ETL indicates that digital signatures are the most reliable electronic signatures under that law.

That does not mean that use of digital signatures is necessary in every case. As discussed above, under the ETL reliability (and presumptions of reliability) is determined by a number of factors including the nature and value of the underlying transaction and commercial reasonableness. So, for low risk and low value transactions a simple Electronic Signature can be viable.

The enhanced reliability afforded to digital signatures under the ETL does not mean that simple Electronic Signatures are not reliable. It simply means that if the reliability of an Electronic Signature were challenged in court, the party relying on that signature would need to establish it is reasonable for them to have done so in that particular case.

While the ETL has been in force since 2006, the uptake of Electronic Signature solutions (particularly CSP solutions or digital signatures) has not been widespread in the UAE. However, the current COVID-19 circumstances, and the need to undertake transactions remotely, has significantly increased the usage of Electronic Signatures, and the courts will be required to have a greater understanding of Electronic Signatures and digital signatures and their reliability. In addition, we understand that there are likely to be changes to the laws to further support the use of electronic and digital signatures.

For further information, please contact Fadi Kilani (f.kilani@tamimi.com) and Andrew Fawcett (a.fawcett@tamimi.com).