ARTICLE:

# Challenges of authentication and certification of e-awards in Dubai and before the Dubai International Financial Centre courts: the electronic signature

By **Omar Husain Qouteshat**

This article evaluates whether an electronic signature is sufficient to fulfil the authentication requirement stated under the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958) (NYC) article IV(1)(a) before the Dubai and Dubai International Financial Centre (DIFC) courts. Dubai is one of the few countries with two jurisdictions in one country. The party who is seeking the enforcement of the award in Dubai may enforce it before the Dubai or the DIFC courts, so the purpose of the comparison is to discuss whether the winning party may benefit from the DIFC. To achieve the objective of the study, this paper evaluates the ability to exclusively rely on secured electronic signatures to fulfil the requirement stated under article IV(1)(a), and to generally consider the validity of the electronic signature in the Dubai and DIFC courts.

## Introduction

The enforcement of the arbitral award is the final and the most important step in arbitration procedures. Upon completion, the winning party will seek to enforce the arbitral award, otherwise the whole process of arbitration is nullified. The final award is recognised and enforced equally as a court judgment, but the importance of arbitration is that its enforceability is easier at the international level than court decisions, due to the international treaties and conventions entrenching the enforcement and recognition of the arbitral award. The Convention on the Recognition and Enforcement of Foreign Arbitral Awards (NYC) is the most widespread and successful arbitration convention in many jurisdictions. Article III of NYC states that the arbitral award shall be considered as binding and enforceable in each contracting state that guarantees the enforcement and recognition of foreign arbitral awards in countries ratifying the Convention.

The NYC provides for the recognition of arbitral awards by excluding any review of the merits of foreign awards. On the other hand, it stipulates a number of provisos to be considered during enforcement, such as the duty of the party seeking enforcement to supply the court at the time of application with an authenticated original or duly certified copy of the award and arbitration agreement. This might raise some enforcement issues, as discussed in detail below. One of the most effective and efficient solutions to authenticate the electronic award in online arbitration is the electronic signature, which might be useful in enforcing the arbitral award. However, its application depends on whether the courts in the enforcement country validate and recognise such a process.

Consequently, the article begins by explaining the authentication and certification of arbitral award in accordance with the NYC rules. It goes on to explore the differences between authentication and certification, and to identify some issues that might arise such as the governing law, the competent authority and the required documents. These concerns might arise at the enforcement stage, since the NYC is silent toward them, which may mean that different interpretations are possible. These issues will be discussed with special reference to the approach of the Dubai and Dubai International Financial Centre (DIFC) Courts.

The second part seeks to clarify the meaning and requirements of the electronic signature, and explains the different types and legislative approaches toward electronic signatures. In respect of the validity of electronic signatures under Dubai and DIFC legislation, the article explores and critically analyses the provisions of the United Arab Emirates (UAE) Federal Law 1/2006 on Electronic Transactions and Commerce (ETCL) in Dubai to test the ability to rely on the electronic signature as a valid method to authenticate electronic awards before the Dubai courts. Moreover, the last section examines the validity of the electronic signature before the DIFC courts.

## Authentication or certification of the award under the NYC

The NYC states the required procedures and documents necessary to enforce and recognise an arbitral award. Article IV provides that:

> 1. To obtain the recognition and enforcement mentioned in the preceding article, the party applying for recognition and enforcement shall, at the time of the application, supply:
>
> (a) The duly authenticated original award or a duly certified copy thereof;
>
> (b) The original agreement referred to in article II or a duly certified copy thereof.
>
> 2. If the said award or agreement is not made in an official language of the country in which the award is relied upon, the party applying for recognition and enforcement of the award shall produce a translation of these documents into such language. The translation shall be certified by an official or sworn translator or by a diplomatic or consular agent.

Under article IV(1), the party seeking the enforcement and recognition of the arbitral award must provide the court of enforcement with authenticated or certified copies of the arbitral award in addition to the original agreement, which should be valid pursuant to the provisions of article II, which aims to reduce the formal requirements to enforce the award formerly required under the Convention on the Execution of Foreign Arbitral Awards (Geneva, 1927) (Geneva Convention). Article 4 of the Geneva Convention did not require 'double exequatur' expressly, but it came to be mandated de facto. The 'double exequatur' requirement means it is better that the party who is seeking the enforcement of the award before the enforcement court obtains recognition and enforcement of the award from the courts at the seat of the arbitration first. Under article 4, annex V.4 of the Geneva Convention, the party seeking enforcement of an arbitral award had not only to provide the award and the underlying arbitration agreement, but also proof that the award had become final in the country where it was made. Because most national laws did not provide for a specific certificate of 'finality' other than getting an award declared enforceable in that country, this was 'practically the only way to prove finality.'[1]

The NYC does not define the term 'authenticated', but the International Council for Commercial Arbitration defines it as 'the process by which the signatures on it [an award] are confirmed as genuine by a competent authority.'[2] According to Julian Lew and colleagues, authentication means that the tribunal signed the award and it is genuine.[3] Consequently, the main aim of authenticating the award is to assure the enforcing court where the party is seeking enforcement that the signature on the award is genuine and has been signed by the arbitrators. In the case of Switzerland/04 October 2010/Bundesgericht/4A_124/2010,[4] it was agreed that the award submitted by the respondent, which was a duly certified copy but only signed by the tribunal chairman, did not affect its enforceability. The form requirements under article IV NYC were not to be interpreted restrictively, since it was the purpose of the NYC to facilitate the enforcement of arbitral awards.

However, if the original copy is not available, then the party should provide the court with a certified copy of the original award. With the same approach to authentication, the NYC does not define the term 'certification'. Its role was explained by the ICCA at II.2.2 as being 'to confirm that the copy of the award is identical to the original'. In addition, Julian Lew and colleagues defined certification as 'an assurance that submitted documents are a true copy of the original'.[5]

Furthermore, the issue might arise whether the certified copy should be a copy of the authenticated original award, or just a copy of the original award. Some decisions[6] and some scholars[7] suggest that the certification of the copy should be a copy of an authenticated original award; otherwise, the certified

[1] Nicola Christine Port, Dirk Otto, Patricia Nacimiento and Herbert Kronke, *Recognition and Enforcement of Foreign Arbitral Awards: A Global Commentary on the New York Convention* (Kluwer Law International, 2010), p 145.
[2] *ICCA's Guide to the Interpretation of the 1958 New York Convention: A Handbook for Judges* (International Council for Commercial Arbitration, 2011), II.2.1.
[3] Julian D. M. Lew, Loukas A. Mistelis and Stefan Michael Kröll, *Comparative International Commercial Arbitration* (Kluwer Law International, 2003), p 705.
[4] Bundesgericht, 4 October 2010 (X AG v. Y AS) Yearbook XXXVI (2011) pp 340-342 (Switzerland no. 42).
[5] *Comparative International Commercial Arbitration*, p 705.
[6] Bezirksgericht, Zurich, 14 February 2003 and Obergericht, Zurich, 17 July 2003 (Italian party v. Swiss company) Yearbook XXIX (2004) pp. 819-833 (Switzerland no. 37).
[7] Frank-Bernd Weigand, ed, *Practitioner's Handbook on International Commercial Arbitration* (2nd edn, Oxford University Press, 2009).

copy does not guarantee that the original award is genuine. It is necessary for the copy to conform to the original. On the other hand, other courts have not required a certified copy of an authenticated award and have considered it sufficient to produce the certified copy of the original award.[8] Arguably, this is the most appropriate approach, because it facilitates the general implementation of arbitration. The requirement of an authenticated original award was a later insertion.[9]

According to the NYC, the court has the choice to determine the applicable law to examine the validity of authentication or certification and the required documents.[10] However, leaving the choice to the court to determine the applicable law may raise other issues with regard to the competent authority authorized to authenticate or certificate the award, and the documents that are necessary to consider that an authentication or certification is valid.[11] Therefore, the next part examines these issues regarding the law governing authentication, competent authority and the required documents to authenticate or certificate an award.

## The issue of the governing law

Since there is no specific law stated by the NYC to govern the authentication or certification validity of the award, different views have emerged among national courts to determine the applicable law. Some courts have applied the law where the award was rendered to examine the authentication validity, and the party seeking enforcement was required to fulfil the requirements of authentication under the law where the award was issued.[12] Other courts have required that in order to consider the authentication to be valid, the governing law is where enforcement and recognition is sought.[13]

The first approach was applied in a case before the Nicosia District Court, where a successful party sought the enforcement and recognition of an award issued by the International Commercial Arbitration Court (ICAC) at the Chamber of Commerce and Industry of the Russian Federation in December 2011. However, the respondents filed an objection, arguing that the court set the award aside on the basis that the winning party had not submitted an original or true copy in accordance with Cypriot law. Moreover, the respondents argued that the award should be certified by a notary officer and printed according to the law of the state in which the decision was made; their argument was upheld, and the judgment determined that the award should be authenticated in the manner required by the law of the country in which the award was made.[14]

In regard to the second approach to authenticate the award, the main advantage of relying on the law of the enforcement court is that the authentication will be easier to verify by the presiding court. According to some scholars, the main disadvantage in applying this approach is that it might lead to a 'double legalization' scenario, whereby documents authenticated according to the law where the enforcement and recognition court is sought should be authenticated according to the law where the award was made as well.[15]

Each approach to determine the applicable law has advantages and disadvantages. Applying the first approach requires the court to rely on the law of the place where the award has been rendered to authenticate the award, which makes it easier for the applicant to authenticate the award once, without the need to obtain authentication according to the law of the enforcement and recognition court each time he seeks enforcement. However, this approach has been criticised, as it does not fulfil the aims of the NYC,

[8] Germany: BGH, NJW 2001, 1730 = XXIX Y.B. Com. Arb. 724, 726–727 (2004); OLG Rostock, BB 2000, Beil. 37, pp. 20, 22–23 = RPS 2000, 20 = XXV Y.B. Com. Arb. 717, 718 (2000).
[9] The text of the draft Convention proposed by the working group originally only referred to 'the original award or a duly certified copy thereof'. See E/CONF.26/L.43, p. 1. A Belgian proposal to modify this text was adopted so that when the original award was supplied, it had to be duly authenticated. See E/CONF.26/SR.17, p 7. See also Albert van den Berg, 'The New York Convention: Summary of Court Decisions' in Marc Blessing (ed.), *The New York Convention of 1958* (ASA Special Series No. 9, JurisNet 1996), p 257.
[10] *Travaux préparatoires*, United Nations Conference on International Commercial Arbitration, Report of the Committee on the Enforcement of International Arbitral Awards, E/2704, E/AC.42/4/Rev.1, Annex, at 14. See also Albert van den Berg, 'The New York Convention: Summary of Court Decisions', p 246.
[11] Emmanuel Gaillard and John Savage (eds.), *Fouchard Gaillard Goldman on International Commercial Arbitration* (Kluwer Law International, The Hague/London/Boston, 1999); Jean-François Poudret and Sébastien Besson, Droit comparé de l'arbitrage international (Schulthess Verlag Zürich, 2002).
[12] Italy: CA Milano, VII Y.B. Com. Arb. 338, 339 (1982); India: Renusagar Power Co. Ltd. v. General Electric Co., XVI Y.B. Com. Arb. 553, 570 (1991); Bulgaria: Sup. Ct. of Appeal, XXV Y.B. Com. Arb. 678, 680 (2000).
[13] Italy: Cass., XXI Y.B. Com. Arb. 607, 608 (1996); France: TGI Strasbourg, II Y.B. Com. Arb. 244 (1977); Spain: TS, VIII Y.B. Com. Arb. 408 (1983); Mexico: Tribunal Superior de Justicia, IV Y.B. Com. Arb. 301 (1979).
[14] Delphine Rooz and Antonio Musella, 'International arbitration and alternative dispute resolution' (2014) *International Business Law Journa*l, p 157.
[15] Italy: CA Brescia, VIII Y.B. Com. Arb. Pp 383, 384 (1983). Frank-Bernd Weigand, ed, *Practitioner's Handbook on International Commercial Arbitration* (2nd edn, Oxford University Press, 2009).

especially as this solution was presented during the deliberations and refused by the drafters.[16]

Some authors have suggested that the parties should not be restricted to a particular law and they shall be allowed to choose between the law of the enforcement court and the law where the award was made.[17] This approach is obviously more flexible and in accord with the aim of the NYC to ease the recognition and enforcement of awards. Otherwise, there should be one approach to authentication, which would help to reduce the confusion of the winning party. For instance, consider the provisions of s 9(2) of the Australian Federal International Arbitration Act 1974 No. 136, 1974 (Compilation No. 11):

> 9 Evidence of awards and arbitration agreements
>
> (1) In any proceedings in which a person seeks the enforcement of a foreign award by virtue of this Part, he or she shall produce to the court:
>
> (a) the duly authenticated original award or a duly certified copy; and
>
> (b) the original arbitration agreement under which the award purports to have been made or a duly certified copy.
>
> (2) For the purposes of subsection (1), an award shall be deemed to have been duly authenticated, and a copy of an award or agreement shall be deemed to have been duly certified, if:
>
> (a) it purports to have been authenticated or certified, as the case may be, by the arbitrator or, where the arbitrator is a tribunal, by an officer of that tribunal, and it has not been shown to the court that it was not in fact so authenticated or certified; or
>
> (b) it has been otherwise authenticated or certified to the satisfaction of the court.

This grants flexibility by referring to the possibility that documents have 'been otherwise authenticated or certified to the satisfaction of the court'. A 'Note by the Secretariat' also discussed this point, at paragraph 54 of the forty-first session in 2008:[18]

> Responses showed that the authentication could be done by the Consul of the State where enforcement was sought, or where the award was made, a court of the State where the award was made or, officials authorized by the law of the State where the award was made. A few replies mentioned that the award might be authenticated by the arbitrator, an official of a permanent arbitral tribunal, or in the case of an award rendered in an ad hoc arbitration, by a notary public.

## The competent authority

Determining the applicable law to authenticate the award effectively determines the competent authority, which might vary from one country to another. For example, in some countries, the foreign ministry is the competent authority for authentication,[19] while in other countries the public authority or a diplomatic or consular officer is authorised to authenticate.[20] In some cases, the members of arbitral institutions (e.g., the secretary general) may authenticate awards.[21] In the United States of America, attorneys or notary public officers have the authority to authenticate documents.

However, the procedure of confirming that a photocopy document is a true copy of the original also varies from one jurisdiction to another. It might be certified by the notary public, a justice of the peace, a judge, solicitor or diplomatic or consular authorities.[22] The different manner of certifying the copy of the award can be a source of confusion for the holder of an award, as he might need to do it according to the

[16] United Nations Conference on International Commercial Arbitration Summary Record of the Seventeenth Meeting, 12 September 1958, E/CONF.26/SR.17, p 7.
[17] Emmanuel Gaillard, Domenico di Pietro and Nanou Leleu-Knobil, *Enforcement of Arbitration Agreements and International Arbitral Awards: The New York Convention of 1958* (London: Cameron May, 2008), para. 1675; Albert van den Berg, 'The New York Convention: Summary of Court Decisions', p 252.
[18] *Report on the survey relating to the legislative implementation of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards* (New York, 1958) Note by the Secretariat (United Nations Commission on International Trade Law, Forty-first session, New York, 16 June-3 July 2008) A /CN.9/656.
[19] Japan: Tokyo High Court, XX Y.B. Com. Arb. 742, 744 (1995).
[20] e.g., Australia: *Transpac Capital Pte Ltd. v Buntoro*, [2008] NSWSC 671 = XXXIII Y.B.Com. Arb. 349 (2008); Switzerland: *Bezirksgericht Zürich*, XXIX Y.B. Com. Arb. 819, 824 (2004); US: *Guang Dong Light Headgear Factory Co., Ltd. v ACI Int'l Inc.*, 2005 U.S. Dist. LEXIS 8810 (D. Kan. 2005) = XXXI Y.B. Com. Arb. 1105, 1109–1110 (2006).
[21] Austria: OGH, XXXIV Y.B. Com. Arb. 409, 413 (2009); OGH, RdW 2003, 385; OGH, IPRax 2000, 429 = ZfRV 1998/23; OGH, ZfRV 1996, 199.
[22] In United States, a J.P, diplomatic or consular authority, attorneys, notary public and judge can certify a document; in Nigeria, a judge (commissioner on oath), diplomatic or consular authority and notary public certifies document; in England and Wales, solicitors and notary public certify documents.

manner required by the law of the enforcing or issuing country.

**The required documents**

The application of article IV of the NYC categorises jurisdictions' into three approaches: countries that took the same approach of the NYC; countries that took a more strict approach than that required under article IV; and countries that took less strict requirements.

**Countries that applied the same approach as the NYC**

The first category refers to the countries that require no more or less strict requirements than those stated under article IV, which is to produce either the authenticated original award or a certified copy and the authenticated original arbitration agreement or certified copy.

The United Kingdom is one of the countries that observes the exact requirements of the NYC. In accordance with s 102 of the Arbitration Act 1996, the party seeking the recognition and enforcement of a foreign award under the NYC before the English courts is required to produce either an authenticated original award or certified copy and an authenticated original arbitration agreement or a certified copy of the agreement. The party seeking enforcement can provide the court with an original copy or a certified copy of the authenticated original copy. Section 8(1) of the Civil Evidence Act 1995 provides as follows:

> (1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved-
>
> > (a) By the production of that document, or
> >
> > (b) Whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the Court may approve.
>
> (2) It is immaterial for this purpose how many removes there are between a copy and the original.

This essentially means that under the English legal system, the party seeking the enforcement may produce the original copy to the court, or if that is not available, a copy of that document or of the material part of it.

Moreover, the English courts have divided the enforcement procedures into two main stages.[23] In the first stage, the court requires the party who is seeking the enforcement to produce the required documents, either authenticated or the certified award and agreement. However, at this stage the court does not examine the validity of the arbitration agreement or any other grounds for refusal. In *Lombard-Knight v Rainstorm Pictures Inc*,[24] the Court of Appeal (Civil Division) overturned a decision by Cooke J in an application that enforcement of an Award should be refused. At the hearing before Cooke J, and in court while waiting for the judge, the defendants, for the first time, indicated that they intended to argue that the Enforcement Order was irregular because *Rainstorm Pictures* had failed to comply with s. 102(1)(b) in that the two arbitration agreements had not been produced to the court in the form of either the originals or certified copies. The judge delivered an extempore judgment, indicating that the initial order was irregular. Tomlinson LJ, in delivering the judgment in the Court of Appeal and overturning the decision, said, at [27]:

> I preface my remarks by observing, as is implicit in what I have already said, that neither the judge nor Rainstorm's counsel had any idea in advance of the hearing that a point on certification would arise. The judge was referred to no authority. Such argument as was proffered to the judge was improvised and unprepared. The judge therefore received no assistance, whereas we have had the benefit of carefully considered argument informed by copious citation of authority and relevant learning derived from the international context.

The Court of Appeal considered that the provisions of s 102 did not require independent certification for the arbitration agreement. Therefore, it was enough to submit the claim form, with the attached copy agreements and a supporting statement of truth in order to fulfil the requirements under s 102. In addition, the court stated that there is no need to verify whether the maker of the statement of truth had compared the copy and the original and found them to be the same. At the second stage, the court

[23] Lord Justice Tomlinson, 'The enforcement of foreign arbitral awards: the CIArb London branch annual general meeting: keynote address, April 27, 2015' (2015) 81(4) *Arbitration* 398.
[24] [2014] 2 Lloyd's Rep 74, [2014] BUS LR 1196, [2014] EWCA Civ 356.

examined whether the award should be set aside as one of the grounds for refusal.

The US approach also conforms to the NYC, albeit under the provisions of 9 U.S. Code Chapter 2 – Convention on the Recognition and Enforcement of Foreign Arbitral Awards, arbitration did not explicitly implement article VI of the NYC. Pursuant to 9 U.S. Code § 207 – Award of arbitrators; confirmation; jurisdiction; proceeding, it requires that the NYC provision be applied for recognition and enforcement of foreign arbitral award. However, in *Matter of Chromalloy Aeroservices (Arab Republic)*,[25] the court held that the foreign award and agreement should be original or duly certified copies, as required by the NYC.

Under the general law principle in the US, the arbitral tribunal determines the authenticity of documents. Under rule 902(3) of the Federal Rules of Evidence, if the award itself is not authenticated, it can be accompanied by a document that states the genuineness of the signature and the official position of the executing or attesting person. In *U.S. v Deverso*,[26] it was held there are two basic requirements for authentication of a foreign document. Dubina CJ said, at 1255 – 1256:

> There is no requirement in Rule 902(3) that the document itself be signed. See *United States v. Squillacote*, 221 F.3d 542, 562 (4th Cir. 2000). "The rules are written in the alternative — foreign documents may be authenticated by a certification from the official executing the document *or* by an official attesting to the document." *Id*.
>
> There are two requirements for the authentication of a foreign document. "First, there must be some indication that the document is what is purports to be. Thus, the proffered document must be executed by a proper official in his official capacity, or the genuineness of the document must be attested to by a proper official in his official capacity." *Id.; see also United States v. Doyle*, 130 F.3d 523, 545 (2d Cir. 1997) (noting that the rule is not concerned with establishing the truth of information contained in the proffered document but, instead, is concerned only with "assuring that evidence is what it purports to be").
>
> "Second, there must be some indication that the *official* vouching for the document is who he purports to be." *Squillacote*, 221 F.3d at 562.

**Stricter requirements**

Some countries require the successful party that is referring the recognition and enforcement to submit additional documents other than those stated in article IV of the NYC. According to a survey by Hong-Lin Yu,[27] it was found that there are eight jurisdictions (India, Indonesia, Latvia, Oman, Sudan, Syria, Taiwan and Yemen) that require further documents as evidence.

**Less strict requirements**

Conversely, some countries require fewer documents than those stated under article IV of the NYC. Hong-Lin Yu found that there are seven countries (Costa Rica, Hungary, Japan, New Zealand, Norway, Peru and Romania) that do not require the original arbitration agreement or a duly certified copy of it to be submitted in order to enforce the arbitral award. Only awards are required in Costa Rica,[28] Hungary,[29] Japan[30] and Peru.[31]. However, in New Zealand, pursuant to section 35(1)(b) of Arbitration Amendment Act 2006, an arbitration agreement is only required if it is made in writing. The courts in Norway require the awards, but may not require the arbitration agreement.[32] Article 171 of the Romanian Law states that the parties may not submit the arbitration agreement at the enforcement stage – that is, the party seeking the enforcement may provide the court with the award only without the arbitration agreement to enforce the award, and the NYC requires both. However, it requires the party relying on the award to provide: (a) the copy of the foreign decision; (b) the proof of its final character; (c) the copy of the proof of the summons having been

[25] 939 F.Supp. 907, D.D.C., 1996.
[26] 518 F.3d 1250 518 F.3d 1250 (11th Cir. 2008), C.A.11 (Fla.) 2008.
[27] Hong-Lin Yu, 'Written Arbitration Agreements – What Written Arbitration agreements?' (2012) 32(1) *Civil Justice Quarterly*, pp 68 – 93.
[28] Ley Nº 8937, Ley sobre Arbitraje Comercial Internacional basada en la Ley Modelo de la Comsión de las Naciones Unidas para el Derecho Mercantil Internacional, (Law No. 8937, International Commercial Arbitration Law based on the Model Law of the United Nations Commission on International Trade Law**)** art. 35.
[29] 1994. évi LXXI. törvény. a **v**álasztottbíráskodásról (Act LXXI of 1994 on Arbitration), Hungary, s.60.
[30] Law no. 138 of 2003, Arbitration Law, Japan, art.46(2).
[31] Decreto Legislativo No 1071 0f 2008, (Arbitration Law) arts 68 and 76.
[32] Lov om voldgift, LOV-2004-05-14-25 (Arbitration Act of May 14, 2004), Norway, s 45.

served, and the act of notification having been communicated to the party which was not present in the foreign hearing, or any other official act attesting that the party against which the decision was made knew of the summons and the notification act in due time; and (d) any other act to prove further that the foreign decision meets all the other conditions under article 167.[33]

There are other countries with less strict rules than those noted in the survey by Hong-Lin Yu, such as the German courts, which consistently hold that a petitioner seeking enforcement of a foreign award in Germany under the Convention need only supply the authenticated original arbitral award or a certified copy.[34] There is no issue arising from the requirement of fewer documentation to enforce the arbitral award, as the court may rely on the application of the most-favourable-law pursuant to article VII of the NYC, which allows courts to apply the law that supports the enforcement of the arbitral award.

## Authentication before the Dubai and DIFC Courts

The UAE is a signatory of the NYC by way of Federal Decree No. 43 for the Year 2006, but there are no rules requiring fewer or more documents to enforce and recognise arbitral awards. The minimum requirements provided by article IV of the NYC should be followed by its jurisdictions at the stage of recognition and enforcement proceedings. In *Maxtel International FZE v Airmec Dubai LLC*,[35] the Dubai Court of First Instance held that:

> The Court's supervisory role when looking to recognize and enforce a foreign arbitral award is strictly to ensure that it does not conflict with the Federal Decree which provided for the UAE to acceded to the New York Convention on the recognition and enforcement of foreign arbitral awards and satisfied the requirements of Articles IV and V of the Decree in terms of being duly authenticated.

However, regarding the governing law of authentication of an arbitral award before the DIFC and Dubai Courts, article 42(3) of the DIFC Arbitration Law and article 237(1) of the Civil Procedure Code states that the authentication shall be made in accordance with the place of arbitration; therefore, the competent authority is determined based on the law of the seat of arbitration.

Last but not least, authentication procedures might vary from one country to another, and the party who is seeking the enforcement should be familiar with the required documents, the competent authority and the law governing authentication before seeking enforcement. Nevertheless, the Dubai and DIFC Courts have both stated clearly that the law governing authentication is the law of the seat of arbitration, which leaves the answer to the question of the competent authority depending on the applicable law. However, the legislation in Dubai and the DIFC has not provided for the provision of different documents to those in the NYC, an approach that could considered the most appropriate one, becuase it does not leave any confusion, especially compared to jurisdictions requiring more documents.

Despite the different application of article IV of the NYC, the main aim of authentication is to confirm that the signature in an arbitral award and the arbitration agreement is genuine. Albert Jan van den Berg supported this idea and stated that 'The authentication of a document is the formality by which the signature thereon is attested to be genuine.'[36]

Between the various approaches and the aim of providing for the authentication of relevant documents, the question arises as to whether the authentication of such documents can be achieved by way of documents in electronic format and electronic signatures. This alternative solution to the traditional approaches to authenticate the award might increase the effectiveness and efficiency of electronic awards. The question is whether an electronic signature is able to fulfil the aim of authentication and replace the traditional manuscript signature. Moreover, if the parties signed the arbitration agreement electronically, the question then arises whether the court will consider the arbitration agreement an original. The same issues arise for the award signed electronically. Therefore, the heart of the issue is whether the present position on digital evidence and electronic signatures is sufficiently acknowledged to

[33] Arbitration of Private International Law Book IV, Code of Civil Procedure arts 340–370 on Arbitration (as amended by Law No.59 of July 23, 1993), Romania.
[34] Germany: Oberlandesgericht, Munich, 12 October 2009 (Swedish Seller v. German Buyer) Yearbook Commercial Arbitration XXXV (2010) pp 383 – 385 (Germany no. 134).
[35] Court of First Instance Commercial Action No. 268/2010, 12 January 2011.
[36] Albert Jan van den Berg, 'The New York Convention of 1958: An Overview'.

replace the manuscript signature to allow the competent authority to authenticate the award and agreement.

The answer to these questions depends on the law of the enforcement court and whether it acknowledges electronic signatures, and if so, which form of electronic signature. Therefore, as the article is concerned with the Dubai and DIFC legislation, we will examine the enforceability of electronic signatures before the Dubai and DIFC courts. We begin with a brief and broad overview of the use of electronic signatures.

## The electronic signature

Online transactions take place over the internet remotely without the parties meeting, which makes it difficult to recognise the identity of the parties who agreed on the contract, which raise the issue of the degree of trust.[37] Therefore, in online arbitration, the parties need a secure procedure in order to recognise the arbitrator and the parties' signature on the agreement.

Besides requiring an authenticated or certified award and agreement, NYC and different national legal systems require the arbitration agreement and award to be signed. Regarding the requirement of a signature for the arbitration agreement, article II(2) has been interpreted widely by different courts. Both the arbitration agreement and arbitration clause can be either signed or contained in an exchange of letters or telegrams (for instance, see *Mar, Inc v Tiger Petroleum Corporation*[38] and *Krauss Maffei Verfahrenstechnik GmbH (Germany) v Bristol Myers Squibb (Italy).*[39] Both the award and the agreement are required to be signed either by the parties or by the arbitrator in order to enforce the arbitral award. See article II:

> 1. Each Contracting State shall recognize an agreement in writing under which the parties undertake to submit to arbitration all or any differences which have arisen or which may arise between them in respect of a defined legal relationship, whether contractual or not, concerning a subject matter capable of settlement by arbitration.
>
> 2. The term "agreement in writing" shall include an arbitral clause in a contract or an arbitration agreement, signed by the parties or contained in an exchange of letters or telegrams.
>
> 3. The court of a Contracting State, when seized of an action in a matter in respect of which the parties have made an agreement within the meaning of this article, shall, at the request of one of the parties, refer the parties to arbitration, unless it finds that the said agreement is null and void, inoperative or incapable of being performed.

Issues regarding the identity of the signature holder might arise before the enforcing court. For instance, it might be necessary to consider the evidential problem of establishing the identity of the arbitrator, parties and witnesses in electronic form, and whether the courts of Dubai and DIFC support the electronic signature.

It is arguable whether some forms of electronic signature are a more reliable method than a manual signature. However, the truth is that both the manual signature and the electronic signature can be stolen and copied.[40] This is supported by Mason, who suggests that machine or system-made evidence should be neither automatically deemed more reliable than human testimony, nor given evidentiary presumptions.[41] The chip and PIN for debit and credit card security, which has replaced reliance on manual signatures, still raises several issues. This is because many banks have tried on numerous occasions with various iterations of technology to provide for the certainty that an identified person is interacting with an automatic teller machine (ATM) when obtaining access to an account – yet thieves continue to manipulate banking systems (that is, ATMs and online banking) successfully, stealing considerable sums of money every year.[42]

[37] Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', Computer and Telecommunications Law Review, 2015, Volume 21, Issue 5, pp 135 – 148.
[38] *Sen Mar, Inc., v Tiger Petroleum Corporation*, 774 F Supp. 879 (S.D.N.Y. 1991).
[39] *Krauss Maffei Verfahrenstechnik GmbH (Germany) v Bristol Myers Squibb (Italy)*, 10 March 2000, (Yearbook Commercial Arbitration XXVI (2001), p. 816.
[40] Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), p 169.
[41] Stephen Mason, *Electronic Signatures in Law*, p 169.
[42] Stephen Mason, 'Debit cards, ATMs and negligence of the bank and customer', *Butterworths Journal of International Banking and Financial Law*, Volume 27, Number 3, March 2012, pp 163 – 173.

Electronic signatures are starting to play a major role in electronic transactions and contracts, and they will increasingly be used in the field of online arbitration.

### The validity test of the electronic signature

There are several of functions for the electronic signature which can be divided into primary and secondary evidential functions. The primary evidential functions express the consent of the signature holder and to make sure that the signatory is adopting the content of the message.[43] On the other hand, the secondary evidential function include establishing the identity of the holder of the signature and to state a particular characteristic or status of the signatory such as a government minister or company director.[44]

There are two ways in which the law might deal with electronic signatures: the function or form, or both of them.[45] If the definition is based on the form of the signature, this approach may include different types of signature, and the list might be extended in the future if any future signature fulfils the form requirements. On the other hand, the other approach is based on the functions that the signature performs, and any signature that satisfies the required functions should be considered valid.[46]

### Types of e-signature

There are various types of e-signature: biodynamic technology, 'I accept' or 'I agree' icon, digital signature and personal identification number (PIN). Parties may agree on the electronic signature format that might be convenient for them and their transaction, guided by relevant local legislation. The admissibility of an electronic signature might be set out in legislation, but it is the court's competence to evaluate the evidentiary weight on a case-by-case basis. The recognition and admissibility of the electronic signature depends on two main aspects: whether the applicable law recognises the electronic signature; and whether the electronic signature fulfils the requirements of the applicable law, such as the capability for identification, attribution and proof of assent or intent of the signer.[47]

In the absence of any relevant case law in Dubai, it is not clear whether the authentication of an electronic signature on its own can be sufficient in fulfilling the requirements under article IV(1)(a). The aim of the authentication of an electronic signature is to establish that the award is genuine and original. There is no reason to prevent an electronic generated copy, with assurances of authorship and integrity, being considered a duly certified copy within the meaning of NYC article IV. The burden of proof that the award has been authenticated relies on the party seeking the enforcement, which might be partially proved by evidence that the document had been digitally signed by the arbitrator.[48]

## Electronic signatures before Dubai courts

In 2002, Dubai issued a law in regard to electronic commerce, the Dubai Electronic Transactions and Commerce Law, in response to which the United Arab Emirates issued the Federal Law 1/2006 on Electronic Transactions and Commerce (ETCL). The new law reflects the Federal government's efforts to regulate electronic transactions and raise users' confidence.[49] The UAE has subsequently made further amendments to the existing legislation to increase conformity with the ETCL. For example, Federal Law No. 36 of 2006 amended the Law of Evidence in Civil and Commercial Transactions promulgated by Federal Law No. 10 of 1992 to state that an electronic signature complying with the provisions of the ETCL is considered equivalent to a manuscript signature. In addition, the new amendments gave electronic writing, communication, records and documents that comply with the provisions of the ETCL the same effect and force as accorded to official and traditional writing and communication under the Law of Evidence. The ETCL itself defined the electronic signature in article 1 as:

> A signature composed of letters, numbers, symbols, sound or electronic processing system attached or logically connected to an electronic message imprinted with intent of ratification or adoption of that message.

[43] Stephen Mason, *Electronic Signatures in Law*, pp 8 – 10.
[44] Stephen Mason, *Electronic Signatures in Law*, pp 8 – 10.
[45] Chris Reed, 'What is a signature?', 2000 (3), Journal of Information, Law & Technology.
[46] Chris Reed, 'What is a signature?'.
[47] Stephen Mason, 'Electronic signatures in practice', (2006) J High Tech L 148.
[48] Gabrielle Kaufmann-Kohler and Thomas Schultz, 'The use of Information Technology in arbitration', *Jusletter*, December 2005; but see the chapter on authentication in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).
[49] S. M. Qudah, 'Legal Insight on the Dubai Electronic Transactions and Commerce Law No. 2 of 2002', (2002) 17(3) *Arab Law Quarterly*, 283 – 296.

The ETCL adopted the two-tier approach, because it sets out several requirements to consider an electronic signature valid, with special reference to the digital signature. According to the law, the electronic signature is considered valid if it meets specific conditions, which are the ability to provide a reliable method of identification of the person who is using it and evidence that the signatory genuinely intended consent.[50] Moreover, the party is entitled to rely on the protected electronic signature if it fulfils the meaning according to article 18 and it is reasonable to rely on it; the required factors set out under article 18 are examined below.

## The limits of relying on e-signature in e-awards

The ETCL provides for several limitations in its application, chiefly concerning matters of civil status including marriage, divorce and wills, title deeds of real estate, bonds in circulation, transactions concerning the sale and purchase of real estates (disposition and rental for periods in excess of ten years and the registration of any other rights related to it), any document required by law before a notary public, and any other document or transaction excluded under a special legal term.[51]

It is possible to rely on an electronic signature in order to authenticate an award and arbitration agreement, providing the notary public is not required to authenticate such an award. As explained above, in the Dubai and DIFC courts, the competent authority to authenticate the award is determined by the law of the seat of arbitration. In addition, there is no problem regarding reliance on a protected electronic signature to authenticate the award as discussed above (the main aim of the authentication is to confirm that the signature on the award is genuine and affixed by a competent authority).

However, there are shortcomings in relying on electronic signatures. The main issue that might arise is the ability to determine whether the signatory was the person who signed the agreement or not. In this regard, Mason explains that 'when a private key to a digital signature is used, a recipient will not know whether it was the owner that actually used the private key'.[52] For instance, in the Portuguese case of (Evora) Ac. RE 13-12-2005 (R.982/2005), despite that the email was sent and attached with a digital signature, the court held it was insufficient to determine that the sender caused the digital signature to be affixed to the message. Despite the shortcomings with the digital signature, it still considered as an ideal approach to authenticate an arbitration agreement and award. The next part examines whether the ETCL is able to provide a reliable authentication procedure and whether it accepts electronic signatures as a valid authentication procedure.

## Electronic signature requirements

In offline transactions or communications it is easier for the parties to identify and recognise each other, as they both rely on customary approaches to credentials such as drivers' licenses or passports.[53] The problem is different for online transactions. Relying on a party's identity card is only sufficient in case that the person who is checking the card is able to perform the biometric checks necessary to establish the connection between the card and the purported true holder.[54] Moreover, there is the matter of the many names that are not unique that might arise in both online and offline transactions.[55]

The importance of a trusted third party to certify the connection between a person and their public key is recognized in article 1 of the ETCL, which defines the third party as the Authentication Services Provider, also known as a Certification Authority:

> Any person or duly accredited party issues electronic authentication certificates or any services or tasks related to it and to electronic signatures regulated by the provisions of the present Law.

One of the main roles that the authorised third party provides is to validate parties with each other, especially those that have not done any previous transactions together, in order to identify each party involved in the transmission of transactional data. Therefore, one of the major functions that the law provides for the Certificate Authority is to confirm the link between the signature and a particular person by

[50] Article 8(1), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[51] Article 2(2), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[52] Stephen Mason, *Electronic Signatures in Law*, p 121.
[53] D. Scott Anderson, 'What trust is in these times? Examining the foundation of online trust', 54 Emory L.J. (2005) 1441, pp 1444 – 1450; for a more in-depth article on this topic, see Nicholas Bohm and Stephen Mason, 'Identity and its verification' *Computer Law & Security Review*, Volume 26, Number 1, January 2010, pp 43 – 51.
[54] Nicholas Bohm and Stephen Mason, Identity and its verification'.
[55] Nicholas Bohm and Stephen Mason, Identity and its verification'.

issuing a certificate to approve the link and attest to some fact about the subject of the certificate.[56]

The formal term under ETCL for a Certificate is 'Electronic Authentication Certificate,' defined as 'A certificate issued by authentication services provider in which he indicates the identity of the person or the party acquiring a specified signature tool.' The ETCL clearly states that the electronic signature supported by a certificate issued by an accredited Certificate Authority would ordinarily comply with statutory requirements as proof.[57]

Regarding the application of the protected electronic signature, the law states that the responsibility to confirm whether the certificate is valid, suspended or revoked lies with the party relying on it. Article 18(2) provides that the relying person is responsible for the consequences of failing to verify the certificate.[58] Article 18(2) states:

> 'When electronic signature is enhanced with electronic authentication certificate, the party relying on that signature shall be responsible for the consequences of his failure to adopt necessary reasonable steps to verify the validity and applicability of such certificate, and whether it is suspended or cancelled, and observance of any restrictions concerning the electronic authentication certificate.'

The factors to be considered by the relying person to decide whether using the electronic signatures is reliable, include the type of transaction, the value or importance of the transaction, whether the relying party took the required steps to verify whether the electronic signature was supported by a certificate, and the dealing or trade usage between the two parties. The ETCL under article 18(3) states other factors that should be determined in order to be able to rely on an electronic signature, including the nature and value of the transaction, and whether the relying party took the required steps to verify that the electronic signature is enhanced by electronic authentication certificate or is supposed to be so, and to verify whether the electronic signature has been revoked.

A protected electronic signature must be verified by authentication procedures. The parties can agree procedures in advance, or procedures might be designated by law. The method of authentication examines whether an electronic signature fulfils a number of requirements, such as being unique to that person and the ability to confirm the identity of that person. In addition, the electronic signature should be under the person's control at the time of signing. Finally, it ought to be possible to link the electronic signature to the data message confirming the party's consent.[59] The protected electronic signature is considered to be reasonable and accepted unless established otherwise.[60] Moreover, the protected electronic signature is considered to be reliable, related to the purported person and reflecting that person's consent to the data message, unless there is evidence to the contrary.[61]

## Certification authorities under the

The ETCL widely regulates matters related to the licensing of the Certification Authority, including issues relating to liability, and the powers to suspend and revoke certificates as required. Under the ETCL, the Minister of Economy and Planning has the authority to appoint the Controller of Certification Services, and the latter is required to regulate the licensing and operational activities of the Certification Authorities. The duties of the Certification Authorities under the ETCL are to provide subscribers or other relevant parties with any representations it makes, to ensure that the information in the Certificate is accurate and complete, to provide access to the relying third party with certain information such as the identity of the Certification Authority, to ensure that the subscriber has control over the private key at certain times, and any other information that might be reasonably accessible. Moreover, the Certification Authority is obliged to employ trustworthy computer information systems, procedures and personnel.[62] It should be noticed that in Dubai, Certificate Authorities are required to have a license.

A person applying for a certificate is required to provide the Certificate Authority with identification

[56] A. Michael Froomkin, 'The essential role of trusted third parties in electronic commerce', 75 Or. L. Rev. (1996) 49.
[57] Article 17(2), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[58] Article 18(4), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[59] Article 17(1), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[60] Article 17(2), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[61] Article 10(3), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[62] Article 18(1), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.

documentation before making the application, then if the Certificate Authority is satisfied that the applicant has provided sufficient evidence to establish their identity and all the required information is correct, then the applicant has to pay the fees.[63] According to article 21(1)(c), the information that should be provided by the Certification Authority in the Certificate is the identity of the subscriber, specifying that the subscriber has control over the private key at the time of issuance of the Certificate, stating any limitations regarding the purpose or value of the Certificate, expressing any liability toward the Certificate by any relevant person and providing that the private key was effective at the time of issuance.

The ETCL is not restricted to one technology. The ETCL defined the Protected Authentication Procedures as:

> Procedures aiming to ascertain that an electronic message is initiated by or to a certain person, and to discover any error or modification in contents, sending or saving an electronic message or an electronic record within a fixed period, this shall include any procedure uses mathematical methods, symbols, words, identification letters, codes, procedures of reply or acknowledgment of receipt and other means of information security procedures.

In this definition, the aim is to give effect to any future technology that might evolve, and not to a particular technology that might exclude other forms.

In order to add more security and reliability to the electronic signature, the ETCL requires that the subscriber inform the Certification Authority and relying third parties when the private key is compromised, or there is a likelihood that the security might be compromised. Further, it obliges the subscriber to employ reasonable care to ensure that all material representations made to the Certification Authority when applying for issuance of the Certificate, and all information contained in the Certificate, are accurate.[64] Failing which, the subscriber is considered to be responsible for any damages occurred by relying third party.[65]

The ETCL aims to provide parties with secure and reliable use of electronic signatures. Therefore, it created the compulsory system of licensing of Certificate Authorities, which is implemented by the Authenticated Services Controller, appointed by the UAE Cabinet. The role of the Certificate Authority is of vital importance, as it ascertains the identity of the subscriber, and establishes whether the electronic signature belongs to the subscriber at the time of signature. In addition, the ETCL provides the Controller with the ability to observe whether the Certificate Authority is capable of carrying out its duties and if it is qualified to carry out its work. Otherwise, the Controller has the right to suspend or revoke the Certificate Authority's license.

The ETCL also provides for a number of crimes punishable by fines, imprisonment, or both, including to fraudulently publish a Certificate, breach a duty of confidentiality, the use of electronic apparatus in order to carry out another crime, and to provide false or unauthorized information to a Certificate Authority. The ETCL imposes several penalties on the party who 'creates, publishes, provides or submits any electronic authentication certificate, which includes or refers to incorrect data with his knowledge of this.'[66] However, the ETCL provides that the Certificate Authority is responsible for any damages caused, unless it clearly excludes its responsibility, or it proves that it was not negligent, or its action were carried out by mistake.[67] The Certificate Authority is considered responsible for any damages caused to a third party relying on a qualified certificate issued by them, unless it is able to prove that it has not acted negligently or any of the conditions stated under article 21(5) apply.[68] Further, the ETCL provides for penalties for the Certificate Authority, such as fines and imprisonment, and it holds it responsible for damages. However, the Certificate Authority may reduce their liability toward a third party by setting a limit for financial transactions or by limiting the use of the certificates to particular transactions.

## Enforceability of foreign certifications

Parties may rely on foreign certificate authorities to authenticate electronic signatures. The question that might arise is whether an electronic signature

[63] Article 22(m), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[64] Article 19(1), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[65] Article 19(2), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[66] Article 26, Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[67] Article 21(5), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[68] Article 26, Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.

certificate provided by a foreign certification service could be valid before the Dubai courts, and what conditions are necessary to validate foreign electronic certificates. In general, the Dubai courts validate and recognise foreign and domestic certificates and electronic signatures equally,[69] but there are certain conditions imposed on the Certificate Authority to recognise foreign issued certificates and electronic signatures. The law in Dubai requires that the foreign Certification Authority have equivalent or higher standards of reliability compared to those required for certification in Dubai, which also applies in respect to electronic signatures.[70]

Parties are allowed to agree on a particular Certification Authority, or a particular category of Certification Authority to be used and a particular class of Certification.[71] Further, any agreement between the parties regarding a particular certificate and electronic signature is enforceable and effective in the Emirate of Dubai.

The law requires the foreign electronic signature to fulfil the essential factors set out in article 21(2) in order to be valid and effective before the courts of Dubai. Article 21(2) requires several factors such as the certificate shall indicate that the person had control over the signature tool at the relevant time and the degree of discrepancy between the law applicable to the conduct of the Certification Authority and the law of the UAE.

## Discussion and recommendations

The ETCL aims to improve the authenticity and integrity of electronic transactions by validating electronic signatures and documents as acceptable substitutes for manuscript signatures. Therefore, parties may rely on electronic documents signed by electronic signature, which fulfils the statutory requirements for manuscript signatures.

Regarding the protected electronic signature, it is suggested that the ETCL should have described it more clearly. The main issue in respect to article 18(1) of the law is that it includes some terms that might be confusing, such as 'reliable is acceptable.' Although the parameters of the term 'reliable being acceptable' are explained in article 18(3), it is still ambiguous.

Article 18(3) explains the factors that should be examined to determine the ability to rely on the electronic signature, which reads as follow:

> To determine whether it is possible for a person to rely on an electronic signature or electronic authentication certificate, the following factors must be considered:
>
> a - Nature of the concerned transaction intended to be enhanced by the electronic signature.
>
> b - Value or importance of the concerned transaction if acknowledged by the party relying on the electronic signature.
>
> c - If the person relying on the electronic signature or electronic authentication certificate, has adopted appropriate steps to determine the extent of reliability of electronic signature or electronic authentication certificate.
>
> d - If the party relying on the electronic signature has adopted appropriate steps to verify that the electronic signature is enhanced by electronic authentication certificate or supposed to be so.
>
> e - If the party relying on the electronic signature or electronic authentication certificate, has known or should have known that the electronic signature or electronic authentication certificate was violated or cancelled.
>
> f - Agreement or previous dealing between the originator and the party relying on the electronic signature or electronic authentication certificate or any other commercial custom common in this matter.
>
> g - Any other related factor.

There is some ambiguity that has yet to be resolved in order to avoid the scenario in which the reliable party may escape his obligations. The same term has been used in article 13(3) of the Electronic Communications and Transactions Act 25 of 2002 in South Africa. Hence, it will be useful to compare the Electronic Communications and Transactions Act 25 of 2002 in South Africa. Article 13(3) reads as follow:

> (a) a method is used to identify the person and to indicate the person's approval of the information communicated: and

[69] Article 23(1), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[70] Article 23, Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.
[71] Article 23(6)(a), Federal Law No. 1 of 2006 concerning Electronic Transactions and Commerce Law.

> (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

Aashish Srivastava and Michel Koekemoer stated that the language used in the act is vague, and it helps parties to evade their obligations:

> Such language in the Electronic Communications and Transactions Act 25 of 2002 gives an opportunity to a party to a transaction that required a signature to attempt to escape its obligations by denying that any of the parties' signatures were valid on the ground that the method of signature employed was not as reliable as appropriate.[72]

Moreover, the reliability test might be use by one of the parties in a way to avoid the agreement. As explained by John D. Gregory,[73] the relying party might know the person who signed the document, although he might try to avoid his liabilities by arguing that the method of the e-signature was unreliable enough for the transaction, in order to invalidate the signature and the whole transaction. The core issue regarding these factors is that they might vary from one party to another, besides which the essential element to consider is whether the electronic signature is protected or not.[74]

Another issue regarding the reliability test has been raised by a number of authors.[75] John D. Gregory criticised the reliability test, and he argued that it is sufficient to rely on the party's experience to decide whether the signature is reliable or not. He also argued that such an approach does not add any value to the signature, although it only transfers the question of reliability from the parties to the judge.[76]

In general, the ETCL provides a framework that increases the use of electronic signatures and ensures the installation of practical electronic certification systems. It also considers the speed at which technological improvements and systems are occurring. By recognising foreign certificates, the ETCL allows the application of international electronic signatures in Dubai. However, the law does not state what factors are required from foreign Certificate Authorities to validate the electronic certificate. Article 23(2) states that in order to consider the foreign electronic certificate valid, it should fulfil the required standards in article 20, but article 20 does not state any requirements. It reads:

> For the purposes of this Law, the Council of Ministers shall designate an authority to control over authentication services and particularly for the purposes of licensing, authentication and controlling the activities of authentication services providers and its supervision.

The most appropriate approach is to set out the required standards in the same article, which will leave no confusion for the parties, especially as article 20 establishes the authority of the Council of Ministers and its main services, but it does not provide any standards to be applied.

In conclusion, the ETCL has come a long way and has kept up to date with technology and laws on identity and security. The effectiveness of a digital signature will depend on the relevant risk management procedures. The law can only go so far in providing for technological security, and it is up to the parties to ensure that it is enforced, adhered to and protected.

## Relying on electronic signature to authenticate electronic awards

As noted above, the law in Dubai supports the validity of electronic signatures, and it provides a reliable method to authenticate the digital signature by relying on a trusted third party. However, the law excludes documents that should be notarized from the application of the electronic signature, an exclusion that might affect the reliance on the electronic signature if the applicable law requires the award to be authenticated by a notary public. Nevertheless, relying on an electronic signature to authenticate an electronic award is capable of being a valid mechanism. The main advantage of relying on an electronic signature in online arbitration is that it helps the parties to identify each other by relying on a trusted third party. However, relying on a third party is not always adequate and sufficient, because there

[72] Aashish Srivastava and Michel Koekemoer, 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview', p 427.
[73] John D. Gregory, 'Must e-Signatures be reliable?', 10 *Digital Evidence and Electronic Signature Law Review* (2013), pp 67 – 70.
[74] Emad Abdel Rahim Dahiyat, 'The legal recognition of electronic signatures in Jordan: some remarks on the Electronic Transactions Law', (2011) *Arab Law Quarterly* p 297.
[75] Stephen Mason, *Electronic Signatures in Law*, pp 103 – 104; pp 257 – 258; John D. Gregory, 'Must e-Signatures be reliable?', 10 *Digital Evidence and Electronic Signature Law Review* (2013), pp 67 – 70.
[76] John D. Gregory, 'Must e-Signatures be reliable?', 10 *Digital Evidence and Electronic Signature Law Review* (2013), 67 – 70.

might be a possibility that the Certificate Authority issues false certificates.[77]

The ETCL does not provide for any requirement for the certification authority to have sufficient financial assets. Arguably, the law should require the certification authority to have the financial capability to compensate the losses of users for any damages occurred because of the failure of the certificate centre, such as if the information contained in the key certificates is vague and inaccurate.[78]

Determining who is responsible for any damage caused because of the unlawful use of a digital signature is a critical issue in the field of electronic signatures. The question of liability might be a significant issue in regard to the authenticating of an electronic award. The final award that is electronically signed and authorised by the certificate authority is directly enforceable before the enforcing court. Hence, any unlawful use of the electronic signature might cause damages and affect the legal rights of the parties where an unknown person has obtained unauthorised access to the electronic signature of the arbitrator.

Moreover, under the ETCL, the foreign digital signature and certificate are explicitly considered valid and equivalent to the domestic electronic signature, which might be considered as a great help, especially in relation to international commercial arbitration.

The application of the digital signature under the ETCL supports the aim of authentication required by the NYC, which is to guarantee that the signature is genuine and related to the holder of the signature at the time of signing the document. As explained earlier, the Certificate Authority has the ability to fulfil these requirements and could replace the competent authority to authenticate.

## Electronic signatures under the DIFC

In comparison to Dubai, the DIFC has not applied a separate law to regulate electronic signatures. However, it has posted the proposed Electronic Transaction Law for public comment; this proposed law aims to create a secure legal environment for companies in the DIFC to undertake electronic transactions.[79] The proposed law is based on the Uniform Electronic Transactions Act 1999 (UETA) drafted by a committee of the National Conference of Commissioners on Uniform State Laws in the US and adopted by most states in the US. The UETA contains provisions derived from, among others, the UNCITRAL Model Law on Electronic Signatures and Canadian law. However, to date it has not been enforced.

According to the current rules of the DIFC, the electronic signature might still be enforceable. Article 6(3) and 6(4) of the Rules of the DIFC courts state:

> 6(3) Where these Rules require a document to be signed, that requirement shall be satisfied if the signature is printed by computer or other mechanical means.
>
> 6(4) Where a replica signature is printed electronically or by other mechanical means on any document, the name of the person whose signature is printed must also be printed so that the person may be identified.

However, relying on the articles above to enforce and validate the electronic signature is not sufficient because it emphasises the signature in printed form, and does not appear to include signatures in electronic format, including digital signatures. The law should consider the regulation of digital signatures, electronic certification and certificate authorities in order to be able to apply and validate digital signatures at the national and international levels and increase its reliability within parties.

## Conclusion

Article IV of the NYC requires the party seeking enforcement to support the application with authenticated or certificated copies of the award and arbitration agreement. There are several issues related to this article, such as the issue of the governing law, the required documents according to different legal approaches and the competent authority. It has been established that the law governing the authentication or certification is of vital importance, as it decides the required documents and the competent authority. Hence, the competent authority might vary from one country to another, as

[77] Stephen Mason, *Electronic Signatures in Law*, p 309; see also the DigiNotar case, when internet hackers maliciously obtained unauthorised access to DigiNotar's CA servers, allowing the issuance of a series of rogue certificates.

[78] Olga I. Kudryavtseva, 'The use of electronic digital signatures in banking relationships in the Russian Federation', 5 *Digital Evidence and Electronic Signature Law Review* (2008), pp 51 – 57; see also Resolution of the Federal Arbitration Court of Moscow Region of 29 October 2007 N KTA40/10952-07 (case NA40-75611/06-47-564).

[79] https://www.difc.ae/news/difc-posts-electronic-transactions-law-public-consultation; the ability of the public to comment ended on 2 January 2009.

it might be the notary public, foreign ministry or registered lawyers in some countries. Moreover, the required documents might vary because of the law of the enforcement country, as some countries have more stringent approaches than the NYC, while others are more relaxed, requiring the award only. The most expeditious approach is to apply the same requirements under the NYC provisions. The applicable approach in Dubai and DIFC is the same as stated in the NYC, however the courts in Dubai and DIFC require the authentication to be done according to the law of the seat of arbitration.

Moreover, relying on a protected electronic signature fulfils the requirements of article IV, which is to confirm that the signature on the award is genuine and added by a competent authority. In this case, the competent authority is the Certificate Authority, which examines the identity of the digital signature holder, and confirms whether the digital signature belongs to the person who used it, guaranteeing that it was controlled by the right person at the creation or usage at time of signing, and it examines whether the electronic record that is linked to the digital signature was not changed or amended. Relying on the protected electronic signature to authenticate an electronic arbitral can be valid and effective.

Enforcing an electronic arbitral award that is signed electronically is not in opposition with the NYC provisions; on the contrary, it supports the NYC approach.

The final part of this article has focused on the enforceability of the electronic signature before Dubai and DIFC courts. However, in regard to the DIFC courts and due to the lack of legislation over the regulation of the electronic signature, it is difficult to rely on the current rules to enforce any form of electronic signature. It is recommended that the DIFC take the same approach as Dubai, and enforces legislation that regulate the enforceability of electronic signature and certificate authorities in the Dubai International Financial Centre.



**Omar Husain Qouteshat** is a PhD student at the University of Central Lancashire. His topic is to examine the enforcement of arbitral awards on online commercial disputes under the New York Convention in relation to the Dubai and Dubai International Financial Centre courts.

OHJQouteshat@uclan.ac.uk