DocuSign®

Whitepaper

Court Support for Electronic Signatures in Mexico

Introduction

The term "electronic signature" is simply defined by Article 89 of the Commercial Code ("CC") of Mexico, as any data in electronic form that is used to identify the signatory in relation to the data message on which it is recorded and to indicate the signatory's approval of that data message. Since this framework is built upon a technology neutrality principle, at the outset, any industry standard and technology that meets the necessary reliability requirements may be used. Such simple electronic signatures ("SES") therefore would be considered valid, produce the same effect as a physical ("wet") signature and are admissible as evidence in court. However, SES has limitations relating to the evidentiary weight this type of electronic signature might have in court. For example, typically a judge takes into account the purpose for which the parties intended to use the electronic signature, the specific circumstances and nature of each case and other evidentiary factors. Often individuals incorrectly believe that merely pasting a digital image of a wet signature into a document will serve as an adequate SES. However, such an approach has the risk of not satisfying the above requirements and/or failing to establish an adequate level of evidentiary weight in court, as is provided with a more rigorous electronic signature service, such as DocuSign's eSignature.

For this reason, signers often look to electronic signature services, such as DocuSign eSignature, which not only satisfy the basic SES requirements, but also the additional requirements of an enhanced type of electronic signature, called an advanced electronic signature ("AES") or reliable electronic signature ("RES"). The CC defines AES / RES as an "electronic signature which complies with certain additional authentication and signatory identification requirements set forth in sections I to IV of Article 97. Within Mexico and elsewhere around the world, electronic signatures that satisfy these heightened AES / RES requirements address approximately 98% of the typical use cases for electronic signatures and are viewed as adequate for evidentiary purposes in court. One warning to avoid confusion when comparing electronic signature requirements in other jurisdictions to unenhanced or unqualified AES / RES electronic signatures in Mexico.

An unenhanced or unqualified AES / RES electronic signature in Mexico typically is more similar to a simple or standard electronic signatures in other regions of the world. Further, an AES electronic signature in Europe, which complies with the European eIDAS requirements, is more analogous to a digital signature, like QES (as described below), than an unenhnanced or unqualified AES / RES electronic signature in Mexico though they share similar names.

A more heightened type of electronic signature, called a qualified electronic signature ("QES"), is a final type of electronic signature that typically is used in very specific use cases with heavily regulated industries and the Mexican government. To generate a QES electronic signature, a Certification Service Provider ("CSP"), which is certified by the Ministry of Economy pursuant to the CC, the Mexican Official Standard (NOM-151-SCFI-2016, published on March 30, 2017 and replaces NOM-151-SCFI-2002) (the "NOM"), and the Advanced Electronic Signature Law (the "AES Law"), "qualifies" an AES / RES electronic signature by issuing a digital certificate as an enhanced identity verification of the electronic signature to create a QES electronic signature. Often QES, which uses a digital certificate as part of the electronic signature to provide enhanced identity verification of the signer. Such a qualified electronic signature often is referred to as a digital signature due to the identity-based digital certificate that is independently issued by a CSP and incorporated into the electronic signature of a third-party service like DocuSign eSignature. Such QES electronic signatures, due to its administrative complexities and often unnecessary heightened level of identity verification, typically are only used in just 2% of global use cases. Another word of caution is that often individuals may erroneously and unintentionally interchangeably refer to electronic signatures and digital signatures as the same thing even though a digital signature is a very specific and heightened type of electronic signature (e.g. QES) in Mexico.

Step 1
General framework of electronic signatures

Unlike many other countries, Mexico does not have a general "umbrella" electronic signature law. Instead, different legal bodies have incorporated the concept of electronic signatures into their laws and regulations. Some of these are aimed at regulating the use of electronic signatures in the public sector, while others regulate their use in the private sector.

Mexican Legal Framework
Private Sector

The foundation for the recognition and validity of electronic signatures in Mexico for commercial and civil transactions is found under the Federal Civil Code ("FCC") and the CC. According to Article 1803 of the FCC, consent may be expressed through electronic means. Similarly, under Article 89 of the CC electronic, optical or any other technology may be used in the acts of commerce and in the formation of the same. Therefore, simple electronic signatures ("SES") may be legally used to grant consent and execute commercial agreements, unless the nature of the act specifically requires a different type of consent or type of electronic signature.

In general, electronic signatures are valid, have the same legal effect as a wet signature and are admissible as evidence in court. However, the evidentiary weight of electronic signatures is determined by a judge taking into account (i) the purpose for which the parties intended to use the electronic signature; (ii) the specific circumstances and nature of each case; (iii) the reliability of the method used to manage, generate, process, sign, archive, communicate or retain the data messages; (iv) the ability to link the contents (including a signature) to the signers; and (v) the ability to access the signed document for subsequent reference. Often individuals believe that merely pasting a digital image of a wet signature into a document will serve as an adequate electronic signature. Such an approach, however, has the risk of not satisfying the above requirements or failing to have the same evidentiary weight, as an electronic signature generated by using a service like DocuSign's eSignature.

AES - Electronic signatures that meet certain additional requirements in terms of authentication and signatory identification, may qualify under Article 97 of the CC as an advanced or reliable electronic signature ("AES" or "RES"), which for purposes of this paper shall be specifically referred to as AES. Such requirements include (i) the signature creation data corresponding exclusively to the signatory; (ii) the signature creation data was, at the time of signature, under the sole control of the signatory; (iii) any alteration to the electronic signature, made after the time of signing, is traceable; and (iv) any alteration to the information in a data message, made after the time of signing, is traceable. Often traceability is addressed by an audit trail similar to DocuSign eSignature's certificate of completion, which is associated with the electronically signed document and includes information about the signatories, IP addresses, time of signature, etc. Electronically signed documents signed through DocuSign eSignature also have tamper evident protections that demonstrate whether a document has been altered after being signed. Therefore, electronic signatures generated through a service like DocuSign eSignature has greater evidentiary value in court than other less rigorous methods of electronic signing..

QES - It is noted that AES sometimes is confused with Qualified Electronic Signatures ("QES") in Mexico. QES is an AES electronic signature which is "qualified" by the CC under Articles 89 and 100 to 113 to have to satisfy certain additional heightened, government-mandated requirements related to in-person identification of signatories, authentication, and tamper evidence. These requirements include the electronic signature being supported by a digital certificate specifically associated with the identity of the signer, which is issued by a third-party vendor or Certification Service Providers ("CSP"), an entity which is licensed to issue such certificates by the Ministry of Economy.

While, at the outset, whether an electronic document has been altered or not, after its execution, is an evidentiary issue that typically is determined by a court on a case by case basis, Mexican regulators have tried to proactively tackle the integrity and inalterability requirement through explicit regulation. The NOM, issued by the Ministry of Economy, sets forth specific requirements to be observed for the conservation of data messages and digitalization of documents with regard to AES and QES. The underlining philosophy followed by the NOM is that only public key infrastructure ("PKI") electronic signature techniques are able to ensure document integrity. Hence, under the technical procedure embraced by the NOM, document integrity is preserved by requesting the CSP to participate in the execution and retention process. Specifically, the CSP receives the electronic envelope (a securely encrypted (hashed) document) from the parties to the agreement and allows for the execution of the document through its own electronic signature process whereby a time stamp also is added. This specific regulated process is known as a "Certificate of Conservation Service" (Servicios de Constancia de Conservación). This separate service is offered as an additional layer of evidentiary security by the CSP, which is in addition to what is already required for AES and is part of the requirements for QES. Hence, companies interested in adding this additional layer of protection in terms of evidential weight, may request a CSP to issue a Certificate of Conservation in connection with the electronic signing of a document.

Even though Section 2 of the NOM sets forth this technical standard as being expected in all business transactions, in reality, failing to adopt this standard does not automatically result in depriving documents signed electronically with adequate evidentiary weight. This interpretation is particularly reinforced by Article 98 of the CC which states the purpose of the qualification by the CSP is to determine and make the signers aware that AES complies with the reliability requirements set forth in sections I to IV of article 97 of the CC. The CC does not provide for such a qualification to be the sole method to assure compliance with the reliability requirements. In addition, the CC confirms that no legal effect, validity or binding force shall be denied to a signing method, solely for being electronic.

Public Sector

Similarly, to what occurs in the Private Sector, in the Public Sector, government entities are entitled by law to develop uses cases for electronic signatures using SES, AES and/or QES.

Since the beginning of this century, the Mexican government has allowed the use of electronic signatures for the filing of documentation with government authorities, such as the Federal Law of Administrative Procedure which under Article 69-C permits the use of electronic means for identification, in substitution of a wet signature or the Federal Law of Administrative Litigation Procedure which, under Article 1-A, XI, considers the use of a particular AES for online administrative procedures. The Mexican Tax Administration Service (SAT) is the most notable for using QES, whereby it embraces a QES model known now as "e.firma". This PKI scheme was developed under the Federal Tax Code (Código Fiscal de la Federación) and requirements for its operation have been further explained in various regulations issued by the Tax Authorities.

Similar to the SAT's QES approach, where it acts as the digital certificate root authority for issuing digital certificates for electronic signatures for the SAT, other government authorities act as the root authorities for their agencies including (i) the Unit for the Control of Signature Certification of the Judicial Branch of the Federation, (ii) the Bank of Mexico; and (iii) The Plenary of the National Institute of Transparency, Access to Information and Personal Data Protection.

Unfortunately, each of these digital certificate root authority regimes were developed independently both in legal and technological terms and each one has authorized specific entities (including its licensed agents) to issue specific digital certificates in connection with their specific transactions under their authority and oversight. For instance, the SAT is root authority for issuing digital certificates in connection with all transactions related to taxes. The Unit for the Control of Signature Certification of the Judicial Branch of the Federation is the root authority for issuing digital certificates in connection with specific AES use cases under its control (e.g. the electronic signature used by public officers for personal estate declarations or the use of AES on public procurement processes, etc.).

In an effort to harmonize these multiple public sector approaches for issuing digital certificates for use with electronic signatures, Mexico issued the AES Law, which is applicable only to government entities. The intention of the AES Law is to ensure that digital certificates issued by the multiple root authorities are compatible with one another, hence fostering the possibility of public entities feeling comfortable to develop further use cases for AES signatures, such as the FIREL signature, adopted by the Judiciary (further set out below). Further, in addition to the use of AES, the Mexican government also uses SES and QES for the provision of various services offered to citizens thereby allowing all three types of electronic signatures (SES, AES and QES) to coexist within the government. For example, payment of utility services or certain fines may be achieved online by using SES and payment of taxes require the use of QES.

Judiciary

Courts have been experimenting with electronic signature regulation since at least 2013 and are generally familiar with electronic signatures. One example is the "General Joint Agreement number 1/2013 of the Supreme Court, the Electoral Tribunal and the Council of the Federal Judiciary, regarding the Certified Electronic Signature of the Federal Judicial Power (FIREL) and the electronic files". This document provides the basis for the creation of a QES used by individuals to log into the judiciary digital system to file lawsuits and other actions, as well, to receive communications, notifications and/or official documents. The use of QES is deemed to have the same effect as using a wet signature.

International Treaties Framework

In addition to the UNCITRAL's Model Law on Electronic Signatures of 2001, there are other international treaties, which further add to the Mexican Legal Framework, including the United States-Mexico-Canada Agreement ("USMCA"). It is notable that the definition of electronic signature in the USMCA is well aligned with the electronic signature definition set forth in the CC. Specifically, the USMCA precludes the signing parties from denying the validity of a signature, just because of its electronic format, thereby reinforcing that electronic signatures generally are acceptable and fully valid in all commercial transactions. In those instances, in which a separate law requires a specific type of electronic signature, the signer must use that specific type of electronic signature to satisfy the specific requirements (e.g. a particular AES or a QES).

With regard to technology neutrality under the USMCA, parties to a commercial transaction, like under the CC, have the discretion to determine the technological methods of authentication or electronic signatures suitable for their particular transaction. With this technology neutral approach, parties have the right to prove to an authority, that their transaction complies with the legal requirements for the authentication of electronic signatures.

Ultimately, both under local laws and international treaties, Mexico has reaffirmed that it is committed to not adopting any future laws that would prevent parties from adopting any future technologies that would comply with these electronic signature requirements. Such an approach provides further certainty that electronic signatures are generally acceptable in Mexico and will continue to be consistently recognized as legally equivalent to a wet signature.

Summary Chart of Legal Framework

In the absence of a general "umbrella" law of electronic signatures applicable to transactions entered by private entities, the Mexican legal framework on electronic signatures has developed at different paces, resulting in an unfortunate and unnecessary complex array of laws and regulations addressing specific substantive and procedural rules. When assessing the effects of electronic signatures, the nature of the transaction, the parties to the transaction and the legal regime applicable to that transaction should be carefully considered.

To help with that evaluation, below is an initial list of laws and regulations that recognize the use of electronic signatures in Mexico:

Public sector

- Ley Federal de Procedimiento Administrativo
- Ley Federal del Procedimiento Contencioso Administrativo
- Acuerdo General Conjunto número 1/2013 de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al expediente electrónico.
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos
- Ley Orgánica de la Administración Pública Federal
- NORMA Oficial Mexicana NOM-004-SSA3-2012 Del Expediente Clínico
- Decreto por el que se establece la Ventanilla Digital Mexicana de Comercio Exterior
- Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación

Private sector

- Código Civil Federal
- Código Federal de Procedimientos Civiles
- Código de Comercio
- Código Fiscal de la Federación
- Circulares del Banco de México
  - Circular Telefax 6/2005
  - Circular Telefax 6/2005 Bis
  - Circular 23/2010
- Ley de Firma Electrónica Avanzada
- Ley de Amparo
- Ley Federal de Protección al Consumidor
- Ley Federal del Trabajo
- NORMA Oficial Mexicana NOM-151-SCFI-2002 Prácticas comerciales- Requisitos que deben observarse para la conservación de mensajes de datos
- Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación
- Reglas de Carácter General relativa a la Autorización como Perito Valuador de Inmuebles Objeto de Créditos Garantizados a la Vivienda
- Modificación a las Reglas de Carácter General relativas a la Autorización como Perito Valuador de Inmuebles Objeto de Créditos Garantizados a la Vivienda
- NORMA Oficial Mexicana NOM-151-SCFI- 2016
- United States-Mexico-Canada Agreement

Step 2
General overview of Mexican judicial system

Mexico is a civil law jurisdiction and its court system is established by the Mexican Federal Constitution. The Mexican Judicial System is composed by the Supreme Court of Justice, the Electoral Tribunal, the Circuit Courts (collegiate and unitary), the District courts and the Federal Judiciary Council. The federal courts have jurisdiction over specific subject matters, as provided in the Constitution (e.g., cases where the Federal Union or its entities are the plaintiff, the defendant or an interested party; cases involving the interpretation of Federal Laws; cases where the law specifically states that it is a Federal Case, among others). The state courts have residual jurisdiction over all remaining subject matters, resulting in the states having their own judicial system.

Article 17 of the Constitution establishes the adversarial principle and wide defense as a fundamental right of litigators in administrative or judicial procedures. Consequently, decisions issued by Lower Courts (first instance) are subject to appeal before a Higher Court (second instance). In some cases, if the parties claim that their human or constitutional rights were violated by the second instance resolution, this can be subject to a legal remedy for the protection of constitutional rights, called an Amparo proceeding, before Circuit Courts, as an extraordinary measure.

As a civil law jurisdiction, decisions issued by the Mexican Courts affect only the parties involved in a certain case and are generally not binding upon third parties (except for some types of binding decisions issued by higher courts, as provided in the applicable procedural law). However, it is customary practice that litigating parties and the judges do rely on precedents or jurisprudence to construe their arguments in other cases. Hence, in practice, uniform precedents tend to be more persuasive and exercise a greater influence over future decisions.

Step 3
Judicial rulings that support the use of electronic signatures

Even though electronic signatures have been generally accepted for some time, the widespread use of electronic signature in commercial transactions in Mexico is relatively new and noticeably increasing. Consequently, a small amount of cases involving the use of standard electronic signatures have been decided to date though there are cases pending before the courts. However, the decisions that have been issued to date do consistently support the admissibility and enforceability of standard electronic signatures, as it is shown in the case summaries to follow.

Judicial rulings

Época: Décima Época

Registro 2014545
Instancia Tribunales Colegiados de Circuito
Tipo de Tesis Aislada
Fuente Semanario Judicial de la Federación
Publicación Libro 43, Junio de 2017, Tomo IV, Pág. 2918
Materia(s) Civil
Tesis I.3o.C.264 C (10a.)

REQUIREMENT FOR AN ELECTRONIC SIGNATURES TO BE CONSIDERED ADVANCED OR RELIABLE

The Court determined that a contract is valid and a source of legal obligations when it is signed with an electronic signature, provided that the following reliability requirements are met: (i) the signature creation data corresponds exclusively to the signatory; (ii) the signature creation data was, at the time of signing, under the exclusive control of the signatory; (iii) it is possible to detect alterations in the electronic signature; and, (iv) it is possible to detect any alteration in the data message.

Época: Décima Época

Registro 2014544
Instancia Tribunales Colegiados de Circuito
Tipo de Tesis Aislada
Fuente Semanario Judicial de la Federación
Publicación Libro 43, junio de 2017, Tomo IV
Materia(s) Civil
Tesis I.3o.C.263 C (10a.)

ELECTRONIC SIGNATURE VALID AND LEGAL SOURCE OF OBLIGATIONS

The Court determined that a contract is valid and a source of legal obligations when executed using an electronic signature. The reliability in the creation of the electronic signature gives certainty to the signatory that only he or she knows about it, so that it can constitute (for him or her) a valid and certain source of obligations.

Época: Décima Época

Registro 2020107
Instancia Primera Sala Tesis Aislada
Fuente Gaceta del Semanario Judicial de la Federación
Publicación Libro 67, Junio de 2019, Tomo II
Materia(s) Civil
Tesis 1a. XLIX/2019 (10a.)

THE PERSONAL IDENTIFICATION NUMBER (PIN) IN BANK CARDS HAS THE CHARACTER OF AN ELECTRONIC SIGNATURE

The Court determined that the legal nature of a PIN number is that of a simple electronic signature, in accordance with the CC, since it involves data consigned, attached or associated in a data message, which serves both to identify the signatory and to indicate that the signatory approves the information contained in the data message. Therefore, simple electronic signatures are a valid method for binding an individual to a contract so long as such electronic signatures permit the identification of the signatory and the signatory's approval of the information is contained in the data message.

Época: Décima Época

Registro 2017776
Instancia Tribunales Colegiados de Circuito
Tipo de Tesis Aislada
Fuente Gaceta del Semanario Judicial de la Federación
Publicación Libro 57, Agosto de 2018, Tomo III
Materia(s) Civil
Tesis Tesis: V.3o.C.T.11 C (10a.)

THE DEFENDANT MUST PROVE THE AUTHORIZATION OF AN ELECTRONIC TRANSFER, BY MEANS OF THE DIGITAL CERTIFICATES WHICH SUPPORTS THE USE OF THE USER'S ELECTRONIC SIGNATURE

The Court determined that (i) electronic signatures are a valid method for binding an individual to a contract, as long as, they include a certificate which allows the confirmation of the link between a signatory and the electronic signature creation data; and (iii) the UNCITRAL Model Law may be used for interpretation purposes and are applicable to Mexican laws.

Conclusion

From the cases referenced above, Mexican Courts have expressly confirmed that: (i) electronic signatures are a valid method for binding an individual to a contract; (ii) electronic signatures are a source of rights and obligations; (iii) the UNCITRAL Model Law and the Guide for Enactment, may be used for interpretation purposes and are applicable to Mexican laws; (iv) the guiding principle of an electronic signature solution is the reliability of the signature creation method; and (v) the burden of proof for the vulnerability of an electronic signature, is for the person that claims it.

In addition, the Courts have determined that a contract is valid when it is signed with an electronic signature, provided that it: (i) allows the confirmation of the link between a signatory and the electronic signature creation data; and (ii) complies with the reliability requirements in the CC. The elements of certainty (e.g. time and date of the transaction) are presumed to the extent that there is reliability in the electronic signature creation process and that the systems are standardized for conducting business transactions through the use of electronic signatures. Following such recognition, the Courts have determined that an SES, such as a PIN number, are a valid method for binding an individual to a contract so long as such an approach permits the identification of the signatory and the signatory's approval of the information contained in the data message.

It should be pointed out that the Court rulings also reinforce the principle that a specific process or technology for electronic signatures is not required and that the above considerations may include any type of electronic signature that is reliable. The above also implies that one type of electronic signature is not necessarily more appropriate or reliable than an electronic signature using a different technology. Ultimately, an individual needs to consider the rigor of the electronic signature platform, such as DocuSign eSignature, that he or she is using and the confidence that such a platform will provide the individual with adequate evidentiary support should the transaction need to be enforced in a court of law.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040

2020.12.04