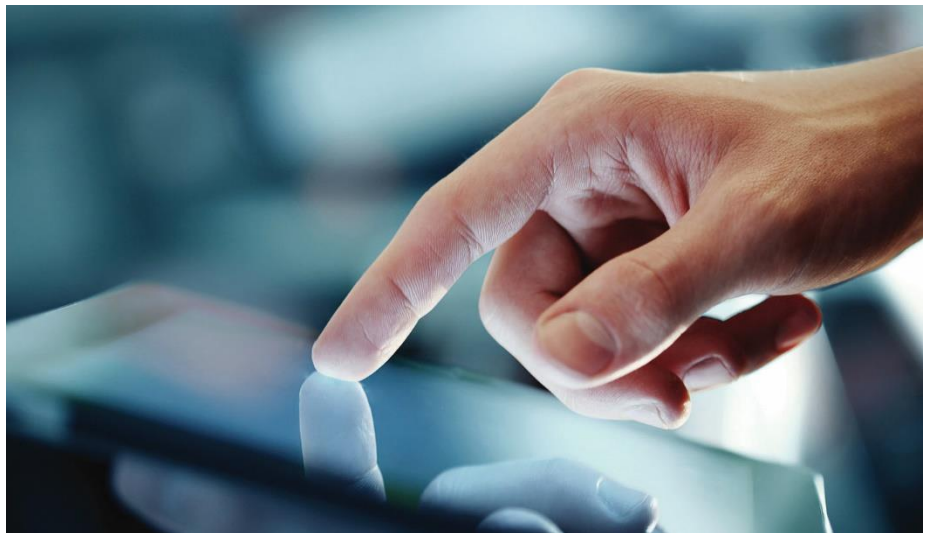


ARTICLE

SIGN ME UP, LOG ME IN, LET ME BEGIN:  
THE RISE OF DIGITAL SIGNATURES

APRIL 2020



---

“AN ELECTRONIC SIGNATURE IS TYPICALLY DEFINED AS DATA IN ELECTRONIC FORM WHICH IS (A) ATTACHED TO OR LOGICALLY ASSOCIATED WITH OTHER DATA IN ELECTRONIC FORM AND (B) USED BY THE SIGNATORY TO SIGN.”

The current COVID-19 crisis means most people are now working from home, at least for the next few weeks or even months. As a result, the use of ‘wet ink’ signatures and the traditional approach of pre-positioning original, hard-copy documents has become much more difficult. Businesses (and some government authorities) are looking more closely at how the use of electronic signatures might assist in overcoming such difficulties. Some like to use the term ‘digital signature’ instead of ‘electronic signature’, but is the difference properly understood?

The introduction of technology into the legal process for executing a legal instrument or taking some other legal action (such as acceptance, consent or approval) creates challenges. Given the variation of what might constitute an electronic signature, including how to recognise one, and the variation of its mode of application, means that lawyers still grapple with them. In addition, practical obstacles remain in relation to the validity of an electronically signed and executed instrument, particularly where it is an entity and not an individual who is the party to the instrument, where there are specific formalities that are difficult to follow. Examples of such formalities include executing a document as a deed, witnessing a document, or where the document needs to be filed and the filing authority does not recognise electronically signed instruments.

The focus of this article is digital signatures. Digital signatures, when used to execute a legal instrument in electronic form (an ‘Electronic Document’) or to take some other legal action electronically, such as acceptance of terms or an offer or the grant of a consent or approval, are a fusion of technology and law.

---

This article explains the difference between an electronic signature and a digital signature, what digital signatures look like, how they work and why they are more secure than 'simple' electronic signatures. It focuses on digital signatures as a technological solution for a legal problem, rather than the legal problem itself (plenty has been written about that already).

Given the firm's role in designing the online platform for the Global Aircraft Trading System ('GATS'), a platform whose core function is the use of digital signatures, this article draws from the GATS platform to illustrate many of the issues discussed.

## WHAT IS AN ELECTRONIC SIGNATURE?

The definition of an 'electronic signature' varies from jurisdiction to jurisdiction but is typically defined in electronic signature legislation as data in electronic form (which could be a symbol, an encrypted 'key', or a process) which is (a) attached to or logically associated with other data in electronic form (for example, an Electronic Document) and (b) used by the signatory to sign. Some electronic signature laws, such as U.S. federal law, additionally require that the signatory intend to sign the legal instrument or other data. Accordingly, an electronic signature could be constituted by a simple action such as checking a box or clicking a button. More commonly, electronic signatures (or visual representations of them) will attempt to mirror the appearance of a 'wet ink' signature and be represented as a scan of an individual's 'wet ink' signature on the signature page of an Electronic Document.

Generally speaking, the laws of most common law jurisdictions are permissive of the use of electronic signatures. Some jurisdictions, including the United States and the European Union, have enacted laws which expressly provide that an electronic signature is not to be denied legal effect solely on the basis that it is in electronic form.

The European Union has one of the most advanced electronic signature laws in the world. Under Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions (the 'eIDAS Regulation'), electronic signatures are categorised into three tiers according to the level of assurance that can be attributed to the authenticity and genuineness of the electronic signature. Thus, in addition to 'simple' electronic signatures, the eIDAS Regulation defines additional requirements for 'advanced electronic signatures' and 'qualified electronic signatures'; the latter, which must meet the highest standards, is given special legal status under the regulation.

## WHAT IS A DIGITAL SIGNATURE?

The term 'digital signature' is often misunderstood or misapplied. As a matter of technological practice, it is an encryption process used to logically and securely associate one set of data with another. However, as a matter of 'legal tech', it usually denotes a special type of electronic signature that has been applied, using an encryption process, to an electronic record, such as an Electronic Document). The encryption process typically utilised is a set of processes, procedures and policies known as 'public key infrastructure' ('PKI').

---

Because many electronic signature laws are deliberately technology-neutral, the term 'digital signature' *per se* does not have any legal meaning. It is purely a technical term and a digital signature can be used in a non-legal context or for non-legal reasons such as data security. Any electronic data is capable of being digitally signed (e.g. it is possible to digitally sign a video file, such as a movie), just as one could, using a wet ink signature, physically sign any object, such as a DVD case. Thus, like a 'wet ink' signature, a digital signature in and of itself may be without any legal meaning, unless under applicable law (a) it constitutes an 'electronic signature', and (b) the act of electronically signing that data has some legal effect or consequence such as executing a legal instrument, or the taking of some legal action, like granting consent.

That said, the cryptographic processes used to manage and generate digital signatures, such as PKI, typically satisfy, in full or in part, the additional requirements under the laws of those jurisdictions (e.g., the eIDAS Regulation) which recognise what are generally known as 'advanced' electronic signatures and which confer on such electronic signatures enhanced legal recognition.

## OBJECTIVES OF THE DIGITAL SIGNATURE METHODOLOGY

The objective of the digital signature methodology adopted by global, reputable and secure digital signature platforms ('Digital Signature Platforms') is to ensure reliability, integrity and security. To achieve this, a Digital Signature Platform, together with the Certificate Authority (see *The Role of the Certificate Authority* below), will need to manage and generate digital signatures which are:

1. uniquely linked to the individual who has applied it;
2. under that individual's sole control; and
3. linked to the Electronic Document to which it has been applied in such a way that any subsequent change to the Electronic Document (or, indeed, transposition of the digital signature onto another instrument) is easily detectable.

Digital signature methodology uses PKI. Under PKI principles, each individual signing documents using a Digital Signature Platform typically has their own 'digital identity', made up of three components:

1. A digital certificate issued to that individual (a 'Digital Certificate'). An individual's Digital Certificate contains information about their identity, about the certificate authority who issued it to them, about the Digital Certificate itself (e.g. its expiry date), and their Public Key (see below)
2. A public cipher or 'key' (a 'Public Key'). The details of an individual's Public Key are described in their Digital Certificate and can be used to verify any digital signature of that individual and make sure the Electronic Document to which it was applied has not been subsequently edited or tampered with.

3. A private cipher or 'key' (a 'Private Key'). When an individual digitally signs an Electronic Document, they do so using their Private Key. Each Private Key must be securely stored by the certificate authority while remaining accessible only to and under the sole control of the individual to whom it belongs.

Public Keys and Private Keys are the mathematical inverse of one another; for example, if data is encrypted using an individual's Public Key, then it can only be decrypted using their Private Key, and vice versa; however, Public Keys and Private Keys are generated in a way to ensure that no Public Key can be used or manipulated to generate its corresponding Private Key, and vice-versa.

While an individual's Digital Certificate is not itself used to digitally sign Electronic Documents or take other legal actions (that is done using the individual's Private Key, which should never be disclosed and should be under their control), the information contained in their Digital Certificate, including their Public Key, forms part of their digital signature. In so doing this allows each digital signature, and its application to the Electronic Document, to be independently verified.

## THE ROLE OF THE CERTIFICATE AUTHORITY

In connection with any Digital Signature Platform, the 'certificate authority' (a 'Certificate Authority') is a publicly trusted party responsible for issuing a Digital Certificate, a Public Key and a Private Key (i.e. a 'digital identity') to each individual user so that they can digitally sign Electronic Documents or take other actions using their digital signature. Sometimes the company hosting the Digital Signature Platform also acts as the Certificate Authority (for example, on the GATS online platform, Fexco, its host, also acts as the Certificate Authority). On other Digital Signature Platforms, the Certificate Authority is a third party and, depending on the platform, the individual may be able choose who they wish to act as their Certificate Authority from an approved list.

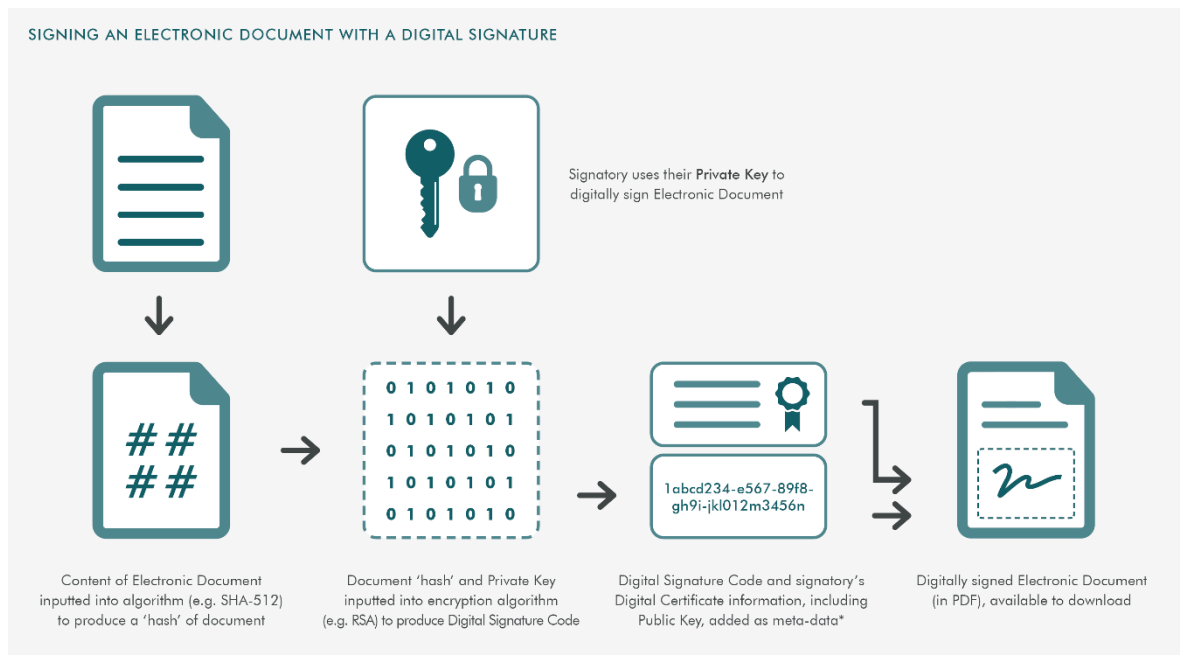
The Certificate Authority is also responsible for verifying the identity of any individual to whom it issues a Private Key and Digital Certificate (N.B. in other (non-legal) applications of digital signatures, identity verification is sometimes performed by a separate 'registration authority'). The existence of some reliable means to verify the identity of the signatory before they are issued with their Digital Certificate and Private Key is vitally important to the security and integrity of any Digital Signature Platform and any digital signature which has been applied to any Electronic Document using its services. Identity verification helps to ensure that, at the first instance, the signatory is who they say they are (i.e. they are not masquerading as someone else) and that their digital signature is uniquely linked to them. On the GATS online platform, this is achieved using a verification app which performs a facial recognition against a government-issued ID by activating the individual's smartphone camera (see *The GATS Online Platform: Customisation; addressing logistical and practical challenges – identity verification* below).

Some electronic signature laws, such as the eIDAS Regulation, provide a statutory framework and set of standards for ensuring the trustworthiness of and confidence in the Certificate Authority. Under the eIDAS Regulation, for example, for a 'qualified electronic signature' to qualify as such (thereby benefiting from additional legal

protections), the Certificate Authority must be a 'Qualified Trust Services Provider', meet certain minimum requirements, appear on a member state's trusted list, assume liability for its actions, and be subject to oversight by the applicable government supervisory body, in each case as set out under the eIDAS regulation.

## SIGNING AN ELECTRONIC DOCUMENT WITH A DIGITAL SIGNATURE

To digitally sign an Electronic Document, an individual uses their Digital Certificate and Private Key. The following diagram illustrates how an Electronic Document is digitally signed using a Digital Signature Platform:



\*Parts of this Digital Signature data are usually visually represented on the digitally signed Electronic Document

The digital signature 'code' (a 'Digital Signature Code') is a long, alpha-numeric string of characters which is generated by inputting the following data into the encryption algorithm: (a) the signatory's Private Key, and (b) a 'digital fingerprint' or 'cryptographic hash' of the contents of the Electronic Document.

Provided that both (a) the algorithm to generate the 'hash' from the contents of the Electronic Document, and (b) the encryption algorithm used to generate the Digital Signature Code from the 'hash' and the individual's Private Key, are strong enough (most Digital Signature Platforms will follow PKI technological standards and practices to ensure it is), it is not possible to reverse engineer the Digital Signature Code to solve for the Private Key, and it is only possible to solve for the document 'hash' using the same individual's Public Key. It is also mathematically impossible for two different Electronic Documents to produce the same Digital Signature Code. Therefore, even if the underlying Electronic Document were to change accidentally or intentionally by a single character, the digital signature would no longer be valid. In this way, the PKI cryptographic process used in digital signature methodology by

---

Digital Signatures Platforms is an important component in ensuring that digital signatures are reliable and secure.

Often in commercial transactions, individuals are not themselves parties to an Electronic Document; rather, one or more transacting legal entities are party to it (a 'Transacting Entity'). Digital Signature Platforms approach this in different ways. On the GATS online platform, individuals, to whom a Transacting Entity has granted signing privileges through the platform, digitally sign the Electronic Document on behalf of that Transacting Entity. Whether or not an individual has the legal authority to sign on behalf of an entity so as to make an Electronic Document binding and enforceable against that entity is a matter of applicable law. Thus, where an individual has digitally signed on behalf of a Transacting Entity using a Digital Signature Platform, other parties will need to request evidence of that Transacting Entity's corporate power and authority (often accompanied by a legal opinion covering such matters) in the usual way.

## WHAT DOES A DIGITAL SIGNATURE LOOK LIKE ON AN ELECTRONIC DOCUMENT, OR WHEN PRINTED?

Digital signatures exist as meta-data to the digitally signed Electronic Document (which is typically in PDF form) and can only be viewed, and technologically interrogated and verified, using special software (in the case of a PDF, typically Adobe Acrobat). Thus, when a digitally signed Electronic Document is printed, that meta-data, including any digital signature associated with it, will not be included in the pages of the printed version of the document. However, if the digital signature has been visually represented on the Electronic Document (see *Visual representation of Digital Signatures* below), that visual representation will remain visible on any printed version of the digitally signed Electronic Document.

A digital signature is technologically valid whether or not it is visually represented on the Electronic Document. Furthermore, under the laws of many jurisdictions, it may not need to be visible to be legally valid in order to constitute a valid electronic signature. However, whether the digital signature is *binding* on the individual who digitally signed it, and whether the document or instrument has been validly *executed* and binding on the Transacting Entity on whose behalf it was executed, are other legal matters which to be determined by applicable law.

Under PKI, the digital signature itself which, as mentioned above, is contained in the meta-data of the signed Electronic Document, is made up of the following:

1. The Digital Signature Code.
2. The information contained in the signatory's Digital Certificate, which includes their Public Key and other information about the individual signing the Electronic Document. This information can be used to validate the digital signature and its application to the Electronic Document (see *Validation of Digital Signatures* below).

---

## VISUAL REPRESENTATION OF DIGITAL SIGNATURES

A visual representation of the digital signature belonging to an individual executing an Electronic Document is often legally necessary where that individual is signing it on behalf of a Transacting Entity, because the visual representation and its positioning in an execution block is helpful (and usually required) to prove under applicable law that the Transacting Entity's execution of the document is legally valid.

On most Digital Signature Platforms, the digital signature of the individual or individuals executing an Electronic Document is visually represented on the 'signature page', and contained in an execution block, mirroring the location of a wet ink signature and the form of a paper-based document; however, the visual representation is not the digital signature itself.

A visual representation may also be necessary, if a digitally signed Electronic Document is to be filed with a government agency, to meet requirements of that government agency's electronic or digital signature policies.

## VALIDATION OF DIGITAL SIGNATURES

Any digital signature, and the exact contents of the Electronic Document to which it was applied, can be independently validated using the signatory's Public Key and other Digital Certificate information, provided that the Certificate Authority can be trusted and the Digital Signature Platform is secure.

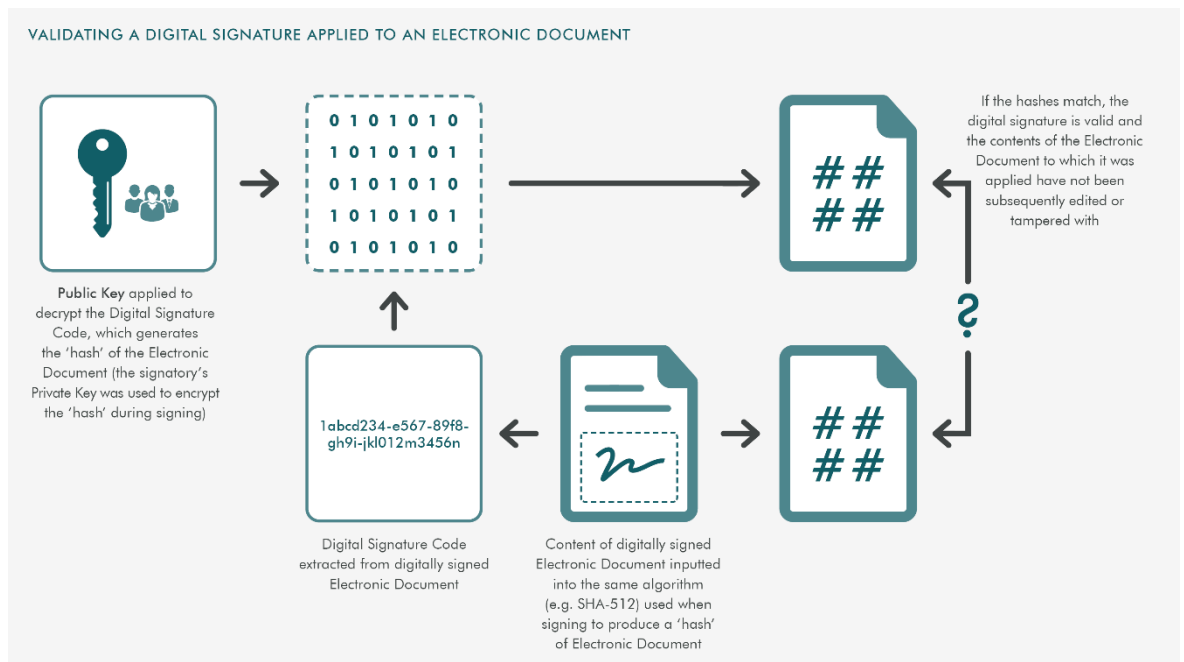
Validation is a major advantage of digital signatures over many other types of electronic signatures and is likely to be of great assistance in any legal dispute arising over its genuineness, authenticity or application to the Electronic Document.

Validation, in the context of using a digital signature to sign an Electronic Document, means demonstrating the following, with a substantial or high assurance level:

1. **Authentication:** Demonstrating that the digital signature is unique to, and therefore has been applied using, the signatory's Private Key. This can be independently validated, with mathematical certainty, using the signatory's Public Key (which forms part of the digital signature). Software that can interrogate the digital signature meta-data, such as Adobe Acrobat, can perform such validation.
2. **Data integrity:** Demonstrating that the contents of the digitally signed Electronic Document have not intentionally or inadvertently changed since the signatory applied their digital signature. This can be independently validated, with mathematical certainty, using the signatory's Public Key (which forms part of the digital signature). Software that can interrogate the digital signature meta-data, such as Adobe Acrobat, can perform such validation.
3. **Non-repudiation:** Demonstrating that the signatory can be identified, and their Private Key was under their sole control when they digitally signed the Electronic Document. This can be partially validated by checking their name

on their Digital Certificate (which forms part of the digital signature). However, the remainder of the validation is dependent on whether (a) the Certificate Authority is trusted and has adequately verified the identity of the signatory before issuing them with their Private Key and Digital Certificate, and (b) the Digital Signature Platform is secure and employs measures, such as two-factor authentication and secure storage of user data, to ensure that, in each case, no person other than the signatory was able to gain control of their Private Key, masquerade as the person to whom that Private Key was issued and fraudulently, innocently or mistakenly sign Electronic Documents using their digital signature.

The following diagram illustrates how a signatory's Public Key can be used to perform the 'authentication' and 'data integrity' elements of validation:



## VISUAL REPRESENTATION OF DIGITAL SIGNATURES ON THE GATS ONLINE PLATFORM

A sample of the visual representation of each individual signatory's digital signature on an Electronic Document executed using the GATS online platform (a 'GATS Instrument') is shown below. The whole execution block which, for each Transacting Entity, may contain one or more signatories (for compliance with applicable law or corporate governance requirements) is also shown for completeness:



<b>ANOTHER LEASING COMPANY, LLC</b> , as Beneficiary	
	By: John Smith
	Title: Manager
	GATS User ID: 012345
	Digital Signature Code: 9aeeee683-f262-41d3-ba4b-cfd080c4189a
	Signature timestamp and other Information: Wednesday 18 March 2020 20:23:10 UTC, DN: e-gats.aero, C: US, ST: Delaware, L: Wilmington, CN: John Smith

The visual representation has the following features and attributes:

1. The individual signatory's digital signature is visually represented on the signature page of the GATS Instrument by:
  - a. the Digital Signature Code being printed next to the printed name of the signatory, as well as their unique GATS User ID (so that that individual can be uniquely identified on the GATS online platform); and
  - b. a QR code containing the Digital Signature Code and other digital signature data.

Both the Digital Signature Code and the QR Code (when scanned using a QR code reader) can be used to authenticate, through the GATS online platform, the valid application of that digital signature by the signatory to the GATS Instrument.

2. The signatory's title within the Transacting Entity on whose behalf they are signing is shown as part of the digital signature data and the execution block.
3. A timestamp is provided identifying when the GATS Instrument was signed by the signatory. This is not the date and time of effectiveness of the GATS Instrument, but the actual time of the digital signature was applied (like the paper-based world, the digital signature is held in escrow until it is released; *see The GATS Online Platform: Customisation; addressing logistical and practical challenges – escrow facility* below).

## THE GATS ONLINE PLATFORM: CUSTOMISATION; ADDRESSING LOGISTICAL AND PRACTICAL CHALLENGES

There are several logistical and practical challenges posed by the use of electronic or digital signatures. The digital certificate methodology of a Digital Signature Platform may address many of these challenges. Outlined below are some of the challenges faced when the GATS online platform was being designed, together with an explanation of how the platform accommodates them.

### *Transacting entities and their signatories*

A core principle of the GATS online platform is that each Transacting Entity must have created an entity profile before it may execute GATS Instruments using the platform. Any individual user (who must have had their identity verified) whose GATS

---

user account is associated with that Transacting Entity is permitted, as a technological (rather than legal) matter, to digitally sign a GATS Instrument on behalf of that Transacting Entity.

#### *Escrow facility*

A core and prominent feature of the GATS online platform is that all GATS Instruments are executed in an 'escrow facility' (a 'GATS Escrow Facility'). The entity who creates the GATS Escrow Facility is appointed as the 'escrow coordinator' of that GATS Escrow Facility (the 'Escrow Coordinator'). The Escrow Coordinator need not be a Transacting Entity within the GATS Escrow Facility. In the GATS Escrow Facility environment, each individual's digital signature applied to execute a GATS Instrument on behalf of a Transacting Entity is held in escrow, analogous to the process of holding manually signed signature pages for paper-based documents. Accordingly, no GATS Instrument in the GATS Escrow Facility becomes effective until all digital signatures executing that GATS Instrument on behalf of the Transacting Entities are released (i.e. until the GATS Escrow Facility has closed).

As part of the GATS digital signature methodology, the process by which all such digital signatures are released, and each GATS Instrument in the GATS Escrow Facility becomes effective, is as follows:


1. Each Transacting Entity, acting through an individual who has a user account on the GATS online platform (and whose identity has been verified through the platform), must consent to the release of each signatory's digital signatures. The consenting individual's digital signature (who is acting on behalf of the relevant Transacting Entity) is also applied to the GATS Instrument to evidence, in the meta-data of the GATS Instrument itself, that such consent was given on behalf of the Transacting Entity and the time and date it was given;
2. After each Transacting Entity has given its consent to release its signatories' digital signatures, and provided that all 'advance requirements' (i.e. the conditions to the transaction that have been uploaded to the platform) have been confirmed as satisfied, the Escrow Coordinator may close the GATS Escrow Facility and release all signatories' digital signatures. Upon closing of the GATS Escrow Facility (a) the digital signature of the individual acting on behalf of the Escrow Coordinator is also applied to the GATS Instrument to evidence, in the meta-data of the GATS Instrument itself, that all signatories' digital signatures have been released, and (b) a timestamp, being the effective time of the GATS Instrument, is written onto the front cover of the GATS Instrument.

Therefore, each digitally signed GATS Instrument will contain multiple digital signatures in addition to those representing those of the signatories executing it on behalf of the Transacting Entities. In so doing, all steps required to make the GATS Instrument effective are given 'equal dignity' and the effectiveness of the GATS Instrument can be proven to the same degree of certainty to an independent adjudicator, such as a court of law.

#### *Configuration of execution block*

The GATS online platform allows each Transacting Entity to customise its execution block, by being able to add multiple layers of intermediate corporate authorisations.

For example, if the beneficiary of a GATS trust is a single member-managed limited liability company, and its sole member-manager is not an individual, this can be accommodated as shown below:


<b>ANOTHER LEASING COMPANY, LLC</b> , as Beneficiary	
	By: AIRCRAFT INVESTMENTS, L.P. Its: Sole Manager
	By: AIRCRAFT INVESTMENT FUND MANAGER, INC. Its: General Partner
	By: John Smith Title: Vice President GATS User ID: 012345 Digital Signature Code: 9aeec683-f262-41d3-ba4b-cfd080c4189a Signature timestamp and other Information: Wednesday 18 March 2020 20:23:10 UTC, DN: e-gats.aero, C: US, ST: Delaware, L: Wilmington, CN: John Smith

#### *Multiple signatories per transacting entity; Witnessing of Digital Signatures*

The GATS online platform allows each Transacting Entity to:

1. customise the number of signatories required to digitally sign the GATS Instrument on its behalf; and
2. toggle the ability to require the digital signature of each signatory to be witnessed and customise how many witnesses per signatory are required.

Where an individual's digital signature is to be witnessed, the witness must also hold a user account on the GATS online platform (they must also have had their identity verified), so that they can apply their digital signature to the GATS Instrument confirming that they witnessed the signatory digitally sign the document. The visual representation of the witness's digital signature on a GATS Instrument is shown immediately below the signatory's, and is visually represented as follows:

Witnessed by:	Jane Smith	
GATS User ID:	543210	
Digital Signature Code:	78hyre6g-s6hh-37g6-1bn0-jd6sgvsd7j89	
Signature timestamp and other Information:	Wednesday 18 March 2020 22:10:05 UTC, DN: e-gats.aero, C: US, ST: Delaware, L: Wilmington, CN: Jane Smith	

It is important to note that, under the electronic signature laws of most jurisdictions, for a witness's attestation to be legally valid, the witness must still, in person (e.g. by looking over their shoulder), witness the signatory apply their digital signature, even if the witness digitally signs as a witness in a separate location and at a later time.

#### *Identity verification*

Prior to an individual being allowed to digitally sign any GATS Instrument on the

---

GATS online platform, the individual is required to download an identification app on their mobile phone or smart device. The individual must then scan identification documentation and upload a live photo. The app compares the live photo against the photo on their identification document.

Identity verification helps to ensure that, at the first instance, the signatory is who they say they are (i.e. they are not masquerading as someone else) and that their digital signature is uniquely linked to them.

#### *Two-factor authentication*

The GATS online platform uses two-factor authentication every time a user logs in. This means that, in addition to being required to type their password, the individual user must also type a single use confirmation code sent to their mobile phone. The individual is required to give their mobile phone number at the time their identity was verified. This makes it very difficult for a person other than the verified user to log in using their account and use their digital signature.

Two-factor authentication helps to ensure that the signatory is the same person that initially set up their user account, and also helps to ensure that their digital signature remains under their sole control.

## CONCLUSION

Executing documents electronically can be made more secure and more convenient through the use of digital signatures and the encryption and identity verification processes on which they are built, but only if the processes are properly understood.

Those of us in the legal profession, especially those practising in cross-border transactions, rightly point to legal issues that may make the adoption of electronic signatures challenging. However, many of those challenges are often (but not always) illusory, because few practitioners in this area are both technologists and lawyers and therefore few have the expertise in both disciplines to bridge technology and law. Technologists, for their part, rarely understand the legal issues and too often trivialise them in technological products; lawyers also, as a notoriously conservative profession formed of many self-confessed technophobes, do not understand how the technology works and do not see an electronic signature as anything more sophisticated than an electronic scan-copy of a person's wet ink signature.

Digital signatures, and the Digital Signature Platforms through which they can be used and applied, will soon become a part of every lawyer's workday. As part of an automation drive, the legal profession is on the cusp of widescale adoption of transaction management applications, document management applications and Digital Signature Platforms being integrated into a single application to streamline the delivery of legal services. Clients, and the business of running a profitable law firm, will demand it. Every lawyer should be telling themselves, when it comes to digital signatures, 'sign me up, log me in, let me begin.'

---

## FOR MORE INFORMATION

---

Should you like to discuss any of the matters raised in this briefing, please speak with the author below or your regular contact at Watson Farley & Williams.



**DOMINIC PEARSON**  
Of Counsel  
London

+44 20 3314 6457  
[dpearson@wfw.com](mailto:dpearson@wfw.com)

Publication code number: Europe\66513693v1 © Watson Farley & Williams 2020

All references to 'Watson Farley & Williams', 'WFW' and 'the firm' in this document mean Watson Farley & Williams LLP and/or its Affiliated Entities. Any reference to a 'partner' means a member of Watson Farley & Williams LLP, or a member or partner in an Affiliated Entity, or an employee or consultant with equivalent standing and qualification. The transactions and matters referred to in this document represent the experience of our lawyers. This publication is produced by Watson Farley & Williams. It provides a summary of the legal issues, but is not intended to give specific legal advice. The situation described may not apply to your circumstances. If you require advice or have questions or comments on its subject, please speak to your usual contact at Watson Farley & Williams.

This publication constitutes attorney advertising.