GATS
Global Aircraft Trading System

MEMORANDUM

GATS DIGITAL SIGNATURE METHODOLOGY

This memo explains what digital signatures are, how they work, and the processes by which the Global Aircraft Trading System (**GATS**) electronic platform (the **GATS Platform**) uses digital signature technology to enable users on the GATS Platform to digitally sign and execute, on behalf of entities, GATS trust instruments and other related instruments, each in electronic form and which has been generated by the GATS Platform from the applicable GATS standard form (**GATS Instruments**), avoiding the need for traditional, paper-based documents and 'wet ink' signatures. The focus of this memo is on the technology and process. The GATS Guidance Materials contain further information, analysis and legal opinions on the enforceability of GATS Instruments digitally signed using the digital signature methodology of the GATS Platform.

Objectives of the GATS Digital Signature Methodology

Like other global, reputable and secure online platforms which facilitate the digital signing and execution of legal documents, the objective of the digital signature methodology adopted by the GATS Platform (the **GATS Digital Signature Methodology**) is to ensure reliability and security. To achieve this, the GATS Platform manages and generates 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 GATS Instrument in such a way that any subsequent change to the GATS Instrument (or, indeed, transposition of the digital signature onto another instrument) is easily detectable.

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 a legal document or instrument in electronic form (**Electronic Documents**). The encryption process typically utilized is a set of processes, procedures and policies known as 'Public Key Infrastructure' (**PKI**).

Because many of 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. Any electronic data is capable of being digitally signed (e.g. it is possible to digitally sign a video file, such as a movie). Thus, 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 authenticating some action, like granting consent.

That said, the cryptographic process used to manage and generate digital signatures, such as PKI, typically satisfies, in full or in part, the additional requirements under the laws of those jurisdictions which recognize what are generally known as 'advanced' electronic signatures and which confer on such electronic signatures stronger legal recognition.

What does a Digital Signature look like on an Electronic Document?

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 document. However, if the digital signature has been visually represented on the Electronic Document (see *Visual Representation of Digital Signatures on the GATS Instruments* below), if the digitally signed Electronic Document is printed that visual representation will remain visible.

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 signature. However, whether the signature is *binding* on the individual who digitally signed it, and whether the document or instrument has been validly *executed* and binding on a legal entity on whose behalf it was executed, are other legal matters which to be determined by applicable law.

Under PKI principles, when an individual digitally signs an Electronic Document, they do so using their own private digital 'key' (a **Private Key**). On the GATS Platform, each Private Key is securely stored in Fexco's encrypted 'key vault' while remaining accessible only to and under the sole control of the Digital Certificate User to whom it belongs.

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

1. A digital signature 'code' (a **Digital Signature Code**). This is a long, alpha-numeric string of characters which is generated by an encryption algorithm from combining two sets of data: (a) that individual's Private Key, and (b) a 'digital fingerprint' or 'cryptographic hash' of the Electronic Document.

2. The information contained in their Digital Certificate, which includes about information about the individual signing the Electronic Documents. This information can be used to verify the digital signature and its application to the Electronic Document.

Digital Certificates and Public Key Infrastructure (PKI)

The GATS Digital Signature Methodology uses PKI. Each individual who has a GATS user account and exists as a Digital Certificate User on the GATS Platform has their own 'digital identity'. Under PKI principles (and on the GATS Platform), a Digital Certificate User's 'digital identity' is made up of three items:

1. A Digital Certificate issued to that individual by Fexco, as the trusted 'certificate authority'. An individual's Digital Certificate contains information about their identity, information about the certificate authority who issued it to them, information about the Digital Certificate itself (e.g. its expiry date), and their Public Key (see below).

2. A public digital 'key' (a **Public Key**). An individual's Public Key is contained in their Digital Certificate and can be used to verify any digital signature of that individual and make sure the GATS Instrument to which it was applied has not been subsequently edited.

3. Their Private Key. 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.

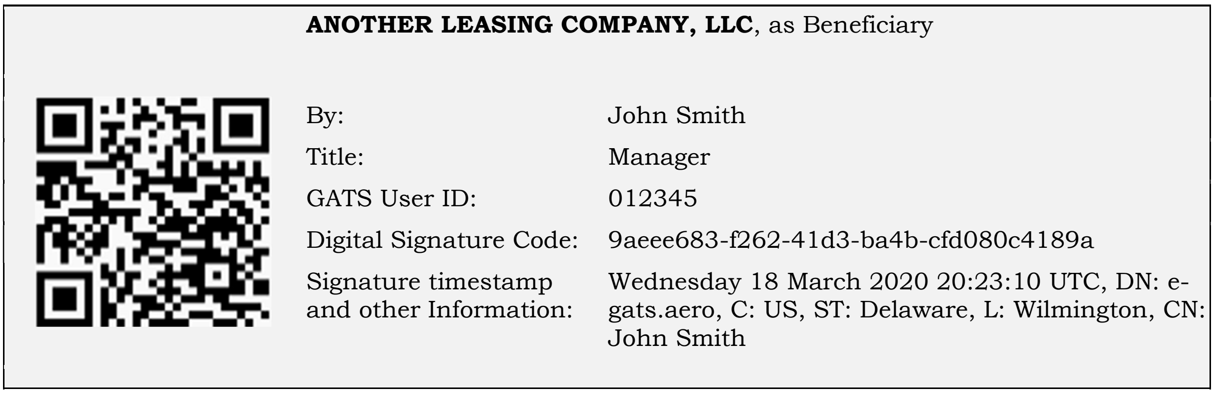
Every Digital Certificate User on the GATS Platform has their own Digital Certificate. While their Digital Certificate is not itself used to digitally sign GATS Instruments or digitally authenticate other actions they take on the GATS Platform (that is done using their Private Key, which is never disclosed and is 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.

Visual Representation of Digital Signatures on the GATS Instruments

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

Accordingly, the digital signature of the individual or individuals executing a GATS Instrument on behalf of each GATS Entity party to it (a **Transacting Entity**) 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. A visual representation may also be necessary, if a digitally signed Electronic Document is to be filed with a government agency (e.g. the FAA or other aviation authority), to meet requirements of that government agency's electronic or digital signature policies.

A sample of the visual representation of each individual signatory's digital signature on 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:



ANOTHER LEASING COMPANY, LLC, as Beneficiary

By:	John Smith
Title:	Manager
GATS User ID:	012345
Digital Signature Code:	9aeee683-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 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 the valid application of that digital signature by the signatory to the GATS Instrument (see *Authentication of Digital Signatures* below).

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 *Consent to Release, Release and Effectiveness of GATS Instruments* below).

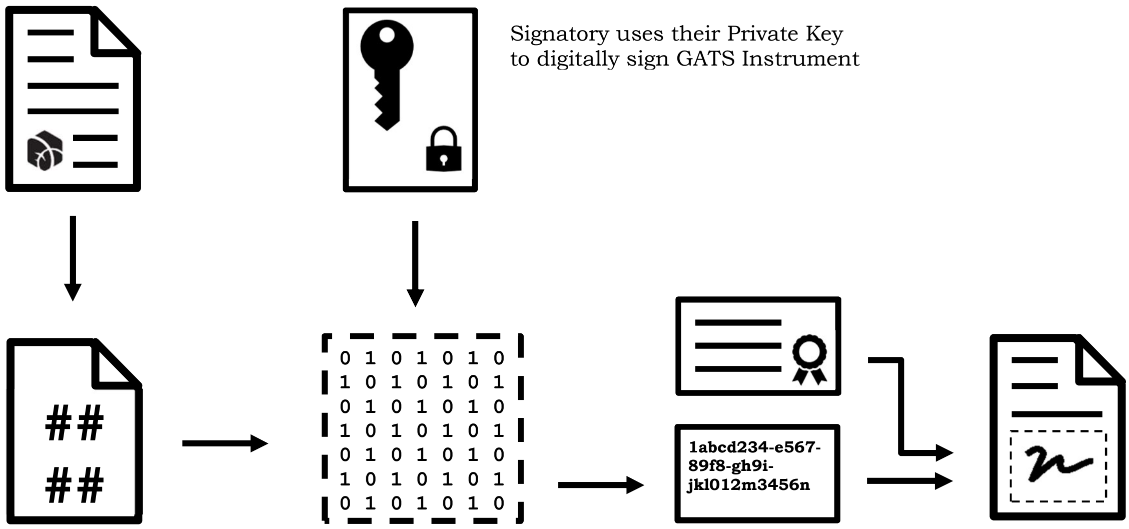
Escrow Facility

A core and prominent feature of the GATS Platform is that all GATS Instruments are executed in an Escrow Facility. The entity who creates the Escrow Facility is appointed as the Escrow Coordinator of that Escrow Facility. The Escrow Coordinator need not be a Transacting Entity within the Escrow Facility. In the 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. At closing, each such digital signature is released and a timestamp, being the effective time of the GATS Instrument, is written onto the front cover of the GATS Instrument. The release process is described in *Consent to Release, Release and Effectiveness of GATS Instruments* below.

Signing a GATS Instrument with a Digital Signature

Individuals are not themselves parties to a GATS Instrument; rather, one or more Transacting Entities are party to it. Individuals, to whom a Transacting Entity has granted signing privileges through the GATS Platform, digitally sign the GATS Instrument on behalf of that Transacting Entity. Whether or not an individual has the legal authority to sign on behalf of an entity so as make the GATS Instrument binding and enforceable against that entity is a matter of applicable law. Thus, users of the GATS Platform will need to request evidence of a Transacting Entity's corporate power and authority (often accompanied by a legal opinion covering such matters) in the usual way.

The following diagram illustrates how an individual, who has a user account on the GATS Platform as a Digital Certificate User, uses their Digital Certificate and Private Key to digitally sign a GATS Instrument (on behalf of a Transacting Entity), and how their digital signature is created on the GATS Instrument:



Signatory uses their Private Key to digitally sign GATS Instrument

Content of legal Instrument inputted into algorithm (SHA-512) to produce a 512 bit 'hash' of document

Document 'hash' and Private Key inputted into encryption algorithm (RSA) to produce Digital Signature Code.

Digital Signature Code and signatory's Digital Certificate information, including Public Key, added as meta-data [*]

Digitally Signed GATS Instrument (in PDF), available to download

[*] Parts of this Digital Signature data are visually represented on the signed GATS Instrument

The Digital Signature Code is generated by inputting the following data into the encryption algorithm: (a) the signatory's Private Key, and (b) a 'hash' of the contents of the GATS Instrument.

Provided that both (a) the algorithm to generate the 'hash' from the contents of the GATS Instrument, and (b) the encryption algorithm used to generate the Digital Signature Code from the 'hash' and the individual's Private Key, are strong enough (the GATS Platform follows 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 or the document 'hash'. It is also mathematically impossible for two different GATS Instruments to produce the same Digital Signature Code. Therefore, even if the underlying GATS Instrument were to change accidently or intentionally by a single character then the digital signature would no longer be valid. In this way, the PKI cryptographic process used by digital signatures is an important component in ensuring that digital signatures on the GATS Platform are reliable and secure.

The utilization of PKI as part of the GATS Digital Signature Methodology means that, provided that only the Digital Certificate User has access to their Digital Certificate and Private Key on the GATS Platform (see further, *Identity Verification of Signatories* and *Two-Factor Authentication* below), it can be mathematically proven to an independent adjudicator, such as a court of law, that only that Digital Certificate User could have digitally signed a GATS Instrument containing their digital signature.

Execution and Digital Signature Customization

To accommodate requirements under applicable law relating to a GATS Instrument or a Transacting Entity executing it, or as required under that entity's constitutional documents, the GATS Platform allows users to customize the execution of GATS Instruments in the following ways.

Configuration of Execution Block

The GATS Platform allows each Transacting Entity to customize its execution block, by being able to add multiple layers of intermediate corporate signatories. 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:

ANOTHER LEASING COMPANY, LLC, 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:	9aeee683-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

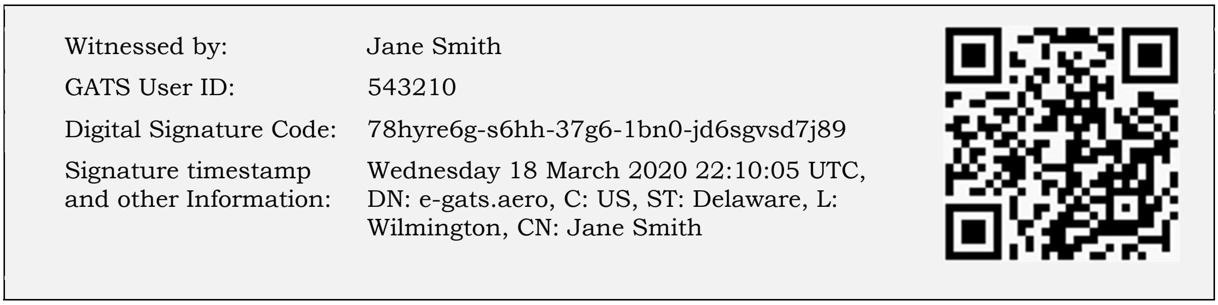
Multiple Signatories per Transacting Entity; Witnessing of Digital Signatures

The GATS Platform allows each Transacting Entity to:

1. customize 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 customize how many witnesses per signatory are required.

Where an individual's digital signature is to be witnessed, the witness must also be a Digital Certificate User with a user account on the GATS Platform, 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 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.

Consent to Release, Release and Effectiveness of GATS Instruments

In the Escrow Facility environment, initially, each signatory's digital signature to a GATS Instrument is held in escrow. Accordingly, no GATS Instrument in the Escrow Facility become effective until all digital signatures executing that GATS Instrument on behalf of the Transacting Entities are released (i.e. until the 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 Escrow Facility becomes effective, is as follows:

1. Each Transacting Entity, acting through an individual who has a user account on the GATS Platform and who must be a Digital Certificate User, 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 (a) all Advance Requirements have been confirmed as satisfied, and (b) if there is one, authorization to close the Escrow Facility exists under the Escrow Facility Agreement, the Escrow Coordinator may close the Escrow Facility and release all signatories' digital signatures. Upon closing of the Escrow Facility, 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.

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 (except for steps, if any, required under an applicable Escrow Facility Agreement) 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.

Identity Verification

Prior to an individual being allowed to digitally sign any GATS Instrument on the GATS Platform, they must become a Digital Certificate User. To become a Digital Certificate User, 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

In order for a Digital Certificate User to login, they must use two-factor authentication. This means that, in addition to being required to type their password, they 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 login 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 as a Digital Certificate User, and also helps to ensure that their digital signature is remains under their sole control.

Checking the Authenticity of Digital Signatures through the GATS Platform

If viewed in Adobe Acrobat, it should be clear using the tools available in the Acrobat software whether the PDF of a digitally signed GATS Instrument is authentic.

If a person is a provided with an electronic scan or printed copy of a digitally signed GATS Instrument, and they are unsure whether it is authentic, they may check the authenticity of the document by downloading a copy of it directly from the GATS Platform. This can be achieved in one of two ways:

1. Using any QR code scanner, by scanning the QR code on the front cover or the QR Code next to the visual representation of any signatory's digital signature.

2. By navigating to http://e-gats.aero/authenticate/ and typing either the Transaction ID (on the front cover of the GATS Instrument) or the Digital Signature Code of any signatory's digital signature, printed in the visual representation of a signatory's digital signature.

END OF MEMORANDUM

Prepared by Watson Farley & Williams LLP for Aviation Working Group, March 2020.