GATS Digital Certificate Policy and Certification Practice Statement

Version 1.0

Fexco Technology Solutions

20 May 2020

Table of Contents **Page**

A. Overview

a. Introduction

This GATS Digital Certificate Policy (the "**Policy**") establishes the rules for accessing and using the facility for signing instruments electronically and digitally on the platform (the "**GATS Platform**") for the Global Aircraft Trading System ("**GATS**") currently hosted on the website, http://e-gats.aero/ (the "**Website**") in accordance with the **GATS E-Terms** and the **GATS Site Terms of Use**.

The GATS Platform includes the computerised ledger and system (the "**GATS e-Ledger**") in which transactions ("**Designated Transactions**"), executed electronically and digitally through the GATS Platform, are entered and recorded.

The GATS Platform is operated by Fexco Unlimited Company ("**Fexco**") on behalf of the Aviation Working Group ("**AWG**").

b. Application

The GATS Platform gives certain users the ability to sign instruments electronically and digitally give effect to Designated Transactions ("**GATS Instruments**"), and to authenticate the taking of other actions, through the GATS Platform using a digital certificate issued to the Digital Certificate User (a "**GATS Digital Certificate**"). A GATS Digital Certificate enables such users to apply their digital signature (a "**Digital Signature**") to such instrument or action.

For more information on digital signatures and their use on GATS, see the **GATS Digital Signature Methodology** memorandum available on the GATS Platform.

This Certificate Policy is intended to inform users of their rights and obligations. It also sets out the terms and conditions that apply to the issue and use of GATS Digital Certificates issued on the GATS Platform.

c. Scope and Limitations

GATS Digital Signatures and the GATS Digital Certificates giving effect to them, are not available to the general public. GATS Digital Signatures are available for use by, and GATS Digital Certificates will be issued only to, natural persons who have:

(i) requested to participate in the GATS Platform by applying to become a Digital Certificate User;

(ii) been cleared as Digital Certificate Users on the GATS Platform; and

(iii) agreed to the GATS e-Terms that apply to using the GATS Platform and to the use of GATS Digital Certificates

(each a "**Digital Certificate User**").

Digital Certificate Users are natural persons who will access or use the GATS Platform for use in connection with that person's trade, business, craft or profession on behalf of a business which has its own legal identity separate from the legal identity of any individual or group or individuals ("**Business Individuals**").

GATS Digital Certificates cannot be issued to entities or bodies corporate or any person that is not a natural person.

GATS Digital Signatures and GATS Digital Certificates cannot be used for any purpose other than use by Digital Certificate Users when effecting Designated Transactions and taking certain other actions on and within the GATS Platform for and on behalf of a GATS Entity, and only in the manner permitted under and subject to the conditions of the **GATS e-Terms**, the **Site Terms of Use** and all other terms, policies, notices, disclaimers and schedules incorporated into the GATS e-Terms and the Site Terms of Use (the "**Associated Documentation**").

Section C of this Policy sets out in more detail the conditions of use of GATS Digital Certificates.

d. Role of Fexco as Certificate Authority

Fexco is the entity responsible for issuing GATS Digital Certificates to Digital Certificate Users for use on the GATS Platform. Fexco's contact details are as follows:

Name	Fexco Unlimited Company
Company Number	83934
Registered Office	Fexco Centre, Iveragh Road, Killorglin, Co. Kerry, Ireland
FAO	The Company Secretary
Telephone Number	+353 669761258
Internet Address	www.fexco.com
24/7 GATS Helpdesk	helpdesk@e-gats.aero

The root certificate used by Fexco in the GATS Digital Certificates is issued by Digicert, Inc. Digicert's contact details are as follows:

Name	Digicert, Inc.
Registered Office	North Thanksgiving Way #500, 2801 Lehi (UT), United States of America
FAO	Support
Telephone Number	+1 8008967973
Internet Address	https://www.digicert.com/
Helpdesk	Americas +1 8017019600 Asia Pacific, Japan +61 396745500 Europe, Middle East Africa +44 2037887741

Fexco, as issuer of GATS Digital Certificates, meets the requirements of:

(i) a 'certification service provider' under and as defined in the Irish E-Commerce Act 2000 (the "**ECA**"), and

(ii) a 'trust service provider' under and as defined in the Regulation (EU) No 910/2014 (the "**eIDAS Regulation**").

GATS Digital Signatures provided by Fexco on the GATS Platform meet the requirements of:

(i) an 'Advanced Electronic Signature' as defined in the ECA, and

(ii) the requirements of an 'Advanced Electronic Signature' as defined in the eIDAS Regulation.

GATS Digital Certificates will meet:

(i) the requirements of a 'qualified certificate' under and as defined in the ECA; and

(ii) the definition of a 'certificate for electronic signature' in the eIDAS Regulation.

Fexco is not a Qualified Trust Service Provider under and as defined in the eIDAS Regulation and in its role as Trust Service Provider in the context of the GATS Platform is not providing any Qualified Trust Services as defined in the eIDAS Regulation.

Section D of this Policy, Operational and Security Controls, sets out the technical standards which GATS Digital Certificates meet.

B. Identification and Verification

This section sets out the identification and verification practices employed by Fexco in order to allow Fexco to issue GATS Digital Certificates to Digital Certificate Users for use on the GATS Platform.

a. Timing of Identity Verification

Business Individuals who wish to use the GATS Platform must first register as Basic Users in the manner described in the Site Terms of Use. On successful completion of that registration, Basic Users can apply to become Digital Certificate Users as more particularly described in paragraph 12 of the Site Terms of Use.

At the time Basic Users are applying to become Digital Certificate User, each such applicant (each, an "**Applicant**"), who must be natural persons who are a Business Individual and submitting an application on their own behalf will engage in an identity verification process with Fexco, that will then enable Fexco to issue GATS Digital Certificates to such Digital Certificate Users to use as they require within the confines and parameters of the GATS Platform.

An application to become or remain a Digital Certificate User will not be successful unless the first and last name with which the Basic User has used to create a User Account matches exactly the first and last name on such Applicant's identification document submitted for registration as a Digital Certificate User.

Before commencing the identification verification process, each such Applicant will be required to confirm their acceptance of the **Site Terms of Use**, which includes an acknowledgment and acceptance that Fexco will, as part of the Digital Certificate User application process, undertake this identity verification process on the Applicant, and will authenticate the data and documentation presented by the Applicant to support the application for verification.

b. Remote Verification

Fexco employs a system of remote verification of each Applicant, using electronic identification software, which is designed to provide equivalent assurance to verification by physical presence. For this purpose Fexco uses a remote identification process provided by a third party provider ("**Identity Verification Provider**").

Applicants will be given a link and instructions on how to download the user verification application (the "**Verification App**") of the Identity Verification Provider via their smartphone or other smart device.

Within 28 days from the time Applicants download the Verification App, the Applicant must complete the following identification verification process:

(i) Applicants must take a photo via the Verification App of either a valid, current passport or current driving licence. The document provided must contain data identifying you using the modern Latin alphabet (i.e. it must not be written exclusively in, for example, Cyrillic or Arabic script); and

(ii) Applicants must take a picture of themselves (a "**Likeness Photo**") via the Verification App and upload it.

By applying to become a Digital Certificate User and submitting the required documentation and information, each Applicant agrees that true, complete and accurate information has been provided when the application was made.

Once the Applicant has submitted the application process to become a Digital Certificate User Fexco will take the following steps to verify the identity of the Applicant:

(i) A series of automated checks will be run by the Identity Verification Provider against the Applicant's identity document presented for verification to confirm its authenticity;

(ii) Facial recognition software will be applied by the Identity Verification Provider to carry out a biometric assessment of the image on the Likeness Photo against the photo on the Applicant's identity document to confirm that these are the same; and

(iii) The application will then be reviewed by Fexco to manually check the information you have provided and to review any other information provided to it by the Verification App relating to your application.

The manner in which the identification documentation and Likeness Photo provided by the Applicant will be processed and stored by AWG is set out in the AWG Privacy Policy and by Fexco is set out in the Fexco Privacy Policy.

c. Manual Verification

If an Applicant does not consent to the processing of biometric data as part of the remote verification process described in (b) above, an alternative, manual verification process will be provided.

In addition, if the remote verification process described in (b) above cannot be completed due to an issue with the information or documentation provided (for example, if the Likeness Photo is blurry or the document is damaged):

(i) The Applicant will be notified by email that the application is not yet complete and that additional verification steps may be required; and

(ii) The application will be continue to be processed in accordance with the **GATS Secondary Verification Policy**.

In the event that, in accordance with the Secondary Verification Policy, an Applicant's application to become Digital Certificate User is determined to be unsuccessful, such determination will not have been made using an automated process.

Applicants who fail to meet Fexco's identity verification requirements will not be issued with GATS Digital Certificates.

d. AWG Additional Registration Requirements

In addition to the identity verification process undertaken by Fexco, AWG requires that, as a condition to becoming a Digital Certificate User, a series of checks will be run against the Applicant's name with sanctioned person databases, watch lists and other public domain databases to obtain other information about the Applicant that is relevant to his or her application.

Failure by an Applicant to pass these AWG checks will result in such Applicant's application to become a Digital Certificate User being unsuccessful, and such Applicant will not be issued with a GATS Digital Certificate.

e. Identification Verification Timeframe

Applicants who have submitted the required documentation and information to the Verification App will be contacted within 24 hours with confirmation as to whether the application has been successful or whether further documentation or information is required.

If further information is required pursuant to and in accordance with the procedures described in the Secondary Verification Policy, this must be submitted as soon as possible and in any event within 28 days of the initial application for registration. Applications which have not completed within 28 days will be automatically be cancelled.

f. Refusal to Register

Applicants will be informed if their application to become a Digital Certificate User is unsuccessful. Neither Fexco nor AWG will be required to justify to the Applicant the reason why their application did not succeed.

g. Non-Verified Information

Some information provided or submitted by users during the process to become a Basic User or a Digital Certificate User or during the process of using any of the functionality on the GATS Platform is not verified by Fexco.

This information (Non-Verified Information) includes the address and telephone number of the Basic or Digital Certificate Users. It also includes any organisational information relating to any GATS Entity or Non-GATS Entity that is created by a user on the GATS Platform (an Entity Administrator), any

association made by an Entity Administrator between a user and a GATS Entity, or any confirmation by an Entity Administrator that a Digital Certificate User is a signatory of a GATS Entity.

Fexco is not responsible for the accuracy or veracity of this Non-Verified Information and Fexco does not undertake any verification of the organisational identity of any GATS Entities created on the GATS Platform.

h. Refreshing Identity Verification

On or prior to each anniversary that a Business Individual became a Digital Certificate User, such users must renew their status as a Digital Certificate User following the same identity verification process set out in (ii) and (iii) above.

Any Digital Certificate User who fails to renew their status and refresh their identity verification in the required timeframe will, in addition to other consequences outlined in the Site Terms of Use, have their GATS Digital Certificate revoked.

i. Naming

All GATS Digital Certificate Users require a Distinguished name ("**DN**") that complies with the X.500 standard for Distinguished Names. This means that Distinguished Names for Certificates must be meaningful so that the certificate can uniquely identify the user to whom the certificate is issued.

A DN is a term that describes the identifying information in a certificate and is part of the certificate itself. A certificate contains DN information for both the owner or requestor of the certificate (the Subject DN) and the CA that issues the certificate (the Issuer DN). The DN in GATS Digital Certificates will be populated with the following information:

- SERIALNUMBER Certificate serial number
- MAIL Email address
- UID or USERID User identifier
- CN Common Name
- T Title
- STREET Street / First line of address
- L Locality name
- ST (or SP or S) State or Province name
- PC Postal code / zip code
- C Country

C. Certificate Life Cycle Operations and Terms of Use

a. Overview

All life-cycle operations of GATS Digital Certificates are managed securely by Fexco by appropriately qualified and experienced personnel within the confines of predefined processes and controls which are strictly regulated. The life-cycle operations managed by Fexco include:

- Certificate Issuance
- Certificate Usage and associated conditions and limitations
- Certificate Renewal
- Certificate Revocation
- Certificate Validation

b. Certificate Issuance

GATS Digital Certificates will be issued by Fexco to Digital Certificate Users automatically at the time they are cleared as Digital Certificate Users on GATS, following successful completion of the identity verification process set out in section B of this Policy, and any other additional registration requirements prescribed by AWG.

The *SHA512WithRSAEncryption* algorithm is used to safeguard the issuance and sealing of GATS certificates.

c. Certificate Usage

GATS Digital Certificates are used by a Digital Certificate User on the GATS Platform to sign GATS Instruments giving effect to Designated Transactions and to authenticate the taking of other actions involving a GATS Entity. The way in which GATS Digital Certificates can be used for these purposes is described in more detail in paragraph 16 of the Site Terms of Use.

GATS Digital Certificates are stored in the GATS Digital Certificate repository which is centrally and securely managed within the GATS Platform. The GATS Digital Certificate for a Digital Certificate User will be automatically applied when a Digital Certificate User uses the functionality on GATS platform to complete a Designated Transaction or authenticates the taking of other actions involving a GATS Entity.

There is no requirement for Digital Certificate Users to store or save any private keys on their device. GATS Digital Certificates are not device specific and Digital Certificate Users can apply their Digital Signature from any device once they have logged in securely to the GATS Platform using their Security Credentials (as defined in the **Site Terms of Use**).

GATS Digital Signatures and GATS Digital Certificates can only be used by the Digital Certificate User to whom the GATS Digital Certificate has been issued. To retain a level of security in this regard,

Fexco uses multi-factor authentication to users wishing to apply a GATS Digital Signature using a GATS Digital Certificate. Each time a Digital Certificate User wishes to use the functionality on the GATS Platform to apply a GATS Digital Certificate the user will need to log in to the GATS Platform and pass the MFA challenge.

d. Conditions and Limitations on Use and Issuance

The use of GATS Digital Certificates on the GATS Platform is subject to limitations in accordance with the **Site Terms of Use**. Digital Certificate Users can only use their GATS Digital Signature when effecting Designated Transactions involving GATS Entities to which they are associated and of which they have been nominated as signatories by an Entity Administrator.

The issued GATS Digital Certificate only contains the subject data that has been verified by Fexco when the Applicant applied to become a Digital Certificate User. The issuance by Fexco of a GATS Digital Certificate to a Digital Certificate User, as a natural person who later becomes an associated user of a GATS Entity on the GATS Platform, is not and should not in any way be construed as Fexco having verified that Digital Certificate User's association with or representation of that GATS Entity. Except in so far as is technically necessary to facilitate such functionality through the GATS Platform Fexco has no role whatsoever in:

- approving GATS Entities for admission onto GATS,
- associating a Digital Certificate User with a GATS Entity; or
- verifying the right of representation of a Digital Certificate User of a GATS Entity.

GATS Digital Certificates are not issued to legal persons or entities.

GATS Digital Certificates are not, and should not be relied on or construed as meeting the requirements of, a 'qualified certificate for electronic signature' as defined in the eIDAS Regulation.

e. Renewal

GATS Digital Certificates automatically expire one year from the date of issue. However,

- provided the Digital Certificate User continues to satisfy the requirement to renew his or her status as a Digital Certificate User and refresh his or her identity verification as set out in section B(v) of this Policy and clause 12 of the **Site Terms of Use;** and
- unless one of the revocation events outlined in section f below has arisen;

each GATS Digital Certificate which has been issued to a Digital Certificate User will be automatically renewed for as long as the user remains a Digital Certificate User on GATS.

Each renewed GATS Digital Certificate will contain the same subject identification data as presented by the Digital Certificate User during the registration/refresh of identity verification process but will contain a new validity period.

Digital Certificate Users will not be formally notified when their GATS Digital Certificate has been renewed but by continuing to have access to the functionality on GATS to apply a GATS Digital Certificate, users can be assured that their GATS Digital Certificate remains valid.

f. Revocation

Revocation terminates the validity of the GATS Digital Certificate before its scheduled expiry. Revocation is permanent and irreversible, and it is not possible to undo the revocation of a GATS Digital Certificate. Fexco will revoke GATS Digital Certificates if any of the events listed below occurs. Where the Digital Certificate User:

(i) notifies Fexco or the GATS Helpdesk that they wish to cancel their Digital Certificate User account on GATS;

(ii) fails to renew their Digital Certificate User status within the permitted timeframe by refreshing their identity verification;

(iii) has their account suspended or terminated in accordance with the **Site Terms of Use**;

(iv) notifies Fexco or the GATS Helpdesk that any of the data included in the GATS Digital Certificate is incorrect or has changed and requests a replacement of the GATS Digital Certificate (GATS Digital Certificates cannot be modified; a certificate with incorrect data will be revoked and re-issued);

(v) notifies Fexco or the GATS Helpdesk that their Security Credentials have been compromised;

(vi) notifies Fexco that they do not agree to the terms of this Policy or any revised version of this Policy from time to time;

(vii) Fexco or AWG becomes aware that the GATS Digital Certificate was used illegally or in a manner prohibited by the **GATS e-Terms** or the **Site Terms of Use**;

(viii) The certificate management process within GATS changes and/or Fexco is no longer the Certificate Authority of GATS Digital Certificates.

Revocation can be initiated by:

(i) The Digital Certificate User;

(ii) AWG (in accordance with the **GATS e-Terms** or the **Site Terms of Use**); or

(iii) Fexco.

A request for revocation will be actioned, once verified, as soon as possible and in any event within 24 hours.

Suspension is a form of revocation that suspends the validity of a GATS Digital Certificate in certain circumstances. GATS Digital Certificates may be suspended from the date an obligation to refresh

identity verification arises until such time as the obligation is met, or if the obligation is not met, until such time as the GATS Digital Certificate is revoked, or if any of the suspension events in the **Site Terms of Use** arise;

The revocation status of a certificate can be checked on the GATS Certificate Revocation List ("**CRL**") which is publicly available on the Verification section of the GATS Platform.

The CRL is a signed list of revoked certificates previously issued by the GATS Platform and is continuously updated. The list includes the serial number of the certificate and the revocation date and time.

Parties seeking to establish the revocation status of a certificate can use the GATS CRL to browse the downloaded CRL file to check what certificates have been revoked and when. The relevant certificate serial number is required to verify the revocation status of a GATS Certificate.

g. Procedure for validating GATS Digital Signatures

By registering as a Digital Certificate User, each such user accepts that the GATS Digital Certificate issued to them will be accessible by and disclosed to anyone reasonably seeking to rely on the GATS Digital Signature. In this context a "**Relying Party**" will include GATS Entities and or any other end entity which reasonably relies on the GATS Digital Certificate.

In order to reasonably rely on a GATS Digital Signature each Relying Party must:

(i) Verify that the GATS Digital Certificate has not been suspended or revoked the using revocation status procedure outlined in section [f] above;

(ii) Verify the validity of the GATS Digital Certificate using the process described below;

(iii) Take account of any limitations and restrictions on the use of GATS Digital Signatures and GATS Digital Certificates as set out in this Policy and/or the **GATS e-Terms** and/or Associated documents;

(iv) Take any other steps as may be necessary as set out in this Policy and the **GATS e-Terms** and Associated Documents.

Subject to the above, where a Relying Party wishes to verify a GATS Digital Signature which has been applied on a GATS Instrument, this can be done in one of the following ways:

1) Signature Code Verification.

   a. Relying Party navigates to verification section of the GAT Platform, clicks on "Verify a Document Signature" and types in (i) the Digital Signature Code (this is the alpha-numeric string of characters which can be seen by clicking into the visual representation of the GATS Digital Certificate, or (ii) the Transaction ID (which appears on the front cover of the GATS Instrument); or

b. Relying Party scans the QR Code on the QR code on the front cover or the QR Code next to the visual representation of any signatory's digital signature to access the Digital Signature Code.

Where either of these steps are taken, the signature information relating to the GATS Digital Signature will appear. Where the GATS Digital Signature cannot be verified, a message will appear stating that the GATS Digital Signature cannot be validated.

2) Strict AdES Validation.

Relying Party can validate all signatures contained in a GATS Document through the standard AdES-based procedure. The Relying Party navigates to Verification section of the GAT Platform and uploads the PDF document with the signatures to be validated. The report for all signatures in the document will be shown with the AdES indication of the result of the validation and the reasons:

a. TOTAL-PASSED: when the cryptographic checks of the signature (including checks of hashes of individual data objects that have been signed indirectly) succeeded as well as all checks prescribed by the signature validation policy have been passed.
b. TOTAL-FAILED: the cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly), or it is proven that the signing certificate was invalid at the time of generation of the signature, or because the signature is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it.
c. INDETERMINATE: the results of the performed checks do not allow to ascertain the signature to be TOTAL-PASSED or TOTAL-FAILED.

The GATS Digital Signature validation process must be performed using a reliable device which complies with all required technical specifications and has been correctly configured. It is recommended that PDF documents are validated in the first instance within the GATS platform as per instructions stated within the documents. Thereafter documents can also be viewed in PDF file browsers with features to view applied digital signatures. It is necessary to accept the GATS root certificate to correctly view the documents in some PDF viewer applications and the GATS root certificate acceptance procedure is more fully described on the GATS platform.

GATS Digital Certificates are maintained by Fexco and are available as evidence for 13 years after the certificate expiration date.

The GATS Digital Signature validation process will only verify the application of the GATS Digital Signature on a GATS Instrument in the manner permitted in this Policy. Relying Parties are wholly responsible for undertaking any required validation process of the association between the Digital Certificate User and the GATS Entity, and /or the right of representation of the Digital Certificate User of the GATS Entity, on whose behalf the Digital Certificate User is purporting to sign.

D. Fexco Operational and Technical Security Controls

a. Overview

Fexco applies operational and technical security controls across all its businesses to ensure a high level of protection of its assets including its information assets. These controls are revised from time to time, to align with industry best practice, emerging threats and the expectations and contractual requirements of Fexco's clients, business partners and regulators.

Fexco maintains a broad range of information technology management policies, including policies specifically focused on information security, which implement its operational and technical security controls. These are approved by management, frequently updated and apply to and are communicated to all relevant staff and third parties where necessary.

Each business within the Fexco Group exercises the necessary administrative and management procedures and processes that are in line with its information technology management policies. Appropriate disciplinary sanctions are applied to staff violating all relevant policies or procedures.

b. Operational and Technical Security Controls

In all business operations Fexco uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

Fexco organises its approach to information security and the protection of its critical systems and data around four key pillars, with three activities within each pillar.

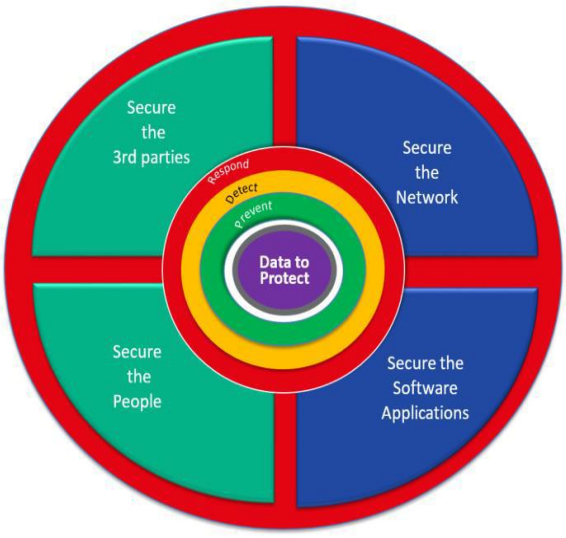
The four pillars of focus for security initiatives are:

1. Secure the Network

2. Secure the Applications

3. Secure the people

4. Secure the third parties



Each pillar focusing on the following three activities:

Prevent	Defend	Respond

More detail is available in the **Fexco Information Security Controls Policy** which is available on request.

GATS Digital Certificates are stored in dedicated storage accounts with access to these accounts limited to only authorised individuals, a small number of trusted technical engineers with strict segregation of duties practices applied. All certificates are stored encrypted at rest. The storage account used to store GATS Digital Certificates are encrypted using FIPS 140-2 compliant block ciphers.

Access to GATS Digital Certificates databases is only available to authorised individuals, a small number of trusted technical engineers with strict segregation of duties practices applied. All data stored is encrypted.

The management service of GATS Digital Certificates, keys and passwords uses industry-standard algorithms and key lengths to allow for:

(i) Secure centralised location for application secrets, limiting attack vectors.

(ii) Full audit history. Who accessed, when accessed and which secret was accessed.

(iii) Simplified administration.

(iv) Securely stores secrets and keys.

c. Procedural and Staff Security Controls

The Fexco Group has implemented an Information Security Policy which is built on ISO 27001:2013, the International Standard for information security management, and which embraces the following information security requirements:

(i) Confidentiality – Protecting information from unauthorised disclosure;

(ii) Integrity – Protecting information from unauthorised modification;

(iii) Availability – Ensuring that information and associated services are available to meet Fexco's business needs.

In accordance with its Information Security Policy, Fexco has put in place all necessary measures to ensure that employees and contractors support the trustworthiness of Fexco's operation of the GATS Platform. Access to the GATS platform system operations is strictly limited to authorised individuals. All staff and subcontractors used by Fexco in the operation of the GATS Platform possess the necessary expertise, reliability, experience, and qualifications and have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

Fexco has created trusted roles for performance of certain tasks relating to operation of the GATS Platform and access rights and functions are managed within these trusted roles in such a way that prevents any individual user from bypassing security protection measures.

More information is available in the **Fexco Information Security Policy Manual** which is available on request.

d. Physical and Environmental Security and Controls

Fexco implements a physical access framework designed to manage, control and monitor physical access to Fexco's Information Resource Facilities (IRF) where an IRF refers to a facility hosting the data and information assets of Fexco or any of its departments or business units including but not restricted to a data room and offices where a Fexco business undertakes its operations.

Fexco's physical access policies and procedures are designed to ensure that Fexco controls the physical access to components of its system whose security is critical to the provision of its services and to minimise risks related to physical security.

More detail is available in the **Fexco Physical Access policy** and the **Fexco Remote Access Policy** which are available on request.

e. Records, Retrieval and Archiving

Fexco has implemented a system, accompanied by defined procedures, within the GATS Platform which will record and keep accessible for an appropriate period of time, including after the activities of Fexco on the GATS Platform have ceased, all relevant information concerning data issued and received by the Fexco in its capacity as operator of the GATS Platform, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

The implemented process enables Fexco to ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its statutory functions and the provision of services relating to the GATS Platform.

For more information on the storage of personal data on and within the GATS Platform see the **AWG Privacy Policy** and the **Fexco Privacy Policy**.

f. Business Continuity Management and Disaster Recovery

Within all Fexco businesses system activities concerning access to IT systems, use of IT systems, and service requests shall be monitored. Fexco has defined and maintains a continuity plan ("**BCP**") to enact in case of a disaster for each of its businesses. Each BCP is designed to ensure that in the event of a disaster, the relevant Fexco business will take all necessary measures to minimise the damage resulting from the incident and to restore all affected services as quickly as possible.

Fexco reviews its BCPs on a regular basis and tests its disaster recovery system periodically to ensure it remains fully operational.

E. Certificate Profile

GATS Digital Certificates have the following structure:

Version	Version 3
Serial Number	Serial number of the certificate
Signature	Sha512, RSA
Issuer	Issuer DN: **Common Name (CN)**: www.e-gats.aero **Organisation Unit (OU):** Fexco Technology Solutions **OrganisationName (ON)**: FEXCO UNLIMITED COMPANY **Locality Name (L)**: Killorglin **Country (C)** : IE
Validity Period	1 Year (expires 1 years from the date of issue)
Subject	**Common Name (CN)**: [SUBJECT NAME] **Organisation Unit (OU):** Empty **OrganisationName (ON)**: Empty **Address (A)**: [SUBJECT ADDRESS] **Postcode (P)**: [SUBJECT POSTCODE] **Locality Name (L)**: [SUBJECT LOCALITY] **State Name (ST)**: [SUBJECT STATE] **Country (C)** : [SUBJECT COUNTRY]
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critical)	Subject Type: CA Path Length Constraint: 0
KeyUsage (critical)	Digital Signature

Certificate Policies (not critical)	GATS Digital Certificate Policy URL: https://ftsprodwegatsstorage.blob.core.windows.net/public-gats-container/CertificatePolicy.pdf

GATS Digital Certificates meet the following technical standards and requirements:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 1: General requirements
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI) Certificate Profiles
- ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)
- EN 319 142-1: AdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- EN 319 142-2: PAdES digital signatures; Part 2: Additional PAdES signatures profiles
- TS 119 142-3: PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- ETSI TS 119 144-4 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of PAdES baseline signatures
- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI);PAdES Baseline Profile

F. General Terms

a. Fees

There is no fee payable to Fexco for issuance of a GATS Digital Certificate. There are fees payable to AWG for using the GATS Platform ("**GATS Fees**"), including a fee payable for becoming a Digital Certificate User, and a fee for renewing a user's status as a Digital Certificate User.

All GATS Fees are set out in the **GATS Schedule of Fees.**

b. Privacy and Storage of Information

Fexco has implemented and respects procedures for protecting personal data in order to ensure the security of personal information collected for the purposes of issuing and managing a GATS Digital Certificate.

The manner in which each Digital Certificate User's details, identification document(s), photo(s) and other personal data will be processed and stored is set out in the **AWG Privacy Policy** and the **Fexco Privacy Policy**.

c. Publication

This Policy is published electronically and is available on the website on which the GATS Platform is hosted: http://e-gats.aero/. Access to this Policy is unrestricted to enable all GATS users, any Relying Party and any other person who wishes to obtain information about the use of GATS Digital Signatures and GATS Digital Certificates to have information on the precise terms and conditions regarding their use and issuance.

d. Acceptance

By using the GATS Platform, you confirm that you accept the terms of this Policy and the terms, conditions and limitations governing the issuance and use of GATS Digital Signature. If you do not agree to this Policy, you must not use the GATS Platform. We recommend that you print a copy of this Policy for future reference.

e. Changes to this Policy

We may change this Policy from time to time, and if we do we will publish the updated Policy on the GATS Platform highlighting any changes to the Policy and the terms and conditions of use of GATS Digital Certificates.

Where the changes consist of significant or material changes to the terms and conditions of use of GATS Digital Signatures or GATS Digital Certificates, Fexco will take steps to inform each Digital Certificate User in advance of the changes and the date on which these changes will take effect.

Every time you wish to use the GATS Platform, please check this Policy to ensure you understand the terms that apply at that time.

By continuing to participate in the GATS Platform after those changes are in effect, each Digital Certificate User agrees to the revised Policy. Where a Digital Certificate User indicates that they do not agree with the revised Policy, Fexco will revoke any GATS Digital Certificate that has been issued to the Digital Certificate User and the Digital Certificate User will no longer be able to apply a GATS Digital Signature on the GATS Platform.

f. Other Applicable Terms

This Policy forms part of and is incorporated into the **Site Terms of Use** and the Associated Documents, which may or will also apply to your use of the GATS Platform.

Defined terms used in this Policy shall unless otherwise stated have the meaning set out in the GATS e-Terms, the Site Terms and the Associated Documents.

g. Availability

We do not guarantee that the GATS Platform, including access to the functionality necessary to use or validate GATS Digital Signatures, will always be available or be uninterrupted. We may suspend or withdraw or restrict the availability of all or any part of the GATS Platform for business and operational reasons. We will try to give you reasonable notice of any suspension or withdrawal.

h. Liability

Fexco's liability in its role as GATS Platform Service Provider, and Fexco's liability to GATS Entities arising from issuance, use or reliance on GATS Digital Certificates issued to Digital Certificate Users and to the application by Digital Certificate Users of GATS Digital Signatures on behalf of GATS Entities, and the limitations on such liability, is set out in the **GATS E-Terms**.

Fexco's liability in its role as GATS Platform Service Provider to any party accessing or using the GATS Platform who is not a GATS Entity, and the limitations on such liability, is set out in the **Site Terms of Use**.

Fexco's liability to any Relying Party who is not a GATS Entity arising from issuance, use or reliance on GATS Digital Certificates to Digital Certificate Users and to the application by Digital Certificate Users of GATS Digital Signatures on behalf of GATS Entities, is set out below.

(i) Nothing in this Policy shall exclude or limit Fexco's liability for:

- death or personal injury resulting from the negligence of the other or their servants, agents or employees; or
- fraud or fraudulent misrepresentation.

(ii) Without prejudice to the above, Fexco provides GATS Digital Certificates for permitted uses described in this Policy only and will be liable only for intentional or gross negligence.

(iii) Fexco will not be liable for any loss or damage, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, even if foreseeable, arising under or in connection with:

- use of or inability to use, or any interruption or unavailability of, any functionality relating to GATS Digital Signatures;
- the accuracy or completeness of any User Data (as defined in the **Site Terms of Use**) or any Non-Verified Information;
- loss of profits, sales, business or revenue;
- loss of agreements or contracts;
- loss of business, opportunity, goodwill or reputation;
- loss of anticipated savings;
- business interruption;
- loss of use or corruption of software, data or information;
- any indirect or consequential loss or damage whether or not foreseeable, even where the likelihood of such loss or damage has been advised;
- any unauthorised use of a GATS Digital Certificate or any purported application by a person other than the Digital Certificate User of a GATS Digital Signature of that Digital Certificate User;
- any failure of a Digital Certificate User or the GATS Entity on whose behalf the Digital Certificate User applies a GATS Digital Signature to ensure that the Digital Certificate User had a right of representation of the GATS Entity;
- any failure by a GATS Entity to meet execution requirements prescribed by statute or its constitutional documents that may be necessary for effective execution of a GATS Instrument; or
- any other action taken or not taken by Fexco pursuant to or in connection with this Policy.

(iv) Fexco excludes all implied conditions, warranties, representations or other terms that may apply to the GATS Digital Signature functionality, including the term implied by section 39 of the Irish Sale of Goods and Supply of Services Act, 1980

(v) Fexco's total liability to any party in relation to all events or series of connected events occurring under this Policy (and whether the liability arises because of breach of contract,

negligence or for any other reason) shall not exceed the total GATS Fees paid by the claimant (if applicable) or the sum of €500, whichever is the lesser.

i. Governing Law, Jurisdiction and Disputes

This Policy, its subject matter and formation (and any non-contractual disputes or claims), shall be construed as being subject in all respect to the laws of Ireland and any person seeking to rely on this Policy agrees to submit to the exclusive jurisdiction of the Irish Courts in the event of any dispute regarding any matter relating to the issue and management by Fexco of GATS Digital Certificates.

Issue Date: 20 May 2020

Change Log

Date	Author	Version	Details
20 May 2020	Margaret Maguire (with input from Helen O'Connor, Jesus De Diego, David O'Brien and Rob Neale)	1.0	

Review and Signoff Log

Role & Organisation	Name	Date Reviewed	Approved
Fexco Policy Committee	Ger O'Sullivan (FEXCO, Chief Financial Officer) Tony Sweeney (FEXCO, Head of Internal Governance) Eleanor Daly (FEXCO, General Counsel) Sheila Cronin (FEXCO, Head of Group Treasury and Commercial Financial Controls)		6 May 2020

Confidential

Fexco

Iveragh Road

Killorglin, Co. Kerry

Ireland

T: +353 66 976 1258

www.fexco.com