United Kingdom Overseas Territories Aviation Circular

OTAC 39-21
145-19

Electronic Signatures, Electronic Recordkeeping and Electronic Manuals for Airworthiness

Issue 1.00
6 May 2022

Effective: on issue

GENERAL

Overseas Territories Aviation Circulars are issued to provide advice, guidance and information on standards, practices and procedures necessary to support Overseas Territory Aviation Requirements. They are not in themselves law but may amplify a provision of the Air Navigation (Overseas Territories) Order or provide practical guidance on meeting a requirement contained in the Overseas Territories Aviation Requirements.

PURPOSE

This Overseas Territories Aviation Circular provides information and guidance on the use of electronic signatures, electronic recordkeeping and electronic manual systems for the purposes of airworthiness information systems.

RELATED REQUIREMENTS

This Circular relates to OTAR Part 39 and OTAR Part 145.

CHANGE INFORMATION

First issue.

ENQUIRIES

Enquiries regarding the content of this Circular should be addressed to Air Safety Support International at the address on the ASSI website www.airsafety.aero or to the appropriate Overseas Territory Aviation Authority.

CONTENTS

1. Definitions

The following terms are used in this OTAC.

(a) Authentication. The means by which a system validates the identity of an authorized user. These may include a password, a personal identification number (PIN), a cryptographic key, smart card, etc. These means may be combined (e.g., a cryptographic card and a PIN) for increased confidence in the identity of the system user.

(b) Computer-Based Recordkeeping System. A system of record processing in which records are entered, maintained, archived, and retrieved electronically. The term “computer-based recordkeeping system” is synonymous with “electronic recordkeeping system”.

(c) Data Backup. Use of one of several recognized methods of providing a secondary means for archiving records, separately from the original or primary. This can be used to reconstruct the format and content of electronically stored records in case of loss, failure, or damage to the primary recordkeeping system.

(d) Digital Signature. Cryptographically generated data that identifies a document’s signatory, with date and time. The result of which, when properly implemented, provides the services of original authentication, data integrity, and signer non-repudiation.

(e) Electronic Manuals. Certificate holder manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, Internet/Intranet based, or various other forms of electronic media, to include commercial off-the-shelf portable electronic device (PED) hardware (e.g., laptop, tablet, phone, etc.).

(f) Electronic Record. A contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(g) Electronic Recordkeeping System. A system of record processing in which records are entered, signed, stored, and retrieved electronically. The term “electronic recordkeeping system” is synonymous with “computer-based recordkeeping system”.

(h) Electronic Signature. Functionally equivalent to a handwritten signature. The term “electronic signature” means an electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent to sign the record.

(i) Password. An identification code or device required to access stored material, intended to prevent information from being viewed, edited, or printed by unauthorized persons.

(j) Signature. A mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation, and to authenticate a record entry. A signature should be traceable to the individual making the entry, and it should be handwritten or part of an electronic signature system.

2. Other Abbreviations

AAIB: Air Accident Investigation Branch
C of A: Certificate of Airworthiness
EFB: Electronic Flight Bag
MEL: Minimum Equipment List
OTAA: Overseas Territory Aviation Authority
OTAC: Overseas Territories Aviation Circular
OTAR: Overseas Territories Aviation Requirement
PED: Portable Electronic Device
UK: United Kingdom

3. Electronic Signatures - General

(a) The handwritten signature is universally accepted because it has certain qualities and attributes that should be preserved in any electronic signature.

For an acceptable electronic signature, the purpose is identical to that of a handwritten signature; therefore, an electronic signature should possess those qualities and attributes that guarantee a handwritten signature's authenticity.

(b) Electronic record-keeping systems may be used to generate aircraft records (e.g. maintenance task cards, aircraft maintenance records, dispatch releases, flight releases, airworthiness releases, and flight test reports) for which there is a need to be able to properly authenticate the user with an electronic signature.

(c) The electronic signature is the online equivalent of a handwritten signature. It is an electronic sound, symbol, visible mark or process attached to or logically associated with a record and executed or adopted by an individual with the intent to sign the record. It electronically identifies and authenticates an individual entering, verifying, or auditing computer-based records.

(d) The use of the wording "electronic signature" in this OTAC is intended to capture broad and diverse categories of solutions which, although they may be differently identified in the expert field of digital security in accordance with their technological features and capabilities, are all in compliance with provisions of 1(c), and 4.

(e) The inaccuracy generated by non-differentiation between categories such as electronic signature, digital signature, advanced electronic signature, secure electronic signature or digital electronic signature is considered irrelevant for these guidelines as long as compliance with 1(c) and 4 is ensured by the solution adopted.

The considerations presented in this OTAC are entirely valid for aviation applications highlighted in other OTACs (e.g., OTAC 39-15, 121-19, 125-18, 135-19 Electronic Flight Bags (EFBs)).

(f) The electronic signature should provide a secure authentication of the signatory and should be linked to the data for which the signature was created in such a way that any subsequent change of the data is detectable.

4. Attributes of an Electronic Signature

There are several attributes that an electronic signature should possess:

(a) **Uniqueness**, which is the feature by which the electronic signature should identify a specific individual and only that individual and should be difficult to duplicate.

An acceptable method of proving the uniqueness of a signature is by using an identification and authentication procedure that validates the identity of the signatory. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. These codes could be encoded onto badges, cards, cryptographic keys, or other objects.

Systems using passwords could also be an acceptable method of ensuring uniqueness. A computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically.

Additionally, a system could use physical characteristics, such as a fingerprint, handprint, or voice pattern, as a method of identification and authorisation.

(b) **Significance**, which is the feature by which an individual using an electronic signature should take deliberate and recognisable action to affix his or her signature. Acceptable, deliberate actions for creating a digital electronic signature include:

(1) badge swipes,
(2) signing an electronic document with a stylus,
(3) typing specific keystrokes or
(4) using a digital signature.

(c) **Scope,** which is the feature by which the scope of information being affirmed with an electronic signature should be clear to the signatory and to subsequent readers of the record, record entry, or document. The electronic record should accurately reflect the information being affirmed by signatory and the signatory should be fully aware of what he or she is signing.

(d) **Security,** which is the feature by which an electronic system that produces signatures should restrict other individuals from affixing another individual's signature to a record, record entry, document, or alter the content without trace.

To this effect, a corresponding policy and management structure should support the computer hardware and software that delivers the information. The system should contain restrictions and procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment. This should be done immediately upon notification of the change in employment status.

(e) **Non-repudiation,** which is the feature by which an electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document.

(f) **Traceability,** which is the feature by which an electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

(g) **Description of Electronic Signature Process**. A description of the electronic signature process must be included in the approval holder's manual. The description should explain how electronic signatures will be used and how electronic signatures are applied throughout the approval holder's operation (e.g., airworthiness releases, and maintenance actions).

(h) **Responsible Personnel**. Policies and procedures should identify the approval holder's personnel who have the authority and overall responsibility for the integrity and security of the electronic signature process and for controlling access to the computer software/application used in the process. Policies and procedures should also identify the persons with the authority and responsibility for modifying, revising, and monitoring the electronic signature process, as well as ensuring the process is followed by all appropriate personnel.

(i) **Identification of Persons** Authorized to Use Electronic Signatures. Certificate holders must have a system for identifying who is authorized to use the electronic signature process, for what purposes, and which records.

(j) **Description of System Support**. Policies and procedures should address system support of any computer hardware or software that is part of the electronic signature process.

(k) **Hardware and Software Capabilities**. Description(s) of the electronic signature hardware to be used and software capabilities for applications of electronic signatures in the certificate holder's system(s).

(l) **Auditing Process**. Electronic signature policies and procedures should include an auditing process to ensure all of the requirements for electronic signatures continue to be met. The process should include unauthorized event recognition, which includes actions to be taken by the certificate holder upon discovery of an attempt by an unauthorized individual to use an electronic signature.

(m) **Data Backup and Retention**. Policy and procedures should address how data backup and retention of data will be accomplished.

(n) **Procedures for Computer System Outages and/or Disaster Recovery**. Policy and procedures should address computer system outages (failure of hardware, software, application, network, etc.) or disaster recovery.

(o) **Training and User Instructions**. A certificate holder's policies and procedures should include any training and instructions necessary to ensure authorized users understand how to access and properly apply the electronic signature process. Procedures should describe how users are notified of changes to the electronic signature process.

5. Electronic Records

(a) The term "electronic record" used throughout this OTAC should be understood as referring to electronic maintenance records and continuing airworthiness records for aircraft, engines, propellers and associated parts.

(b) The information pertaining to aircraft maintenance and continuing airworthiness is often recorded, certified and stored in a paper format. The accepted paper-based practice capabilities are challenged and limited in supporting real time accurate and complete records when faced with the increase of information volume and complexity associated with modern aircraft operation and maintenance.

The OTAAs should consider the approval and oversight of electronic record-keeping processes and procedures to be implemented by air operators, aircraft manufacturers and maintenance organisations.

(c) An electronic record-keeping system should be a system of record processing in which records are entered, electronically endorsed, stored, and retrieved electronically by a computer system rather than in the traditional “hard copy” or paper form.

(d) Any electronic record-keeping system and the record it generates, processes and stores should be described in the operator’s Maintenance Control Manual, be acceptable to the OTAA and meet the requirements set forth by the OTAA for the operator’s maintenance and operational activity. This should include unrestricted OTAA access for auditing and the capability of the organisation to provide paper copies of records if required by the OTAA.

(e) The electronic record generated, processed and stored per OTAA requirements should be considered as original documents. Use of a complete electronic record-keeping system should be acceptable to the OTAA.

Electronic records signed electronically should be considered equivalent to aircraft maintenance and continuing airworthiness records authenticated with non-electronic signatures. Any printout of an electronic record required by the OTAA (see above provision 3 (d)) should have a watermark displayed on the page background stating “PRINTED FROM ELECTRONIC FILE”.

(f) The exchange of electronic records between aviation organisations, under the same or different OTAA oversight responsibility, should be accomplished on a voluntary basis where both the issuer and receiver agree on the electronic transfer of the records.

(g) Paper-based aircraft maintenance records should continue to be acceptable to the OTAA if the air operator, aircraft manufacturer or maintenance organisation adopts a traditional paper-based system.

Notwithstanding the capability stipulated in provision 3 (d) above, the OTAA should not require that a dual system be implemented if the organisation adopted an electronic record system in accordance with para 3 (e) of this OTAC.

A combination of electronic and paper-based maintenance record-keeping system should be acceptable to the OTAA if the air operator, maintenance organisation or aircraft manufacturer adopts the traditional paper-based system as a backup system in case of situations where a full electronic record cannot be created.

(h) The adoption of the electronic records system should be conditional to providing to all system users the adequate training that includes security awareness and policy and procedures relevant to the system adopted. The assurance of its implementation is, thus, as important to an electronic records system as the architecture itself. The OTAA should validate, before acceptance of the electronic records system, not only the technical capabilities of the proposed system but also the organisational readiness to adopt the system.

(i) The electronic records are essentially linked in most cases to the date and time information regarding the moment in which they were created, modified and signed-off. Such information should be appropriately addressed by the time stamping capability of the electronic record-keeping system.

6. Security and Integrity

(a) A corresponding policy and management structure should support the computer hardware and software that delivers the information. Appropriate physical security and electronic record backup procedures should be established for current, operational, stored and archived records.

(b) The electronic record system should protect confidential information.

(c) The electronic record system needs to ensure that the information is not altered by operating any unauthorised changes to the record.

(d) Procedures should be established allowing the organisation to correct documents that were electronically signed in error. The original entry should be superseded anytime a correction related to that entry is made. (The original entry should be voided but remain in place. Reference to a new entry should be made and electronically signed and dated). It should be clearly identified that the original entry has been superseded by another entry.

(e) Procedures should be established to describe how the operator will ensure that the electronic records are transmitted in accordance with the appropriate regulatory requirements to stakeholders who need access to the records.

(f) Procedures should be established for reviewing the computerised personal identification codes system to ensure that the system will not permit password duplication.

(g) Procedures should be established for auditing the computer system periodically to ensure the integrity of the system. A record of the audit should be completed and retained on file as part of the operator's record retention requirements. This audit may be supported by system automatic self-testing.

(h) Procedures should be established for non-recurring audits of the computer system if the integrity of the system is suspect.

(i) Audit procedures should be established to ensure the integrity of each computerised workstation. If the workstations are server-based and contain no inherent attributes that enable or disable access, there is no need for each workstation to be audited. The procedures should be applicable to both fixed (e.g. desktop computers) and mobile equipment (e.g. laptops, tablets).

(j) An information security assessment process should be established for the electronic record system to determine how effectively each entity being assessed (e.g. host, network, procedure, person) meets specific security objectives. The effective implementation of such established process should employ password cracking and security penetration testing procedures.

7. Archiving and transferability

(a) In addition to physical safety of the archives, specific procedures for archiving electronically signed documents should be established. A means of safely archiving electronically signed documents should be part of any electronic signature computer software. This will provide for and adequately support the retention, access and future authentication of electronic records.

(b) Procedures should be established to ensure that all relevant maintenance and continuing airworthiness records are made available at aircraft transfer to support the Export C of A.

(c) The electronic record-keeping system should include the necessary protocol to allow for secure transfer of the records to another electronic record-keeping system.

8. Electronic Manuals and Content

(a) Like printed manuals, electronic manuals should provide instructions and information necessary to allow personnel concerned to perform their duties and responsibilities with a high degree of safety. An electronic manual should provide equivalent or better data integrity, accuracy, and accessibility to what would otherwise be provided by a printed manual.

(b) The content of each electronic manual should be clearly identifiable and viewable by the user and should correlate and be comparable to what would be available in a printed version of the manual. An electronic manual should contain elements that generally comprise a printed manual. These elements typically include:

(1) The manual title.

(2) Revision control pages or sections from which the user can readily determine whether the manual is current.

(3) List of effective pages.

(4) Indication of OTAA approval (e.g., signature or stamp) for those manuals or manual sections that require OTAA approval.

(5) Chapter numbers.

(6) Chapter headings.

(7) Section numbers.

(8) Topic headings.

(9) Page numbers.

(10) Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (when applicable for minimum equipment list (MEL) and maintenance purposes); and

(11) The person with the authority and responsibility for manual content.

9. Electronic Manual System

(a) An electronic system for delivering manual content should comply with regulatory requirements for currency, availability, and distribution to the appropriate personnel. A certificate holder's electronic manual system should address any OTAA requirements for "must" or "should" that apply to their operation(s) into their electronic manual system. An electronic manual system should describe/address:

(1) **Currency.** Each certificate holder's electronic manual system method of keeping each manual current.

(2) **Access, Availability, and Distribution.** Each electronic manual system should provide distribution and/or access to manual(s) by the appropriate personnel, in a form and method acceptable to the Governor.

(3) **MEL Direct Access Requirement.** As required by OTAR Part 91, Part 121, Part 125, and Part 135, certificate holders who conduct operations under Part 91, 121, 125, or 135 should provide flight-crews with direct access to the MEL through printed or other means approved by the Governor. An EFB is an example of other means that may be approved by the Governor.

(4) **OTAA/UK AAIB Access.** The certificate holders should provide access to the electronic manual system to the appropriate OTAA representatives assigned to the certificate holder.

When providing such access, a certificate holder should provide the OTAA's representatives with instructions on how to access the system. Certificate holders should provide any requested information to the UK AAIB in the event of an accident or incident. When a certificate holder is required to provide manuals or manual information to the OTAA or UK AAIB, it should be provided in the desired format of the requesting agency whenever possible.

(5) **Responsible Personnel.** The system description should include the certificate holder's personnel who have the authority and responsibility for maintaining the system, implementing, modifying, revising, and monitoring the electronic manual software and ensuring the overall integrity of the content of manuals that are part of the system.

(6) **Prevention of Unauthorised Access and Data Corruption.** The Manual system computer hardware and software should prevent unauthorised access and/or modification to electronic manual content.

(7) **Storage and Retrieval.** The computer hardware and software system should store and retrieve the manual's content under conditions of normal operation and use. The system should not permit unauthorised modification of the data it contains.

(8) **Functionality.** Users should be able to easily access, navigate, and retrieve manual content via computer or comparable device. Manual users should be able to print any information contained in an electronic manual.

(9) **Revision Control.** A certificate holder's electronic manuals should be easy to revise. The electronic manual system should include revision control procedures for making revisions (incremental, temporary, and scheduled) in a timely manner. Procedures should include the accomplishment of revisions by personnel to whom manuals are issued. The revision control procedures should address at least the following:

i. **Communication of Revision Information.** Procedures should include the method of communicating revision information, similar to what would be provided for a paper manual revision.

Revision information should provide the revision content, effective date, and any instructions required for ensuring the revision is uploaded or incorporated into the electronic manual.

Revision information should allow the user the ability to compare the current revision to the previous version, or it should explain the effect of the change. The revision system should make changes under the current revision readily apparent. An example of this would be change bars. An electronic manual should contain a revision control page or section from which the user can readily determine whether the manual is current.

ii. **Revision Status of Each Manual Page.** Each page of a manual should contain the date of the latest revision for that particular page.

If an electronic manual is distributed via a device that displays the manual in a continuous flow format, as opposed to page-by-page, then each section or block of information displayed on the device should contain the date of the latest revision.

iii. **Date and Time Stamp of Printed Information.** When information from an electronic manual is printed, there should be a means to identify the date and time of printing.

iv. **User Responsibility for Current Information.** Users of electronic manuals who need or elect to print material (data information, instructions, procedures, etc.) from the electronic manual should ensure the printed information is the most current available prior to use. Users should discard printed manual information after using it to ensure printed information does not become outdated.

v. **Distribution and Submission of Electronic Revisions to the OTAA.** Revision control procedures should include the certificate holder's method of distributing electronic revisions to the OTAA.

vi. **OTAA Approval or Acceptance** When a particular manual requires OTAA approval or acceptance, the certificate holder's procedures should explain how the certificate holder will submit an electronic revision to the OTAA for approval or acceptance of the revision content.

(10) **Special Considerations in Displaying Information.** Information retrieved from an electronic manual may be displayed in a format that differs from what would appear on paper. The display format may even vary by user. For example, the display of manual content could be different for pilots on the flight deck of an aircraft versus what is displayed to ground personnel at a computer workstation. This may occur for reasons such as screen resolution, software application, or authorised display device. Information displayed on any authorised device on the flight deck should correlate to information displayed at an authorised computer workstation or authorised portable device.

Additionally, any information displayed should be easily traceable and comparable to the source document. The electronic manual content should remain the same, regardless of the display format or device. Any displayed manual information should be identical in content for all users.

(11) **Data Archiving.** An electronic manual system should have a method of archiving technical and procedural data superseded by revision. A certificate holder should archive earlier versions of manuals to provide for future needs to duplicate, regenerate, or reconstruct instructions.

(12) **Preservation of Archived Data.** An electronic manual system should have procedures to ensure the integrity of the archived technical and procedural data. These procedures should include at least:

i. A method of ensuring that no unauthorised changes can be made.

ii. A method or medium that minimises the deterioration of data.

iii. A method to protect the archived data against hazards and natural disasters.

(13) **Transferring Data to Another System.** Technological hardware or software advances may make it desirable and/or necessary for a certificate holder to update its electronic manual system. When transferring manual data from one electronic system or application to another, certificate holders should ensure that data integrity is maintained during transfer. This includes ensuring that archived information remains intact. This may entail running redundant systems for a brief period of time.

(14) **Backup Method.** A certificate holder that uses an electronic manual system should have a backup method of maintaining, distributing, or otherwise providing access to manuals, in case of system hardware or software failure.

(15) **System Maintenance and Support.** Each certificate holder's electronic manual system should include maintenance and support function that identifies hardware and software failures within the system. System maintenance and support should include provisions for system outages and for switching over to the backup method.

(16) **Description of the Electronic Manual System.** The electronic manual system description should include the methods for distribution and/or access to manual(s) (including manual revisions and replacements) by the appropriate personnel.

(17) **Delivery Media.** The electronic manual system description should include an explanation of the media by which the manuals will be distributed to required personnel.

10. Training and User Instructions

(a) Each electronic signature, recordkeeping and manual system should contain training and user instructions for the persons responsible for entering, maintaining, and retrieving data from the system.

(b) Training should include security awareness and system integrity, as well as procedures that are necessary to authorise access to the electronic recordkeeping system. User instructions should include those for OTAA personnel who are provided direct access to the system.