Australian Government
Civil Aviation Safety Authority

DRAFT

Advisory Circular

AC 11-3(0) **OCTOBER 2012**

ELECTRONICALLY FORMATTED CERTIFICATIONS, RECORDS AND MANAGEMENT SYSTEMS

CONTENTS

1. REFERENCES

- Electronic Transaction Act 1999 (ETA)
- Electronic Transactions Regulations 2000
- Civil Aviation Act (CAA) 1988
- Civil Aviation Orders (CAOs)
- Civil Aviation Safety Regulations (CASR) 1998
- Civil Aviation Regulation (CAR) 1988
- Manual of Standards (MOS)

This Advisory Circular (AC) is to be read in conjunction with Part 11 of the CASR 1998

2. PURPOSE

This AC provides guidance on the use of electronically formatted certifications (signatures), records, organisation manuals and electronic management systems to satisfy regulatory requirements under the CAA, CASR, CAR, MOS and the CAOs. This AC also provides guidance on the CASA approval of electronic systems.

The document expresses CASA's policy on the acceptance of the electronic equivalent of many matters previously accomplished using paper format.

Advisory Circulars are intended to provide advice and guidance to illustrate a means, but not necessarily the only means, of complying with the Regulations, or to explain certain regulatory requirements by providing informative, interpretative and explanatory material.

Where an AC is referred to in a 'Note' below the regulation, the AC remains as guidance material.

ACs should always be read in conjunction with the referenced regulations.

This AC has been approved for release by the Executive Manager Standards Division.

3. STATUS OF THIS AC

3.1 This is the first Advisory Circular (AC) to be written on the subject.

4. ACRONYMS

AC Advisory Circular
AOC Air Operator's Certificate
AMO Approved Maintenance Organisation
ARN Aviation Reference Number
CASR Civil Aviation Safety Regulations 1998
CAR Civil Aviation Regulations 1988
CRS Certificate of Release to Service
ETA Electronic Transactions Act 1999
LAME Licensed Aircraft Maintenance Engineer
MEL A minimum equipment list, as defined in subsection 9A.2 of CAO 20.18
MOS Manual of Standards
NAA National Aviation Authority

5. DEFINITIONS

For the purposes of this AC, the following definitions apply:

***Authentication*:** the means by which a system validates the identity of an authorised user. This may include a password, a personal identification number (PIN), a cryptographic key, a badge, or a stamp. Authenticate means to validate or establish to be genuine such that the matter being authenticated will have legal force or be legally binding.

***Electronic Signature*:** is any signature made using an electronic communication. Where an electronic signature is used to satisfy a requirement under Commonwealth law, the method used must be as reliable as is appropriate for the circumstances of the information communicated and comply with the relevant Government agency's requirements for applying that method. An electronic signature can combine cryptographic functions of digital signatures with the image of a person's handwritten signature or some other form of visible mark that would be considered acceptable in the circumstances.

***Signature*:** is any method used to identify a person and to indicate their approval of information communicated (e.g. to attest to the completion of, or a person's involvement in, an act, or to certify a record entry). Signatures can be handwritten or electronic.

6. WHO DOES THIS AC APPLY TO?

6.1 This AC has general application to anyone seeking to meet the regulatory requirements set under the CAA, CASR, CAR, MOS and the CAOs; especially those involved in designing, certifying, operating or maintaining aircraft.

6.2 The information and concepts described within this AC are intended to address both a web based (online) and stand-alone system.

7. BACKGROUND

7.1 As the complexity of aircraft design, certification, operations and maintenance processes increased, the number of records and documents generated and required to be retained by aircraft registered operators, manufacturers and approved maintenance organisations expanded significantly. The development of electronic information storage and retrieval systems has significantly enhanced the ability of the aviation industry not only to meet regulatory record-retention requirements; but also to manufacture, operate, and maintain today's highly complex aircraft and aircraft systems in a demanding operational environment.

7.2 There is now a far greater community acceptance and promotion of the advantages of electronic versions of certifications, logbooks [chronological compliance records] and use of electronic programs/controls (e.g. electronic tablets) containing navigation charts and weight and balance calculators. The use of electronic signatures enhances the ability to identify a signatory and helps to eliminate the traceability difficulties associated with illegible handwritten entries and the deterioration of paper documentation.

8. RELEVANT LEGISLATIVE PROVISIONS

8.1 The key legislative provisions relating to electronically formatted certifications, records and management systems are contained in the ETA 1999 and Part 11 of the CASR 1998.

Electronic Transactions Act

8.2 The ETA provides that a Commonwealth law requiring or permitting written information, a signature, or the retention of information, can be satisfied electronically (unless specifically excluded by another Commonwealth law). It allows people to communicate electronically with Government agencies and to use electronic communications/record systems to satisfy their legal obligations.

8.3 Section 8 of the ETA 1999 establishes a general rule that for the purpose of a law of the Commonwealth a transaction is not invalid because it takes place wholly or partly by means of one or more electronic communications. The ETA provides that the following requirements under a law of the Commonwealth can be met in electronic form:

- a requirement to give information in writing (section 9 of the ETA 1999);
- a requirement to provide a signature (section 10 of the ETA 1999);
- a requirement to produce a document (section 11 of the ETA 1999); and
- a requirement to record and retain information (section 12 of the ETA 1999).

8.4 These provisions are subject to certain criteria being met. In relation to electronic communications that are required or permitted to be given to Government agencies, the following criteria apply:

- ***Readily accessible condition*** – It must be reasonable to expect that, at the time information in the communication is given, recorded or generated, the information would be readily accessible so as to be useable for subsequent reference.
- ***Integrity*** - The information contained in the communication must retain its integrity. This means the information must remain complete and unaltered (apart from the addition of an endorsement, or any immaterial change arising in the normal course of communication, storage or display). This may include, for example, information added to the communication that is necessary to identify the message for storage purposes.

- ***Specified information technology requirements*** – Where an agency specifies particular information technology requirements for accepting the communication (e.g. that it must be provided in a particular format) those requirements must be met.
- ***Specified verification procedure*** – Where an agency specifies a procedure for verifying the receipt of the communication, the person providing the communication must comply with and complete that procedure.

8.5 In relation to a requirement to provide a signature under a Commonwealth law, section 10 of the ETA 1999 specifies that the following elements that must be satisfied if an electronic signature method is used:

- the method identifies the person and indicates the person's approval of the information communicated; and
- the method is as reliable as is appropriate for the purposes for which the information is communicated.

8.6 The following factors may be taken into account when determining the appropriateness of the signature method adopted:

- the function of the signature requirements in the relevant statutory environment;
- the type of transaction;
- the capability and sophistication of the relevant communication systems; and
- the value and importance of the information in the electronic communication.

Civil Aviation Safety Regulation

8.7 The CASR authorises CASA to specify particular forms for authorisation applications and other documents. Regulation 11.015 of the CASR 1998 defines 'authorisation' as:

- a civil aviation authorisation (as defined in section 3 of the CAA 1988) other than an AOC, a delegation or an appointment of an authorised person;
- an approval or qualification of a document or thing under the CASR or the CAR (other than a material, part, process or appliance to which Subpart 21.K of the CASR 1998 applies); or
- a certificate capable of being granted to a person under the CASR or the CAR.

8.8 Sub regulation 11.030 (1) of the CASR 1998 provides that an application for an authorisation is not taken to have been made unless:

- it is made in the manner approved by CASA for that purpose;
- if CASA has approved a form for the application — it is in the approved form and includes all of the information required by the form;
- it includes all the information required by the CASR or the CAR;
- it is accompanied by every document required by the CASR or the CAR; and
- if a fee is payable for the application — that fee has been paid.

8.9 Regulation 11.018 of the CASR 1998 provides that if CASA has approved a form for a document, other than an application for authorisation, the document is not taken to have been completed unless it:

- is in the approved form; and
- includes all of the information required by the form.

Civil Aviation Act

8.10 The CAA also contains provisions authorising CASA to specify particular forms for civil aviation authorisations. For example, section 27AA of the CAA 1988 states that an application for an AOC must be in a form approved by CASA.

9. APPLICATION OF LEGISLATIVE PROVISIONS TO CASA

9.1 The ETA sets a framework for Government agencies to manage their information resources in a manner that will allow for greater electronic engagement with stakeholders, improve the utility of information for users and enhance the capacity for information to be stored electronically. It means that people engaging with CASA in relation to its statutory functions can generally conduct transactions (e.g. making applications, lodging returns or certificates, or giving information) electronically.

9.2 The aviation regulations have not specifically restricted the use of electronic information management systems or the use of electronic signatures. Nor do the regulations specify that forms required by CASA in relation to its civil aviation functions must be in a particular format. However in many cases they do anticipate a paper based outcome; as a result paper based systems have traditionally been preferred to electronic ones.

9.3 However the legislative provisions discussed above do provide that CASA may do any of the following:

- approve a form for an AOC application under section 27AA of the CAA 1988 in either an electronic or paper format;
- require a person giving information to do so by means of a particular kind of electronic communication and according to particular information technology requirements;
- require a person giving information to take a particular action to verify the receipt of the information; and
- specify that it will receive information on particular forms made available on its website or elsewhere.

10. THE GENERAL OUTCOMES REQUIRED OF AN ELECTRONICALLY FORMATTED CERTIFICATION, RECORD OR MANAGEMENT SYSTEM

10.1 Where an aviation regulation specifies a requirement to:

- give information in writing,
- provide a signature,
- produce a document,
- record information, or
- retain a document,

that requirement can be met in electronic form, subject to the following.

10.2 The attributes of the electronic systems used to meet those requirements must be able to deliver the following outcomes:

- The electronic display of a record that is a log (chronological record history) can provide the display in chronological order.
- The person responsible for the retention of records can inform CASA of a person who has custody of the record and who is able to produce that record.

- If the custody of an aircraft or operational record has been transferred from another person (e.g. when an aircraft is imported into Australia) the transferred records are retained as part of the record that can be produced if required.
- The requirement to produce a document is not nullified by the destruction of a primary data storage. The electronic system needs to be capable of reconstructing the record if there is a requirement to retain a signature, document or information.
- There is a reliable means of assuring the maintenance of the integrity of the information. This could be accomplished by having a record of transactions including records of entries and alterations of entries which identifies the person by name, date and ARN who makes the entry and any alteration. Corrected errors are alterations to the record that need to be identified as and include the reason for the correction.
- The system design takes account of the effort involved in recording information (e.g. the ease of carriage for the electronic recording, certification or management device and the accuracy/continuity of the recorded information).
- There is a mechanism for version control to ensure that, where a document is changed, those changes can be tracked and all users can access the current version.

10.3 Irrespective of how a required document is generated, or what format it takes, the applicant must be able to demonstrate that all the necessary legislative requirements from CAA 1988, CASR 1998, CAR 1988 and associated MOS/CAO are met.

10.4 Where employees require access to on-line documents, this must be considered in the system design. Access would need to be such that the system is sufficiently stable and incorporates any backup mechanisms required to allow the organisation to meet access requirements in the case of any system failure.

11. ELECTRONIC RECORD KEEPING SYSTEMS – GENERIC DESCRIPTORS

11.1 As described below, the ways in which organisations utilise electronic recordkeeping systems—and the degree to which they use them—varies. The following examples reflect the various levels of technology that may be used and outline how each system can meet the requirements of a certification/record keeping system.

11.2 Paper records. Such a system is based on an electronically generated records consisting of work packages printed on paper. The paper record controls the activities to be performed and any required certification is recorded by hand. The paper data record is then entered into the electronic data base. This level of electronic recording does not have a separate log of certifications so the paper records containing the certifications would need to be retained. If the paper records are scanned for retention in a database then the paper record of certifications would not need to be retained.

11.3 Paperless – Single Function System. Such a system is paperless and meets the requirements for an electronic controlled system of certification. The maintenance requirements may be electronically generated from a database or manually input from a paper document. Worksheets will be electronically generated viewed on a monitor or display and records are stored electronically.

11.4 For an AMO example:

- A maintenance certification for the conduct of the maintenance task is electronically recorded by the person performing the maintenance and an electronic CRS for all of the maintenance tasks on the aircraft is signed at completion.
- The record is then electronically closed and filed; however, if the work task is part of a comprehensive maintenance package the system architecture may allow for that record to be retained in 'stasis' until the completion of the maintenance package is coordinated.

11.5 Paperless – Integrated Functions. Such a system is the most sophisticated and is a true paperless system that covers a fully integrated package; it would typically be used by a major airline or a large maintenance organisation. For the airline example the integration could include:

- Flight Operations – electronic flight plans, electronically ordering fuel, electronic weather reports, etc.
- Flight Services – electronic passenger list, catering and in-flight services ordered and confirmed electronically.
- Maintenance – maintenance planning, maintenance watch control, stores/supply (e.g. component tracking by bar code) line and heavy maintenance terminals.
- Load control – electronic transmission to aircraft loaders and trim sheet to flight crew and dispatch.
- Ramp Services – aircraft servicing requirements, electronic notification of fuel loaded to flight crew and load control.
- Flight Crew – (in cockpit) electronic notification of aircraft readiness, load sheet, fuel docket, final flight plan, passenger loading complete. Release by maintenance including MELs and deferred defects.
- Personnel – Record - training and currency.

12. ELECTRONIC SIGNATURES

12.1 General. Before electronic signatures were commonly recognised, a handwritten signature was the primary means by which an individual could comply with the requirement for a signature on any required record, record entry, or document. Although an electronic signature may be essentially a new form of signature, its purpose is identical to that of a handwritten signature or any other form of signature currently accepted by CASA. However to be acceptable, the method used for making an electronic signature must possess those qualities and attributes specified at paragraph 8.5.

12.2 Regulatory requirements. An electronic record keeping system that includes electronic signatures requires approval by CASA; normally during exposition and organisational approval/entry control. Some of the considerations relating to electronic signatures that must be assessed are:

- Relevant records are available to CASA in a readily accessible condition for monitoring and review purposes and are capable of displaying the following:
  - personnel identity (e.g. LAME) – signature and ARN issued by CASA; and
  - organisational identity (e.g.) AMO – signature and identification issued by AMO.

    Note: *A signature comprising merely a person's name and initials may sometimes be acceptable for these purposes.*

- All electronic records must be available in a readily accessible condition so that they:
  - are readable in plain language on the display unit; and
  - can be printed in hard copy where required.
- To guarantee the authenticity of records, the system must be capable of:
  - establishing if the records have been altered by any person or process;
  - establishing the reliability of software applications used to create records;
  - displaying the time and date records were created or altered;
  - demonstrating the name and identity of any person who created, accessed or altered them; and
  - displaying an altered record prior to and after its alteration.

12.3 Recommended Practice. An electronic signature should not be capable of being affixed to a record where the person's qualification and authorisation are not appropriate to the record. Examples of the way in which such a system would work include:

- an B2 Avionic LAME prevented from affixing their electronic signature to a B1 mechanical specific task;
- where the employee's recurrent/continuation training or skill level requirements are not appropriate to the task being carried out the system provides a warning or prevents an entry; or
- where two separate signatures are required (e.g. an independent inspection for a flight critical task), the system requires both signatures and identification for the record to be complete.

12.4 Forms of Electronic Signatures. An electronic signature may be in the form of a digital signature, a digitised image of a paper signature, a typed notation, an electronic code, or any other acceptable form of individual identification that can be reliably used to attest a record, record entry, or document. Not all identifying information found in an electronic system may constitute a signature. For example, the entry of an individual's name in an electronic system may not constitute an electronic signature.

12.5 The Functions and Characteristics of a Signature. A signature is capable of performing a number of functions, namely it can:

- identify the signatory;
- provide certainty as to the personal involvement of a particular person in the act of signing;
- associate a particular person with the contents of the document;
- attest to the intention of a person to be bound by the contents of the document;
- attest to authorship of the document by the signatory; and
- attest to some written agreement which may have been written by some third party who is not a party to the binding agreement.

12.6 Before CASA can accept an electronic signature for certification purposes, the method used must be able to reliably identify the signatory in a way that is difficult for an unauthorised person to duplicate. This can be done by using an authentication procedure that validates the identity of the signatory. For example, an individual using an electronic signature should be required to identify themselves and the system that produces the electronic signature should then authenticate that identification. The signature must also include the licence or certificate number issued by CASA or, where the person is exercising an authorisation issued by an organisation, that identification.

12.7 A computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically. Access to issued stamps or authentication codes should be limited to the user. Although a signature may take many forms, CASA emphasises that all electronic entries may not necessarily satisfy the criteria that would qualify an electronic entry as an acceptable signature.

12.8 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 PINs or passwords memorised by an individual could also serve as an acceptable method of ensuring uniqueness. Additionally, a system could also use physical characteristics, such as a fingerprint, handprint, or voice pattern, etc as a method of identification and authorisation.

12.9 Significance. An individual using an electronic signature should take deliberate and recognisable action to affix his or her signature (e.g. using badge swipes, signing an electronic document with a stylus, inputting a specific keystroke(s), or using a digital signature).

12.10 Scope. The scope of information attested by an electronic signature must be understood by the signatory and be apparent to subsequent readers of the record, record entry, or document. While handwritten documents use the physical proximity of the signature to the information in order to identify those items attested to by a signature, electronic documents may not use the position of a signature in the same way. It is therefore important to clearly delineate the specific sections of a record or document that are affected by a signature from those sections that are not affected. Acceptable methods of delineation of the affected areas include, but are not limited to: highlighting, contrast inversion or the use of borders or flashing characters. In addition, the system should notify the signatory that the signature has been affixed.

12.11 Signature Security. The security of an individual's handwritten signature is maintained by ensuring it is difficult for another person to duplicate or alter it. An electronic signature should maintain an equivalent level of security. Due to the reproduction capability inherent in an electronic system, an electronic system used to produce a signature should restrict the ability of any person to cause another individual's signature to be affixed to record, record entry, or document. Such a system enhances safety by precluding an unauthorised person from certifying required documents, such as a maintenance release. The signatory must also know who else holds the privilege for access to the electronic authentication key.

12.12 Non-repudiation. An electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. The more difficult it is to duplicate a signature, the greater the likelihood that a signature was created by the signatory. Those security features of an electronic system that make it difficult for another person to duplicate a signature or alter a signed document tend to ensure that a signature was indeed made by the signatory.

12.13 Traceability. An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

12.14 Approval prior to the use of a system using Electronic Signatures. Organisations intending to use electronic signatures should consult with CASA before implementing an electronic signature system of certification. A written description of how electronic signatures will be used in maintenance or other activities should be submitted along with draft copies of the applicable regulatory required manuals. CASA will review the electronic signature methods proposed. If an amendment to the organisation expostion and approval is required the CASA will charge for the approval in accord with the relevant fees regulations.

12.15 Acceptance of Systems. The prior acceptance of a system of electronic recordkeeping system or a system using electronic signatures by an aircraft designer/manufacturer does not mean an automatic acceptance by CASA for use of the product by your organisation. Whilst the software and hardware may be the same, the assessment will be carried out based on how you will use the system (as described in your exposition/procedures manual) and what you propose to do with that system. A statement of conformity of your system (by the software vendor) that the system is being used by an organisation equivalent to your own may assist in the approval process. The organisation must provide a copy of the procedures to be used for implementing an electronic record keeping system, for approval, to the CASA Operations office with oversight jurisdiction.

13. SECURITY OF ELECTRONIC RECORD KEEPING SYSTEMS

13.1 Security. The security mechanisms provided for an electronically formatted certification, record or management system requires the following attributes:

- The electronic system must maintain information confidentially.
- The system must ensure that there cannot be unauthorised alterations to the record.
- A corresponding policy and management structure must support the hardware and software that delivers the information.
- Before introducing an electronic system, the organisation's exposition/procedures must include the following:
    - a mechanism for version control;
    - an audit procedure that can ensure the integrity of each computerised workstation and verify whether records have been accessed improperly;
    - a procedure for conducting a review of the use of any personal identification codes by the system to ensure that it will not permit password duplication;
    - a procedure that establishes an audit of the computer system at a frequency sufficient to ensure the integrity of the system (e.g. by demonstrating that access to records is restricted to authorised persons or applications);
    - a procedure that describes how it will ensure that the computerised records will be transmitted to other organisations in a format acceptable to them.
    - a procedure for making required records available to CASA personnel (e.g. by providing access to the system via a logon portal) so that they can make paper copies of viewed information;

- guidelines for the use of electronic signatures for contractors; and
- a description of the training procedure and requirements to authorise access to the system.

14. ELECTRONIC MANAGEMENT SYSTEMS

14.1 There are now devices available within an organisation or aircraft that can replace paper based systems. As an example the Electronic Flight Bag can be used as a replacement for paper in the flight compartment; see CAAP 233-1 - *Electronic Flight Bag*.

14.2 The range of electronic devices and programs now available to assist in the conduct and management of aircraft related activity is ever expanding. Depending on where the systems will be used, and what the programs will be used to accomplish, CASA may or may not be involved in the approval of the electronic management system.

14.3 Matters to be considered for an electronic management system include: confirmation that the calculations used in the program are correct; connectivity – wireless systems; power connections; software applications; hardware; mounts; cabling; stowage; security; electromagnetic interference, electromagnetic compatibility; procedure and updates. Devices used in aircraft may require airworthiness approval.

14.4 If in doubt, contact CASA for advice in regard to any specific electronic management system (and associated devices) and the need for any approval of such a system.

Executive Manager
Standards Division

October 2012