Australian Government
Civil Aviation Safety Authority

Advisory Circular

AC 43-32(0) OCTOBER 2003

ACCEPTANCE AND USE OF ELECTRONIC SIGNATURES AND ELECTRONIC RECORDKEEPING SYSTEMS

CONTENTS

REFERENCES

This AC is to be read in conjunction with the *Civil Aviation Safety Regulations 1998* (CASR) Part 21, 43, 121, 133, 144, 145 & 146.

2. STATUS OF THIS AC

This is the first AC to be written on the subject.

3. PURPOSE.

3.1 This advisory circular (AC) provides guidance on the acceptance and use of electronic signatures and electronic record keeping systems.

3.2 Although this AC addresses airworthiness and maintenance, the contents may be suitable advice for manufacture, training, design, distribution or operational needs, and expresses CASA's policy on the acceptance of electronic signatures.

Advisory Circulars are intended to provide recommendations 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 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

4. RELATED READING MATERIALS

- Electronic Transaction Act: available from http://scaleplus.law.gov.au

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.

Note: The Macquarie Dictionary defines "authenticate" as "to make authoritative or valid; to establish as genuine". Further the term "valid" is defined in part as "legally sound, effective, or binding; having legal force; sustainable at law".

***digital signature technology*:** is the foundation of a variety of security, e-business, and e-commerce products. This technology is based on public/private key cryptography, digital signature technology used in secure messaging, public key infrastructure (PKI), virtual private network (VPN), web standards for secure transactions, and electronic digital signatures.

electronic signature: is a method of electronically identifying and authenticating an individual entering, verifying, or auditing computer-based records. An electronic signature combines cryptographic functions of digital signatures with the image of a person's handwritten signature or some other form of code or visible mark that would be considered acceptable in a traditional signing process, authenticates data with a hashing algorithm, and provides permanent secure user-authentication.

***signature*:** is any form of identification used to attest to the completion of an act and authenticate a record entry, must be traceable to the person making the entry, and must be handwritten or part of an electronic signature system or other form acceptable to CASA.

***organisation*:** means and includes the following: Air Operators Certificate Holder (AOC's), Approved Maintenance Organisations (AMO's), Production Certificate Holder's Maintenance Training Organisation (MTO's), Approved Design Organisation (ADO's) and Approved Distribution Organisation Certificate Holders.

6. WHO DOES THIS AC APPLY TO

6.1 This AC applies to persons carrying out any maintenance activity under CASR Part 43 and who wish to use an electronic certification or recording system.. However, the contents are applicable for other regulatory record keeping and procedural requirements that include but are not limited to:

- operators under CASR Part 121A/B or Part 133 ;
- operators under CASR Part 91;
- maintenance organisations under CASR Part 145;
- manufacturing organisations under CASR Part 21;
- training organisations under CASR part 147;
- distribution organisations CASR part 144; and

- design organisation under CASR part 146.

This AC specifies provisions pertinent to electronic certification and recording system procedures, consistent with the relevant regulations.

7. BACKGROUND

7.1 The Electronic Transactions Act 1999 (ET Act), and Commonwealth Government policy sets the framework for Commonwealth and State Government agencies to implement procedures for managing their information resources in a manner that will improve the utility of information for users and for archiving information in electronic format. In addition the Commonwealth Government and Australian Government agencies give legal effect to electronic signatures.

7.2 Previously the regulations governing the use of signatures to satisfy maintenance, manufacture and operational requirements did not reflect advances in information storage and retrieval technology. These earlier requirements were developed at a time when the use of electronic media for the storage and retrieval of data was neither available nor contemplated.

7.3 As the complexity of aircraft design, operations, and maintenance processes increased, the number of records and documents generated and required to be retained by aircraft registered operators, manufacturers, and maintenance organisations expanded dramatically. 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.

7.4 Although previous regulations did not legislatively restrict the full implementation of electronic information storage and retrieval systems and the use of digital or electronic signatures, there were technological limitations for records or documents that required the affixation of a signature.

7.5 The Commonwealth Government and other government agencies recognise the limitations imposed on the use of electronic signatures and are revising the regulations governing the use of signatures to facilitate the use of electronic signatures. The National Electronic Authentication Council (NEAC) has been established by the Commonwealth Government to enhance business and consumer confidence in e-commerce through overseeing the development of a national framework for electronic authentication of online communications.

7.6 Acceptance of electronic signatures will promote the use of electronic maintenance logbooks to comply with record retention and record entry requirements because all regulatory required aircraft records authenticated using an electronic signature are acceptable to both CASA and many other NAAs. Electronic signatures will also simplify application and approval process for AARs and speed up the process by which changes are made to documents or manuals within an approved electronic system.

7.7 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 SYSTEM ACCEPTABILITY

8.1 An electronic record keeping system that includes electronic signatures will be acceptable to CASA.

8. 2 To allow acceptance of such a system, all details of the system require assessment: Features of such a system are:

- The ability to make all records available to CASA where required by regulations.
- That all records be available to be printed or copied in a secure format and show the following in plain language:
  - LAME: Signature and Licence Number issued by CASA
  - AMS: Signature and Certificate Number issued by CASA
  - AMT: Signature and authorisation issued by AMO
  - AAR: Signature and Certificate Number issued by CASA

  Note: a signature may be the persons name and initials
- All records displayed in an electronic format should be available in plain language on the display unit and meet the requirements in the item above.
- All records that have been modified or edited by any person within the organisation should display in plain language the name and identification of the person accessing and modifying or editing the record and should display the modified or edited record prior to editing and post editing on the same screen.
- An electronic signature may not be affixed to a record where the persons Qualification and authorisation are not appropriate to the record. e.g. a mechanical LAME should be prevented from affixing their electronic signature to an avionic specific task, or any other task for which they are not qualified.
- An electronic signature may not be affixed to a record where the persons recurrent, continuation training or skill level requirements are not appropriate to the task being carried out.
- Where aircraft worksheets require two separate signatures for a person carrying out a task and a person signing for a task then both signatures and identification must be available on the one electronic record.

9 CRITERIA FOR ELECTRONIC SIGNATURES

9.1 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 unique form of individual identification that can be used as a means of authenticating a record, record entry, or document. Users of electronic signatures should be aware that not all-identifying information found in an electronic system might constitute a signature. For example, the entry of an individual's name in an electronic system may not constitute an electronic signature.

9.2 Can an Electronic Signature be accepted as a Signature?

Yes, an electronic signature can be accepted as a signature because:

- electronic signatures are marks capable of being affixed by the person or by some person authorised by the person intending to be bound;
- an electronic signature can be affixed via mechanical means, as can a traditional signature;
- an electronic signature can be either highly secure or highly insecure as can a traditional signature;
- at the time of making the electronic signature, the intention can be satisfied regardless of whether a signature is applied physically or electronically. In this regard the mechanism used to make the electronic signature should ensure that it makes provision to detect any detachment of the electronic signature from the document. This should activate the verification process and cancel the document.

9.3 Uniqueness

Uniqueness can be achieved by many methods. eg. Badges, cards, cryptographic keys, PIN numbers or other acceptable methods. Additionally, a system could also use physical characteristics, such as a fingerprint, handprint, or voice pattern, etc as a method of identification and authorisation.

9.4 Scope

It is important to clearly delineate the specific sections of a record or document that are affected by a signature. 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.

9.5 Signature Security

An electronic signature should maintain a level of security. Such a system should enhance safety by precluding an unauthorised person from certifying required documents, such as a return to service document. The signatory should also know who else holds access privileges.

9.6 Traceability

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

Computer entries used, as a signature, should have restricted access that is limited by an authentication code that is changed periodically. 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.

9.7 Approval prior to the use of a system using Electronic Signatures

Organisations intending to use electronic signatures should consult with their local CASA Office before implementing an electronic signature system of certification. A written description of how electronic signatures will be used should be submitted along with draft copies of the applicable regulatory required manuals. CASA will review the electronic signature methods proposed.

9.8 Acceptance of Systems

The prior acceptance of a system of electronic record keeping system or a system using electronic signatures does not mean an automatic acceptance by CASA. Whilst the software and hardware may be the same the assessment must be carried out based on how you use the system (your procedures manual) and what you propose to do with that system.

10 CRITERIA FOR ELECTRONIC RECORD KEEPING SYSTEMS.

There are a number of options available using electronic record-keeping systems. The underlaying facts which require consideration are how much the organisation wishes to pay for the record keeping system.

10.1 System Management.

The system management is based on documented procedures and would include as a minimum:

- Details of the System Security Principles.The identification of the person who has the right to access to the information and the rights and methods of tracking that access, described in a procedures manual**.** The electronic system must protect the information confidentiality and sustainability.
- address all information management system/human interface activities.
- protocols for allocation, management and storage of passwords and digital signatures
- address procedures for keeping the manual current.
- detail a system auditing process (an electronic system integrity check, typically an electronic log) including:
    - detection of security breaches
    - unauthorised data manipulation
    - retention of electronic log related to such activity
    - Detail audit procedures that are frequent enough and adequate to assure the accuracy of the records
- The frequency and scope of these procedures should reflect the complexity of the computer-based record keeping system and the size of the database.

The organisation must provide a copy of the procedures to be used for implementing an electronic record keeping system, for approval, to the CASA Airline or Area Office with oversight jurisdiction.

Bill McIntyre
Executive Manager
Aviation Safety Standards