ADVISORY INFORMATION *02/2025*

28th March 2025

ACCEPTANCE OF ELECTRONIC SIGNATURE AND RECORDKEEPING FOR AIRCRAFT MAINTENANCE AND CONTINUING AIRWORTHINESS

1 Introduction

1.1 This Advisory Information (AI) is to provide guidance to aviation organisation seeking to establish and develop procedures for electronic signatures and electronic recordkeeping.

1.2 The Electronic Government Activities Act 2007 [*Act 680*] was enacted to provide for legal recognition of electronic messages in dealings between the Government and the public, the use of the electronic messages to fulfil legal requirements and to enable and facilitate the dealings through the use of electronic means and other matters connected therewith. An aviation organisation intending to transition to an electronic system shall ensure that its system complies with the provision of this Act. The aviation organisation shall ensure seamless data continuity during the transition from legacy paper-based system (i.e. hard copy) to an electronic system.

1.3 The Digital Signature Act 1997 [*Act 562*] shall continue to apply to any digital signature used as an electronic signature in any Government activities as stipulated in Act 680.

1.4 Throughout this AI, the term “electronic signature” refers to either electronic or digital signatures, depending on the system application and user preferences.

2 General

2.1 The information pertaining to aircraft maintenance and continuing airworthiness is currently recorded, certified and stored in paper formats. However, this approach faces challenges in managing the increasing volume and complexity of modern aviation operations. Transitioning to electronic systems addresses these limitations, enhancing real-time accuracy and data integrity.

2.2 An electronic recordkeeping system shall 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-based formats.

2.3 Electronic signature and any electronic record-keeping system and the record it generates, processes and stores shall be described in the aviation organisation's exposition, be acceptable to the Civil Aviation Authority of Malaysia (CAAM) and meet the requirements set by CAAM for the purpose of aviation organisation's maintenance and continuing airworthiness activity. This shall include unrestricted CAAM access for auditing and the capability of the aviation organisation to provide paper copies of records if required by CAAM.

2.4 In developing the procedure, the aviation organisation shall carefully consider the standard baseline outlined in the following reference standards or their equivalent:

a) ATA Spec 2000 e-business Specification;

b) ATA iSpec 2200 Information Standards for Aviation Maintenance;

c) ATA Spec 2300 Data Exchange Standard for Flight Operations;

d) ATA Spec 42 Aviation Industry Standards for Digital Information Security;

e) S1000D International Specification for Technical Publications Using a Common Source Database;

f) ARINC-811 Commercial Aircraft Information Security Concepts of Operation and Process Framework;

g) RTCA/EUROCAE documents DO-355/ED-204 - Information Security Guidance for Continuing Airworthiness.

2.5 The electronic record generated, processed and stored shall be considered as original documents. Use of a complete electronic record-keeping system shall be acceptable to CAAM. Electronic records signed electronically shall be considered equivalent to aircraft maintenance and continuing airworthiness records authenticated with non-electronic signatures. Any printout of an electronic record required by CAAM shall have a watermark displayed on the page background stating "PRINTED FROM ELECTRONIC FILE".

2.6 A combination of electronic and paper-based maintenance record-keeping systems may be acceptable to CAAM provided that the aviation organisation adopts the traditional paper-based system as a backup for situations where a full electronic record cannot be created.

2.7 The adoption of the electronic records system should be conditional upon providing all system users with the adequate training, including security awareness and the relevant policies and procedures for the implemented system. The assurance of its implementation is, thus, as important to an electronic records system as the architecture itself. CAAM shall 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.

3 Identification, Authentication and Authorisation

3.1 To facilitate the establishment for the electronic system, procedures shall be specified enabling and ensuring verification of the identity of various parties that are involved in the issuance of a credential. The credential shall be the basis of establishing the identity of an electronic record system user.

3.2 The electronic record system shall perform the user's identity authentication. This shall consist of means by which the system validates an authorised user's identity. These means may include, but are not limited to, a password, a Personal Identification Number (PIN), a cryptographic key, or a badge swipe, all in correlation with the implemented solution and processes.

3.3 The level of identity assurance and authentication should commensurate to the class of activity for which the electronic record system is authorising the user's access.

3.4 The user's identity assurance should comprise both initial and continuing (i.e. periodic) procedures with which the user has to comply.

3.5 The aviation organisation to which the user belongs at the time of interacting with the electronic record should be responsible for the correlation between the management of the user's identity and the user's scope of authorisation.

4 Electronic Signature

4.1 A handwritten signature is universally recognised and valued for its qualities of authenticity, integrity, and intent, which establish trust and accountability. To ensure these qualities are preserved, an electronic signature must fulfil the same purpose and maintain the key attributes of a handwritten signature. It must reliably confirm the signatory's identity and validate the intention to approve or authenticate the associated document.

4.2 An electronic signature is the online equivalent of a handwritten signature. It may take the form of any letter, character, number, sound, symbol, visible mark or any any combination thereof in an electronic form adopted by a person as a signature. This signature is executed or adopted by an individual to signify intent to sign the document. It securely identifies and authenticates the signatory during the processes of creating, verifying, or auditing computer-based records. Additionally, the electronic signature must be intrinsically linked to the data it authenticates, ensuring that any subsequent changes to the record are immediately detectable.

4.3 There are several attributes that an electronic signature shall possess:

a) Uniqueness

1) An electronic signature shall identify a specific individual and shall be difficult to duplicate. This can be achieved through robust identification and authentication procedures that validate the signatory's identity.

2) Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes encoded onto badges, cards, cryptographic keys, or other secure objects.

3) Systems employing PINs or passwords or physical characteristics, such as fingerprints, handprints, or voice patterns could also be an acceptable method of ensuring uniqueness in identification and authorisation. To enhance security, authentication codes must be periodically updated, and access to electronic signatures should be tightly restricted.

b) Significance

1) An electronic signature must be affixed deliberately by the signatory, ensuring conscious acknowledgment of the act.

2) Recognisable actions that signify deliberate intent include: badge swipes, signing an electronic document with a stylus, typing specific keystrokes or using a digital signature. These actions provide a clear indication of the signatory's intent to affirm the document or record.

c) Scope

1) The scope of information being affirmed with an electronic signature shall be clear to the signatory and to subsequent readers of the record, record entry, or document.

2) The electronic record shall accurately reflect the information being affirmed by the signatory and the signatory shall be fully aware of what he or she is signing.

d) Security

1) An electronic system that produces signatures shall restrict other individuals from affixing another individual's signature to a record, record entry, document, or alter the content without detection.

2) Policies and management structures shall support the system's security, and procedures must ensure that electronic signatures are immediately disabled when an employee leaves or terminates employment.

e) Non-repudiation

An electronic signature shall prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. This ensures accountability and legal enforceability.

f) Traceability

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

4.4 The electronic signature solution adopted should adhere to CAAM requirements and industry standards regarding: the strength of the user/system identification credential employed in creating signatures, the proof-of-possession algorithm for identification credentials, the cryptographic algorithm for protection of data and alternatives that may provide similar protection if the previously enumerated are deemed impractical.

4.5 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.

4.6 CAAM only accepts aviation organisation that subscribe to the approved certification authority before implementing the digital signature as prescribed in Act 562. CAAM may recognise certification authorities outside Malaysia provided that it satisfies with Act 562.

5 Security and Integrity Exemption

5.1 A robust policy and management structure shall support the computer hardware and software systems that manage electronic records. Appropriate physical security and electronic backup measures shall be established for current, operational, stored and archived records.

5.2 The electronic record system shall safeguard confidential information and ensures/guarantee the integrity of the data by preventing unauthorised modifications or alterations to the record. Any changes must be appropriately tracked and documented.

5.3 Procedures shall be established allowing the aviation organisation to correct documents that were electronically signed in error. The original entry shall 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 shall be clearly identified that the original entry has been superseded by another entry.

5.4 Procedures shall be established to describe how the aviation organisation will ensure that the electronic records are securely transmitted to stakeholders who require access to the records.

5.5 Procedures shall be established to periodically review the computerised personal identification code systems to prevent password duplication and enhance user security.

5.6 Procedures shall be established to periodically audit the computer system to maintain system integrity. A record of the audit shall be completed and retained on file as part of the aviation organisation's record retention requirements. This audit may be supported by automated system self-testing.

5.7 Procedures shall be established for non-recurring audits of the computer system if there is suspicion of system integrity issues, ensuring rapid resolution of vulnerabilities.

5.8 Audit procedures shall be established to ensure the integrity of each computerised workstation. For server-based systems, where workstation-level access attributes are managed centrally, individual audits on workstations may not be required. The procedures shall be applicable to both fixed (e.g. desktop computers) and mobile devices (e.g. laptops, tablets, PMATs etc.).

5.9 An information security assessment process shall be established for the electronic record system to evaluate how effectively each entity being assessed (e.g. hosts, networks, procedures, personnel) meets specific security objectives. The effective implementation of such established process should involve password cracking and security penetration testing procedures.

6 Archiving and Transferability

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

7 Application Submission

Aviation organisations must submit a formal application (i.e. in writing) to CAAM along with the required exposition outlined in paragraph 2.3. The applicant is required to demonstrate its processes for electronic signatures and electronic record-keeping, ensuring compliance with CAAM requirements.

8 Conclusion

CAAM recognises the potential benefits of digital technologies being applied in the various sectors of the aviation industry. When aviation organisation implement the use of electronic signature and electronic record-keeping in accordance with proper policies, processes and procedures, this will further enhance aviation safety, operational efficiency and sustainability in aircraft maintenance and continuing airworthiness.

DATO' CAPTAIN NORAZMAN BIN MAHMUD
Chief Executive Officer
for Civil Aviation Authority of Malaysia
28 March 2025