Carriage of electronic documents on board aircraft

Guidance for EASA Member States

Issue no.: 1

(valid until further notice)

Date:	16.12.2021
Author / FS2 Focal point:	(Lia CALLEJA BARCENA / Dangerous Goods Expert)
Reviewed:	(Micaela VERISSIMO / Section Manager - Air Operations Standards)
Approved:	(Eduard CIOFU / Head of Department - Air Operations & Aerodromes)

Contents

Revision record

Issue	Date of issue	Summary of changes
01		Initial issue

Change Revision Summary

Paragraph no.	Description of change

1. Purpose of these Guidelines

This document provides guidance for Member States on the carriage of electronic documents on board aircraft.

2. Executive Summary

Commission Regulation (EU) No 965/2012[1] establishes the list of documents that must be carried on board an aircraft. However, it does not differentiate between paper and electronic documents and, thus, does not prevent the issuance or use of electronic documents. Therefore, nothing in the rules prevents operators from carrying documents in electronic form.

The framework for electronic identification and trust services for electronic transactions in the internal market is established in Europe by Regulation (EU) No 910/2014[2] (the eIDAS Regulation). This regulation contains the information and definitions of the different electronic signatures and seals.

Establishing administrative law is a prerogative of EU Member States (MS). This guidance is therefore intended to clarify that there are no barriers in the EU operational regulations to the carriage of electronic certificates and provide general information to EU MS on the levels of security for them to develop their national requirements.

This guidance only focuses on the EU system and does not cover the international recognition of electronic certificates. Further work is ongoing at ICAO level on this topic, to which EASA is contributing.

[1] *Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council*

[2] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*

3. Background information

CAT.GEN.MPA.180 of Annex IV (Part-CAT) to Commission Regulation (EU) No 965/2012[3] establishes the list of documents to be carried on board aircraft performing commercial air transport (CAT) operations. Similar lists can be found in NCC.GEN.140, NCO.GEN.135 and SPO.GEN.140.

Under CAT.GEN.MPA.180, most of the referred documents can be carried as "*originals or copies*", except for:

— the certificate of registration, the certificate of Airworthiness (CofA) and the radio licence, where it is specified that the original is required; and

— the air operator certificate (AOC), where it is specified that a certified true copy is required.[4]

AMC1 CAT.MPA.GEN.180 clarifies that "*The documents, manuals and information may be available in a form other than on printed paper. Accessibility, usability and reliability should be assured*".

Therefore, Commission Regulation (EU) No 965/2012 does not differentiate between documents in paper and electronic form **and does not prevent operators from carrying documents and certificates in an electronic form.**

4. Applicability and legal framework

4.1 Types of Certificates: Original, copy and certified true copy

As we have seen, documents listed under CAT.GEN.MPA.180 shall be carried as either original, (simple) copy, or certified true copy. Without prejudice to national administrative law of the Member States (MS) establishing rules and procedures for the issuance of certificates, these categories of document forms can be interpreted as follows:

(1) An 'original' can mean that the certificate is issued either as a 'paper' original or an 'electronic' original by the entity responsible for the issuance of the certificate.

(2) A (simple) 'copy' can materialize in the form it was originally issued (e.g. paper copy of a paper original) or in a form other than its original form (i.e. paper to/from electronic).

(3) Whereas the notion of 'certified true copies' are not defined by Commission Regulation (EU) No 965/2012. GM1 CAT.GEN.MPA.180(a)(5)(6) clarifies that such documents may be provided "*directly by the competent authority*" or "*by persons holding privileges for certification of official documents in accordance with the applicable Member State's legislation, e.g. public notaries, authorised officials in public services*". Traditionally, paper-based documents have been subject to such certification procedure, where the authorised person attests on the paper copy that it's identical to the original document, thus having the same probative value of the original. Nevertheless, with the expansion of electronic means in administrative processes, it is not excluded (in fact, examples already exist at a national level) that an original

[3] *Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council*

[4] In the case of other types of operations, NCC.GEN.140, NCO.GEN.135 and SPO.GEN.A40 only require the certificate of registration and the CofA to be originals. For all other documents, simple copies are acceptable.

paper document is digitised into a certified electronic copy which would have the same probative value as the paper original, provided that the rules for making electronic copies of a paper document are followed. The establishment of such administrative rules is reserved to the MS.

4.2 Legal Framework within the EU

Regulation (EU) No 910/2014[5] (the eIDAS Regulation) establishes a legal framework for electronic identification and trust services for electronic transactions in the internal market. Its objective is to enhance trust in electronic transactions by providing a common foundation for secure electronic interaction between citizens, businesses, and public authorities. The eIDAS Regulation includes rules on electronic identification means, such as electronic signatures and seals. According to the eIDAS Regulation:

(1) an electronic signature/seal (i.e. simple, advanced, qualified) is admissible as evidence in courts in the EU and shall not be denied legal effect solely because of being in electronic form or not meeting the requirements for qualified electronic signature/seal[6];

(2) a qualified electronic signature shall have the equivalent legal effect of a handwritten signature[7]; and

(3) qualified electronic signature/seals that are based on a qualified certificate enjoy mutual recognition as qualified electronic signatures/seals in all MS[8]. Under certain conditions, advanced electronic signatures/seals based on a qualified certificate can also benefit from recognition between MS[9].

However, the eIDAS Regulation does not dictate when a signature/seal is needed or what type of signature/seal is necessary per type of document.

Although the qualified signature/seal represents the highest level of security, that doesn´t necessarily mean that all processes must rely on this type of assurance. Below is more information on the different signatures and seals and their associated levels of protection.

4.3 Competencies and recognition within the EU

In general, establishing administrative law is the prerogative of EU MS, which can develop requirements within their legislation addressing when a signature/seal is needed and which type of signature/seal is necessary per document. For example, if, by law, written formalities are required for a transaction, contract, etc., a qualified electronic signature may be required. Considering these

[5]Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[6]cf. Art. 25(1) and 35(1) of the eIDAS Regulation

[7]cf. Art. 25(2) of the eIDAS Regulation

[8]cf. Art. 25(3) and 35(3) of the eIDAS Regulation

[9] cf. Art. 27 (1)-(2) and 37 (1)-(2) of the eIDAS Regulation, see also Commission Implementing Decision (EU) 2015/1506

principles, MS are free to set up their national requirements on electronic identification schemes[10] and electronic identification means[11] to be used.

EASA cannot, therefore, provide a concrete suggestion on the introduction of electronic procedures, the issuance of specific electronic certificates, or the use of specific electronic identification means. However, as we have already seen, Regulation (EU) No 965/2012 does not prevent the issuance or use of electronic documents.

MS can thus decide to set up electronic processes for managing the relations between the competent authority and the overseen persons/organisations, including those resulting in:

— issuing electronic certificates (e.g. those required by Regulation (EU) 965/2012),

— allowing for digitalisation of original paper certificates into a certified electronic copy; or

— establishing how an electronically issued original can be transformed into a certified paper copy.

A national example of digitalisation provided by the Spanish competent authority (AESA) can be found in Annex I.

5. Level of Protection

5.1 Establishing a minimum level of security and protection

The main purpose of establishing administrative requirements to issue a certificate (both in paper or electronic form) is to guarantee a minimum level of protection by ensuring the certainty of the document's origin, in particular its authenticity and the integrity of its content. This way, the certificate document can be relied on by third parties.

Therefore, when setting up electronic processes, MS should carefully assess the level of security and protection needed for each type of document. Based on this assessment, MS can choose the adequate types of electronic signatures or seals to be used.

The following paragraphs include information on the different levels of protection afforded by different types of signatures and seals. Following further discussion with MS, the Agency intends to issue additional guidance, such as best practices and other relevant material, to support national authorities in issuing and accepting certificates in electronic form.

5.2 Types of signatures and protection levels

In addition to the traditional, wet signature, the use of electronic – in the international/ICAO context, also called digital – signature is becoming more widespread in the EU.

(1) Wet signature

[10] 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons (cf. Art. 3(4) of the eIDAS Regulation)

[11] 'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service (cf. Art. 3(2) of the eIDAS Regulation)

A signature on paper, or wet signature, is any mark that a person places on a paper document to authenticate the document. Furthermore, the signature serves to identify the signatory since each person's signature is unique to them.

(2) Electronic signature

There are several types of electronic signatures depending on the level of technical complexity and security. There are three different electronic signatures in accordance with the eIDAS Regulation[12]:

(a) 'electronic signature'[13] means data in electronic form, which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

(b) 'advanced electronic signature'[14] (AES) means an electronic signature that is uniquely linked to the signatory, capable of identifying the signatory, has been created using electronic signature creation data that the signatory can, with a high level of confidence, use under his/her sole control, and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. Furthermore, MS requiring advanced signatures to use an online service, offered by or on behalf of a public sector body, shall recognise advanced and qualified signatures in the formats or using methods defined in implementing acts established by the European Commission[15].

(c) 'qualified electronic signature'[16] (QES) means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. It, therefore, represents the most advanced stage of electronic signature security and has the equivalent legal effect of a handwritten one. There are very specific requirements as to how the identity of the signatory is verified and how the signature key is protected. Qualified electronic signatures based on qualified certificates issued in one Member State shall be recognised as qualified electronic signatures in all other Member States.

The three types of electronic signature differ on the level of security they have and the complexity of the verification system they use to identify the signatory. Thus, the strength lies in the degree of confidence that it provides as regards the identification of the signatory and the assurance that the document signed is indeed the correct one.

[12] More detailed information can be found in https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature and in the documents addressing Trust Services under the eIDAS Regulation published by the European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/publications#c5=2011&c5=2021&c5=false&c2=publicationDate&reversed=on&b_start=0&c10=Trust+Services&c8=Trust+service+providers. In particular, their paper on QES: https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures.

[13] cf. Art. 3(10) of the eIDAS Regulation

[14] cf. Art. 3(11) and Art. 26 of the eIDAS Regulation

[15] cf. Art. 27 of the eIDAS Regulation, see also Commission Implementing Decision (EU) 2015/1506

[16] cf. Art. 3(12) of the eIDAS Regulation

5.3 Electronic seal

An electronic seal is defined by the eIDAS Regulation as "*data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity*". As happens with the signatures, they shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals[17].

Electronic seals can also be simple, advanced, and qualified. The level of security can be therefore compared to that of the signatures.

Whereas the simple electronic seal would only have to meet the definition above, the advanced electronic seal shall meet the requirements established in Article 36 of the eIDAS regulation and, thus, is:

(1) uniquely linked to the creator of the seal;

(2) capable of identifying the creator of the seal;

(3) created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(4) linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

A qualified electronic seal provides the next level of security. It is an advanced electronic seal, which is created by a qualified electronic seal creation device[18] and based on a qualified certificate for electronic seal[19][20].

6. Conclusions

The Air Operations Rules mandate the carriage of certain documents on board aircraft. In some cases, the rules require these documents to be originals or certified true copies. However, the rules do not prescribe a specific format for these documents, which means that electronic/digital documents are fully acceptable.

MS are fully competent to establish, under the applicable EU and national law, electronic processes to manage the relations between their national aviation authorities and their stakeholders, up to, and including, the issuance of electronic/digital certificates.

When doing so, MS should carefully consider the level of security and protection needed for each type of document. Based on this assessment, MS can choose the adequate types of electronic signatures or seals to be used.

---

[17] cf. Art. 35 of the eIDAS Regulation

[18] 'electronic seal creation device' is defined in Art. 3 of the eIDAS Regulation as an electronic seal creation device that meets mutatis mutandis the requirements laid down in its Annex II.

[19] 'qualified certificate for electronic seal' is defined in Art. 3 of the eIDAS Regulation as a certificate for an electronic seal that is issued by a qualified trust service provider and meets the requirements laid down in Annex III.

[20] For more information see Security guidelines on the appropriate use of qualified electronic seals (https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-seals)

Annex I: Example – Digitalisation in the Spanish CAA

1. Background, Legal Framework and Content

Spain has developed the necessary mechanisms to implement an "electronic administration". The most relevant regulations are Law 39-2015[21] and Law 11-2007[22], the latter one recognising the citizens' right to use electronic means for all administrative processes. This results in an obligation for the Government to ensure all the necessary mechanisms to this end.

Multiple systems were created and integrated in AESA[23] (Spanish Aviation Safety and Security Agency). Existing business applications were integrated using new "horizontal" tools to achieve the electronic administration functionalities. The following components were developed to issue documents:

— **Electronic Headquarters**. Article 38 of Law 40/2015[24] establishes that the Electronic Headquarters is an electronic address that serves as an official point of telematic access for the citizens to the Administration. The owner (either a Public Administration or one or several public organisms of Public Law when applying their competences) is responsible for the integrity, veracity and update of the information and services offered by it. Its identification is done through a server certificate or an equivalent mean, as established by Royal Decree 1671/2009[25]. Publication of information, services and transactions respect the principles of accessibility and use established by the regulations and all other applicable standards.

— **Verification safety code (CSV)**. It permits identifying and finding each and every document issued by the Administration by simply introducing an alphanumeric code.

— **Electronic signature of the certificates**. It is regulated in 59/2003[26]. It ensures identification of the signatory, integrity of the document, and that the document cannot be repudiated.

— **Printable version**. Is an original document format that shows both the content and the relevant information associated to its electronic signature. It is produced in the Electronic Headquarters and signed with the electronic seal and can be printed to obtain a paper copy.

2. System – Business support

The system used has more than 25 business processes. It puts together all the relevant information of many related processes that interact between them. It has more than 219,300 documents signed, 63,200 files created and 500 different document templates. It is used for Operations, Continuous Airworthiness, Initial Airworthiness, Licenses and Unmanned Aircraft Systems.

---

[21] *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*

[22] *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*

[23] *Formerly DGAC, General Directorate of Civil Aviation*

[24] *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*

[25] *Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*

[26] *Ley 59/2003, de 19 de diciembre, de firma electrónica*

3. Case study: AOC certificate

3.1 Information sources

To issue an AOC certificate, the following information, obtained from different sources, is necessary:

— Initial application from the interested party.

— Information regarding the registration of the Aircraft (external to SIPA).

— MEL.

— CAMO.

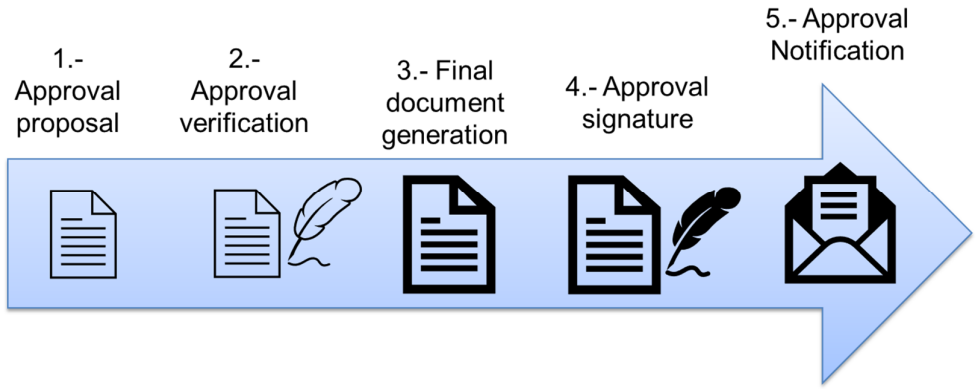
— Special approvals.

— Other relevant information.

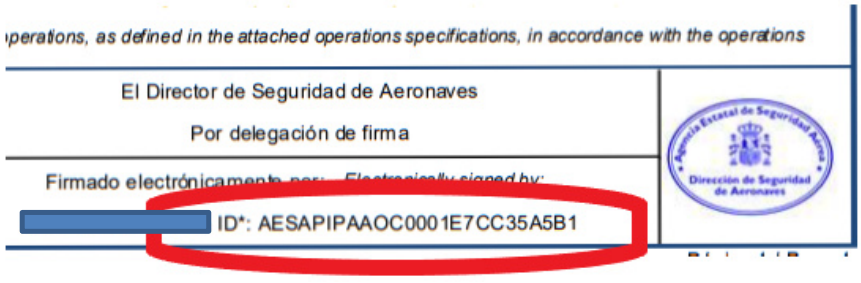
All this information is produced and integrated into the system, as appropriate, and, after undergoing all the necessary processes of inspection and validation, it allows generating the proposal for approval.

3.2 Approval life cycle

A graphic illustrating the process of issuance of an AOC approval is shown below:



The approval issued has its verification code printed in the document:



This code can be consulted in the Electronic Headquarters of AESA. Entering the code in the webpage provides access to all the information related to the document (https://sede.seguridadaerea.gob.es/CID/FrontController).