Agencia Estatal
de Seguridad Aérea

User's guide
Electronic documents in the context of Airworthiness

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA
AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PUBLIC DOCUMENT

INDEX

1. INTRODUCTION

Aeronautical regulations were born and developed in a context where documentation was exclusively paper-based. Nowadays, it is rare to find technical documents in this kind of medium. However, documents pertinent to airworthiness management, releases to service, logbooks, workcards, etc. had not transitioned yet. It is more and more evident that in this field, a new medium based in digital records is gaining ground. This transition from an analogic world to a digital one is never direct nor simple. Furthermore, in this field the responsibility implications, validity of the registers and legal guarantees of the documents must be taken especially into consideration.

Las normativas aeronáuticas nacieron y se desarrollaron en un entorno en el que la documentación tenía un soporte exclusivamente en papel. Es raro, hoy en día, encontrar documentación técnica que tenga este tipo de soporte. No obstante, la documentación relativa a la gestión de la aeronavegabilidad, puestas en servicio, logbooks, workcards, etc., aún no habían dado el salto. Cada vez parece más claro que ese entorno está dando paso a otro nuevo basado en soportes digitales. El paso de un mundo analógico a uno digital nunca es una translación directa y sencilla. Además, en este entorno se debe considerar de forma especial las implicaciones de responsabilidad, validez de registros y garantías legales de los documentos.

2. OBJECT AND SCOPE

This document is intended to establish, for those organizations related with initial and continuous airworthiness and whose responsibility as Aeronautical Authority for their supervision fall on AESA, the minimum requirements that guarantee that the applications substituting paper registers within the airworthiness field give support to the compliance of Regulation (EU) no. 748/2012 and Regulation (EU) no. 1321/2014, as well as the applicable regulations for electronic signature (Regulation (EU) no. 910/2014) and other rules or technical references that might be relevant (Royal Decree 203/2021, dated March 30, which approves the Regulation for proceeding and working by electronic means in the public sector)

Se pretende establecer, para aquellas organizaciones relacionadas con la aeronavegabilidad inicial y la aeronavegabilidad continuada cuya responsabilidad como Autoridad Aeronáutica de supervisión recaiga en AESA, los requisitos mínimos que garanticen que las aplicaciones que sustituyan a los registros en papel dentro del entorno de la aeronavegabilidad den soporte al cumplimiento del Reglamento (UE) 748/2012 y el *Reglamento (UE) Nº 1321/2014*, así como el de las normativas aplicables de firma electrónica (*Reglamento (UE) Nº 910/2014*) y a otras normativas o referencias técnicas que pudieran ser de interés (Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos).

The final purpose is to standardize its application by establishing several and minimum technical criteria that should be fulfilled, both for the documents digitally signed and for the applications bearing them, concerning safety, interoperation and legal warranties.

La finalidad es estandarizar su aplicación estableciendo una serie de criterios técnicos mínimos que deberán cumplir, tanto los documentos firmados electrónicamente, como las aplicaciones que los soporten, en cuanto a seguridad, interoperabilidad y garantías legales.

They are listed below, as example, some registers prone to be converted into digital form. Therefore, its management should be subjected to above mentioned minimum criteria.

A continuación, se listan, a modo de ejemplo, registros que son susceptibles de ser convertidos a un formato digital, y por tanto su tratamiento debería ser sometido a dichos criterios mínimos.

- Aircraft certificates of release to service (CRS, TLB)
- Authorized release certificate (EASA Form 1, EASA Form 52, EASA Form 53, Permit to fly)
- Maintenance tasks signatures (Task/Job/Work card, double inspection, supervision)
- Internal documents of the organizations (CAME, MOE, CAE, MTOE, Certification authorization, competence evaluation, NDT certificates, etc.)

- Recognition certificates as per formats EASA 148 and 149, issued by Part 147 Maintenance organizations.

- Certificados de puestas en servicio de aeronaves (CRS, TLB)
- Certificados de aptitud para el servicio (EASA Form 1, EASA Form 52, EASA Form 53 y Permiso de vuelo)
- Firma de tareas de mantenimiento (Task/Job/Work Card, doble inspección, supervisión)
- Documentación interna de las organizaciones (CAME, MOE, CAE, MTOE, Autorizaciones de certificación, Evaluación de la competencia, Certificados NDT, etc.)
- Certificados de reconocimiento según formatos EASA 148 y 149 emitidos por las organizaciones Parte 147.

This guide does not refer to the documentation issued or delegated by AESA (such as an ARC issued by an independent PRA in the SIPA deck), as its development and legal warranties are subject to the rules and regulations made by such Administration. It is neither the object of this guide the TLP operations part without maintenance tasks.

No es objeto de esta Guía, la documentación emitida o delegada por AESA (ejemplo: un ARC emitido por un PRA independiente en la plataforma SIPA), ya que su desarrollo y garantías legales están sujetas a la normativa y reglamentación desarrollada por la propia Administración. Tampoco es objeto de esta guía la parte del TLB de operaciones sin tareas de mantenimiento.

This procedure is applicable to AESA personnel from the Aircraft Safety Directorate, from the Headquarters, from the Flight Safety Offices and equally applicable to the personnel from the Instrumental Societies when performing activities commanded by AESA for specific tasks indicated in the pertinent subject.

Este procedimiento es aplicable al personal de AESA, de la Dirección de Seguridad de Aeronaves, de los Servicios Centrales, de las Oficinas de Seguridad en Vuelo e igualmente aplicable al personal de las Sociedades Instrumentales en el ejercicio de las actividades encomendadas por AESA para la realización de las tareas determinadas en el objeto.

Any suggestion for modifying this guide, or mistakes or improvements, must be communicated to the pertinent service (depending on the organization type) using the following email addresses, which will record such suggestions for their assessment when the procedure be revised again.

Cualquier sugerencia de modificación de la guía, por errores o mejoras, deberá comunicarse al Servicio correspondiente dependiendo del tipo de organización, a través de los siguientes correos electrónicos, que archivarán dichas sugerencias para ser evaluadas en la siguiente revisión del procedimiento.

- Maintenance organizations: mantenimiento.aesa@seguridadaerea.es
- Continuous Airworthiness Maintenance Organizations: camo.aesa@seguridadaerea.es
- Combined Airworthiness Organizations: cao.aesa@seguridadaerea.es
- Part 147 Training Organizations: aesa.parte147@seguridadaerea.es
- Production and Design Organizations: poa-doa.aesa@seguridadaerea.es

3. DEFINITIONS

Electronic register: a document that register data or statements and has an electronic base. **Its difference with the electronic document is that the register endures data or statements of proof nature.**

Electronic document: any information of any nature electronically based, kept in an electronic device according to a concrete form and prone for a differentiated identification and treatment.

Electronic signature: Data in an electronic form, attached or associated in a logical way to an electronic document, which identify the signatory unmistakably and ensure:

- The integrity of the document signed
- That the document signed is exactly the same as the original one, thus it has not suffered any alterations and/or manipulations
- No rejection of the document signed (the data used by the signatory to sign the document are unique and exclusive, therefore the signatory cannot state later on that the document has not been signed).

Authentication: A procedure to verify the digital identity of a person in his/her interactions in the digital field, typically by means of factors such as "something that is known" (passwords or concerted keys), "something that is hold" whether logical components (as software certificates) or physical devices (tokens), or "something existing" (biometrical elements). These factors can be used isolated or combined with each other.

Advanced electronic signature: refers to the signature based in a certificate, not identifying the type of certificate or signature used. This may be used when the equivalence to the hand signature is not necessary to be guaranteed, with all the legal and safety warranties of the signatory person. The requirements that apply to the advanced electronic signature are indicated in article 26 of *Regulation (EU) no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

Qualified electronic signature: According to *Regulation (EU) no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,* this is an advanced electronic signature created by means of a qualified creator of electronic signatures, based on a qualified certificate of electronic signature. It can only be created with qualified digital certificates issued by a Trustworthy Services Provider, duly accredited. **They have full legal force and guarantee the enforceability of a document against third parties.**

Time Mark: Assigning date (and time where appropriate) by electronic means to an electronic document.

Time stamp: Assigning **a time mark** with the intervention of a services certification provider, which ensures the accuracy and integrity of the document time mark. The time stamp might be **advanced**, if it complies with the requirements of an advanced time stamp, or **qualified,** if in addition, it uses devices and qualified services providers.

Interoperability: It refers to the ability of the different information systems, technologies and applications to communicate and data interchange, as well as the use of such information with the purpose of obtaining a bigger operational level of the system. In the airworthiness context, that easiness for information interchange must be done with three actors: airworthiness providers, airworthiness clients and airworthiness supervisory authority. An example of an acceptable standard is the *Air Transport Association (ATA) Spec 2000 Chapter 16*, which allows the data interoperability for certificates of release to service (EASA Form 1 and FAA 8130-3).

Electronic signature policy: A set of guidelines and technical rules applicable to the use of certificates and electronic signature in its scope of use.

Electronic documents management policy: Orientations or guidelines defined by an organization for the creation and management of authentic, reliable and available documents through time, according to the functions and activities inherent to them. Policy is approved at highest level within the organization, and it

assigns responsibilities concerning coordination, applicability, supervision and maintenance program management of the document through all their life.

Cascade signature (countersignature): A multiple signature in which the order of the signatories is relevant, as each signature must countersign or certify the previous one. This contrasts with the **co-signature**, in which the signatories are required with no particular order or prevalence.

Trustworthy Services Provider: Providers or Certification Services Providers are the private individuals or legal entities that issue electronic certificates or provide other different services related to the electronic signature. Certification Services Providers, both Spanish and European, can be identified following these links:

- List of Spanish providers:
  https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx

- List of European providers:
  https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

VALIDe: It is an online validation service for Spanish providers, and verification and issuance of electronic signatures. It is a reference solution to comply with the identification and authentication measures as per *Law 39/2015 Procedimiento Administrativo Común de las Administraciones Públicas (Common administrative procedure for public administration).*

The purpose of this service is allowing a user to check that the Spanish certificate used is a valid certificate which has not been revoked. It also allows to check the validity of an electronic signature made with an digital certificate issued by an avowed services provider, and proceed with signatures with digital certificates , whose pertinent private password be known.

https://valide.redsara.es/valide/ejecutarValidarFirma/ejecutar.html

Registro electrónico: Documento que registra datos o declaraciones y cuyo soporte es electrónico. **Se diferencia del documento electrónico en que soporta datos o declaraciones con naturaleza de prueba.**

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Firma electrónica: Datos en formato electrónico anejos o asociados de manera lógica con un documento electrónico que identifican al firmante de manera inequívoca y aseguran:

- la integridad del documento firmado,
- que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación,
- el no repudio del documento firmado (los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento).

Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe» (contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.

Firma electrónica avanzada: Es aquella que está basada en un certificado, sin entrar a definir qué certificado ni qué sistema de firma se usa. Puede usarse allí donde no sea necesario garantizar la equivalencia a la firma manuscrita, con todas las garantías legales y de seguridad de quien hizo la firma. Los requisitos que debe cumplir la firma avanzada están definidos en el artículo 26 del *Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE*.

Firma electrónica cualificada: Según el *Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE* es una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. Solo puede realizarse con certificados digitales cualificados emitidos por un Prestador de Servicios de Confianza debidamente acreditado. **Tiene un valor legal completo y garantiza la exigibilidad de un documento frente a terceros**.

Marca de Tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Sello de tiempo: Asignación de una **Marca de Tiempo** con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento. El sello de tiempo puede ser **avanzado**, si cumple requisitos de sello de tiempo avanzado, o **cualificado** si, además, usa dispositivos y prestadores de servicio cualificados.

Interoperabilidad: Habilidad de diferentes sistemas de información, tecnologías y aplicaciones para comunicarse e intercambiar datos, así como utilizar dicha información con el objetivo de alcanzar un mayor nivel funcional del sistema. En el entorno de la aeronavegabilidad esa facilidad de intercambio de información tiene que darse entre tres actores: proveedores de aeronavegabilidad, clientes de aeronavegabilidad y autoridad supervisora de aeronavegabilidad. Como ejemplo de un estándar aceptable está el *Air Transport Association (ATA) Spec 2000 Chapter 16*, que permite la interoperabilidad de datos para certificados de puesta en servicio (*EASA Form 1* y *FAA 8130-3*).

Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación**.**

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Firma en cascada (contrafirma): Es una firma múltiple en la que el orden en el que se firma es importante, ya que cada firma debe refrendar o certificar la firma anterior, en contraposición con la **cofirma**, en la que los firmantes se requieren sin ninguna prevalencia.

Prestador de Servicios de Confianza: Los Proveedores o Prestadores de Servicios de Certificación son las personas físicas o jurídicas que expiden certificados electrónicos o prestan otros servicios en relación con la firma electrónica. Los Proveedores de Servicios de Certificación tanto nacionales como europeos se pueden consultar a través de los siguientes enlaces:

- Listado proveedores españoles: https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx
- Listado proveedores europeos: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

VALIDe: Servicio online de validación de certificados españoles, y verificación y generación de firmas electrónicas. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en la *Ley 39/2015* de Procedimiento Administrativo Común de las Administraciones Públicas.

El objetivo de este servicio es permitir a un usuario comprobar que el certificado español utilizado es un certificado válido y que no ha sido revocado. También permite comprobar la validez de una firma electrónica realizada mediante certificado digital emitido por un prestador de servicios de certificación reconocido, y realizar firmas mediante certificado digital del que se disponga de la clave privada correspondiente.

https://valide.redsara.es/valide/ejecutarValidarFirma/ejecutar.html

4. GENERAL REQUIREMENTS FOR THE ELECTRONIC REGISTERS

The procedures to be developed by the organization for the issuance and management of their electronic registers must define the following main features:

- A system for the register support and warranties. Data safety
- Management of the electronic register within the organization, and its features
- Registers interoperability
- Electronic signature

All this is reflected in an Electronic Documents Management System, which must include an Electronic Signature Policy.

Los procedimientos que desarrollen las organizaciones para la emisión y gestión de sus registros electrónicos deberán definir los siguientes aspectos principales:

- Sistema de soporte del registro y sus garantías. Seguridad de los datos.
- Gestión del registro electrónico dentro de la organización y sus propiedades.
- Interoperabilidad de los registros.
- Firma electrónica.

Todo ello se refleja en una **Política de gestión de documentos electrónicos** que deberá incluir **una Política de firma electrónica.**

4.1 WARRANTY SYSTEMS AND VALIDITY CHECK

An electronic register system compiling airworthiness registers must consider:

- A definition of register
- The basis system to be used
- Which warranties are established for:
    - Data security (back-ups)
    - Access security
    - Access ability and its universality
- Which checking systems for validation of third parties are going to be used. It is applicable to those registers issued by an organization but destined to third parties. It must include how the register itself refers to a checking system for the validation of the electronic signature.

Un sistema de registro electrónico de registros de aeronavegabilidad deberá contemplar:

- Definición del registro.
- Sistema de soporte que usará.
- Qué garantías se establecen en cuanto a:
    - Seguridad de datos (back-ups).
    - Seguridad de acceso.
    - Facilidad de acceso y universalidad del mismo.
- Qué sistemas de comprobación de validez para terceros se van a usar. Aplicable a aquellos registros que emite la organización, pero van destinados a terceros. Debe contemplar el modo en que el propio registro remite a un sistema de comprobación de validez de la firma electrónica.

4.2 MANAGEMENT OF THE ELECTRONIC REGISTER WITHIN THE ORGANIZATION

It has to be defined the way to give electronic support to the information that the register must record. Also within that definition they must be the requirements for managing the register. It has to be included:

- How the register is originated in the organization and its systems
- How the register is completed
- Some considerations on work load, origin, assignments, destination parts and process end, which will all define the life of the register in full. Signatures in cascade.
- Some considerations on the policy of editing the registers, mandatory fields, optional fields, annexes, etc.

Deberá definirse cómo se da soporte electrónico a la información que el registro debe retener. También se incluirá en esa definición los requisitos de manejo del registro. Esto deberá incluir:

- Cómo se genera el registro en la organización y sus sistemas.
- Cómo se completa el registro.
- Consideraciones de flujo de trabajo, origen, asignaciones, destinarios y final del proceso que definan al completo la vida del registro. Firmas en cascada.
- Consideraciones en cuanto a la política de edición del registro, campos indispensables, campos opcionales, información anexa, etc.

4.3 INTEROPERABILITY OF THE REGISTERS

It must be defined how the electronic registers must be transferred between the different parts of the organization, and in case it is necessary, to third parties. This will be supported by adopting data formats which allow an adequate interoperability.

Specially, it must be considered the possibility that the registers may be used both by the organization conformity control and by the Authority.

Deberá definirse de qué modo los registros electrónicos deben ser transferidos entre las partes de la organización y, si esto fuera necesario, con respecto a terceros. Eso se soportará con la adopción de los formatos de datos que permitan una interoperabilidad adecuada.

Deberá contemplarse especialmente la posibilidad de que los registros pueden ser auditados tanto por control de conformidad de la organización como por la Autoridad.

4.4 ELECTRONIC SIGNATURE

The electronic signature is defined as the system that supports the necessity of identifying the signatory of the electronic registers (release to service signature, workcards, etc.), and/or the capacity to access to specific information (technical documentation, registers, etc.), as well as the warranty to control the access to the registers.

Within the organization, an electronic signature policy must be defined. It will design the different types of signature to be used and the way (with which systems) it will be done. The design of the electronic signature must be done taking into consideration the necessity to give legal support to the signature of the electronic registers. Such necessity will determine the security level of the signature to be used.

At any case, the following qualification must be met:

- Registers with effects to third parties and with a necessity of prevalence in time (i.e. Form 1, Release to service, DO-PO agreement, design planes, data approval statement, Technical log book)
- Registers with no effects to third parties, only valid within the organization scope (i.e. workcards signature, competence validations, internal processes, access to restricted registers, production command, design configuration, etc.)

Deberá definirse la firma electrónica como sistema que da soporte a la necesidad de identificar al firmante de registros electrónicos (firma de puestas en servicio, workcards, etc.) y/o la capacidad de acceder a determinada información (documentación técnica, registros, etc.), así como la garantía de control de acceso a los registros.

Dentro de la organización se definirá una política de firma electrónica que diseñe los diferentes tipos de firma a usar y de qué modo (con qué sistemas) se realizarán las mismas. El diseño de la firma electrónica debe realizarse atendiendo a la necesidad de soporte legal a la firma de registros electrónicos. Dicha necesidad determinará el nivel de seguridad de la firma a usar.

En cualquier caso, deberá atenderse a la siguiente calificación:

- Registros con efectos a terceros y necesidad de pervivencia en el tiempo (p.e. Form 1, Release to Service, acuerdo DO-PO, planos de diseño, declaración de aprobación de datos, Technical log book).
- Registros sin efectos a terceros, válidos solo en el entorno de la organización (p.e. firma de Workcards, validaciones de competencia, procesos internos, acceso a registros restringidos, orden de producción, configuración de diseño, etc.).

4.5 DEFINITION OF THE ELECTRONIC SIGNATURE POLICY

- Identification of the signatory and if necessary, of the organization in whose outline the signature is verified.
- Information that the signature must include, relevant data (time, date, authorization reference, etc.)
- The kind of security level will be applied to the signature
- Date interoperability standards

- Identificación del firmante y en su caso de la organización dentro de cuyo esquema se verifica la firma.
- Información que deberá incluir la firma, datos relevantes (hora, fecha, nº de autorización, etc.)
- Qué nivel de seguridad se aplicará a la firma.
- Estándar de Interoperabilidad de datos.

4.6 SYSTEM TO MANAGE THE ELECTRONIC SIGNATURE

- A safeguarding system to prevent:
  - Signed blank documents
  - That the boxes marked as mandatory remain empty
  - That, if a systems exists in the documents editing and/or in the signatures, the editing system respects such chronology and does not allow to complete or pass to another step without being complete or signed the previous one. Cascade signatures.

- Sistema de salvaguarda para evitar:
    - Firma de documentos en blanco,
    - Que las casillas que se definan como imprescindibles no queden nunca sin rellenar,
    - Que, si hay un orden implicado en la edición de documentos y/o de las firmas, el sistema de edición respete esa cronología y no permita firmar o completar un paso sin haber sido rellenado o firmado el precedente. Firmas en cascada.

4.7 LEVELS OF ELECTRONIC SIGNATURE

Following the directions of *Law 6/2020 dated 11 November* and *Regulation (EU) no. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,* three levels of applicability of the different types of electronic signature have been established, depending on the responsibility implied in the signed electronic document.

Siguiendo las directrices de la *Ley 6/2020 del 11 de noviembre* y el *Reglamento (UE) Nº 910/2014 del Parlamento Europeo y Del Consejo De 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE,* se establecen tres niveles de aplicabilidad de los tipos de firma electrónica en función de la responsabilidad exigida al documento electrónico firmado.

4.7.1 LEVEL 3: SIMPLE SIGNATURE

An electronic signature system applicable to all documents that do not have effects on third parties and be only part of internal processes within the organizations, without an associated responsibility component adhered or with a very low one.

In a **simple electronic signature** is used by signing data in electronic format which are also enclosed to other electronic data or associated with them in a logical way used by the signatory to sign.

It is advisable that a recognized standard of data interoperability be applied to these data and their signature. A typical example of this kind of signature is that with user/password mechanism.

The simple electronic signature system may be used to control the access and authentication, which might be also achieved by systems without electronic signature (user and password). This level of security must be listed within the management policy of the electronic documentation in the organization.

Non-exhaustive examples:

- Access to systems based in certificates
- Systems to control the presence
- System to coordinate shifts, communications between the workers
- Access to application systems for tools/materials/information.

Se trata de un sistema firma electrónica que se aplicará a aquellos documentos que no tengan efectos a terceros y que constituyan solo partes de procesos internos de las organizaciones sin un componente de responsabilidad asociado o un componente de responsabilidad muy bajo.

Una firma electrónica simple es aquella en la que se firma usando datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

Es recomendable que se aplique a estos datos y su firma un estándar reconocido de interoperabilidad de datos. El ejemplo típico de este tipo de firma es el de mecanismos de usuario/contraseña.

El sistema de firma electrónica simple puede ser usado para control de acceso y autenticación, que también puede realizarse por sistemas sin firma electrónica (usuario y contraseña). Este nivel de seguridad deberá estar contemplado en la política de gestión de documentación electrónica dentro de la organización.

Ejemplos no exhaustivos:

- *Acceso a sistemas basados en certificados*
- *Sistemas de control de presencia.*
- *Sistemas de coordinación de turnos, comunicaciones entre trabajadores.*
- *Accesos a sistemas de solicitud de herramientas/materiales/información.*

4.7.2 LEVEL 2: ADVANCED ELECTRONIC SIGNATURE

It is an electronic signature with medium responsibility. It will be applied to those documents showing the willingness and responsibility of the signatory in the tasks execution, acknowledgment receipts or validation issues, thus registers associated to the responsibility within an organization but without impact on third parties.

The advanced electronic signature must guarantee (as defined in eIDAS):

a) A unique bound to the signatory

b) The identification of the signatory

c) That it has been created using developed data of the electronic signature that the signatory may use, with a high level of confidence, with his exclusive control, and

d) Be bounded to the data signed therein, so any ulterior modification to the data be easily noticeable.

It is recommended that:

- A recognized standard of data interoperability be applied to the signed registers
- The warranties be assured by using signature certificates. This make easier to show the compliance with the requirements.

Non-exhaustive examples:

- Signatures for internal processes
- Oversight of internal tasks
- Critical tasks sign off
- Assessment of the competence
- Signature for training courses certificates
- Signatures for transfers in workcards for shift changing
- Signatures of quality meeting/management sytem Acts where the Responsible Manager/General Manager has intervened.
- Certification authorizations.
- Check or green light of a production command
- Supplementary procedures to the manual

Es una firma electrónica de responsabilidad media. Se aplicará a aquellos documentos que demuestran la voluntad y la responsabilidad del firmante en la ejecución de tareas, acuses de recibo o emisión de

validaciones, serían registros que se asocian a responsabilidad dentro de la organización sin impacto en terceros.

La firma electrónica avanzada tendrá que garantizar (tal como define eIDAS):

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma, de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Es recomendable que:

- se aplique a los registros firmados un estándar reconocido de interoperabilidad de datos.
- que las garantías se aseguren con el uso de certificados de firma, ya que hacen más sencilla la demostración de cumplimiento con los requisitos.

Ejemplos no exhaustivos:

- *Firmas de procesos internos.*
- *Supervisión de tareas internas.*
- *Sign off tareas críticas.*
- *Evaluación de la Competencia.*
- *Firma de Certificados de cursos de formación.*
- *Firma de traspasos en tarjetas de trabajo por cambios de turnos.*
- *Firmas de actas de reuniones de calidad/sistema de gestión donde intervenga el Gerente Responsable/Director Responsable.*
- *Autorizaciones de Certificación.*
- *Chequeo/Visto Bueno de una orden de producción.*
- *Procedimientos complementarios al manual.*

4.7.3 LEVEL 1: QUALIFIED ELECTRONIC SIGNATURE

It is the highest security level. It will be applied to those documents with responsibility effects on third parties, i.e., outside the organization issuing the document. A standard will be applied to this level of signature, allowing data interoperability; in the other levels this action is only advisable.

The qualified electronic signature is an advanced one requested to the certification services providers qualified as per eiDAS requirements.

Additionally, it is recommended to add to the qualified signature a time stamp that guarantees the signature date by using the systems provided in the eiDAS regulation, so the validity of the signed document and its date will last further than the validity of the used certificates.

In any case, the pertinent mechanisms will be established to guarantee that the time validity safeguards set in the rule be met.

Non-exhaustive examples:

- Release to service certificates (CRS, EASA Form 1, TLB comprising aircraft CRS)
- Recognition formats as per EASA formats 148 and 149, issued by Part 147 organizations.

- Organizations manuals

Es el nivel de seguridad más alto. Se aplicará a aquellos documentos que tengan efectos de responsabilidad frente a terceros, es decir, fuera de la organización que emite el documento. A este nivel de firma se le aplicará un estándar que permita una interoperabilidad de datos, mientras que en los otros niveles esto es solo recomendable.

Es una firma electrónica avanzada a la que se le exige que los prestadores de servicios de certificación estén cualificados según requisitos de eIDAS.

Adicionalmente se recomienda añadir a la firma cualificada el uso de un sello de tiempo que garantice la fecha de firma usando los sistemas previstos en el reglamento eIDAS, de modo que la validez del documento firmado y su datación se extienda en el tiempo más allá de la caducidad de los certificados usados.

En todo caso, se establecerán los mecanismos pertinentes para garantizar que las salvaguardas de validez temporal establecidas en la norma se vean atendidas.

Ejemplos no exhaustivos:

- *Certificados de puesta en servicio (CRS, EASA Form 1 y TLB que soporte CRS de aeronave).*
- *Certificados de reconocimiento según formatos EASA 148 y 149 emitidos por las organizaciones Parte 147.*
- *Manuales de las organizaciones.*

5. ANNEX I: TRANSITION PLANNING IN A MAINTENANCE ORGANIZATION

Here down, a transition proposal is provided to implement the electronic signature system in a maintenance organization from a traditional (handwritten and stamps) signature system.

This proposal must be adapted to each organization, depending on the extent of the proposed electronic signature system and the size of the organization itself. At the same time, it must be agreed with the AESA Head Maintenance Manager.

The transition planning may be developed in the manual itself or as a separate manual, as long as it is agreed with the AESA oversight responsible and duly associated to the pertinent manual (MOP, MOE, CAE, CAME, MTOE, POE, DOH).

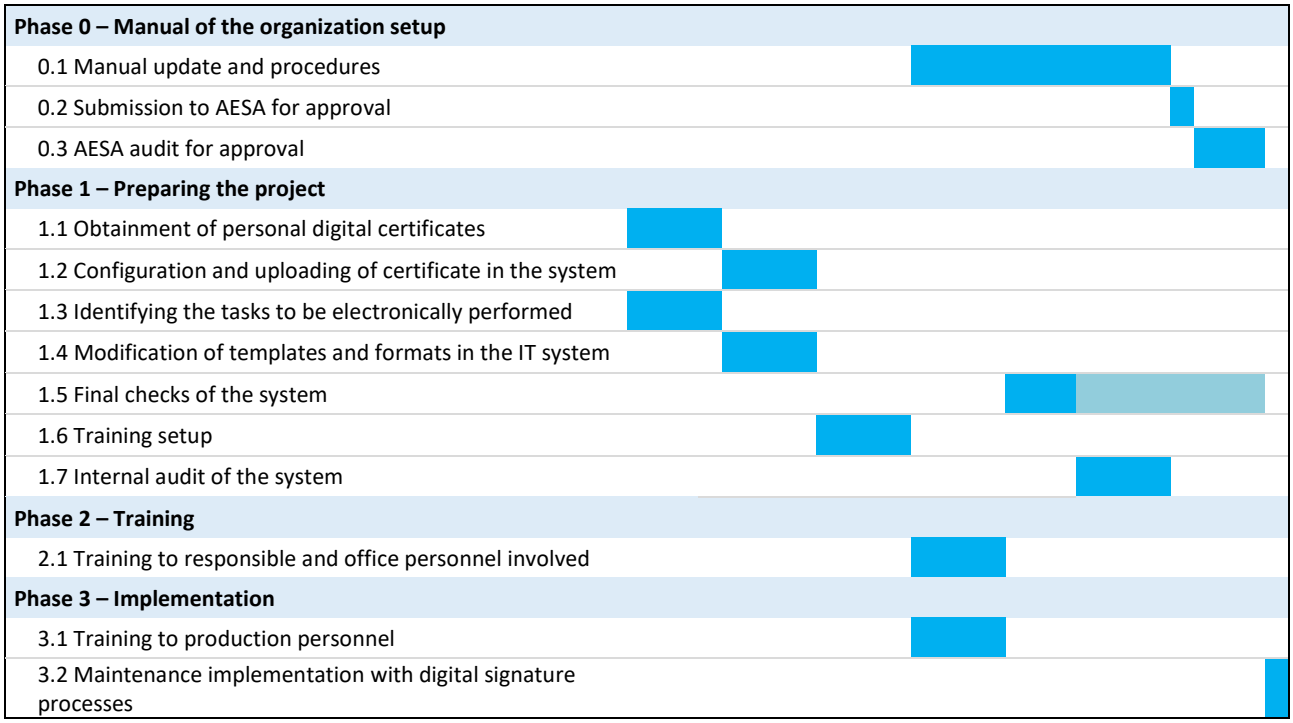
The proposal establishes different phases that may be carried out simultaneously. The following Gantt diagram details the proposal:

A continuación, se traslada una propuesta de transición para la implementación del sistema de firma electrónica en una organización de mantenimiento desde un sistema de firma tradicional manuscrita con sellos.

Esta propuesta deberá ser adaptada por cada organización, en función del alcance del sistema de firma electrónica propuesto y del tamaño de la propia organización, y a su vez, acordada con el Principal de Mantenimiento de AESA.

El plan de transición se podrá desarrollar en el propio manual o como un manual aparte siempre que esté acordado con el Principal a cargo de la supervisión de AESA y debidamente asociado al manual correspondiente (MOP, MOE, CAE, CAME, MTOE, POE, DOH).

La propuesta establece varias fases que pueden realizarse de manera simultánea. El siguiente diagrama de Gantt expresa la propuesta:



Point **"1.5 Final checks of the system"** is divided in two:

a) First block : should imply realistic maintenance, certified in a traditional way, performed simultaneously with the electronic signature system.

b) The second block : depending on the complexity of the electronic signature system implemented, it indicates that, once the final checks of the system have been passed, the production and office personnel continue to use the electronic signature system parallel to the traditional and handwritten signature, in order not to lose skills in the use of the electronic signature system until its final launch.

El punto **"1.5 Pruebas finales del sistema"** se ha dividido en dos bloques:

a) El primer bloque : debería consistir en trabajo de mantenimiento real, certificado de manera tradicional, realizado simultáneamente en el sistema de firma electrónica.

b) El segundo bloque : en función de la complejidad del sistema de firma electrónica implantado, representa que una vez superadas las pruebas finales del sistema, el personal de producción y de oficina continúe usando el sistema de firma electrónica paralelamente al método tradicional de firma manuscrita para no perder pericia en el uso del sistema de firma electrónica hasta su puesta en servicio definitiva.

Point **"0.3 AESA audit"** will assess the manual of the organization and the correct implementation of the transition plan, and may supervise with further details any phase (for example, in-situ evaluation of sub phase **"1.5 Final checks of the system"**).

El punto **"0.3 Auditoría de AESA"** evaluará el manual de la organización y la correcta implantación del plan de transición, y podrá entrar a supervisar en mayor detalle cualquier fase (ejemplo: evaluación in-situ de la subfase **"1.5 Pruebas finales del sistema"**).

6. REFERENCED DOCUMENTS

GENERAL REFERENCES			
CODE	**TYPE OF DOCUMENT**	**TITLE**	**ISSUANCE**
LAW 6/2020	LAW	LEY 6/2020, DE 11 DE NOVIEMBRE, REGULADORA DE DETERMINADOS ASPECTOS DE LOS SERVICIOS ELECTRÓNICOS DE CONFIANZA.	N/A
RD 203/2021	ROYAL DECREE	REAL DECRETO 203/2021, DE 30 DE MARZO, POR EL QUE SE APRUEBA EL REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS.	N/A

* Last issuance in force is applied.

SPECIFIC REFERENCES			
CODE	**TYPE OF DOCUMENT**	**TITLE**	**ISSUANCE**
BR	REGULATION (EU)	REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 4 JULY 2018 ON COMMON RULES IN THE FIELD OF CIVIL AVIATION AND ESTABLISHING A EUROPEAN UNION AVIATION SAFETY AGENCY, AND AMENDING REGULATIONS (EC) NO 2111/2005, (EC) NO 1008/2008, (EU) NO 996/2010, (EU) NO 376/2014 AND DIRECTIVES 2014/30/EU AND 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, AND REPEALING REGULATIONS (EC) NO 552/2004 AND (EC) NO 216/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL AND COUNCIL REGULATION (EEC) NO 3922/91	N/A
REG. 1321/2014 (IR)	REGULATION (EU)	COMMISSION REGULATION (EU) NO 1321/2014 OF 26 NOVEMBER 2014 ON THE CONTINUING AIRWORTHINESS OF AIRCRAFT AND AERONAUTICAL PRODUCTS, PARTS AND APPLIANCES, AND ON THE APPROVAL OF ORGANISATIONS AND PERSONNEL INVOLVED IN THESE TASKS. (REWRITING REGULATION (CE NO 2042/2003).	N/A
REG. 910/2014	REGULATION (EU)	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.	N/A

* Last issuance in force is applied.

7. ACRONYMS

ACRONYM	DESCRIPTION
AESA	AGENCIA ESTATAL DE SEGURIDAD AÉREA *(SPANISH STATE AVIATION SAFETY AGENCY)*
ATA	AIR TRANSPORT ASSOCIATION
CA	COORDINACIÓN DE AERONAVEGABILIDAD *(AIRWORTHINESS COORDINATION)*
CAE	CONTINUOUS AIRWORTHINESS EXPOSITION
CAME	CONTINUING AIRWORTHINESS MANAGEMENT EXPOSITION
CRS	CERTIFICATE OF REALEASE OF SERVICE
DAEA	DIVISIÓN DE APROBACIONES Y ESTANDARIZACIÓN DE AERONAVEGABILIDAD *(APPROVAL AND AIRWORTHINESS STANDARDIZATION DIVISION)*
DAI	DIVISIÓN DE AERONAVEGABILIDAD INICIAL *(INITIAL AIRWORTHINESS DIVISION)*
DSA	DIRECCIÓN DE SEGURIDAD DE AERONAVES *(AIRCRAFT SAFETY DIRECTORATE)*
EASA	EUROPEAN AVIATION SAFETY AGENCY
eIDAS	ELECTRONIC IDENTIFICATION, AUTHENTICATION AND TRUST SERVICES
MOE	PART 145 MAINTENANCE ORGANIZATION EXPOSITION
MTOE	MAINTENANCE TRAINING ORGANIZATION EXPOSITION
NDT	NON-DESTRUCTIVE TESTS
OSV	OFICINA DE SEGURIDAD EN VUELO *(REGIONAL OFFICE)*
TLB	TECHNICAL LOG BOOK