BDLI
Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e.V.

White Paper
Digital Approval Processes

Digitally signed documents in paperless approval processes in Aerospace Industry

BDLI AG Digitale Zulassungsprozesse

BDLI WG Digital Approval Processes

Version 3 – 15.01.2022

Content

This White Paper is the result of a number of meetings of the BDLI WG Digital Approval Processes.

1. BDLI WORKING GROUP

The BDLI Working Group 'Digitale Zulassungsprozesse' was founded in 2018 with the aim of developing recommendations and best practices on how to implement and use the electronic signature in paperless approval processes in the aerospace industry.

The electronic signature was identified as a key enabler for fully digitized (end2end), automated, secure processes in all 4 major domains of the product lifecycle in aerospace: development, production, maintenance and continuing airworthiness.

From the start, it was the intention of the BDLI Working Group to ensure, that their results and recommendations fully meet the acceptance of the relevant aerospace authorities – e.g. EASA, LBA, LufABw, other European Aerospace Safety Agencies (civil/military).

It is envisaged that the content of this White Paper will be implemented – all or in part – in the EASA rules and regulations as AMC – Acceptable Means of Compliance or as GM – Guidance Material.

The following companies contributed to the work of the BDLI WG Digital Approval Processes:

Airbus Defence & Space GmbH
Airbus Deutschland GmbH
Airbus Helicopters Deutschland GmbH
BDLI e.V.
Deutsche Aircraft GmbH (328 SSG GmbH)
Diehl Aviation Laupheim GmbH
Elbe Flugzeugwerke GmbH
ESG - Elektroniksystem-und Logistik-GmbH
Hensoldt Sensors GmbH
Liebherr Aerospace Lindenberg
Lufthansa Technik AG
MT Aerospace AG
MTU Aero Engines AG
Northrop Grumman LITEF GmbH
Premium AEROTEC GmbH
Rolls-Royce Deutschland Ltd & Co KG
VINCORION - Jenoptik AG

Working Group coordination

Dr. Wirtz, Jörg; Airbus Defence & Space GmbH
Zwiener, Axel; BDLI e.V.

Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e.V.
Friedrichstrasse 60
10117 Berlin
E-Mail: zwiener@bdli.de

2. MOTIVATION

The current requirements and regulations regarding signatures on certification / certification-related documents in both, civil and military aviation, largely originate from a time when a ‘wet signature’ was the only means to document defined process steps/activities (e.g. start, completion, review, release, approval, etc.).

Meanwhile digitization in industry has come to a stage, where almost all data/documents are created electronically in a company IT-system. However, without a fully implemented electronic signature process, documents will still have to be printed out – for example for an approval run and then be passed around for a ‘wet signature’, often across locations, company sites and even across national borders. In addition, the original document must then be archived physically at the end for proof and review.

It should also be mentioned, that due to the constantly growing integration of digitization (e.g. IoT) and of digital toolsets (e.g. CAD, CAM, etc.), a large amount of data cannot be printed and subsequently not be signed anymore in the conventional, non-electronic way.

It is therefore of the utmost importance to the industry to push end2end digitization processes in order to be faster, more efficient – and to be competitive.

The European legislators have created a regulation (eIDAS) for electronic identification and trust services. In the regulation, it is stated, that ‘wet signatures’ can only be replaced by a ‘qualified electronic signature’ in a legally binding setup – on the grounds, that the ‘qualified electronic signature’ represents the maximum level of trust regarding the identity of the signatory.

With this White Paper it is intended 1. to identify those scenarios, where a ‘wet signature’ is required by law and 2. in all other scenarios, to challenge the specific requirement, that the ‘qualified digital signature’ is the only digital equivalent to a ‘wet signature’.

On the assumption that there is a significant difference if the signatory is a ‘common person’ – in general, an individual, not widely known – or an employee in industry – in general, a company representative, evaluated, approved, authorized by the company – the BDLI Working Group has compared the different types of electronic signatures – including a company specific IT-based workflow validation – with regard to the required level of trust in specific situations/stages in industry (approval/certification) processes.

In this White Paper, the BDLI Working Group will deliver proof, that, if applied in an industry/company controlled environment, almost any form of electronic signature or IT-based workflow validation has a higher level of trust and is more secure than a non-validated ‘wet signature’ due to rigorous archiving requirements in combination with automatic time stamping of electronic activities within a company-IT-system.

3. LEGAL/REGULATORY FRAMEWORK:

3.1. EIDAS

eIDAS (electronic IDentification, Authentication and trust Services regulation) is a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

The eIDAS regulation defines in Art. 3 No. 10–12 the following types of electronic signatures:

- **(Simple) Electronic Signature:** Any electronic declaration of intent (e.g. signature under an email, scan of wet signature copied into electronic documents)

- **Advanced electronic signature** (digital signature): An electronic signature that uses an encrypted digital certificate linking the signature to the signatory by providing unique identifying information. The signatory has sole control of the data used to create the electronic signature. If the signed data has changed after signature, the content is marked invalid.

- **Qualified electronic signature**: Same as advanced electronic signature, but certificates have to be provided by qualified trust centers and signatures have to be performed by using qualified devices.

The law holds that an electronic signature shall not be denied legal effect just based on the cause that it is electronic. On the other hand, it also states that only the ‘qualified electronic signature’ is the fully legally binding replacement of a ‘wet signature’.

It is undisputed, that the qualified electronic signature represents the highest level of trust.

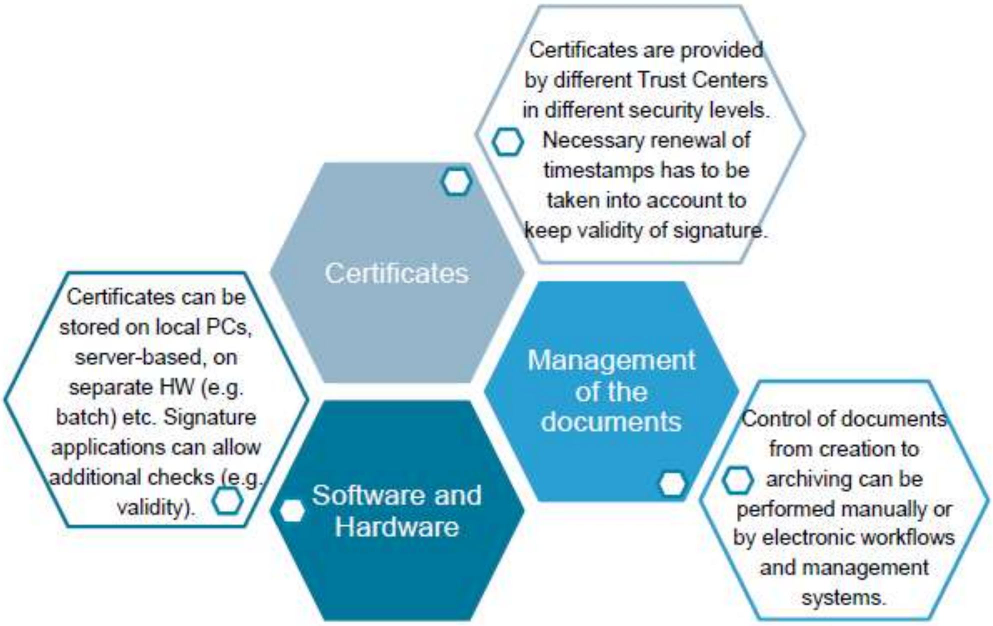
If a document is signed with a qualified electronic signature, the signatory can instantly be identified via publicly accessible qualified/accredited trust centers and the status of the content of the document (forged/changed/tampered with or original) can also instantly be verified.

Two additional basic assumptions underlying the thoughts in this White Paper are:
- The type of signature to be used depends on the level of trust required – either by law or on the basis of a mutual agreement between parties.
- The higher the level of trust, the higher the associated effort and costs.

Therefore, it is the following question the BDLI Working Group is trying to answer with this White Paper:

If the qualified electronic signature represents a level of trust of 100%, are there scenarios in which the parties involved can agree on a lower or somewhat lower level of trust and still be sure that all contractually defined rights or obligations are observed and are legally enforceable in the event of a challenge?

The overall level of trust is the result of the combination of three perimeter, that can be independently managed – Certificates, Management of the documents and Software/ Hardware.


Certificates are provided by different Trust Centers in different security levels. Necessary renewal of timestamps has to be taken into account to keep validity of signature.
Certificates
Certificates can be stored on local PCs, server-based, on separate HW (e.g. batch) etc. Signature applications can allow additional checks (e.g. validity).
Management of the documents
Software and Hardware
Control of documents from creation to archiving can be performed manually or by electronic workflows and management systems.

Combining different levels of security inside each of these perimeters defines the resulting level of trust.

3.2. VERTRAUENSDIENSTEGESETZ

When eIDAS came into force it was automatically adopted by all members of the European Union and thus, for example replaced the German “Signaturgesetz” (SigG) and the related “Signaturverordnung” (SigV). Through this approach laws on the use of electronic signatures are widely harmonized and mutual recognition of electronically signed documents is ensured within the European Union.

Additionally and complimentary to eIDAS, the German legislator created the “Vertrauensdienstegesetz” (VDG), which is dealing with the requirements for trust services in Germany and is establishing the “Bundesnetzagentur” as notified agency for accreditation and oversight of relevant trust service organizations. The VDG was put into force on 29th July 2017.

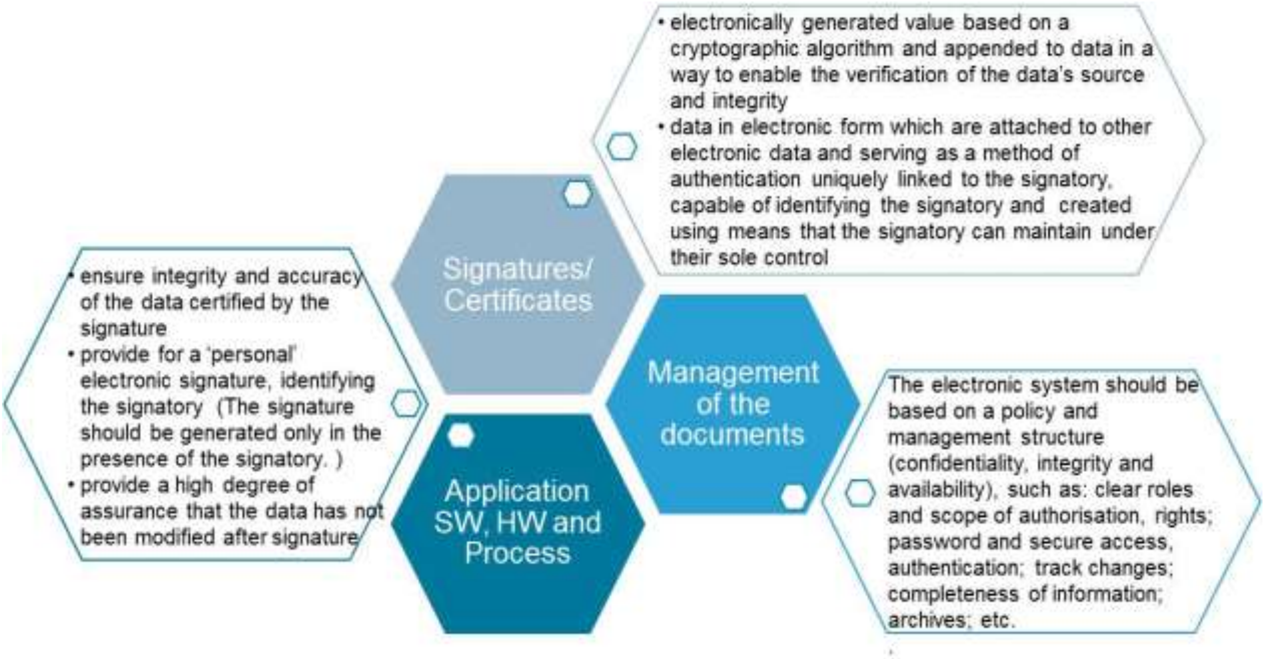
3.3. EASA AMC NO.1 TO 21.A.163(C)

AMC No.1 to 21.A.163(c) “Computer generated signature and electronic exchange of the EASA Form 1” is describing the requirements the EASA sets forth with regard to the use of electronic signatures on the Airworthiness Release Certificate EASA Form 1.

The following non-exhaustive overview gives an insight on how these requirements can be allocated to the set of implementation perimeters mentioned above (see Chapter 3.1).

The complete mapping of the BDLI WG’s recommendations on EASA AMC No.1 to 21.A.163(c) is described in the annex (see Chapter 8b).

It should be noted, that similar AMCs are already released for other EASA Regulations/Parts.



Signatures/ Certificates

- electronically generated value based on a cryptographic algorithm and appended to data in a way to enable the verification of the data's source and integrity
- data in electronic form which are attached to other electronic data and serving as a method of authentication uniquely linked to the signatory, capable of identifying the signatory and created using means that the signatory can maintain under their sole control

Application SW, HW and Process

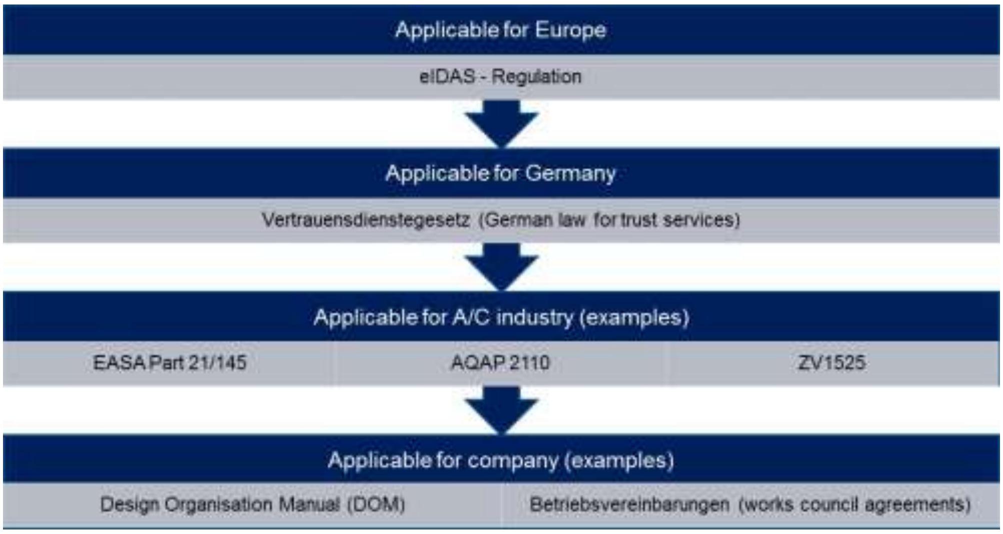
- ensure integrity and accuracy of the data certified by the signature
- provide for a 'personal' electronic signature, identifying the signatory (The signature should be generated only in the presence of the signatory.)
- provide a high degree of assurance that the data has not been modified after signature

Management of the documents

The electronic system should be based on a policy and management structure (confidentiality, integrity and availability), such as: clear roles and scope of authorisation, rights; password and secure access, authentication; track changes; completeness of information; archives; etc.

3.4. COMPANY REGULATIONS

The introduction and application of a framework for the use of electronic signatures within an industry/company environment is not only dependent on eIDAS. The following picture gives an overview of additional legal or contractual requirements an aerospace company may be facing.



Applicable for Europe

eIDAS - Regulation

Applicable for Germany

Vertrauensdienstegesetz (German law for trust services)

Applicable for A/C industry (examples)

EASA Part 21/145 | AQAP 2110 | ZV1525

Applicable for company (examples)

Design Organisation Manual (DOM) | Betriebsvereinbarungen (works council agreements)

And last, but definitely not least, economic, social and environmental aspects are also part of the overall equation – efficiency, return on investment, digitization, decentralization of work, mobile office, reduction of carbon footprint, etc.

3.5. INTERNATIONAL OVERVIEW

When using electronic signature outside the borders of the EU, the variety of international laws and regulations has to be taken into account.

The following link(s) may serve as a good reference:

Global Guide to eSignature Law: Country by country summaries of esignature law and enforceability (adobe.com)

E-signatures, digital signatures compliance, international laws | Adobe Trust Center

4. TECHNICAL BACKGROUND OF ELECTRONIC SIGNATURES

4.1. NON-CERTIFICATE BASED ELECTRONIC SIGNATURES

Basically all expression of will in a digital format like ASCII or bitmap/jpg, etc. are regarded a non-certificate based electronic signature. However this document will focus in later chapters on electronic signatures implemented in workflows and backend systems with strong administrative control on user identification and user access rights.

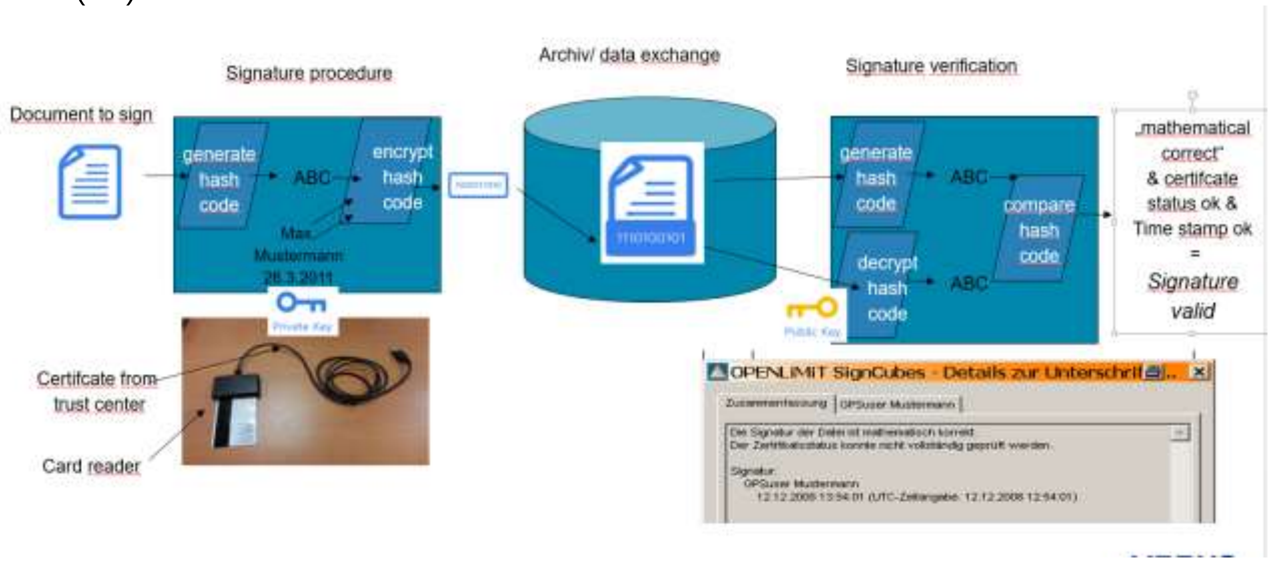
4.2. CERTIFICATE BASED (PKI - PUBLIC KEY INFRASTRUCTURE) SIGNATURES

When a signatory electronically signs a document in a public key infrastructure, the signature is created using the signatory's private key (= certificate), which is required to always be securely kept by the signatory. The mathematical algorithm acts as a cipher, creating data matching the signed document, called a hash, and encrypting that data. The resulting encrypted data is the digital signature. The signature is also marked with a timestamp, at the time the document is signed.

If the document is intendently or unintendently changed after signing, the digital signature becomes invalid.

For example, Jane D. signs an agreement to sell a timeshare flat using her private key. The buyer 1. receives the document and 2. also receives a copy of Jane D.'s public key. If the public key cannot decrypt the signature (via the cipher from which the keys were created), it means the signature is not Jane D.'s, or the document has been changed after it was signed. The signature is then considered invalid and cannot be trusted.

To protect the integrity of the signature, PKI requires that the keys are created, applied, and saved in a secure manner – this may require the services of a reliable Certificate Authority (CA).



Die Signatur der Datei ist mathematisch korrekt.
Der Zertifikatsstatus konnte nicht vollständig geprüft werden.

Signatur:
OPSuser Mustermann
12.12.2008 13:54:01 (UTC-Zeitangabe: 12.12.2008 12:54:01)

5. APPYLING ELECTRONIC SIGNATURES ON AEROSPACE CERTIFICATION DOCUMENTATION

This chapter explains the different types of signatures and the recommendations of the Working Group which type of signature to be applied on which type of document.

The Working Group executed the following steps to establish their recommendations:

a) Identification of documents in the context of aerospace certification processes
b) Identification of electronic signature types and classification according to eIDAS legal framework (see chapter 3)
c) Assessment of these signature types with regard to required effort and resulting trust/legal evidence level and selection of signatures types for 1. medium trust/evidence level and for 2. high trust/evidence level
d) Recommendation to apply selected signature types on certification documents as identified in chapter 4

The Working Group analyzed a large number of documents/types with regard to signatory requirements (see annex B).

The following electronic signature types were identified in Working Group discussions as established practice in industry:

a) **Type 1a Self-Created electronic signature certificate (e.g. with Adobe PRO)**
This electronic signature type describes uncontrolled creation of a signature certificate by an end-user within a standard office tool capability. No relevant level of trust exists, as no identity control/check is applied. This signature has approximately the same low trustlevel as a scanned, cut & paste signature. The local CPU timestamp that is created is also not fully trustworthy.

This type of electronic signature can be classified as a (simple) electronic signature according to eIDAS

b) **Type 1b Personal note - scan and copy of a handwritten signature**
A re-production of a handwritten signature (scanned), copied under a document, provides a personal note to a document’s content. This type of signature is not covered by any regulation and cannot be associated with a relevant level of trust.

With regard to eIDAS, this type of electronic signature can also be classified as a (simple) electronic signature.

c) **Type 1c Electronic Validation (e.g. PDM or ERP release workflow)**
An approval of a document or set of data (e.g. in a tool workflow), which can be clearly traced back to an individual person with a specific role & responsibility assigned by the company. The level of trust associated with this type of signature results from the unique combination of user sign-in and password/PIN.

Nevertheless, with regard to eIDAS, this type of electronic signature is also to be classified as a (simple) electronic signature.

d) **Type 2a Basic (advanced) Digital Signature**
The *Basic (advanced) Digital Signature* (in accordance §3 XI + §26, eIDAS) is based on digital trust center certificates. Identity control is ensured by company Human Resources processes (Identification, Evaluation, Approval, and Authorization by the company). The

certificate for the creation of electronic signatures are provided by company-specific trust centers, which as such do not require a specific accreditation of the infrastructure.

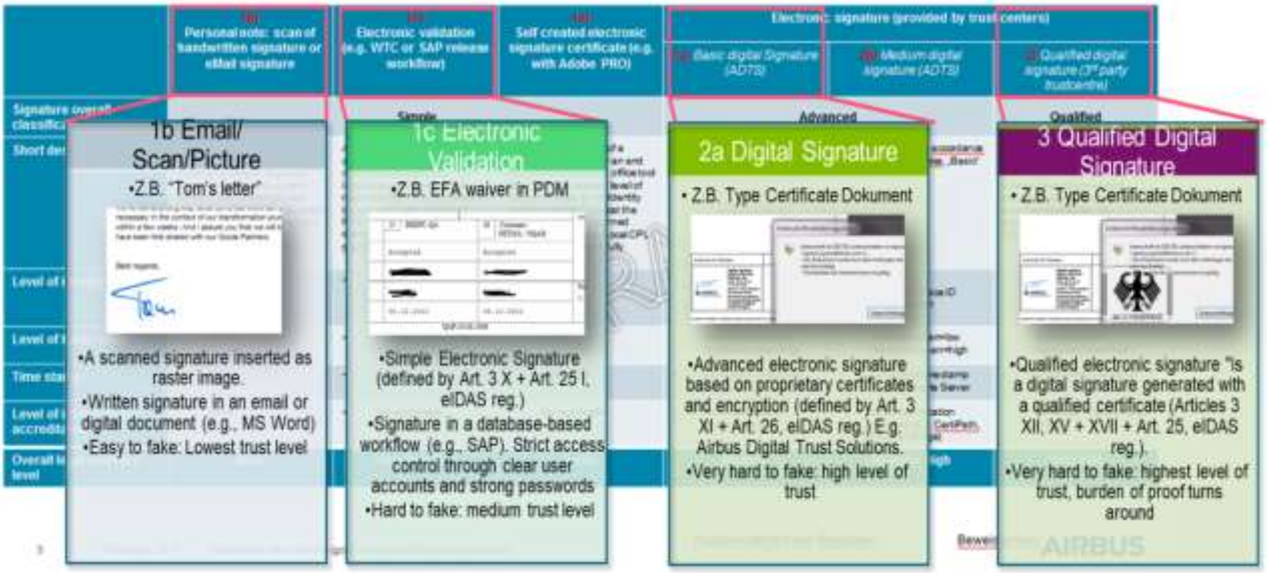
This type of electronic signature can be classified according to eIDAS as an advanced electronic signature.

e) **Type 2b Medium (advanced) digital signature**
The *Advanced Digital Signature* (in accordance §3 XI + §26, eIDAS) is based on digital trust center certificates. Identity control is ensured by company Human Resources processes (Identification, Evaluation, Approval, and Authorization by the company) and a face2face ID-verification performed by trusted agents before the certificate for the creation of electronic signatures are provided by company-specific trust centers, which as such do not require a specific accreditation of the infrastructure.

This type of electronic signature can be classified according to eIDAS as an advanced electronic signature.

f) **Type 3 Qualified digital signature**
The Qualified digital signature provides the highest level of trust on the grounds of rigorous and independent ID-validation of the individual person and the provision of the certificate for the creation of electronic signatures by independent, accredited and authorized trust centers (in accordance with §3 XII, XV + XVII +§ 25, eIDAS Reg.).

This type of electronic signature can be classified according to eIDAS as a qualified electronic signature.


Personal note: scan of handwritten signature or eMail signature
Electronic validation (e.g. WTC or SAP release workflow)
Self created electronic signature certificate (e.g. with Adobe PRO)
Electronic signature (provided by trust centers)
Basic digital Signature (ADTS)
Medium digital signature (ADTS)
Qualified digital signature (3rd party trustcentre)
Signature overall classifica
Short de
Level of
Level of
Time sta
Level of accredit
Overall le level
Simple
Advanced
Qualified
Bewe
AIRBUS

1b Email/ Scan/Picture
- Z.B. "Tom's letter"
- A scanned signature inserted as raster image.
- Written signature in an email or digital document (e.g., MS Word)
- Easy to fake: Lowest trust level

1c Electronic Validation
- Z.B. EFA waiver in PDM
- Simple Electronic Signature (defined by Art. 3 X + Art. 25 I, eIDAS reg.)
- Signature in a database-based workflow (e.g., SAP). Strict access control through clear user accounts and strong passwords
- Hard to fake: medium trust level

2a Digital Signature
- Z.B. Type Certificate Dokument
- Advanced electronic signature based on proprietary certificates and encryption (defined by Art. 3 XI + Art. 26, eIDAS reg.) E.g. Airbus Digital Trust Solutions.
- Very hard to fake: high level of trust

3 Qualified Digital Signature
- Z.B. Type Certificate Dokument
- Qualified electronic signature "is a digital signature generated with a qualified certificate (Articles 3 XII, XV + XVII + Art. 25, eIDAS reg.).
- Very hard to fake: highest level of trust, burden of proof turns around

After a first screening of the different electronic signatures established in industry, the Working Group decided to limit the next steps of the analysis to the following types of electronic signature:

1. Type 1c : Electronic Validation
2. Type 2a : Basic (advanced) Digital Signature
3. Type 3 : Qualified Digital Signature

Reasons for excluding the following electronic signatures:

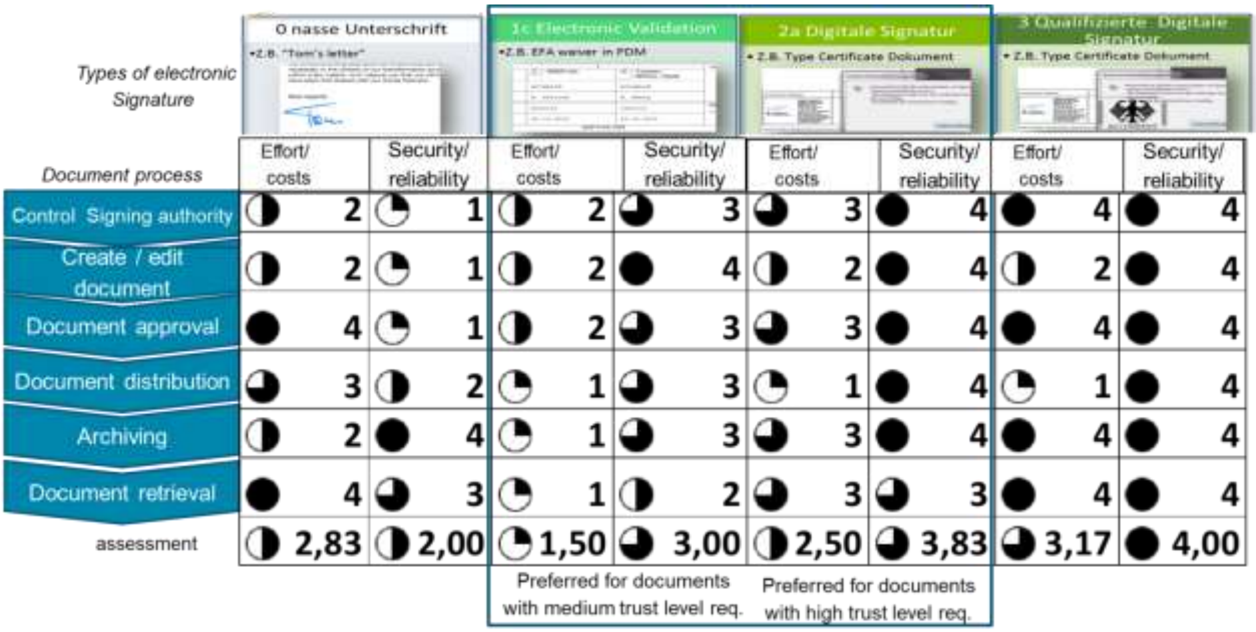
Type of Electronic Signature	Reason
Self-created signature certificate 1a	No root certificate can be exchanged between users, therefore no level of trust can be guaranteed. Additionally documents with other valid certificates on a document can become invalid.
Scanned Image 1b	No level of trust submitted, everybody is able to re-use a scanned image of signature of another person
Medium Digital Signature 2b	This signature type is considered as a small evolution of 2a, which adds small trust level benefits but significant workload in a company. Therefore it was assessed only as an alternative for companies to 2a.

5.1. ASSESSMENT OF SIGNATURES WITH REGARDS TO PROCESS EFFORT AND TRUST/LEGAL EVIDENCE LEVEL RESULTING IN THE PROCESS

In this step of the analysis the Working Group did asses the selected electronic signature types 1. with regard to process effort and costs and 2. with regard to trust/legal evidence level. The results were then be compared to results regarding an assessment of process effort/trust level of existing non-digital signature ('wet signature').

The process used as a reference was the typical lifecycle of a document (create/edit, approve, distribute, archive and retrieve) plus the process step of management/control of the signing authority.

The results of this discussion/assessment are depicted in the table below - with regard to effort/costs and security/reliability.



Types of electronic Signature	0 nasse Unterschrift •Z.B. "Tom's letter"		1c Electronic Validation •Z.B. EFA waiver in PDM		2a Digitale Signatur • Z.B. Type Certificate Dokument		3 Qualifizierte Digitale Signatur • Z.B. Type Certificate Dokument	
Document process	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability
Control Signing authority	◑ 2	◔ 1	◑ 2	◕ 3	◕ 3	● 4	● 4	● 4
Create / edit document	◑ 2	◔ 1	◑ 2	● 4	◑ 2	● 4	◑ 2	● 4
Document approval	● 4	◔ 1	◑ 2	◕ 3	◕ 3	● 4	● 4	● 4
Document distribution	◕ 3	◑ 2	◔ 1	◕ 3	◔ 1	● 4	◔ 1	● 4
Archiving	◑ 2	● 4	◔ 1	◕ 3	◕ 3	● 4	● 4	● 4
Document retrieval	● 4	◕ 3	◔ 1	◑ 2	◕ 3	◕ 3	● 4	● 4
assessment	◑ 2,83	◑ 2,00	◔ 1,50	◕ 3,00	◑ 2,50	◕ 3,83	◕ 3,17	● 4,00
			Preferred for documents with medium trust level req.		Preferred for documents with high trust level req.			

The Working Group concluded from the analysis, that **all electronic signature types provide a higher trust level compared to the existing wet/non-digital signature!**

The results further show, that the electronic signature types 1c and also 2a are associated with significantly lower process effort and cost, compared to the existing wet/non-digital signature.

Another reason to prefer the digital signature over the classic 'wet signature'.

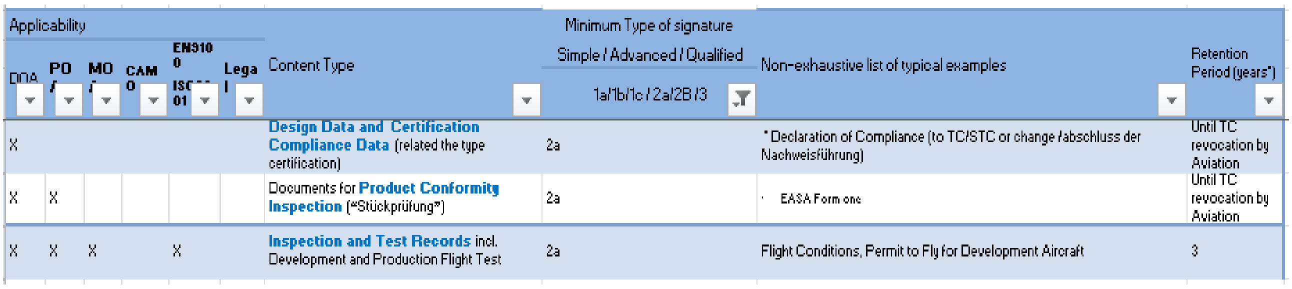
The 'qualified electronic signature' obviously provides the highest level of trust, but also creates the highest process effort/costs because of requirements regarding the accreditation of the infrastructure (tools/devices/external trust centers).

As their conclusion of this analysis the Working Group recommends to apply type 1c: **electronic validation – on all document types with medium trust level requirements** and recommends to apply type 2a: **Basic (Advanced) Digital signature – for all documents with high trust level requirements**.

5.2. RECOMMENDATION TO APPLY SELECTED SIGNATURES TYPES ON CERTIFICATION DOCUMENTS

Recommendations of the Working Group:
- Use Electronic Validation (1c) or Basic Digital Signature (2a)

Set of documents (example), where Basic Digital Signature (2a) is recommended to be applied as a minimum:



Applicability							Minimum Type of signature		
DOA	PO /	MO /	CAM O	EN910 0 ISO 01	Lega l	Content Type	Simple / Advanced / Qualified 1a/1b/1c / 2a/2B /3	Non-exhaustive list of typical examples	Retention Period (years*)
X						**Design Data and Certification Compliance Data** (related the type certification)	2a	* Declaration of Compliance (to TC/STC or change /abschluss der Nachweisführung)	Until TC revocation by Aviation
X	X					Documents for **Product Conformity Inspection** ("Stückprüfung")	2a	· EASA Form one	Until TC revocation by Aviation
X	X	X		X		**Inspection and Test Records** incl. Development and Production Flight Test	2a	Flight Conditions, Permit to Fly for Development Aircraft	3

In many cases these types of documents contain several signatures – not all of them eventually need to be of type 2a. In a fully digitized process, some signatures can be obtained from workflow approval (type 1c). At a minimum a basic digital signature (type 2a) shall be used and shall be applied at the end of the approval workflow.

For all other documents assessed (see annex B) the Working Group recommends to apply the electronic validation (1c) as a minimum.

6. END2END PROCESS ELECTRONIC SIGNATURE IN AEROSPACE CERTIFICATION (ELECTRONIC VALIDATION & DIGITAL SIGNATURE)

This chapter describes the technical recommendation how to implement the electronic signatures.

6.1 IDENTITY, ACCESS AND CERTIFICATE MANAGEMENT:

This chapter defines recommendations to ensure trust in electronic validation and digital signature by

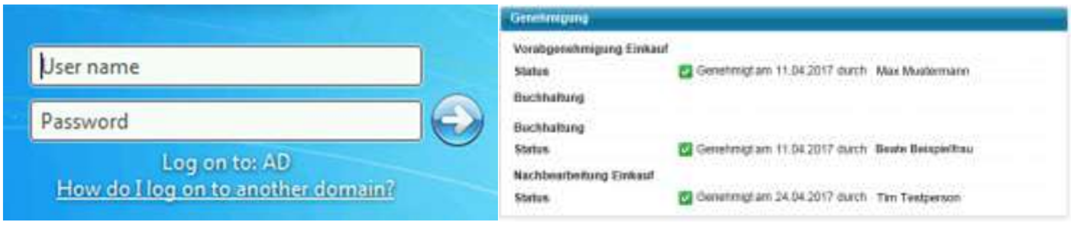
1. performing identity management of personnel receiving credentials for:
   a) electronic validation (1c, simple electronic signature) and
   b) Basic Digital Signature (2a, advanced digital signature)

2. performing access management to back-end systems where document validation workflows take place

3. performing certificate management by using corporate trust centers

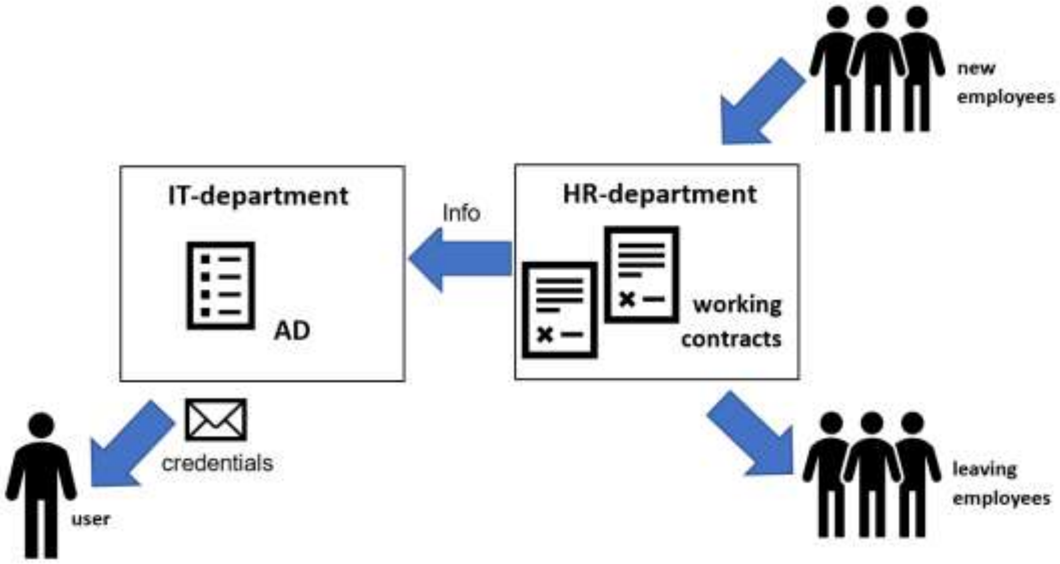
6.1.1 Recommendation how to perform identity management of personnel receiving credentials for Electronic Validation (1c, (simple) electronic signature):

Usually all members of a company are registered in an "active directory" (AD). Persons registered in such AD can log-in on computer terminals of their company by entering user name and password. While the person is logged-in, he or she can accept or deny steps of ongoing workflows, sign-off work steps, etc. Every transaction is tracked within the company-IT-system and allocated to the person logged-in.



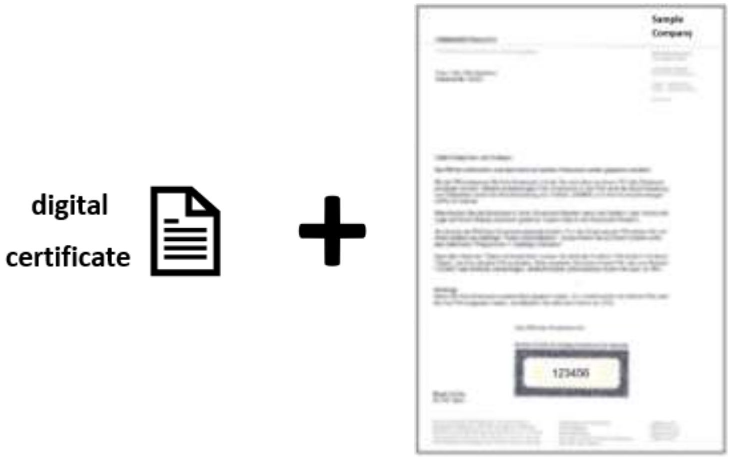
Vorabgenehmigung Einkauf
Status ☑ Genehmigt am 11.04.2017 durch Max Mustermann
Buchhaltung
Buchhaltung
Status ☑ Genehmigt am 11.04.2017 durch Beate Beispielfrau
Nachbearbeitung Einkauf
Status ☑ Genehmigt am 24.04.2017 durch Tim Testperson

The AD, generally, is maintained by company administrators, located in a central IT-department. Information about new or leaving company members are provided by the Human-Resources-department to the administrators of the IT-department. Company members receive their credentials (user name and password) individually from the IT-department. After changing the initial password, the credentials are only known to the specific user.

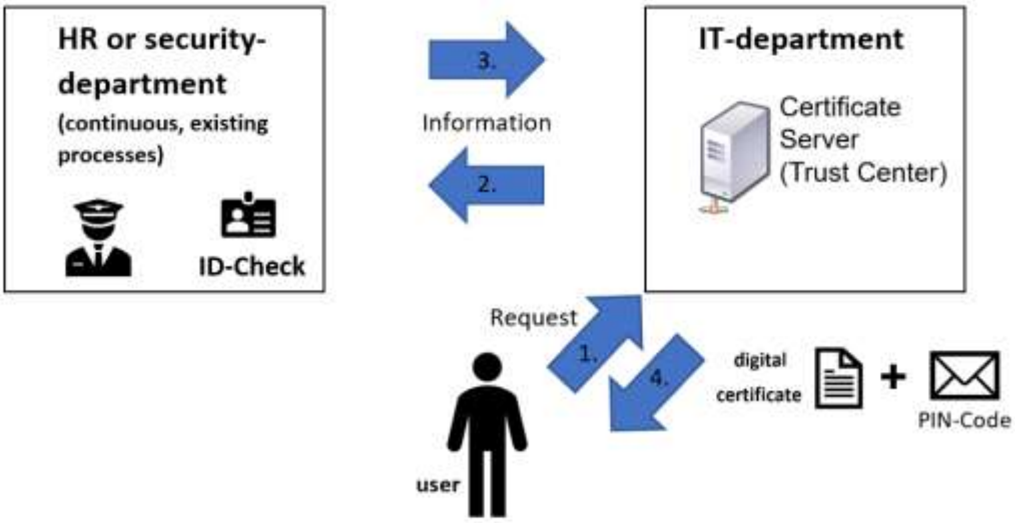


6.1.2 Recommendation how to perform identity management of personnel receiving credentials for Basic Digital Signature (2a, advanced digital signature):

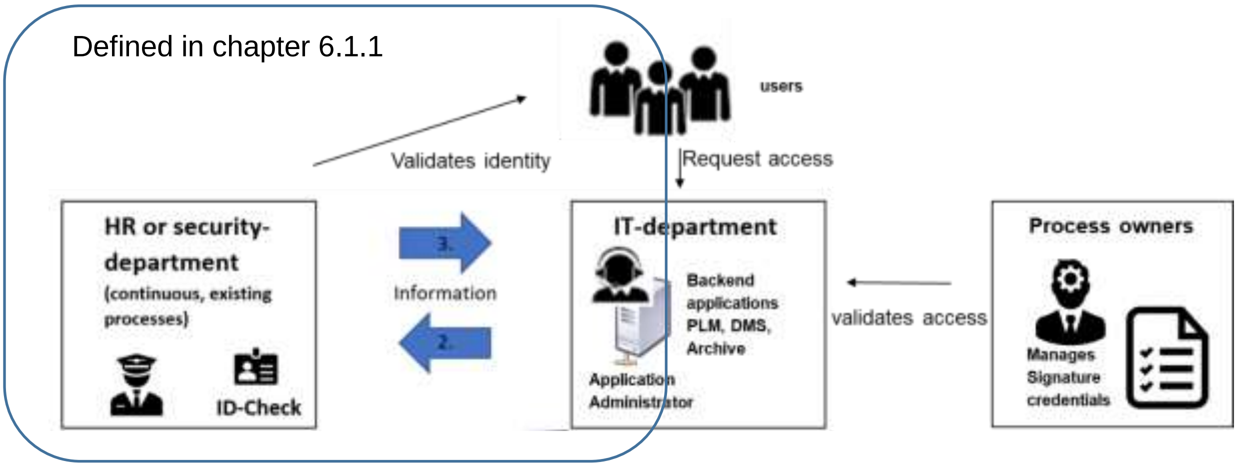
For creating a Basic Digital Signature, a digital certificate, which is in possession of the user, as well as a PIN-Code, which is only known by the user, is required.



To receive the digital certificate the user shall send a request to a central department of the company, where his or her identity is checked by exchanging information with other departments like Human Resources or security, prior to providing the digital certificate. Additionally, the user receives a PIN-Code in a sealed letter from the IT-department, which is in charge/manages the company trust center.


HR or security-department
(continuous, existing processes)
ID-Check
3.
Information
2.
IT-department
Certificate Server (Trust Center)
Request
1.
4.
digital certificate
+
PIN-Code
user

6.1.3 Recommendation how to perform access management to backend systems where document validation workflows take place


Defined in chapter 6.1.1
users
Validates identity
Request access
HR or security-department
(continuous, existing processes)
ID-Check
3.
Information
2.
IT-department
Backend applications PLM, DMS, Archive
Application Administrator
validates access
Process owners
Manages Signature credentials

Especially to keep trust in electronic validation (signature type 1c), the issuing company shall establish adequate processes and structures to ensure, that only appropriate personnel (according to the signature lists) with a validated identity receives access/credentials and that this assignment of credentials/access corresponds to specific roles required by backend applications and is traceable.

6.1.4 Recommendation how to perform certificate management by using corporate trust centers

The server(s) that are part of the platform are sensitive components. Therefore, access to these servers and the information they contain must be physically and logically restricted to persons with the appropriate rights and credentials. The measures to be taken concern:

- Protection of physical access to the server. Selection of a host environment that is suitable in terms of availability for the requirements of signature applications (emergency power conditioning and power supply networks, automatic fire detection and extinguishing systems, etc.).

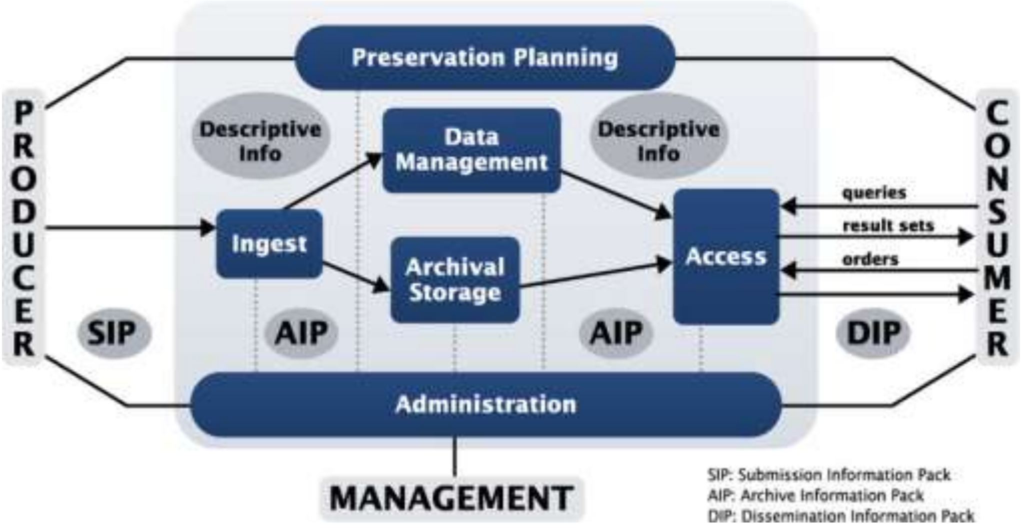
- Restriction of the logical access to the server and data only for authorized persons. The number of people who have access to this platform is strictly limited and these people are identified and authenticated.
- The servers are monitored to prevent interference, physical interference or interference occurring from telecommunication networks.

These processes ensure the adequate / protected generation and management of certificates thereby satisfying PKI-requirements. Encryption (hash) algorithms have to be kept on the latest technology level (e.g. following BSI requirements).

7. ARCHIVING

Archiving and long term archiving define the systematic capturing, ordering, retention and handling of validated/stable original document or data. Archiving is based on rules for immutability, retrieval and reproducibility. In archiving science, the term “long term” is equivalent to “for eternity” (e.g. the German “Bundesarchiv” is a long term archive).

Digital long term archiving in the aerospace environment is defined in the EN 9300 standard series, which are based on the OAIS reference model (see figure below). Therefore, the term “Long Term Archiving” should only be used if all aspects of this reference model apply. The wording “archiving” or better “audit-proof-archiving” is used when documents are managed as defined above as long as at least specifically defined document retention periods are reached.



As the general reference model does not contain specific information regarding archiving of digitally signed documents and especially no focus on the longevity of digital signatures applied on documents in the archive, this section of the White Paper is intended to provide the recommendations for the industry.

Problem of archival infrastructure

Changes of an already archived object are forbidden; therefore each action in the electronic archive system must be logged for traceability purposes.

Recommendation on archiving infrastructure WORM or suitable protective measures according to BSI TR03125

Write once, read many (WORM) describes a data storage device in which information, once written, cannot be modified. Three different kinds of WORM are available:

1. Hardware based WORM (hardware design ensures that data can only be written once and not removed)

2. Systemic WORM (by architecture logical design) → used at e.g. EMC Centera services

3. Software WORM (by Software design (code))→ used at e.g. NetApp SnapLock Enterprise services

If the WORM technology is not used or cannot be used, a suitable security measure must be installed acc. to BSI Technical Guideline TR03125 / Chapter 6.4 IT Infrastructure.

4. Physical security measures must be used to protect the IT infrastructure for archiving evidence and the corresponding storage media against loss, destruction and unauthorized modification. In addition to the access protection mechanisms of the upstream IT applications, a suitable authorization concept must also be implemented in the ECM/long-term storage to protect the archived data and documents (see BSI Technical Guideline TR03125 / Chapter 6.4 IT Infrastructure).

Also combinations of these infrastructure technologies are possible.

Problem of archiving digitally signed documents

The first challenge for digitally signed documents is the selection of an appropriate archiving format, generally accepted and capable to have certificate based digital signatures embedded. Such a long-term-format today is for example PDF/A (ISO19005). The problem regarding archived documents which contain digital signatures in this context is the aging of algorithms used to generate the digital signature. Over time the algorithms are becoming vulnerable to security threats. Therefore the validity of signatures shall be ensured by sufficient technical means and processes which are covering the complete retention period.

Recommended solution for certificate preservation in archiving system

Solutions for archiving of digitally signed documents in the aerospace industry shall apply the recommendations of TR-ESOR technical guideline (BSI TR 03125 TR-ESOR Preservation of Evidence of Cryptographically Signed Document).

According to this guideline, for each newly saved document in an archive, a **hash value** is calculated based on the most recent, strongest hash algorithm and recorded in a **hash tree** at the first level (see figure below).

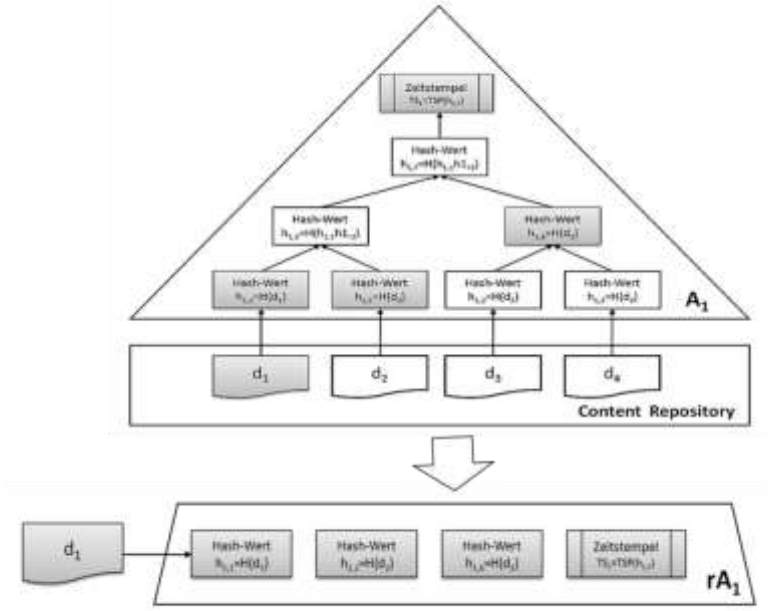
Once a document is needed for evidence in court, a copy of the document is retrieved from the Content Repository and its **Evidence Record** created, which contains a timestamp and in addition the test results of the signatures.

TR-ESOR and WORM based on the level of an electronic Signature

The minimum archive architecture requirements always apply. If the requirements of the BSI standard TR-ESOR are needed to be fulfilled, the following additional security measures apply:

Type of signature on document	Minimum archive architecture	Additional security measures
Electronic validation (1B)	• WORM or comparable	• Electronic time stamp • Evidence records (re-hashing)
Basic digital signature(2A)	• WORM or comparable + electronic time stamp	• Evidence records (re-hashing)

According to BSI standard TR03125 the older the document and its cryptographic signature / seal / timestamp, the higher the risk of not being able to prove a previous manipulation and the original evidence no longer exists, because the underlying algorithms are vulnerable to obsolescence and can therefore be recalculated or the validity of the Certificates according to the validity model expire.



Problem of archiving period versus time between new formats, life of computers, operating systems etc.

The lifetime of an aerospace product can be 70 years and more, but the life of an operating system is normally about 18 months, the life of a computer is normally 3 years, the time between CAD versions are 6 months and the life of a CAD system is about 10 years.

Solution of handling objects through their archiving period

Two methods are available for archiving:

1. Migration to long-term-formats as defined in EN9300 (e.g. PDF/A for documents, TIF for drawings, STEP for Full-3D, etc.)
2. Emulation of the environment were the object was created (Archiving of software environments)

The second option is in most cases too expensive to be used, because the software environment has to be mirrored several times as soon as a change happens in the environment and of cause the security restrictions have to be kept up to date as long as the software environments are mirrored.

7.1 DOCUMENT DISTRIBUTION AND RETRIEVAL

This chapter defines recommendations how to ensure trust in electronically signed documents for all stakeholders of industry, authorities and customers.

An end2end certification process requires the involvement of stakeholders from several organizations. Therefore also digital documents and their electronic signatures need to be accessible and usable for the process stakeholders of several organizations not degrading the trust level in the digital artefacts.

As a consequence the following recommendations on compatibility and openness of trust solutions need to be ensured:

a) Option 1: Third party signatory (document sender) receives a certificate from document receiving company trust center. Stakeholders from external organizations need to be able to get access to the PKI (personal key infrastructure) and the necessary means to apply them. The companies issuing certificates to external participants have to ensure appropriate identity management also for the external participants.

b) Option 2: The receiver accepts certificates from third parties with root certificate. The IT department receives root certificate from trusted third party and adds this certificate to list of trusted certificates globally. As a consequence all documents received from this trusted partner are displayed as documents with valid signature.

c) Option 3: The receiver accepts documents with individual certificates. The document recipient receives a document with an unknown certificate from document signatory and adds this certificate to the list of trusted certificates of his company, if the originating root-certificate has been individually checked.

d) A possible way to facilitate this compatibility and openness with regards to PKI especially for small companies who cannot afford the setup of huge and open PKI-infrastructure, could be the use of third party service vendors for PKI-services (e.g. Adobe Approved Trust List (AATL) or Microsoft Root Trust List) or the establishment of a European Aerospace PKI-service.

e) The approved aerospace organization need to ensure, that signed and archived documents can be made available to stakeholders from external organizations in need to know case throughout the airworthiness required lifecycle time of an aerospace product.

f) External stakeholders shall be enabled to authorize documents signed with Basic (advanced) Digital Signature (2a).
Especially in the case, that documents are not directly accessed through tools from document holder but exchanged, not all process participants will necessarily execute signatures or view documents in the same tools, therefore access to trust servers for these signing and viewing tools need to be ensured.
The target shall be, that all process participants can perform all three authentication validation steps at signing/viewing to ensure trust level:
   a. Granting proof the content was unchanged since signature was done
   b. Granting proof of the identity of the signatory with appropriate certificate
   c. Granting proof regarding the time stamp of signing

g) In case documents with electronic validation are exchanged, the authentication validation can be achieved by auditing the management system (e.g. DMS/ERP/PLM) with a link to archiving system.

8. RECOMMENDATION FOR IMPLEMENTATION IN AEROSPACE INDUSTRY:

Recommendation
Under consideration of the explained framework the BDLI aerospace industry recommends as next steps for implementation:

8.1 BASIC STANDARD

The present BDLI white paper serves as the basic standard for the implementation of electronic signatures for digital approval processes in the aerospace industry.

8.2 ENVISIGED ACCEPTANCE BY AUTHORITIES

- Acceptance by authorities (EASA, LBA and LufABw) that the fundamental confidence level is sufficient if the white paper is applied as the basic standard for digital certification by the aerospace business.
- Civil:
  On short term: Release of certification memorandum (mainly based on the present BDLI white paper) by EASA.
  On long term: AMC should be prepared by EASA with support of industry
- Military:
  On short term: Letter of acceptance of the aforementioned civil certification memorandum.
  On long term: Update of regulation (C1-275/2-8956 (former A1-1525/0-8901 & 02) respectively A1-275/3-89xx)

8.3 ESTABLISHMENT OF A WG IN ASD (SIMILAR TO THE BDLI WG)

- Action 1: BDLI supports to establish Working Group on ASD-level to achieve an European aligned approach

- Action 2: Support/promotion of the implementation of electronic signatures for digital certification in the European aerospace business (mainly small and medium-sized companies as well as sub-tier chain)

- Action 3: Further development of the White Paper due to new technical developments (e.g. Block Chain)

9. ANNEX

A. LITERATURE

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"

Signaturgesetz (SigG): Gesetz über Rahmenbedingungen für elektronische Signaturen; Es wurde am 1. Juli 2016 weitgehend durch die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eiDAS-Verordnung) verdrängt, trat am 29. Juli 2017 außer Kraft und wurde durch das Vertrauensdienstegesetz (VDG) abgelöst.

Vertrauensdienstegesetz (VDG)

LOTAR 9300 series set: LOTAR LOng Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data: ASD-STAN prEN 9300-001 P1; ASD-STAN prEN 9300-002 P1; DIN EN 9300-003:2012; DIN EN 9300-004:2013; DIN EN 9300-005:2017; DIN EN 9300-007:2017; ASD-STAN prEN 9300-010 P1; DIN EN 9300-011:2013; DIN EN 9300-012:2013; DIN EN 9300-013:2013; DIN EN 9300-014:2013; DIN EN 9300-015:2013; ASD-STAN prEN 9300-100 P1; ASD-STAN prEN 9300-110 P2; ASD-STAN prEN 9300-115 P1; ASD-STAN prEN 9300-200 P1

ISO 14721:2012 Space data and information transfer systems — Open archival information system (OAIS) — Reference model

ISO 10005:2018 Quality management — Guidelines for quality plans

ISO 10303-1:1994 INDUSTRIAL AUTOMATION SYSTEMS AND INTEGRATION — PRODUCT DATA REPRESENTATION AND EXCHANGE — PART 1: OVERVIEW AND FUNDAMENTAL PRINCIPLES

AMC No.1 to 21.A.163(c) “Computer generated signature and electronic exchange

B. LIST OF DOCUMENTS ASSESSED FOR ELECTRONIC SIGNATURE

Applicability						Content Type	Non-exhaustive list of typical examples
DOA	**POA**	**MOA**	**CAMO**	**EN9100** **ISO9001**	**Legal**		
				X		Business /Quality **Management Review Reports / Records**	Minutes of Meeting, Quality Improvement Plans, Quality / Environment Policies, Evaluations
X	X	X	X	X		Business / Quality **Management System Documentation**	Quality Management System documents which do not include product related Technical Instructions: □ company policies, directives, methods; □ company manuals (e.g. QMH, POM, DOM, MOM, …); □ procedures, instructions and manuals; □ quality plans
				X		**Customer Commercial Records**	Contract Documents: □ Purchase / Lease Agreements and Amendments □ Subcontract Licences □ Customer Purchase Orders
							Pre-contractual documents: □ Proposals □ Bids □ Approved Submissions □ Quotations
							Contract Review Records
X				X		**Design Documentation**	Design Review documentation: □ Design Baseline documents □ minutes of design review meeting □ supporting documents to design review meeting
X						**Design Data and Certification Compliance Data** (related the type certification)	□ Technical specification, customer specification incl. approved deviations from specifications, concessions and limitations □ Documentation for the compilation, testing and maintenance of SW, if affected □ Construction documents: Construction and functional details, Drawings, Design Schemes, 2D/3D models, Lists (of drawings, items, parts, material, standard parts, etc.), General plans (e.g. circuit diagrams), material and process specifications □ Military: Type certification program; civil: certification plan and means of compliance * Declaration of Compliance (to TC/STC or change /abschluss der Nachweisführung) □ Compliance reports as requested by type certification program (e.g. qualification/certification test results, inspection records of critical parts)

						□ ~~Type certificate,~~ Airworthiness Notice, Authorised Signatories List
X				X	**Design Verification**	Verification / compliance demonstration Records: □ Verfication Review reports □ Verification reports □ Reports to explain /simulate/test or demonstrate the technical verification result
X	X	X	X	X	**Evaluation of suppliers**	Supplier Audit and Assessment Reports, Supplier Qualification acceptance (approval only not linked to product), performance evaluations, quality trends, verifications, supplier purchase orders
						Contract – short term
						Contract – long term
	X			X	Records related to **supplier product**	Supplier First Article Inspection (FAI) records; source inspection records, supplier certificate of compliance, receiving Inspection Reports
X	X	X		X	Control of **customer supplied products**	Discrepancy reports, inspection reports, calibration reports, or other reports used for porduct certification
	X			X	Documents which support and demonstrate the **identification of the product**	For traceable items: traceability records, storage records, serial or batch number registration, records of procurement sources, receiving inspection records
						For non-traceable items: records of procurement sources, receiving inspection records
X	X				Documents for **Product Conformity Inspection** (“Stückprüfung”)	□ Type design documentation (type design documentation list, technical specifications, inspection schedules, A/C functional test procedure incl. product conformity check, flight regulations) □ Compliance demonstration documentation (inspection reports, debriefing reports, certificates of conformance and inspection reports for supplied products) □ Equipment History records, condition tags
						· EASA Form one
X	X	X			Document for **Airworthiness Reverification** (“Nachprüfung”)	□ documentation required for Airworthiness Reverification (operation, repair and maintenance manuals, technical instructions, operating records, Equipment History records, condition tags, functional test procedures) □ Compliance demonstration documentation (inspection reports, debriefing reports, certificates of conformance and inspection reports for supplied products)
	X			X	Records and information generated and used during the **preparation and production phases**	For traceable items: Manufacturing records (e.g. identification sheets, plans, work cards, shop order travellers), Engineering Change records (e.g. RfAs), As-Built Information sheets, product related Special Processes Records (e.g. heat treatment) and Equipment Records

						For non-traceable items: manufacturing records, Engineering Change records (e.g. RfAs), As-Built information sheets, special processes and equipment records
X						Manufacturing Documentation as part of the military type certification documentation: □ Machining, manufacturing and test procedures □ Details on materials and working procedures as well as manufacturing and assembly methods
X	X	X		X	**Inspection and Test Records** incl. Development and Production Flight Test	For traceable items: records of inspection and test completion, records for First Article Inspection (FAI)
						Inspection (incl. FAI) and Test Records, Certification Records
X						Flight Conditions, Permit to Fly for Development Aircraft
						For non-traceable items: Inspection and test information, certification records, records of FAI
	X	X		X	Records to control **Inspection, Measuring and Test Equipment**	Record for equipment registration/first approval, (re)calibration records, (re)calibration historical information
X	X			X	**Non-conformance records**	Deviations, concessions, waivers Quality surveillance reports, analysis of non-conformance information, investigation reports, re-inpsection notice
X	X			X	**Corrective / Preventive Action Records**	Corrective / Preventive Action Reports, investigation information, report of the cause of the non-conformance, record of eveluation of effectiveness of corrective action
X	X	X	X	X	**Internal Quality Audit Records**	Reports of Quality System Audits, Process Quality Audits, Product Quality Audits and Service Quality Audits conducted for internal purposes

X	X	X	X	X	X	**Personnel** Records	Recriutment Records, Validation of Qualifications, Training Records, Contract of Employment History, Job descriptions Experience and training records of personnel making decisions affecting Airworthiness (e.g. certifying staff, CVEs, etc) or Environmental Protection
							Records of Certifying Staff / Information for Qualifying and Following up Authorised Signatories: Authorization Record Sheet (ARS) for Aircraft Authorized Personnel ; On-the-Job-Training Form ; Qualification Card for Aircraft Certifying Staff ; Authorization Record Sheet for EASA Form 1 Certifying Staff ; Authorization Withdrawal for POA Authorized Personnel (including Quality Authorization); Aircraft Authorized Personnel Stamp Allocation, List of Authorised Signatories ; Surveillance of Aircraft Conformity Managers/Certifying Staff. NDT Certification Record (Record of Trainings, Qualifications & Certification)
							Records of Airworthiness Review Staff
X						Instructions for **Continued Airworthiness** (ICA)	Technical Publications (e.g. handbooks, Service Bulletins)
	X		X			Status and Detailed **Maintenance Records** to determine the Continuing Airworthiness and Configuration of the A/C relevant for future Maintenance.	Technical Logbook for in-service Aircraft
							Latest Product Status (Modification/Repair Status, Compliance with A/C Maintenance Programme)
				X		**Environmental Records**	Product Process Records, Product Records, Review of Process Audits, Management Reviews, Incidents, Anomalies

C. MAPPING OF AMC REQUIREMENTS ON ELECTRONIC SIGNATURES FOR EASA FORM 1 ON BDLI RECOMMENDATIONS

	AMC No.1 to 21.A.163(c)	BDLI Working Group solution
	password and secure access, authentication, protections, confidentiality;	The systems are password-protected and require a personal user account. The systems have rights management which corresponds to the required status (groups and roles)
	track changes;	All changes are traceable. Systems have versions (linked to check-in / check-out)
	minimum blocks to be completed, completeness of information;	Mandatory attributes are stored in the systems
	archives;	The DMS/PDM/ERP systems are linked to archives
	The electronic system generating the EASA Form 1 may contain additional data such as: manufacturer code; customer identification code; workshop report; inspection results; etc	The DMS / PDM / ERP systems have bibliographic metadata and should print them out on the form.
	Characteristics of the computer generated signature To facilitate understanding and acceptance of the EASA Form 1 released with an electronic signature, the following statement should be in Block 13b: 'Electronic Signature on File' .	The DMS / PDM / ERP systems should appropriately print the information on the form.
	When the electronic file contains a hyperlink to data, required to determine the airworthiness of the item(s), the data associated to the hyperlink, when printed, should be in a legible format and be identified as a reference from the EASA Form 1.	The DMS / PDM / ERP systems should appropriately print the information on the form.

	Additional information not required by the EASA Form 1 completion instructions may be added to the printed copies of EASA Form 1 as long as the additional data do not prevent a person from filling out, issuing, printing, or reading any portion of the EASA Form 1. This additional data should be provided only in block 12 unless it is necessary to include it in another block to clarify the content of that block.	The DMS / PDM / ERP systems should print the information on the form appropriately and the process is defined in specific process descriptions depending on the company.
	Electronic exchange of the electronic EASA Form 1	Is not currently taking place. However, every system has export functions and can output necessary metadata. The BDLI Working Group proposed a standardized exchange format

D. ACRONYMS

AD
active directory

BDLI
Bundesverband der Deutschen Luft- und Raumfahrtindustrie
The German Aerospace Industries Association

BSI
Bundesamt für Sicherheit in der Informationstechnik
(German) Federal Office for Information Technology

DMS
Document Management System

EASA
European Union Aviation Safety Agency

eIDAS
Electronic IDentification Authentication and trust Services

ERP-system
Enterprise Resource Planning System

IT
Information Technology

LBA
Luftfahrt Bundesamt
German National Aviation Authority

LufABw
Luftfahrtamt der Bundeswehr
German National Military Aviation Authority

OAIS
Offenes Archiv-Informations-System
Open Archival Information System

PDM-System
Product Data Management System

WORM
Write once, Read many