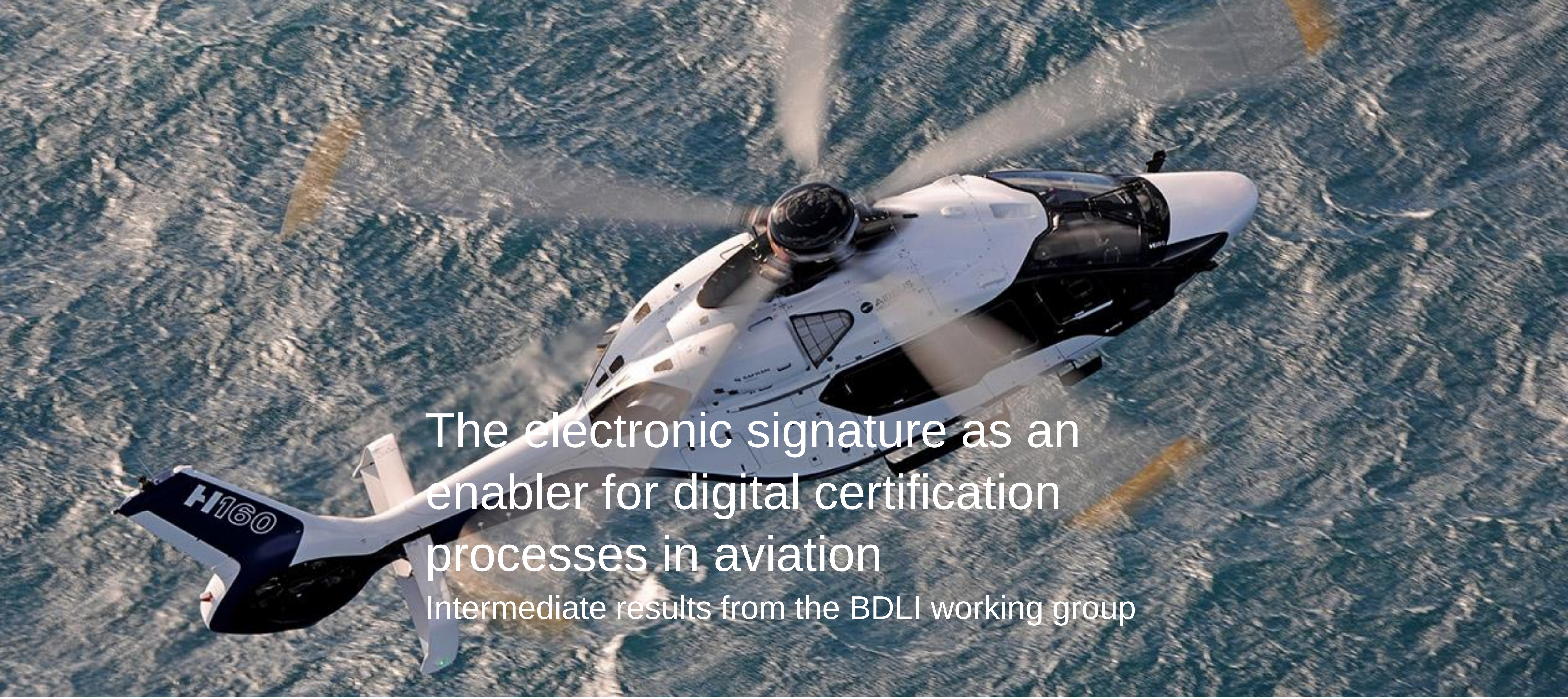


The electronic signature as an enabler for digital certification processes in aviation

Intermediate results from the BDLI working group

HELICOPTERS

Dr. Jörg Wirtz,

IAQG supplier forum Berlin 18th Ocober

AIRBUS

Agenda

1. Status quo in Aviation
2. Concepts & building bricks of digital trust
3. Results of BDLI WG:
   a) how to apply electronic signatures on TC-documents
   b) how to archive digitally signed TC-documents
4. Implemenation of digital signature at Airbus Helicopters
5. A proposal how to include authorities, supplier and partners in digital signature processes
6. Outlook: model base engineering
7. Next steps

Status quo in Aviation

Aircraft development and production

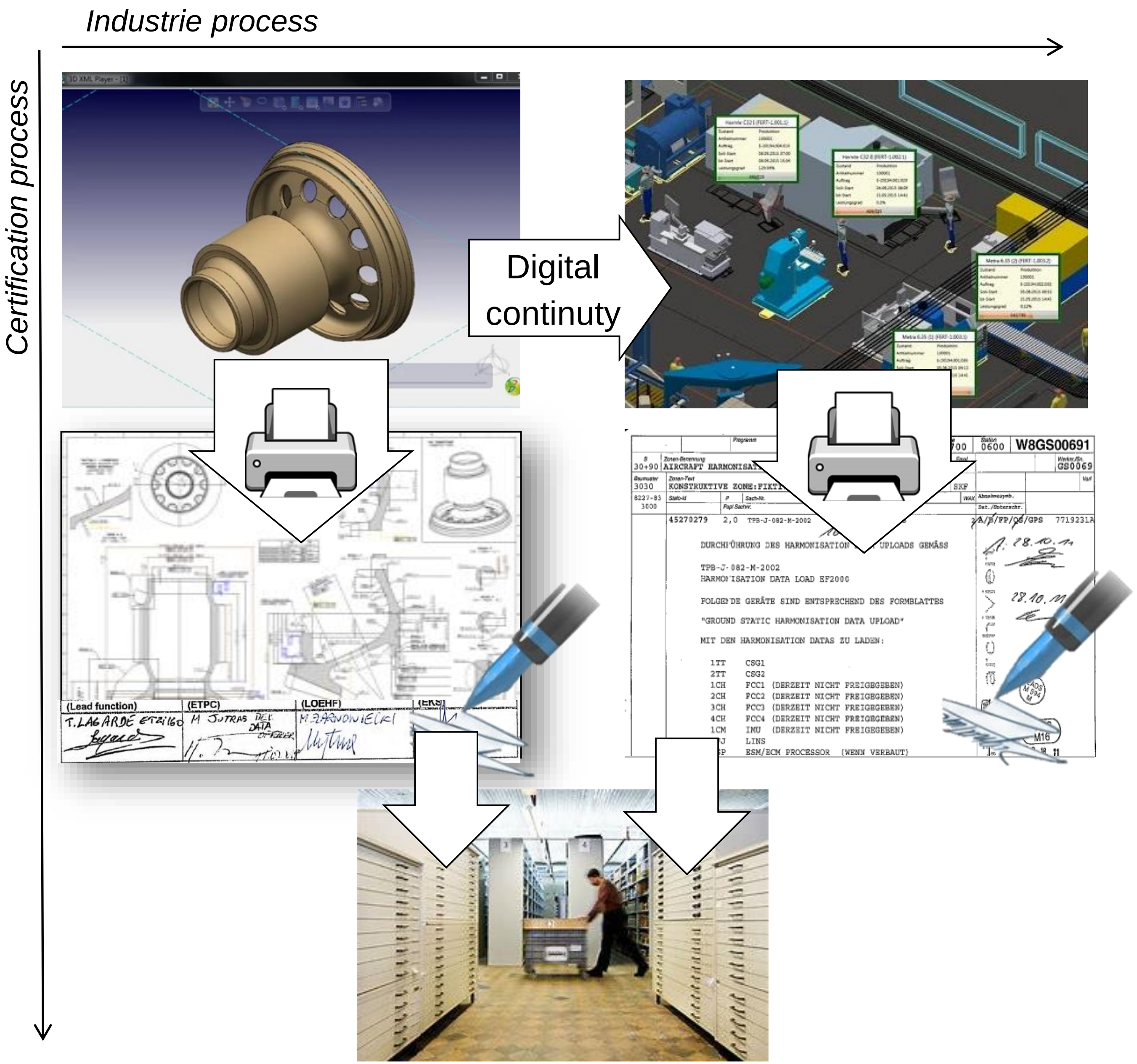
Data Collection
Digitaler Wandel
Social Machines
Intelligente Systeme
Energieeffizienz
Digitalisierung
Industrie 4.0
Echtzeit-Daten
Cyber-physische Systeme
Netzwerke
Internet
Automatisierung
Vernetzung
Smart Factory
Factories of the Future
Smart Products
Internet der Dinge
Big Data

Aircraft certification

Status quo in Aviation

- In digital tools, all product and production process data are defined and processed in the process chain
- However, signatures on released data in the digital environment are still not fully accepted by regulatory agencies.
- Therefore for all certification purposes, paper based documents have to printed out, wet signed and finally archived
- The missing confidence results from:
  - Missing accepted industrial best practice on applying digital signatures = digital trust service on aviation certification documents
  - Missing accepted industrial best practice on Long Term Archiving of digitally signed type certificate documents
  - Missing accepted industrial best practice on including authorities, supplier and partners in digital signature processes

This led to building of the BDLI-working group in 2018



Industrie process

Certification process

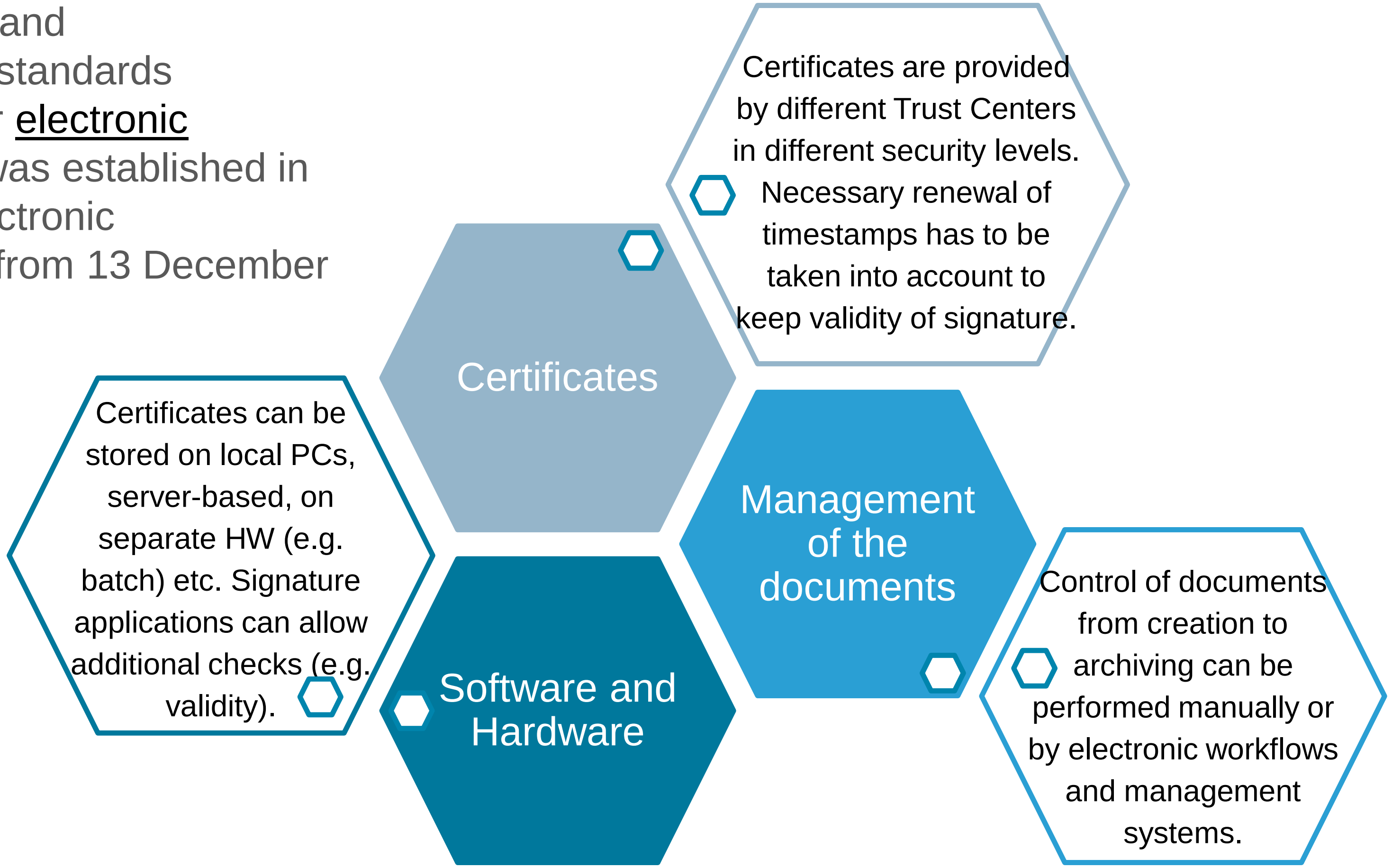
Digital continuty

3D XML Player
(Lead function)
(ETPC)
(LOEHF)
T. LAGARDE
M. JUTRAS
W8GS00691
30+90 AIRCRAFT HARMONISAT
3030 KONSTRUKTIVE ZONE:FIKTI
GS0069
45270279 2,0 TPB-J-082-M-2002
DURCHFÜHRUNG DES HARMONISATION UPLOADS GEMÄSS
TPB-J-082-M-2002
HARMONISATION DATA LOAD EF2000
FOLGENDE GERÄTE SIND ENTSPRECHEND DES FORMBLATTES
"GROUND STATIC HARMONISATION DATA UPLOAD"
MIT DEN HARMONISATION DATAS ZU LADEN:
1TT CSG1
2TT CSG2
1CH FCC1 (DERZEIT NICHT FREIGEGEBEN)
2CH FCC2 (DERZEIT NICHT FREIGEGEBEN)
3CH FCC3 (DERZEIT NICHT FREIGEGEBEN)
4CH FCC4 (DERZEIT NICHT FREIGEGEBEN)
1CM IMU (DERZEIT NICHT FREIGEGEBEN)
LINS
ESM/ECM PROCESSOR (WENN VERBAUT)
28.10.11
M16

AIRBUS

Concepts & building bricks of digital trust : The eIDAS regulation

eIDAS-Verordnung
eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation on / a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC from 13 December 1999..



Certificates

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 can be stored on local PCs, server-based, on separate HW (e.g. batch) etc. Signature applications can allow additional checks (e.g. validity).

Software and Hardware

Management of the documents

Control of documents from creation to archiving can be performed manually or by electronic workflows and management systems.

Concepts & building bricks of digital trust

Die EIDAS Verordnung defines in Art. 3 Nr. 10–12 the following types of electronic signatures:

simple electronic signature
Any digital declaration of intent: e.g. Signature under an email

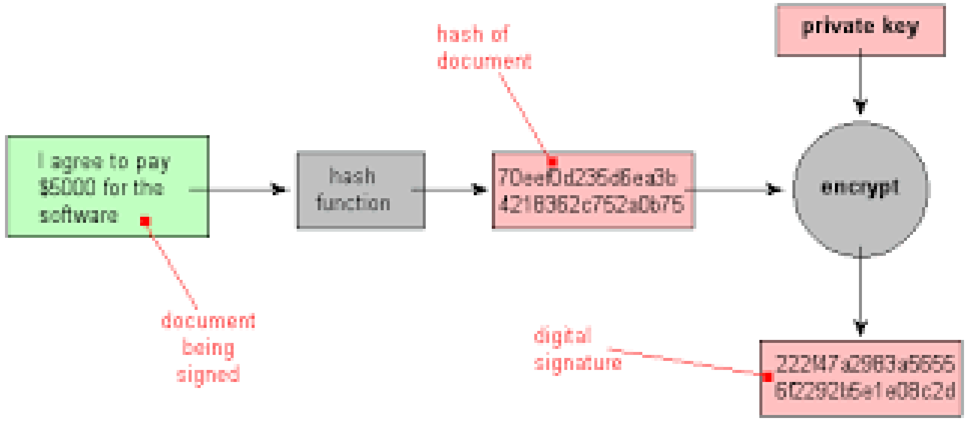
Advanced electronic signature (certificate based):

- There is a certificate for electronic signature, electronic proof that confirms the identity of the signatory and links the electronic signature validation data to that person.
- It provides unique identifying information that links it to its signatory.
- The signatory has sole control of the data used to create the electronic signature.
- It must be capable of identifying if the data accompanying the message has been tampered with after being signed. If the signed data has changed, the signature is marked invalid.

Qualified electronic signature (certificate based)
an advanced electronic signature that is created by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.

Certificate based digital signature

Private key= certificate from Trust center linked to identity of signee


hash of document
private key
I agree to pay $5000 for the software
hash function
70eef0d236d6ea3b 4218362c752a0b75
encrypt
document being signed
digital signature
2224f7a2983a5656 6f2292b6e1e08c2d

Results of BDLI WG :The BDLI working group & approach

Authorities

Thomas Glose, Bundeswehr ;

Bichtemann, Bernd, Bundeswehr;

Wienen, Sarah, Bundeswehr

Müller , Andreas LBA;

Working Group coordination:
Wirtz, Jörg -; Airbus Helicopters
Zwiener, Axel; BDLI

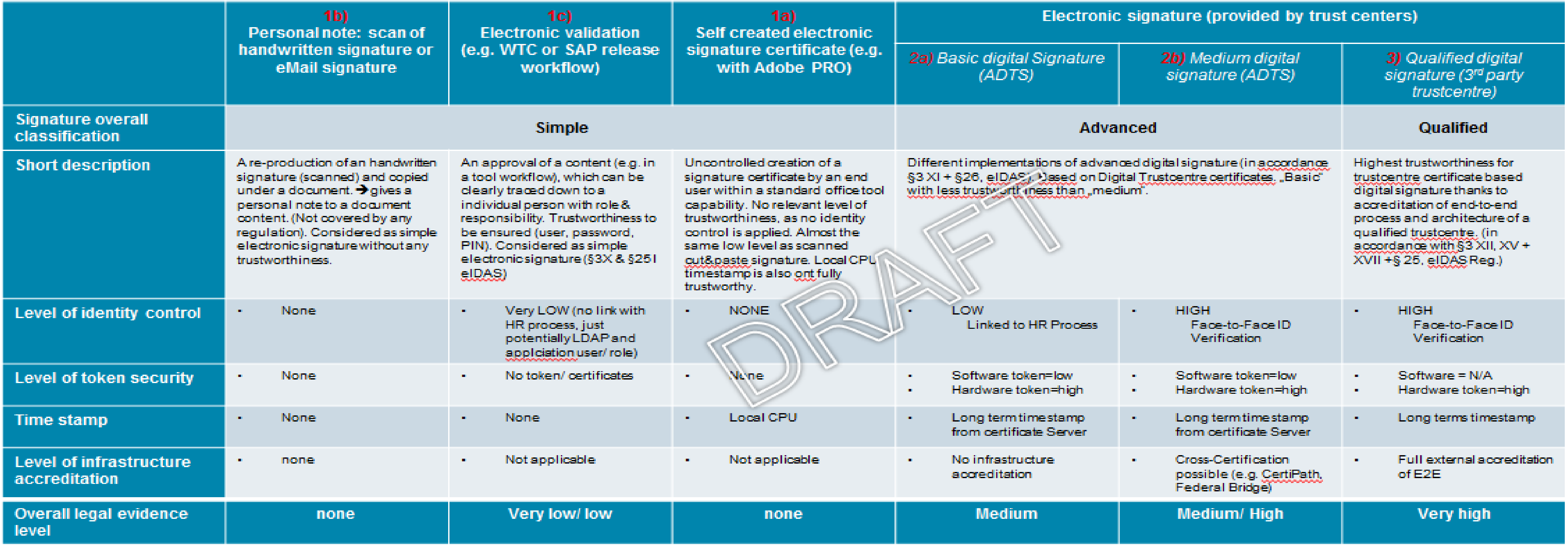
Industrie
Kubon, Rene ESG;
Kotziok, Alexandra ; Airbus Defence & Space;
Schumann, Andreas; Premium Aerotec
Geisenberger, Anton; Premium Aerotec
Prassek, Arnd.; MTU
Mayr, Claus MTU;
Friese, Daniel; Airbus Defence & Space
Krueger, Eike; Airbus
Frank Müller Hensoldt;
Fichtner, Frank Hensoldt;
Godde, Hans. Diehl;
Groth, Harald. Jenoptik.;
Bracklo, Holger; Position Elbe-Flugzeugwerke
Wirtz, Jörg; Airbus Helicopters
Poerner, Marc; Airbus Helicopters

Kochs-Kämper, Markus (RUAG Aero
Albrecht, Michael, MT-aerospace;
Loges, Michael Rolls-Royce.
Wojahn, Michael Rolls-Royce
Fischer, Michaelpeter; Jenoptik;
Haarmann, Robert Hensoldt;
Salbach, Holger Northrop Grumman LITEF;
Kläsner, Sascha; Liebherr.;
Tietsche, Volker; Northrop Grumman LITEF;
Wolski, Timo;Siemens
Fischer, Lena; Northrop Grumman LITEF;
Huber, Rebecca; MTU;
Zebib, Ursula.DIEHL;

The BDLI working group has set itself the goal of developing a proposal as to which requirements with regard to electronic signature are to be placed on which document / data types of the type certifcate process

Results of BDLI WG :how to apply electronic signature in TC documents

Initially, various electronic signature types and existing processes from industrial practice were identified and described



	1b) Personal note: scan of handwritten signature or eMail signature	1c) Electronic validation (e.g. WTC or SAP release workflow)	1a) Self created electronic signature certificate (e.g. with Adobe PRO)	Electronic signature (provided by trust centers)		
				2a) Basic digital Signature (ADTS)	*2b) Medium digital signature (ADTS)*	*3) Qualified digital signature (3rd party trustcentre)*
Signature overall classification	**Simple**			**Advanced**		**Qualified**
Short description	A re-production of an handwritten signature (scanned) and copied under a document. ➔ gives a personal note to a document content. (Not covered by any regulation). Considered as simple electronic signature without any trustworthiness.	An approval of a content (e.g. in a tool workflow), which can be clearly traced down to a individual person with role & responsibility. Trustworthiness to be ensured (user, password, PIN). Considered as simple electronic signature (§3X & §25I eIDAS)	Uncontrolled creation of a signature certificate by an end user within a standard office tool capability. No relevant level of trustworthiness, as no identity control is applied. Almost the same low level as scanned cut&paste signature. Local CPU timestamp is also ont fully trustworthy.	Different implementations of advanced digital signature (in accordance §3 XI + §26, eIDAS). Based on Digital Trustcentre certificates. „Basic" with less trustworthiness than „medium".		Highest trustworthiness for trustcentre certificate based digital signature thanks to accreditation of end-to-end process and architecture of a qualified trustcentre. (in accordance with §3 XII, XV + XVII +§ 25, eIDAS Reg.)
Level of identity control	- None	- Very LOW (no link with HR process, just potentially LDAP and applciation user/ role)	- NONE	- LOW Linked to HR Process	- HIGH Face-to-Face ID Verification	- HIGH Face-to-Face ID Verification
Level of token security	- None	- No token/ certificates	- None	- Software token=low - Hardware token=high	- Software token=low - Hardware token=high	- Software = N/A - Hardware token=high
Time stamp	- None	- None	- Local CPU	- Long term timestamp from certificate Server	- Long term timestamp from certificate Server	- Long terms timestamp
Level of infrastructure accreditation	- none	- Not applicable	- Not applicable	- No infrastructure accreditation	- Cross-Certification possible (e.g. CertiPath, Federal Bridge)	- Full external accreditation of E2E
Overall legal evidence level	**none**	**Very low/ low**	**none**	**Medium**	**Medium/ High**	**Very high**

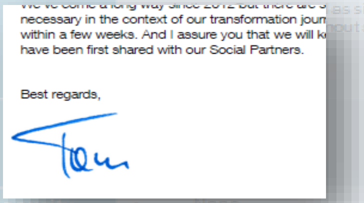
Results of BDLI WG : how to apply electronic signature in TC documents

Finally 4 electronic signature types were taken into account for the mapping with aviation type cetrificte documentation

	1b) Personal note: scan of handwritten signature or eMail signature	1c) Electronic validation (e.g. WTC or SAP release workflow)	1a) Self created electronic signature certificate (e.g. with Adobe PRO)	Electronic signature (provided by trust centers)		
				2a) *Basic digital Signature (ADTS)*	2b) *Medium digital signature (ADTS)*	3) *Qualified digital signature (3rd party trustcentre)*
Signature overall classification		Simple		Advanced		Qualified
Overall legal evidence level	none	[illegible]	none	Medium	Medium/ High	Very high

1b Email/ Scan/Picture

- Z.B. "Tom's letter"



necessary in the context of our transformation journ
within a few weeks. And I assure you that we will k
have been first shared with our Social Partners.

Best regards,

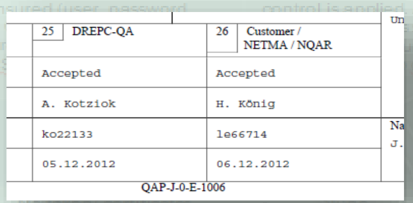
Tom

- 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

Not recommeded To use

1c Electronic Validation

- Z.B. EFA waiver in PDM



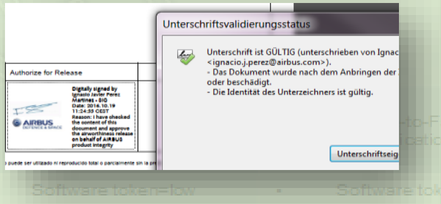
25 DREPC-QA	26 Customer / NETMA / NQAR	Un
Accepted	Accepted	
A. Kotziok	H. König	
ko22133	le66714	Na J.
05.12.2012	06.12.2012	

QAP-J-0-E-1006

- 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



Authorize for Release

Digitally signed by Ignacio Javier Perez Martinez - SIG
Date: 2016.10.19 11:24:35 CEST
Reason: I have checked the content of this document and approve the airworthiness release on behalf of AIRBUS product integrity

puede ser utilizado ni reproducido total o parcialmente sin la pr

Unterschriftsvalidierungsstatus

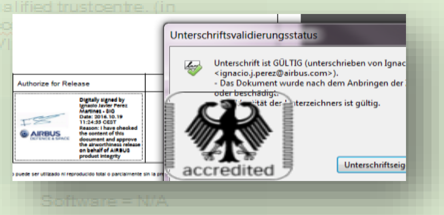
Unterschrift ist GÜLTIG (unterschrieben von Ignac
<ignacio.j.perez@airbus.com>).
- Das Dokument wurde nach dem Anbringen der
oder beschädigt.
- Die Identität des Unterzeichners ist gültig.

- 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

Nachweispflicht beim "Beklagten"

3 Qualified Digital Signature

- Z.B. Type Certificate Dokument



Authorize for Release

Digitally signed by Ignacio Javier Perez Martinez - SIG
Date: 2016.10.19 11:24:35 CEST
Reason: I have checked the content of this document and approve the airworthiness release on behalf of AIRBUS product integrity

puede ser utilizado ni reproducido total o parcialmente sin la pr

Unterschriftsvalidierungsstatus

Unterschrift ist GÜLTIG (unterschrieben von Ignac
<ignacio.j.perez@airbus.com>).
- Das Dokument wurde nach dem Anbringen der
oder beschädigt.
- Die Identität des Unterzeichners ist gültig.

- 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

Beweislastumkehr

HELICOPTERS

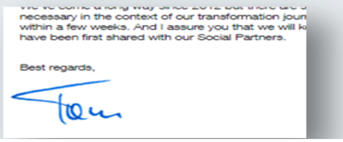
Evaluation of wet & electronic signature types in terms of process costs and process reliability

Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V.

Types of electronic Signature

0 nasse Unterschrift

•Z.B. "Tom's letter"



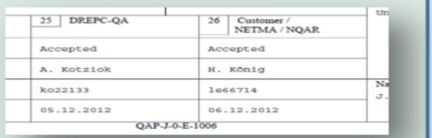
We've come a long way since 2012 but there are s
necessary in the context of our transformation jour
within a few weeks. And I assure you that we will k
have been first shared with our Social Partners.

Best regards,

Tom

1c Electronic Validation

•Z.B. EFA waiver in PDM

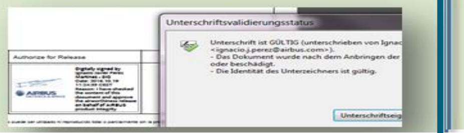


25 DREPC-QA	26 Customer / NETMA / NQAR
Accepted	Accepted
A. Kotziok	H. König
ko22133	1e66714
05.12.2012	06.12.2012

QAP-J-0-E-1006

2a Digitale Signatur

• Z.B. Type Certificate Dokument



Unterschriftsvalidierungsstatus

Unterschrift ist GÜLTIG (unterschrieben von Ignac <ignacio.j.perez@airbus.com>).
- Das Dokument wurde nach dem Anbringen der oder beschädigt.
- Die Identität des Unterzeichners ist gültig.

3 Qualifizierte Digitale Signatur

• Z.B. Type Certificate Dokument

Unterschriftsvalidierungsstatus

Unterschrift ist GÜLTIG (unterschrieben von Ignac <ignacio.j.perez@airbus.com>).
- Das Dokument wurde nach dem Anbringen der oder beschädigt.
- Die Identität des Unterzeichners ist gültig.

accredited

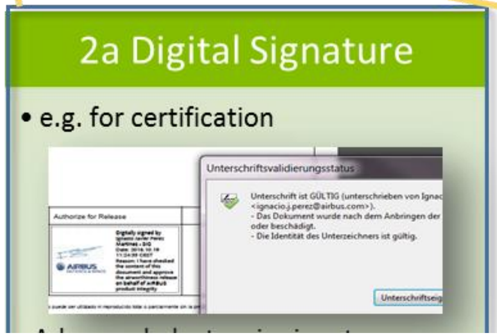
Types of electronic Signature	0 nasse Unterschrift		1c Electronic Validation		2a Digitale Signatur		3 Qualifizierte Digitale Signatur	
Document process	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability	Effort/ costs	Security/ reliability
Control 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

1c Electronic Validation: Preferred for documents with medium trust level req.

2a Digitale Signatur: Preferred for documents with high trust level req.

AIRBUS

Results of BDLI WG : how to apply electronic signature in TC documents



2a Digital Signature

- e.g. for certification

Authorize for Release

Digitally signed by Ignacio Javier Perez Martinez - DIG Date: 2016.10.18 11:24:38 CEST Reason: I have checked the content of this document and approve the airworthiness release on behalf of AIRBUS product integrity

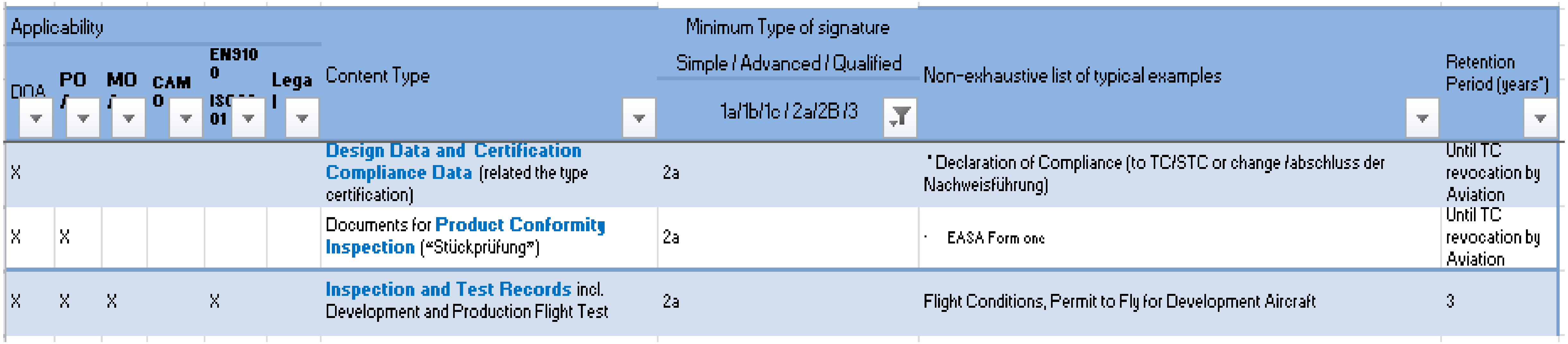
Unterschriftsvalidierungsstatus

Unterschrift ist GÜLTIG (unterschrieben von Ignac <ignacio.j.perez@airbus.com>).
- Das Dokument wurde nach dem Anbringen der oder beschädigt.
- Die Identität des Unterzeichners ist gültig.

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

Recommendation of BDLI WG:

Set of TC documents, where digital signature type 2a shall be applied



Applicability						Content Type	Minimum Type of signature Simple / Advanced / Qualified	Non-exhaustive list of typical examples	Retention Period (years*)
DOA	PO /	MO /	CAMO	EN9100 ISO 01	Legal		1a/1b/1c / 2a/2B /3		
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

Results of BDLI WG :how to archive digitally signed TC-documents

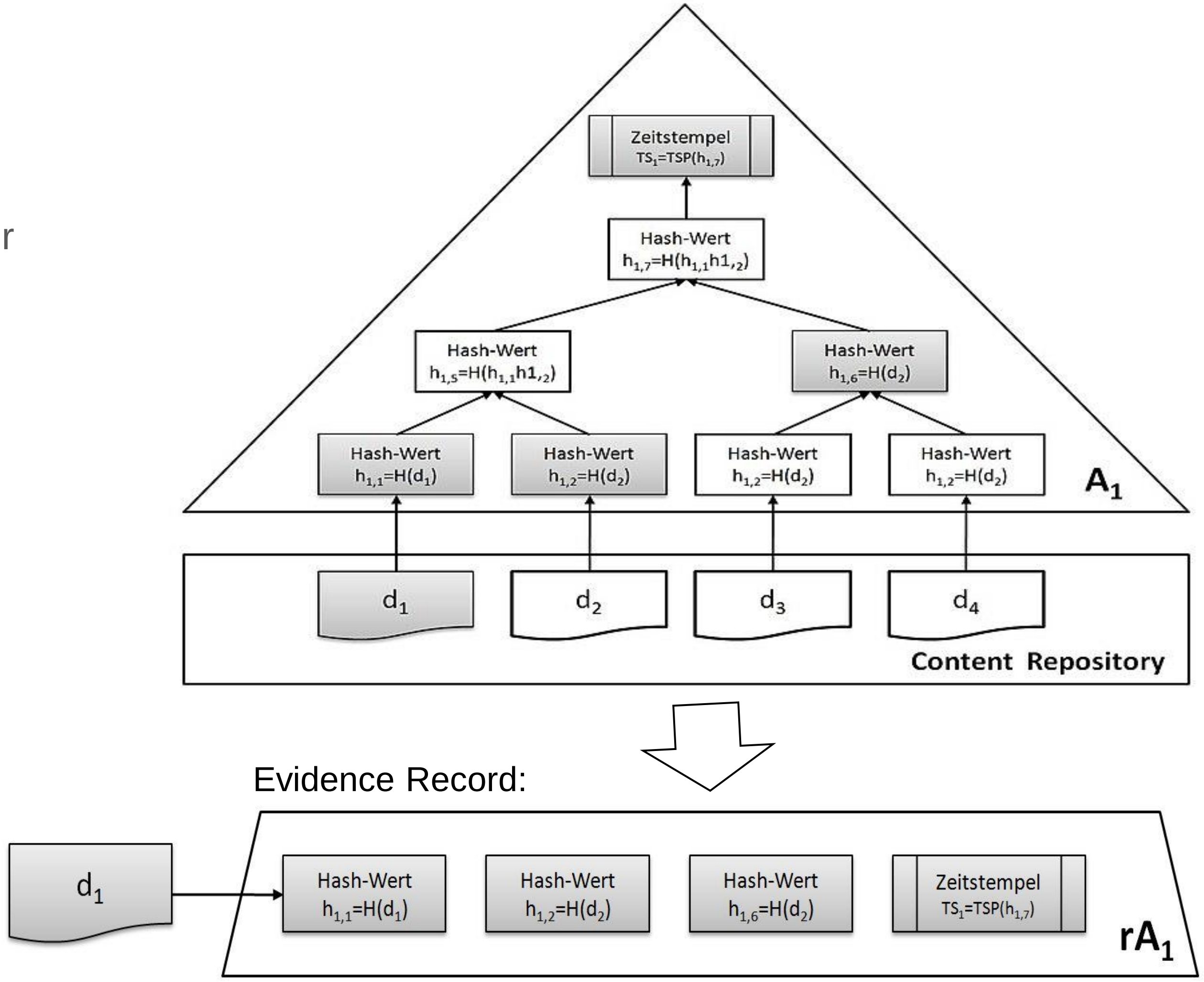
Problem of long term archiving digtal signatures

The problem is the aging of algorithms used to generate an electronic signature. With age, the algorithms are vulnerable, i. H. With enough computing power, someone could spend for another or create another document to the previous hash value.

From working group recommended
Solution in archiving system

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

Now, if one of the documents 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 so-called reduced archive timestamp and in addition to the test results of the signatures.

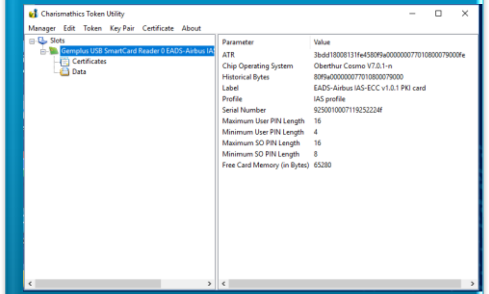


Implemenation of digital signature at Airbus Helicopters

DSignIT

- **Application to digitally sign documents**
- Client solution for local digital signature without document uploads.
- Available in SW center for installation (Win7/10).
- Re-deployment of solution from ADS with additional capabilities for AH.

CSSI & MyID



Charismathics Token Utility

Parameter	Value
ATR	3bdd18008131fe4580f9a000000077010800079000fe
Chip Operating System	Oberthur Cosmo V7.0.1-n
Historical Bytes	80f9a000000077010800079000
Label	EADS-Airbus IAS-ECC v1.0.1 PKI card
Profile	IAS profile
Serial Number	9250010007119252224f
Maximum User PIN Length	16
Minimum User PIN Length	4
Maximum SO PIN Length	16
Minimum SO PIN Length	8
Free Card Memory (in Bytes)	65280

- **Middleware to allow usage of smartcards (badge) with HW certificates**
- Packaging of Win10 versions of middleware required for usage of hardware certificates
- Action taken over from Win10 project as additional scope due to inactivity.

VeraPDF

- **Client solution of PDF/A format checker to allow end users pre-checks.**
- Same solution is put in place in BFLOW PDF archiving workflow.

BFLOW

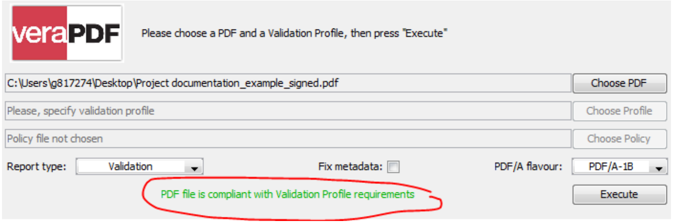
- **PDF/A archiving incl. format check with PDF check server solution**
- **Evidence records solution** by usage of Airbus commercial API (software as a service) to ensure long term preservation of digitally signed documents.
- AH/ACA solution already raised interest of ADS.

AIRINA: **Ai**rbus Enterprise **In**formation **Ar**chive (formerly ZAMIZ)

Implemenation of digital signature at Airbus Helicopters

Signature process & Tools

Verify PDF/A



veraPDF

Please choose a PDF and a Validation Profile, then press "Execute"

C:\Users\g817274\Desktop\Project documentation_example_signed.pdf | Choose PDF

Please, specify validation profile | Choose Profile

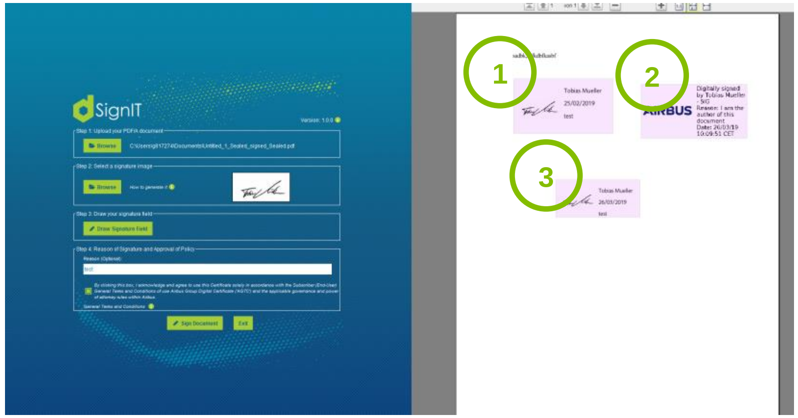
Policy file not chosen | Choose Policy

Report type: Validation | Fix metadata: □ | PDF/A flavour: PDF/A-1B

PDF file is compliant with Validation Profile requirements

Execute

Sign PDF/A



DSignIT

Version: 1.0.0

Step 1: Upload your PDF/A document

Browse | C:\Users\g817274\Documents\Untitled_1_Sealed_signed_Sealed.pdf

Step 2: Select a signature image

Browse | How to generate it

Step 3: Draw your signature field

Draw Signature Field

Step 4: Reason of Signature and Approval of Policy

Reason (Optional): test

☑ By clicking this box, I acknowledge and agree to use this Certificate solely in accordance with the Subscriber (End-User) General Terms and Conditions of use Airbus Group Digital Certificate (AGTC) and the applicable governance and power of attorney rules within Airbus

General Terms and Conditions

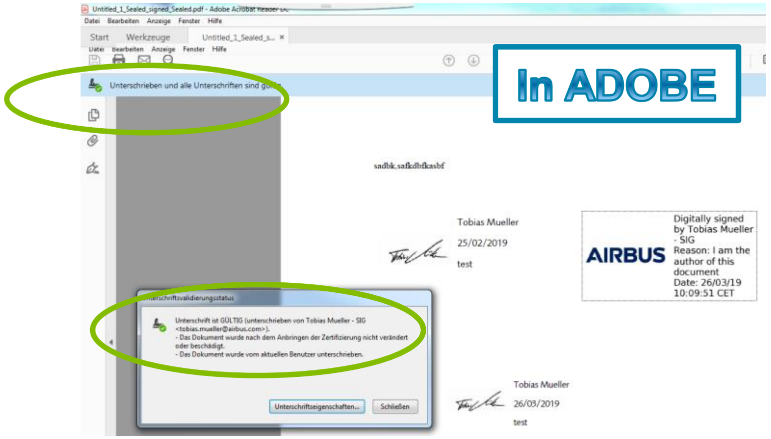
Sign Document | Exit

1
Tobias Mueller
25/02/2019
test
2
AIRBUS
Digitally signed by Tobias Mueller - SIG
Reason: I am the author of this document
Date: 26/03/19 10:09:51 CET
3
Tobias Mueller
26/03/2019
test

1. 1st Signature with DSignIT
2. 2nd signature with DSIG
3. 3rd signature with DSignIT

Adobe Acrobat Document

Verify signature



In ADOBE

Untitled_1_Sealed_signed_Sealed.pdf - Adobe Acrobat Reader DC

Datei Bearbeiten Anzeige Fenster Hilfe
Start Werkzeuge Untitled_1_Sealed_s... ×

Unterschrieben und alle Unterschriften sind gültig.

sadbk.safkdbfkasbf

Tobias Mueller
25/02/2019
test

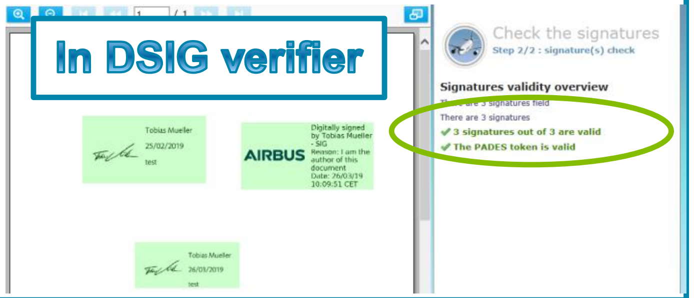
AIRBUS
Digitally signed by Tobias Mueller - SIG
Reason: I am the author of this document
Date: 26/03/19 10:09:51 CET

Unterschriftsvalidierungsstatus

Unterschrift ist GÜLTIG (unterschrieben von Tobias Mueller - SIG <tobias.mueller@airbus.com>).
- Das Dokument wurde nach dem Anbringen der Zertifizierung nicht verändert oder beschädigt.
- Das Dokument wurde vom aktuellen Benutzer unterschrieben.

Unterschriftseigenschaften... | Schließen

Tobias Mueller
26/03/2019
test



In DSIG verifier

Tobias Mueller
25/02/2019
test
AIRBUS
Digitally signed by Tobias Mueller - SIG
Reason: I am the author of this document
Date: 26/03/19 10:09:51 CET
Tobias Mueller
26/03/2019
test

Check the signatures
Step 2/2 : signature(s) check

Signatures validity overview

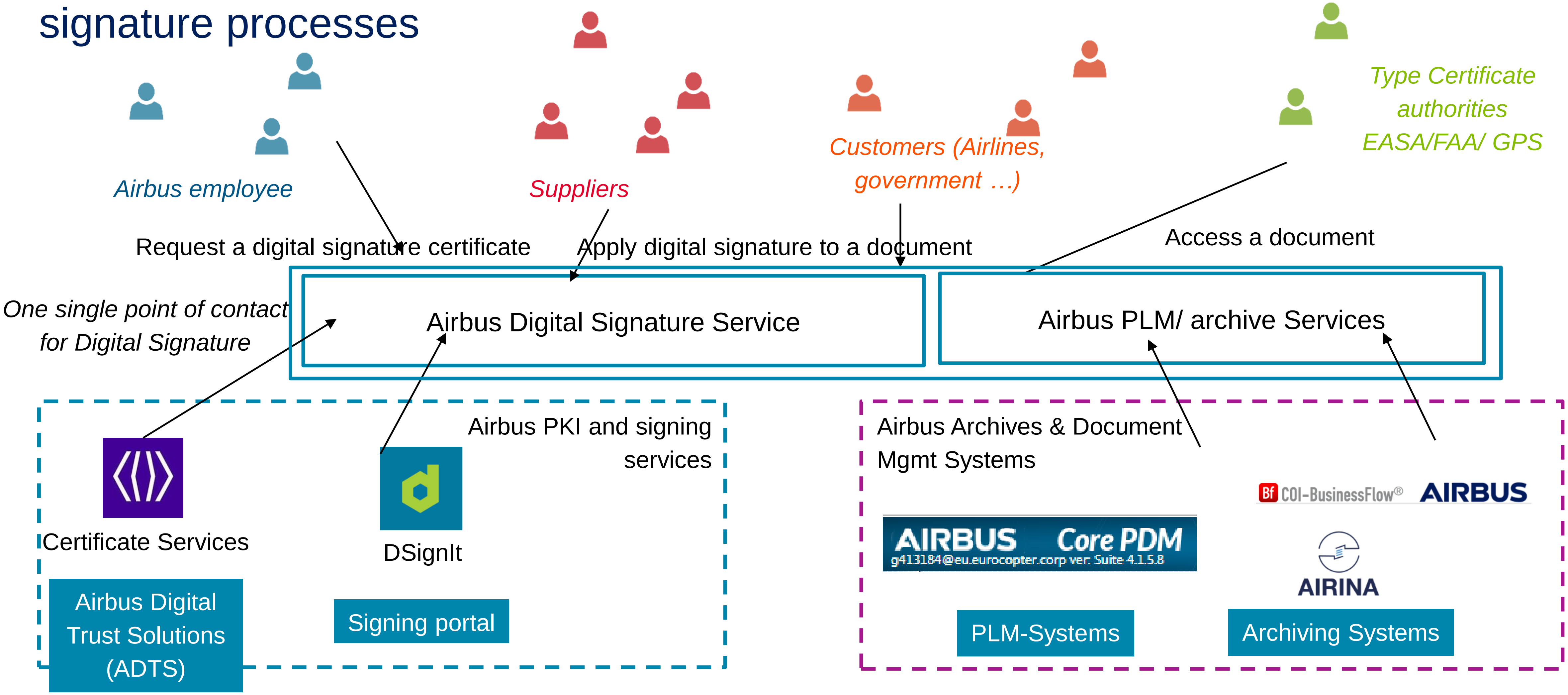
There are 3 signatures field

There are 3 signatures

✓ 3 signatures out of 3 are valid

✓ The PADES token is valid

A proposal how to include authorities, supplier and partners in digital signature processes



Airbus employee

Suppliers

Customers (Airlines, government …)

Type Certificate authorities EASA/FAA/ GPS

Request a digital signature certificate

Apply digital signature to a document

Access a document

One single point of contact for Digital Signature

Airbus Digital Signature Service

Airbus PLM/ archive Services

Airbus PKI and signing services

Certificate Services

DSignIt

Airbus Digital Trust Solutions (ADTS)

Signing portal

Airbus Archives & Document Mgmt Systems

PLM-Systems

Archiving Systems

AIRBUS Core PDM
g413184@eu.eurocopter.corp ver: Suite 4.1.5.8
Bf COI-BusinessFlow® AIRBUS
AIRINA

Outlook: from document management to model based engineering

- ***CAD***: ***Computer Aided Design***:
  The computer data model is a tool/mean for creating the delivery item document

- ***MBD: Model based Design***
  MBSE: Model based System Engineering
  The computer data model is the delivery item

- Process efficiency through continuous product model enrichment instead of document sharing and media breaks

On digital data models you can not sign wet anymore!

In the context of an Industry 4.0, the electronic signature is inevitable!

3D XML Player - [1]
1 element selected

Conclusion & Next steps

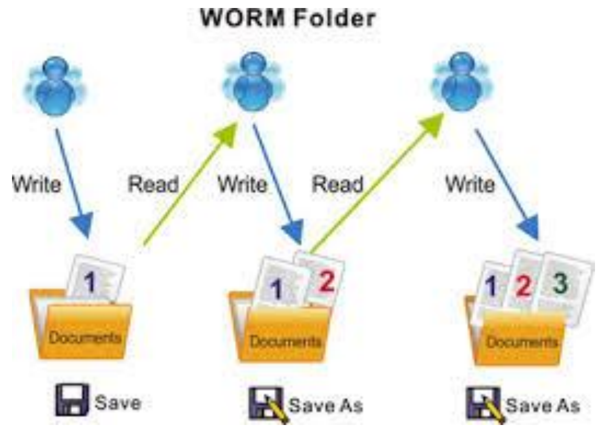
Conclusions from last BDLI working group meeting
All participants of the last BDLI working group meeting with LBA and GPS in August agreed that a very good basis for a common understanding to use the digital signature was created. The recommendation to apply the advanced electronic signature for documents with a high Level of trust in an industrial environment was supported by the participants.
The same applies to the approach, to categorize documents after the required trust level and the corresponding level of the electronic signature (electronic validation or advanced electronic Signature= digital signature).

Next steps
- LBA /GPS - Evaluation of the working group developed document list for the Development company with the appropriate stage of electronic signature
- BDLI-WG - Development of a catalog of requirements for the industry on the basis of the work results, if necessary as the basis for an EASA AMC to use the electronic signature / digital signature
- BDLI - Extension of work results on Documents of the manufacturing / maintenance company
- Alignement on this digital signature approach with AIQG and FAA

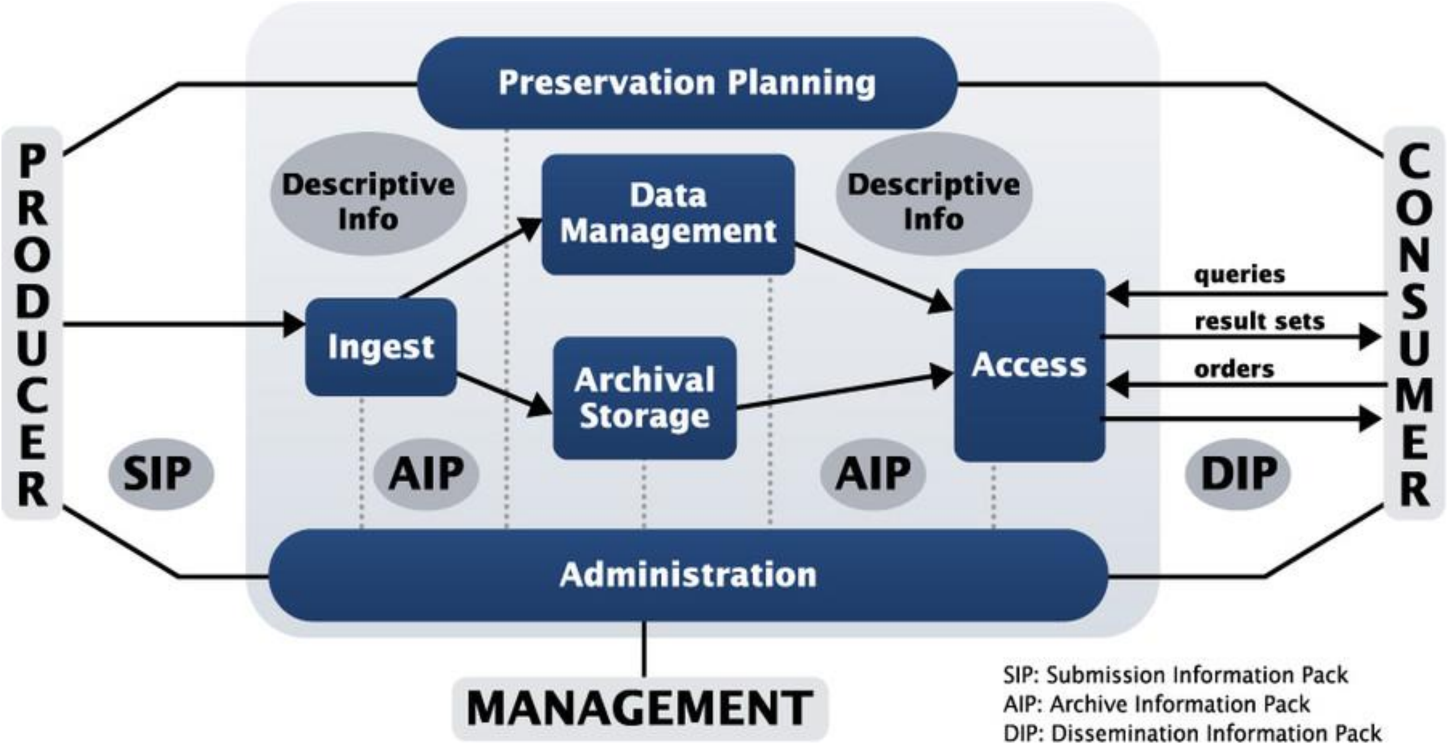
ANNEX

2. WORM & OAIS Referenzmodell für Archivsysteme

write once read many (WORM)
als technische Infrastruktur des Archivs



Offenes Archiv-Informations-System ist ein Referenzmodell für ein dynamisches, erweiterungsfähiges Archivinformationssystem und der ISO-Standard 14721



Das OAIS-Referenzmodell und WORM-Speicher, müssen firmenspezifisch umgesetzt werden

Thank you