Photo by Agence Olloweb on Unsplash

OctoberPDFest
ONLINE

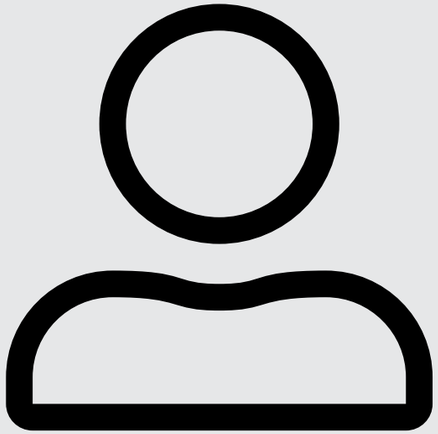
How to validate digitally signed PDFs correctly?

Validation can be a real challenge

Agenda

- What's validation?
- Signing and Validating PDFs
- Modifying Signed PDFs
- Necessary Post-Signing Modifications
- Caveats in Validation
- Summary

What's Validation?

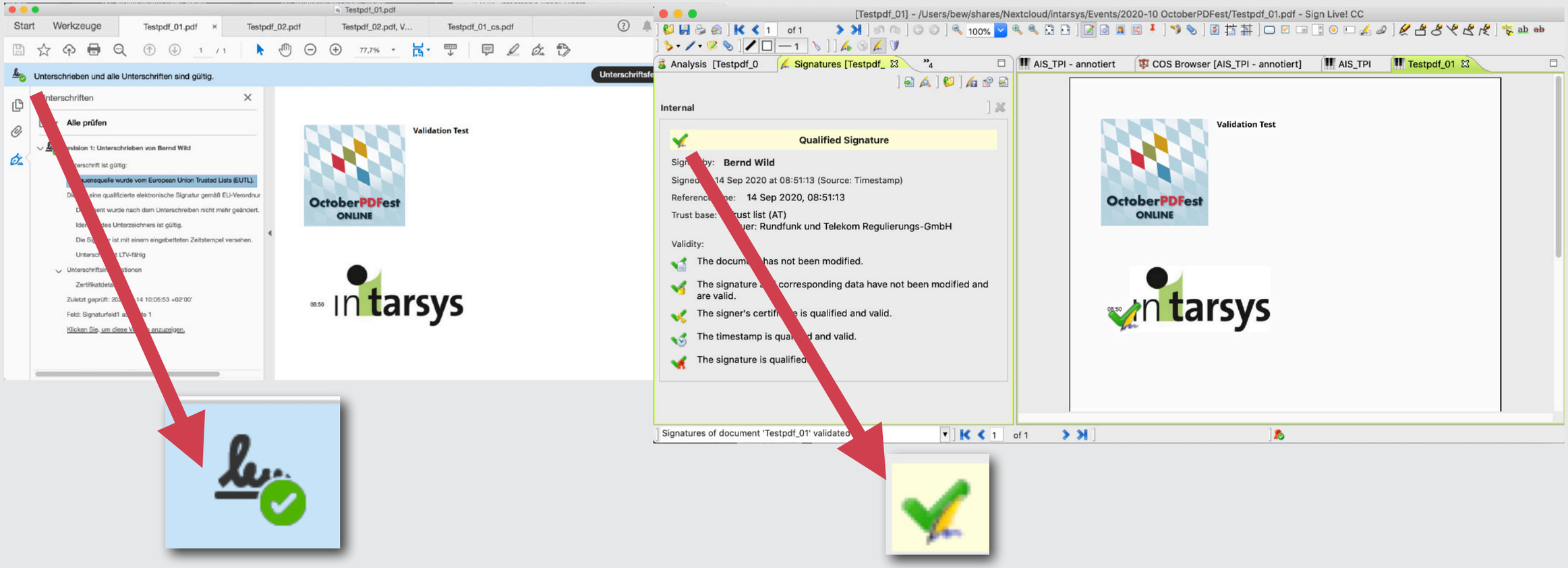


Proofing Identity of Signer

Proofing Integrity of Content

- More complex than signing
- Special Case PDF
  - Proofing identity is the same process than with other data or document types (e.g. CAdES, XAdES)
  - Proofing integrity can be a nightmare - due to flexibility and capabilities of PDF

What's Validation?



- User's Perspective: All what's necessary to get the „Green Checkmark"

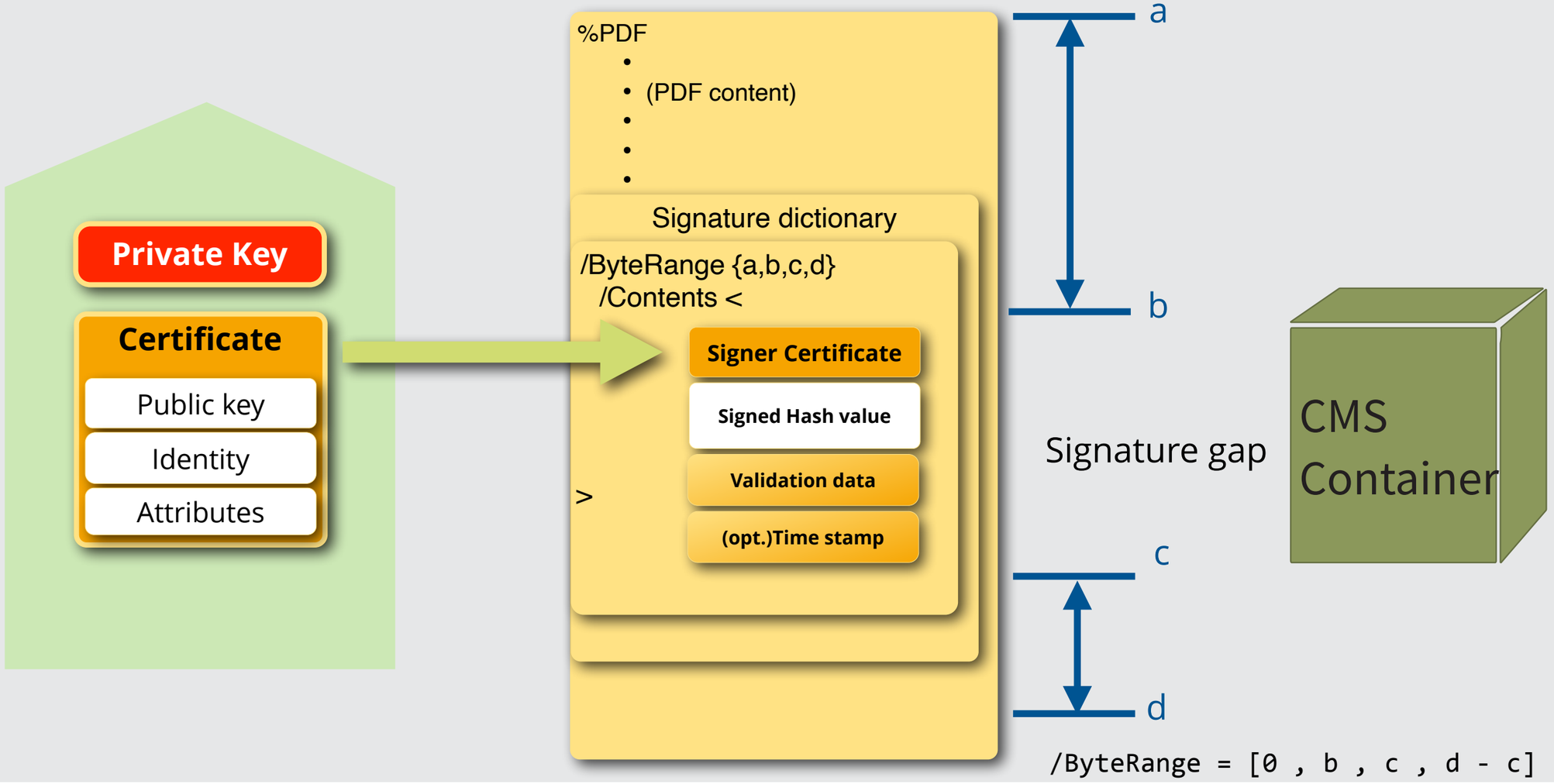
PDF and Signature Types

- **CertSig**: Certification or Author Signature
  - Special type for form-based workflows
  - Whole document
  - If used must be the first signature in the document
  - Allows to restrict post-signing modifications
- **AppSig**: Approval Signature
  - „Standard“ signature
  - Whole document
  - Allows post-signing Markup Annotations
  - Like CertSig but no restrictions
  - Can be applied multiple times

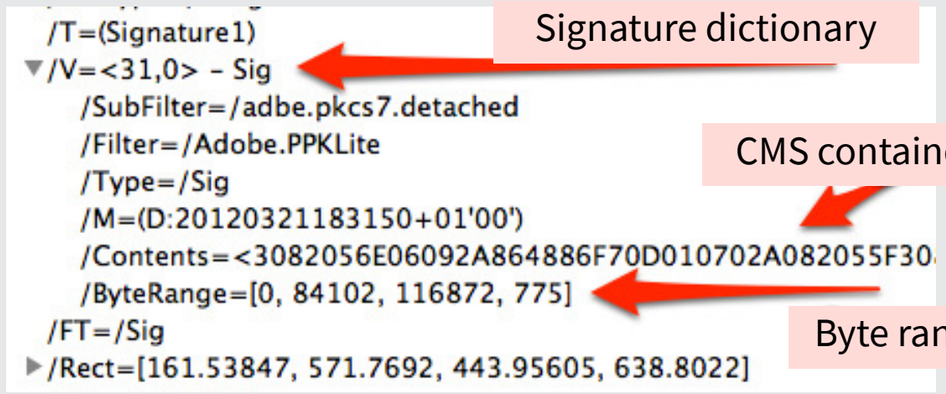
Standards for PDF-Signing/Validation

- Signature
  - ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
  - ETSI EN 319 142-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
  - ETSI TS 119 142-3 V1.1.1 (2016-12) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
  - ISO 32000-1 and ISO 32000-2
- Validation
  - ETSI TS 119 102-1 V1.2.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
  - ETSI TS 119 102-2 V1.2.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
  - ISO 32000-1 and ISO 32000-2

Signing of a PDF Document



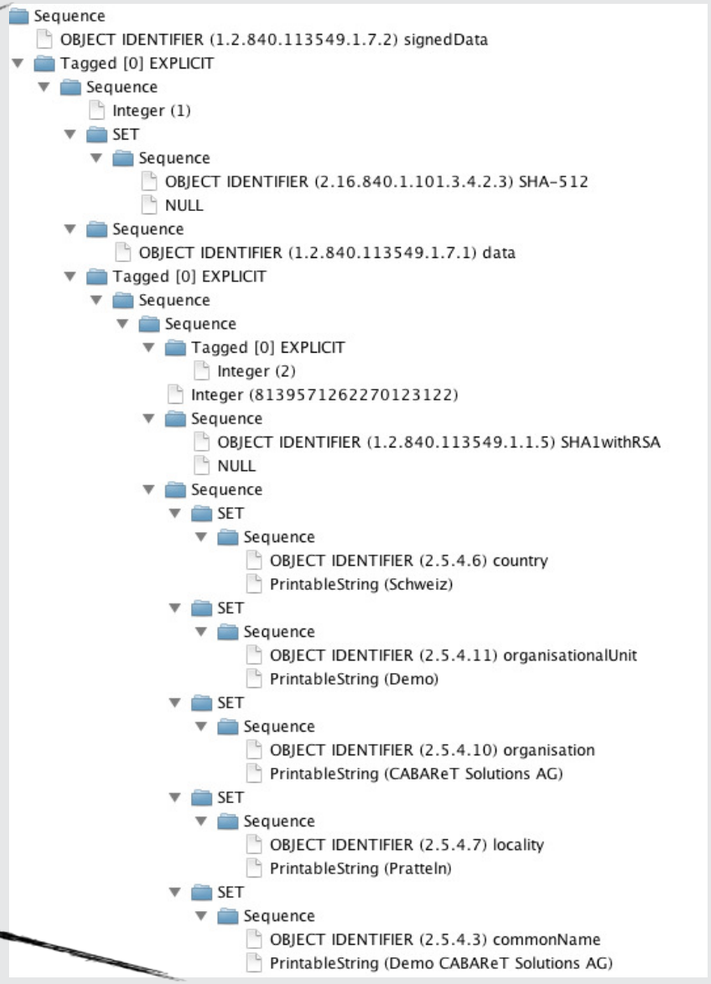
Embedding of the Signature



The remaining gap is filled up with zeros

Embedding of the Signature

ASN.1 encoded data structures



The Byte Range

- Every signature has a related byte range
  - `/ByteRange [start1_byte,no_of_bytes1,start2_byte,no_of_bytes2]`
  - The gap is `start2_byte - (start1_byte + no_of_bytes1)` wide
- No object based signatures (historical feature till PDF 1.6)
- Is part of the signed area

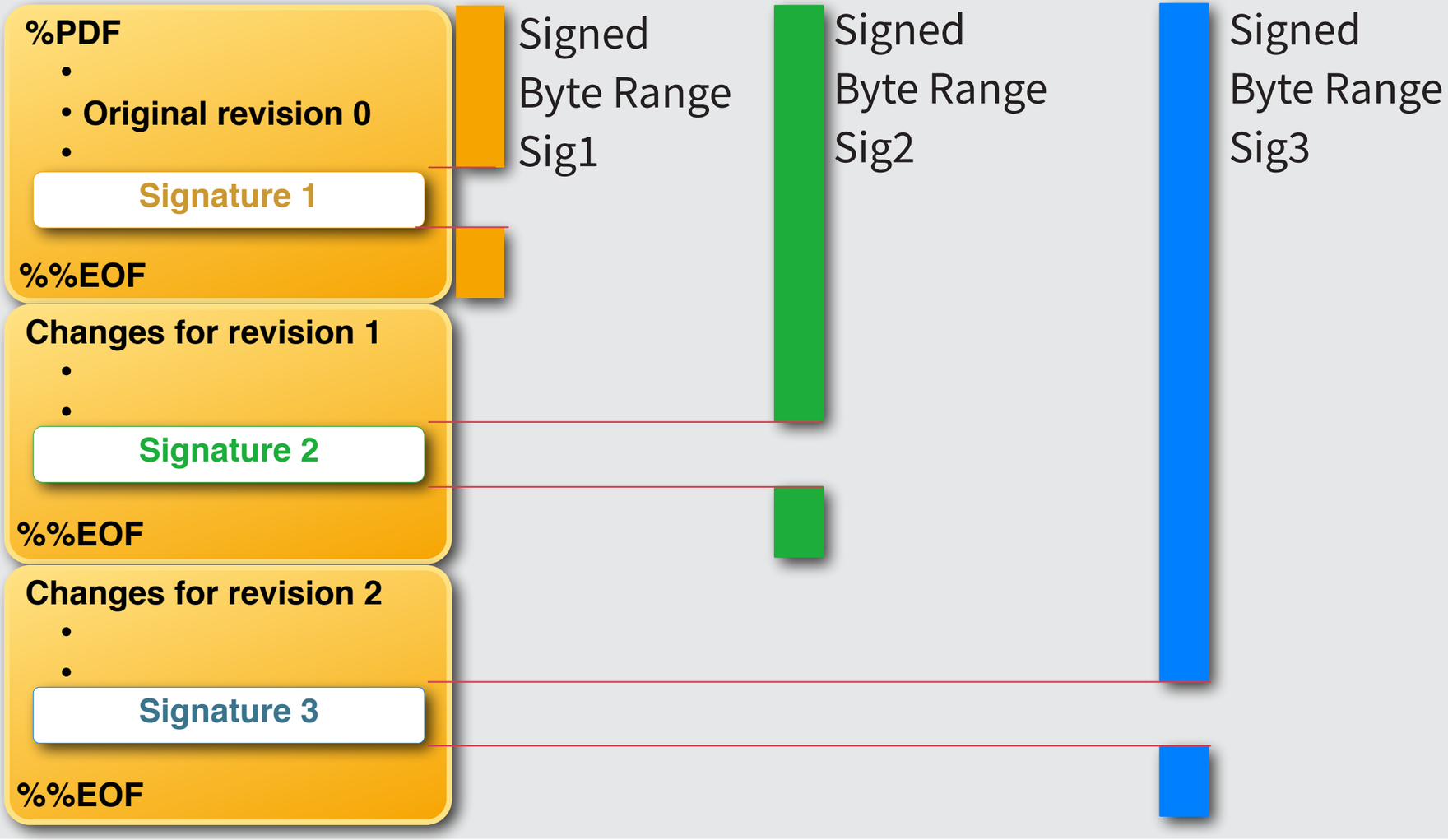
Signer Identity Validation

- Read the CMS structure
- CMS >> signer certificate
  - Read signer certificate
  - Find issuer of certificate
    - Look for validation information URL of certificate issuer
      - Either via CRL >> download CRL from URL
      - Or OCSP >> request OCSP information from URL
      - Or read embedded validation informationen if present (e.g. LTV signatures)
  - Repeat the last step until you reach a Root Certificate which
    - is Member of a public Trusted List (national eIDAS TSL, EU LOTL, AATL)
    - Or is marked „Trusted“
    - Or is „not known“

Signer Identity Validation II

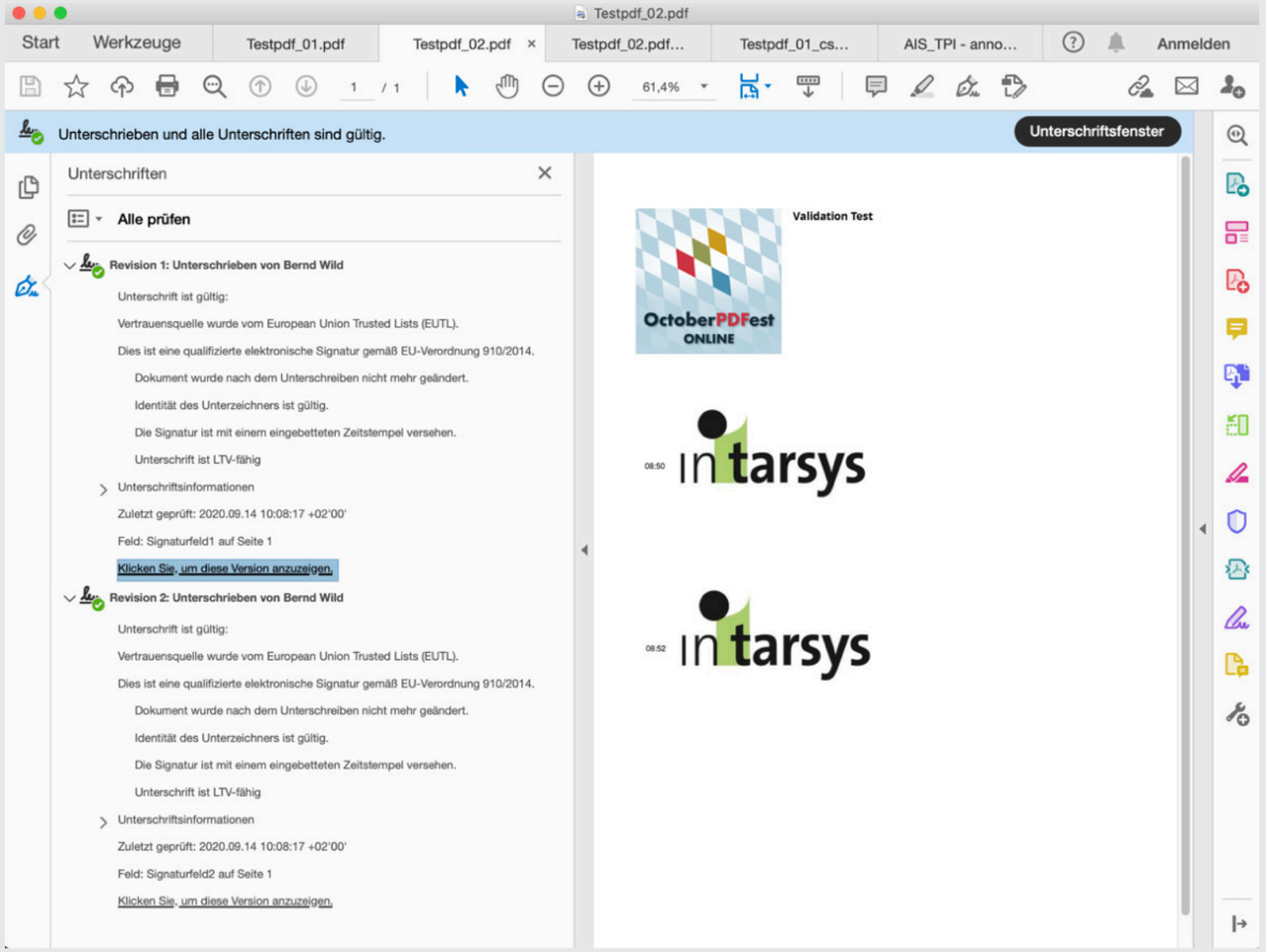
- Search for an AcroForm field with field type `/Sig`
- Locate dictionary key `/V`
- Derive `/ByteRange [A,B,C,D]`
  - Read all bytes of the PDF file according to the byte range
    From A ➔ A + B & From C ➔ C + D
- Derive `/Contents`
  - Read signature Container (typically CMS/PKCS#7 Container, other formats like PKCS#1 or RFC3161 as well)
  - Interpret the signature container concerning Digest (Signed Hash) and used Hash Algorithm
- Calculate Hash with indicated Hash Algorithm
- Decrypt Signed Hash using Public Key of Signer
- Compare both Hash Values

Serial Signatures

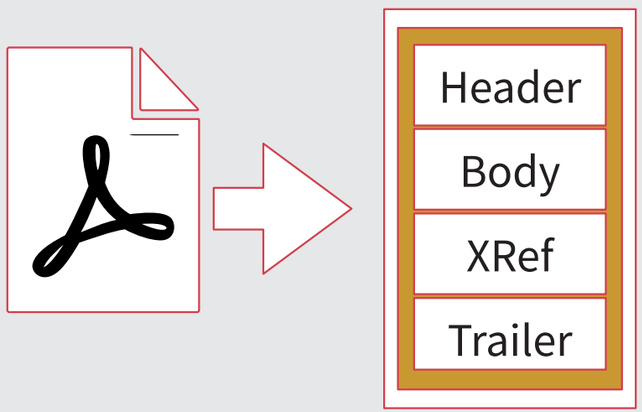


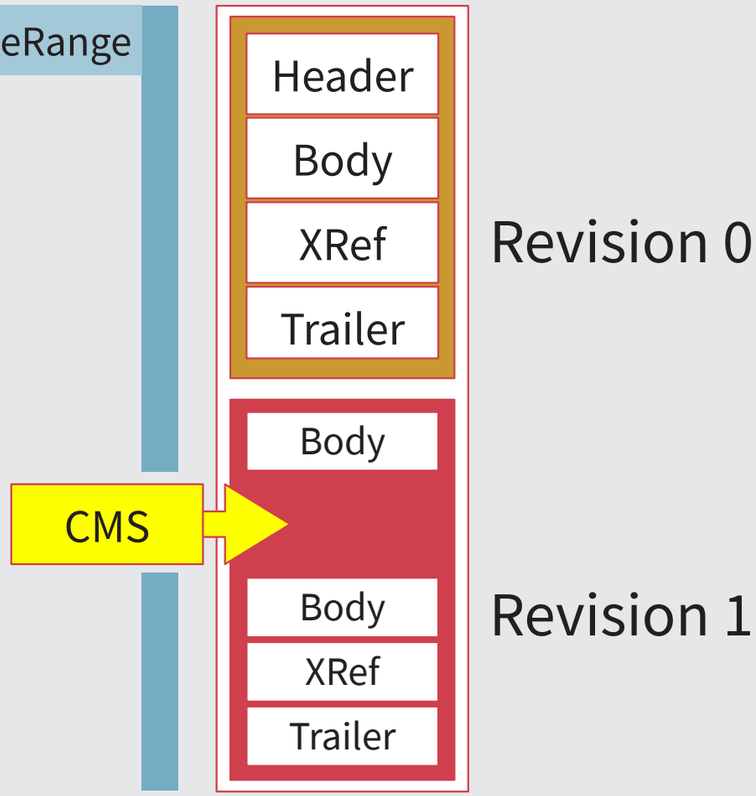
Serial Signatures

- Serial signatures are detected automatically



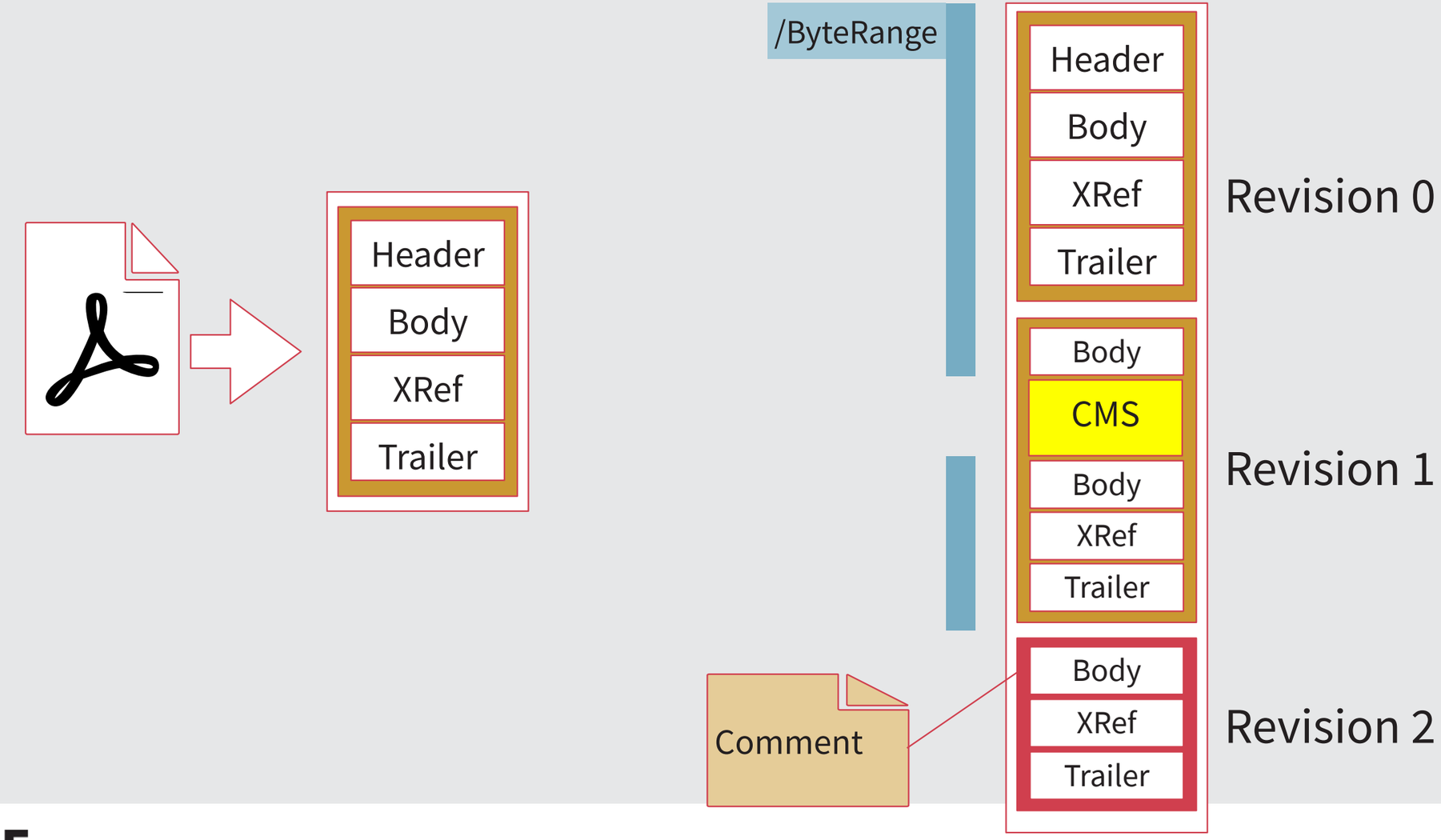
How it’s Really Done …





Signing the PDF

… and how Annotations are added.

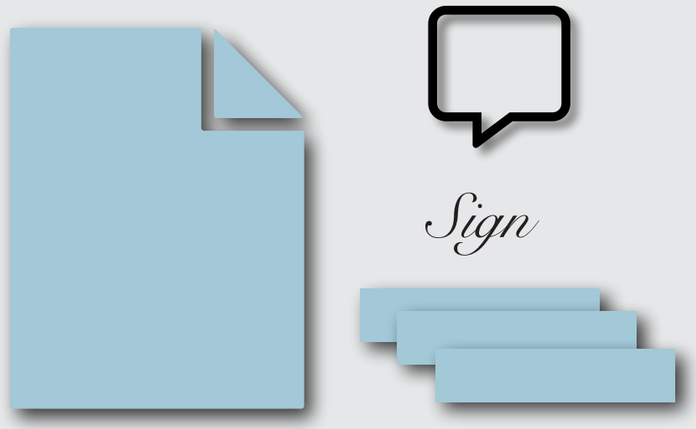


Annotations

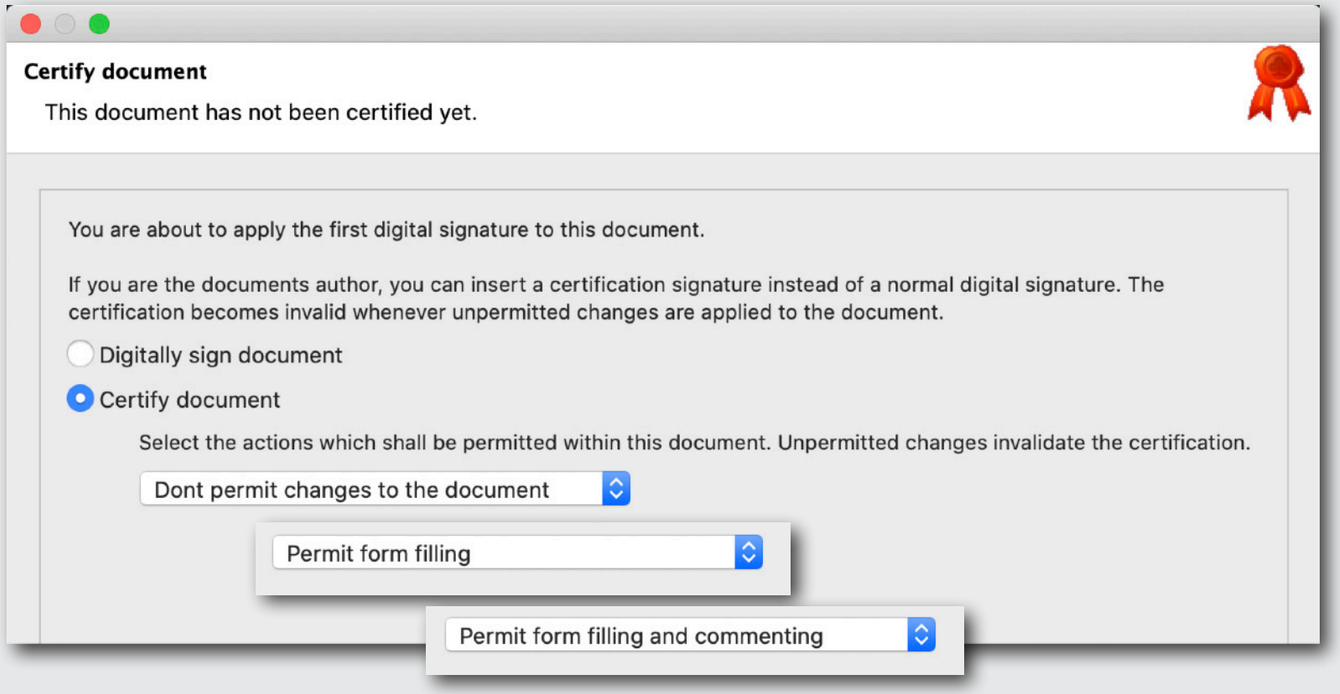
- From ISO32000-1
  - „PDF supports the ability to add incremental updates (ISO 32000-1 [i.1], clause 7.5.6) to the end of the document representing new or changed objects. If the printable representation is placed in an incremental update section, it will not invalidate the hash of the document's signature. However, the way in which the printable representation is added to the visible page content will impact the validation status displayed by a conforming ISO 32000-1 [i.1] reader. „
  - „When adding the representation as standard page content, a conforming reader will identify the document as changed as the actual page content has been modified and so **it is no longer what was actually signed**. **However, the use of annotations (ISO 32000-1 [i.1], clause 12.5) to add additional information on a top layer of information does not invalidate the signature.** Therefore the use of annotations is strongly recommend in a workflow involved embedded signatures. „
- ETSI SR 003 232 V1.1.1 (2011-02) Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES); Printable Representations of Electronic Signatures

Certification Signature

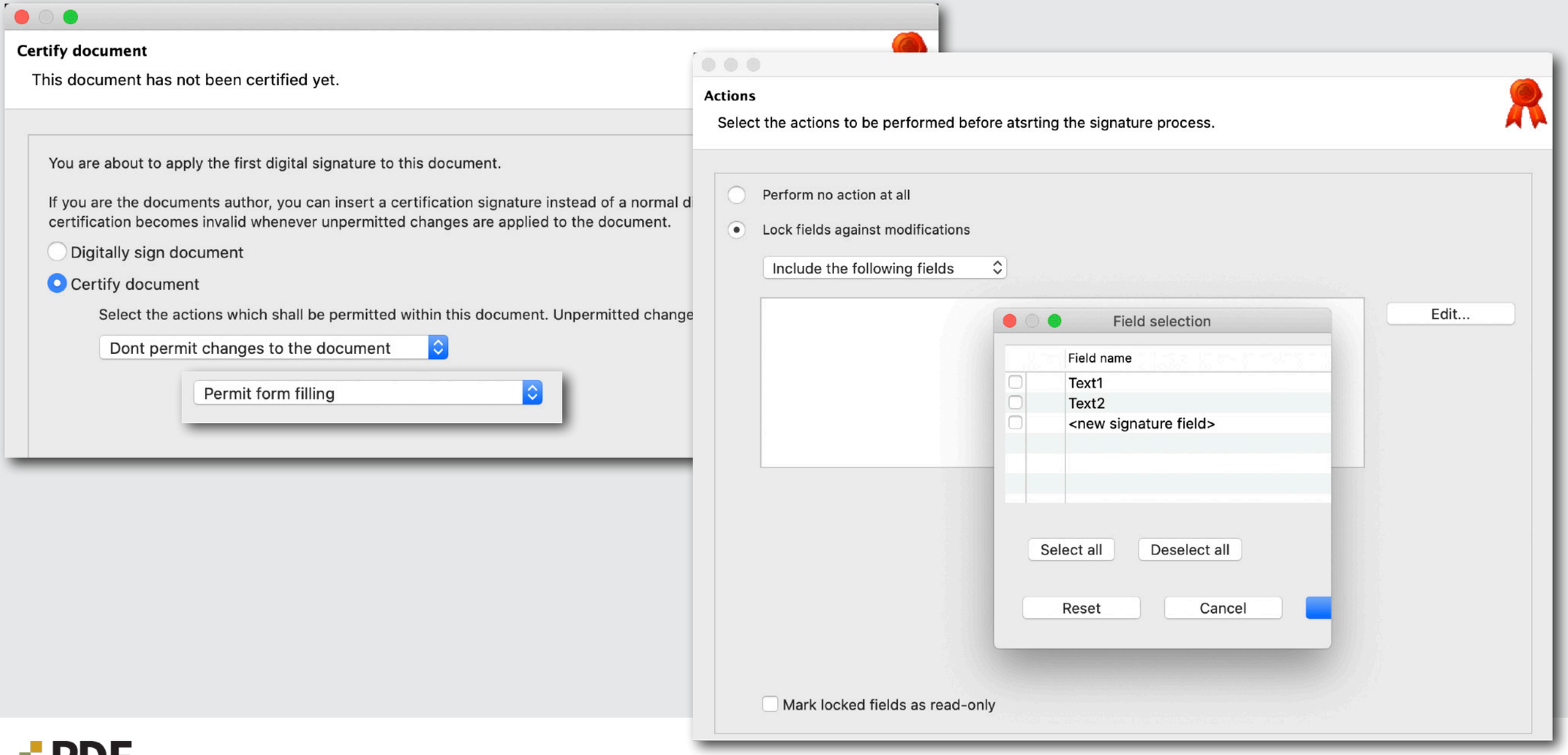
- Introduces 2 new dictionaries
  - DocMDP
    - Controls serial signing, field changes and annotations
  - FIELDMDP
    - Contains list of non-modifiable fields



Certification Signature



Certification Signature



Modification Analysis

- Actually there's no clear specification, what are „good" modifications and what are „bad" ones
- Adobe sets the „de facto" standard —> „calibration scale"
- During PDF development this was a evolutionary process
- Heuristic approach

Field_1: Modified

Field_1: Modified

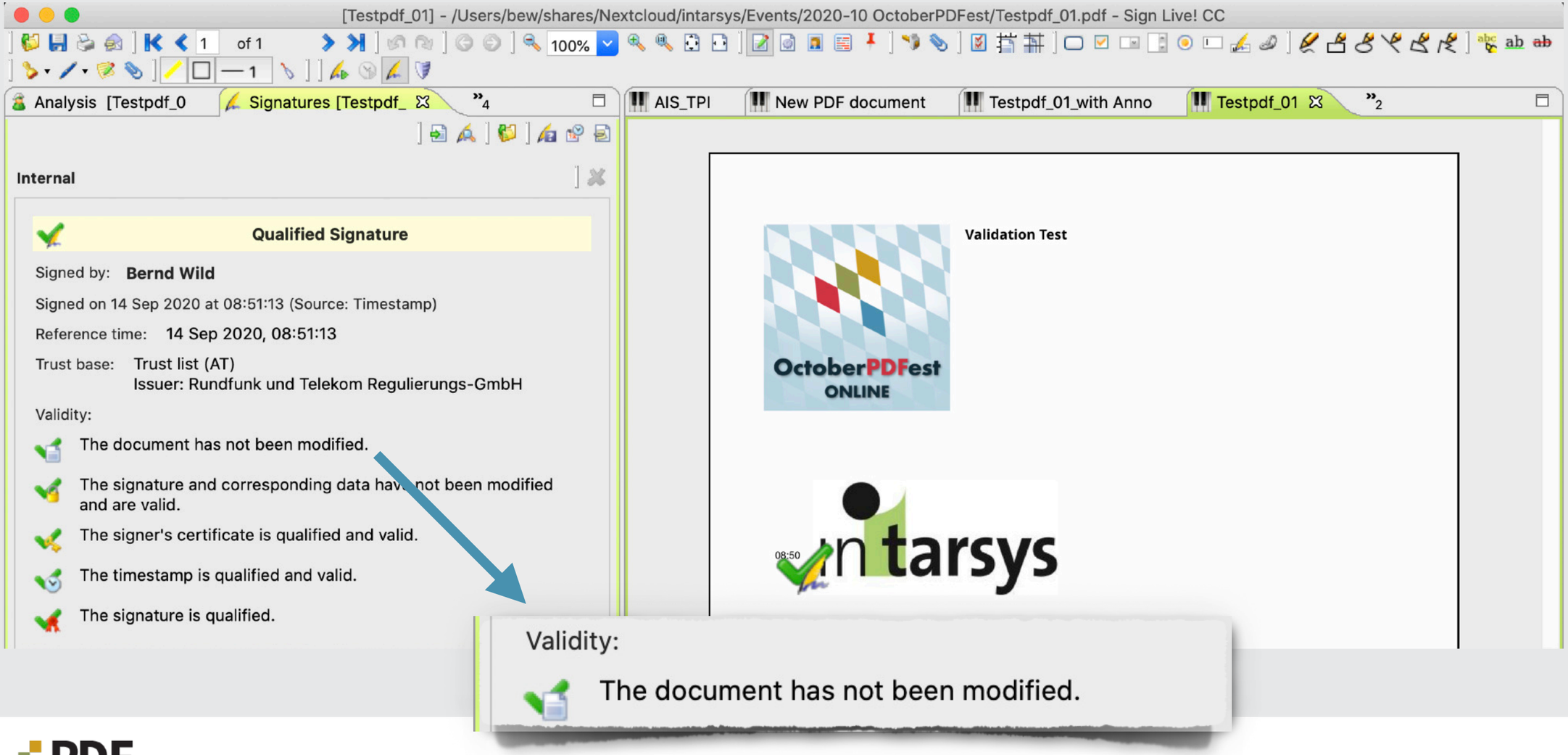
Modification Analysis

- Determine the number of revisions *n*
- Take revision *i* if signature is in revision *I - 1*
- Check all MarkUp annotations (text marking, comments, graphical notes)
- Check page object modifications
- Check updates in XREF table
- Finally check against restrictions of certification signature (if present)

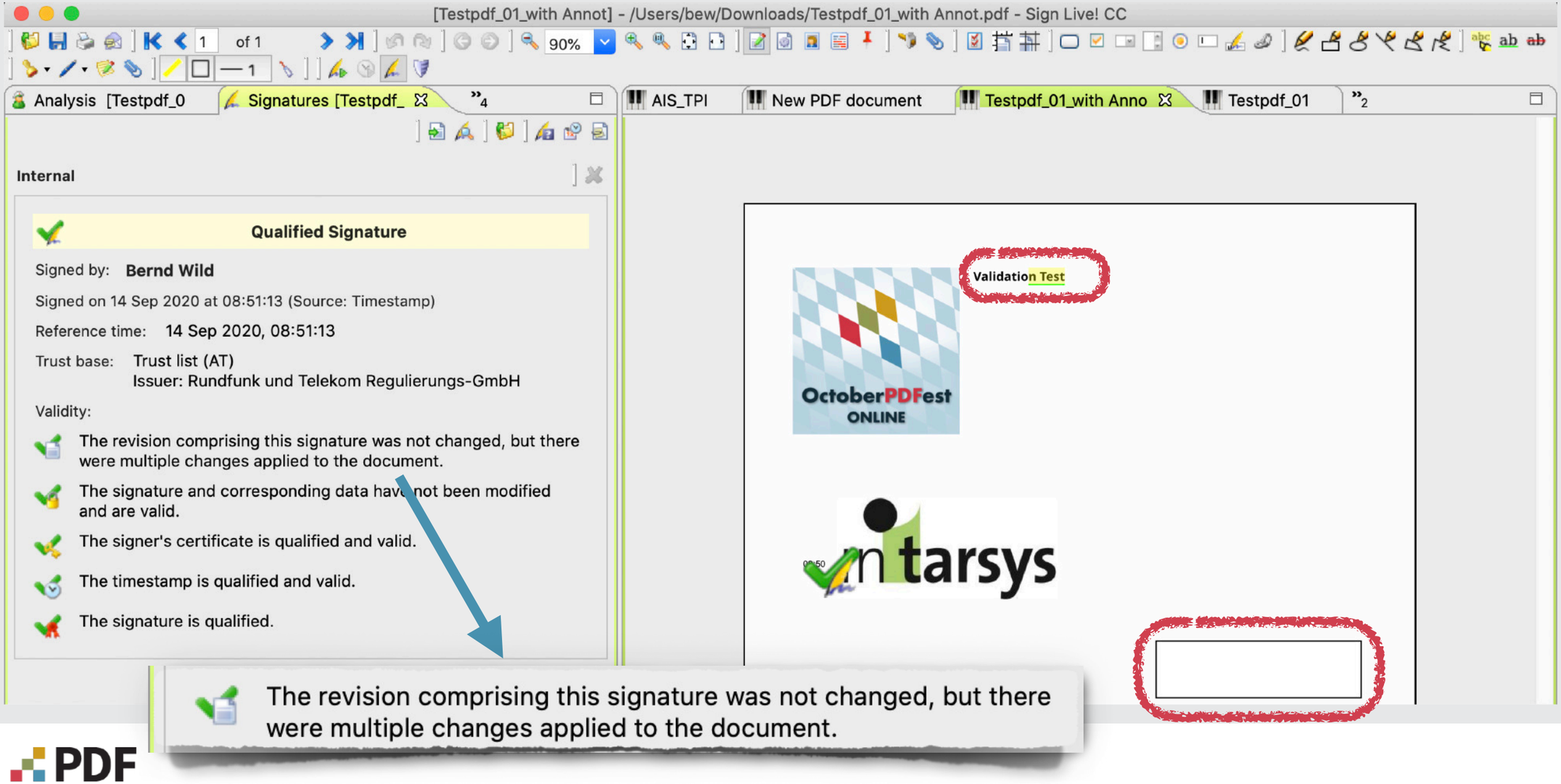
Field_1: Modified

Field_1: Modified

Post-Signing Modifications



Post-Signing Modifications



The DSS and the VRI Dictionary

- Document Security Store /DSS
  From EN319142-1 „*… a single place where all of the validation-related information for some or all signatures in the document should be placed.*“
- Validation-Related Information /VRI
  From EN319142-1 „*… shall contain validation-related information (VRI) for a specific signature in the document…*“

PAdES-B-LT

- Requires a Document Security Store /DSS
- Contains all informations necessary to validate a PDF signature offline
  - Certificate chains
  - OCSP responses
  - CRLs
- Should be written before signature applies
- Problem: for short-term certificates („ad-hoc certificates“) there are no CRL or OCSP responses before the signing —> transient

```
20 0 obj
<<
/Pages 3 0 R
/Type /Catalog
/Version /1.7
/Perms 43 0 R
/DSS 49 0 R
/AcroForm 26 0 R
/Extensions <<
/Type /Extensions
/ESIC <<
/Type /DeveloperExtensions
/BaseVersion /1.7
/ExtensionLevel 5
>>
```

```
49 0 obj
<<
/Certs 56 0 R
/Type /DSS
/CRLs 50 0 R
/OCSPs 53 0 R
>>
endobj
```

Example from a PAdES-B-LT signed PDF

PAdES-B-LT

- Via incremental update (—> new revision) a DSS can be appended after the signature happened
- „Validation Augmentation“ —> make signed documents longterm validatable
- Can be done in a batch process

The Shadow Attack

- Refer to https://www.pdf-insecurity.org/ (July 2020)
- The post-signing modification allowance can be misused to obfuscate the visual state of the document the signer originally signed
- Usage of the incremental update feature
- Most test documents don’t comply with basic PDF rules and standards
  - BUT: the tools are too indulgent and try to correct the buggy PDF without user feedback
- May a validator decide whether a visual annotation may compromise the signed content?

Summary - Actual Work on Standardization

- ETSI works on clarifications and specifications on how PDF Signature validation can be made more „comprehensible“ and „usable“
  - TS 119 102-3-1: Work on Extended Validation Procedures: Introduction and General Problems
    - how the “visual” content might change, even if the signed bytes are the same
  - TS 119 102-3-2: Work on Extended Validation Procedures: PAdES
    - Classifying what are allowed and what are non-allowed changes? What visual changes can be introduced by allowed updates like signatures/timestamps /adding DSS directory
  - Target: Common rules which can also be referenced by ISO
  - Timeline: Expected Release in 2021

Intarsys

Dr. Bernd Wild
intarsys AG
Kriegsstrasse 100
76133 Karlsruhe
bwild@intarsys.de
www.intarsys.de
+49 721-38479-0

- Member of the Board of PDF Association
- Chair of TWG Digital Signatures

- ***Sign Live!*** **software for Electronic Signature (covering the whole range from biometric to qualified electronic signatures)**
- **Personal, Batch and Mass Signing**
- **Support for Smartcards, Cryptotokens and HSMs**
- **Certified signature kernel (Common Criteria EAL3+)**
- **Cloud-based Signature Platform „Sign Live! Cloud suite gears“ for signing and validation**
- **Encryption and authentication**
- **Founding Member of Cloud Signature Consortium**
- **PDF/A validation and correction**

Sign Live!

Sign anywhere and as you like!

intarsys

Facts and Figures

17 longtime employees

More than **1.100** customers from various industries

More than **40** partners

More than **5 Mio.** signatures per month

More than **5 Mio.** validations per month

18 European trust service providers

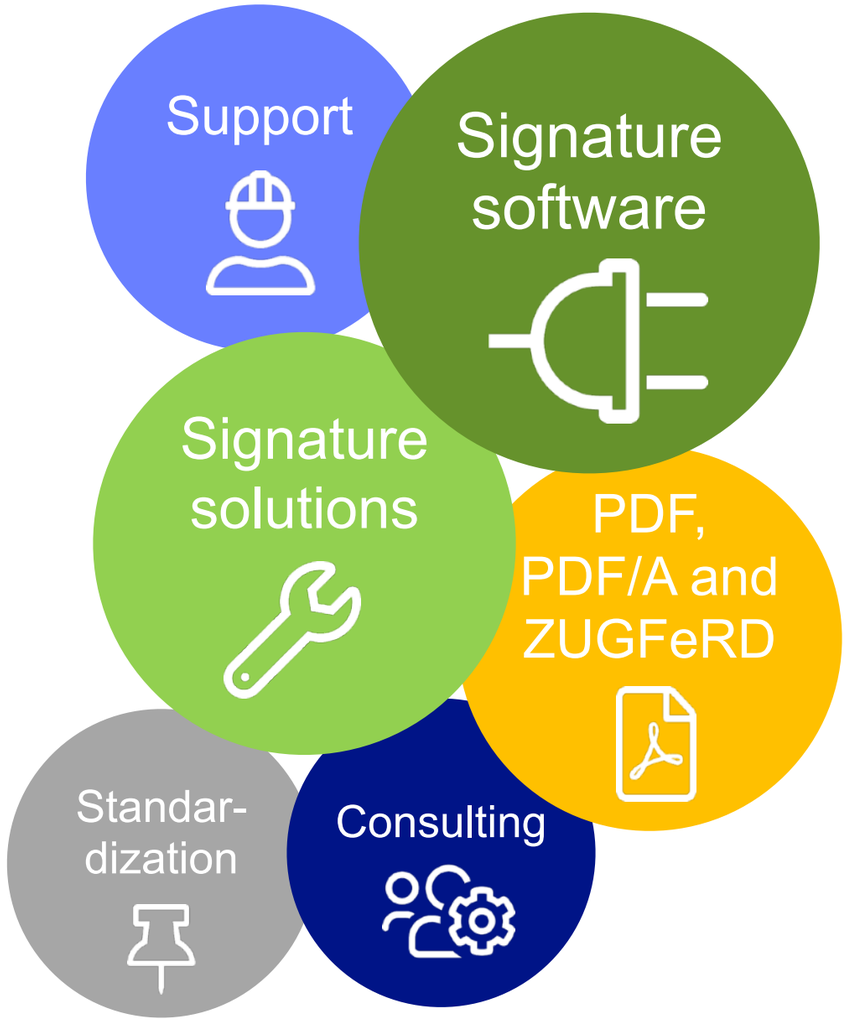
intarsys AG - founded in 1996

Location: DE-76133 Karlsruhe

Technology leader for software for creation and validation of local and remote signatures, local and remote seals and timestamps compliant to eIDAS and PDF/A for longterm archiving.

Easy and fast on-premise installations and/or integration of our software at the customer's site.

We support customers 360° with extensive know-how and corresponding competence and offer them solutions from one source.



BITKOM · CLOUD SIGNATURE CONSORTIUM · ETSI · PDF association · FeRD Forum elektronische Rechnung Deutschland

Trust Services by eIDAS

eIDAS

Electronic Identification

- Electronic identification systems and means

Trust Services

- Electronic Signature / Remote Signature
- Electronic Seal / Remote Seal
- Electronic Timestamp
- Preservation Services
- Electronic Trusted Email Services
- Web site authentication

Secure signing

Secure validating

Secure preserving

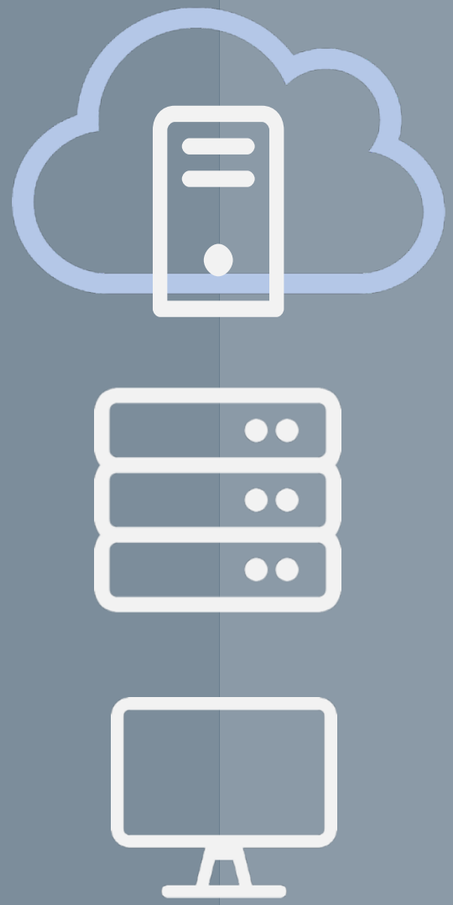
Some of Our Customers

CHERRY
REINERSCT
dgnservice
medisign
swisscom
swiss sign
Ein Unternehmen der Schweizerischen Post
BUNDESDRUCKEREI
eurodata
AOK Die Gesundheitskasse
Helaba Invest
CABARET
dvbern
FACHVERLAG Jüngling-gbb
ELO Digital Office
Q-SOFT
d.velop
SEALSYSTEMS THE DIGITAL PAPER FACTORY
windream.
D·M·I
ELEKTA
BITMARCK®
Fraunhofer SIT
SEEBURGER BUSINESS INTEGRATION
Giesecke & Devrient
T··Systems·
abraxas
paperless group
Deutsche Post DHL
GS1
INFOMA® Software Consulting GmbH
DDG Deutsches Dienstleistungszentrum für das Gesundheitswesen GmbH
i-SOLUTIONS HEALTH
BECHTLE
compart

Signing with Sign Live!

Signatur - Seal - Timestamps

For Continuous Digital Processes



Remote Signature and Seal

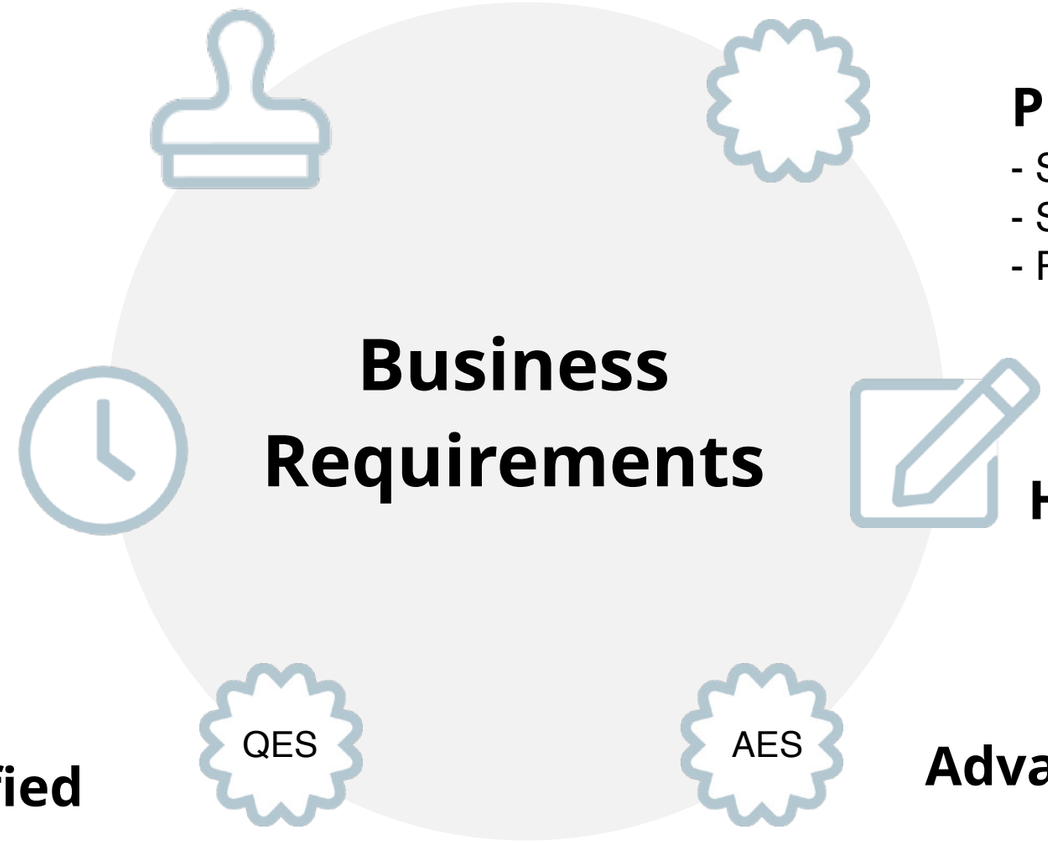
Local Signature and Seal

Local and remote Timestamps

Sign As You like!

SEAL
- Smartcard
- HSM
- Remote Signing Service

TIMESTAMP
- Local simestamp server
- Remote timestamp service



PERSONAL SIGNATURE
- Soft certificate
- Smartcard
- Remote Signing Service

Handwritten signature

Qualified

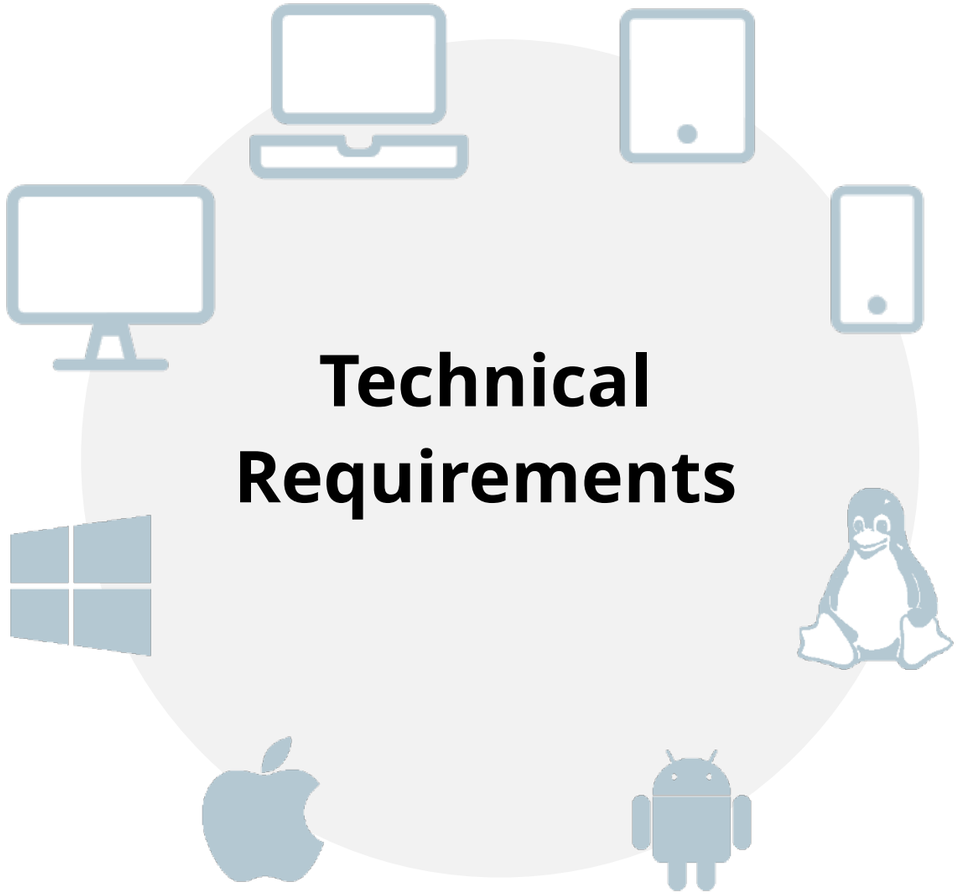
Advanced

Sign As You like!

No App or software plug-in

No rollout, no administration of local software

No „**upload**“ of documents to the cloud
The documents never leave your realm



Desktop and **mobile** devices with web browsers

Trusted Viewer for document preview

On-premise „**inhouse**“ server application

Hash Value Signature

Remote Signature with Sign Live! CSG Cloud Suite Gears