PDF working together!

PDF Days Europe 2022

Making digital signatures in PDF more usable

About User Experiences And Pitfalls

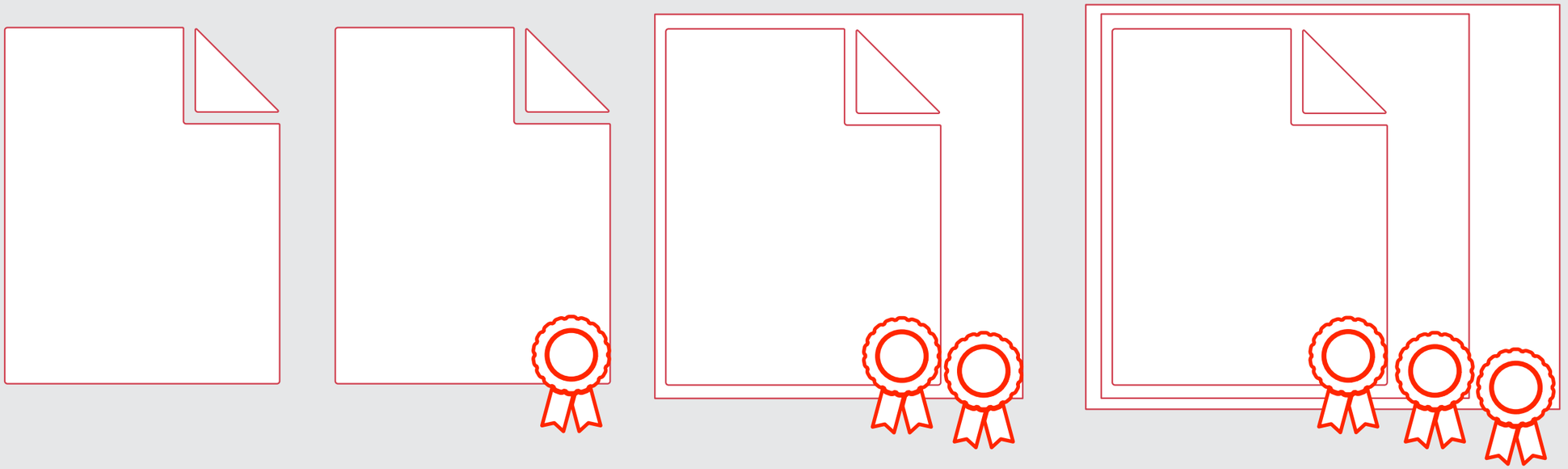
Agenda

- State of Play in digital signing of PDF
- Is this enough or what's on the wish list?
- Some proposals from the community
- Work at ETSI ESI and Cloud Signature Consortium
- If tomorrow was Christmas what would I wish for
- Summary

State of Play in Digital Signing of PDF

working together! PDF

PDF Days Europe 2022



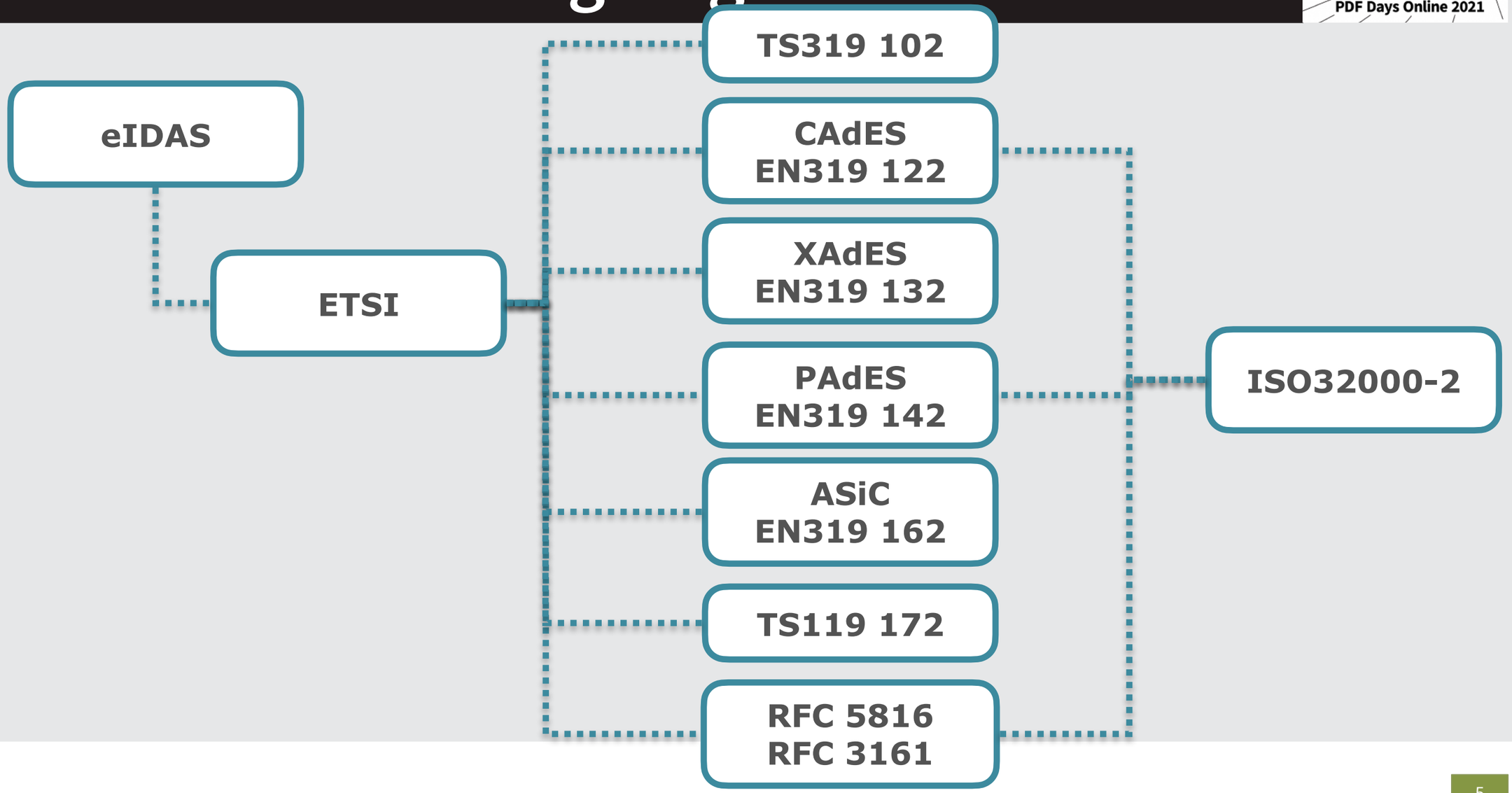
ISO 32000-1 + RFCs

ISO 32000-2 + ETSI CADeS/PADeS

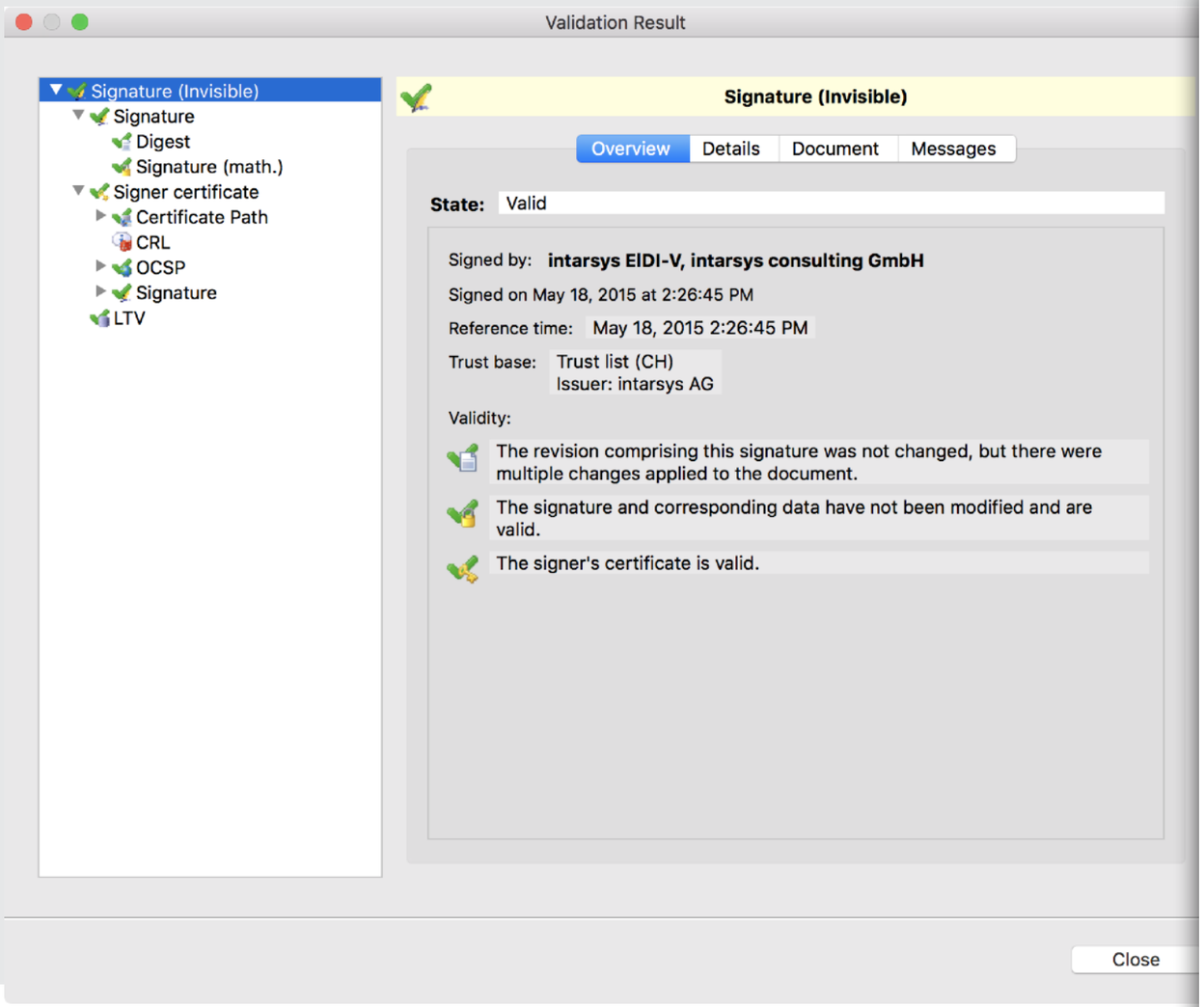
Some ETSI Standards for Creation and Validation

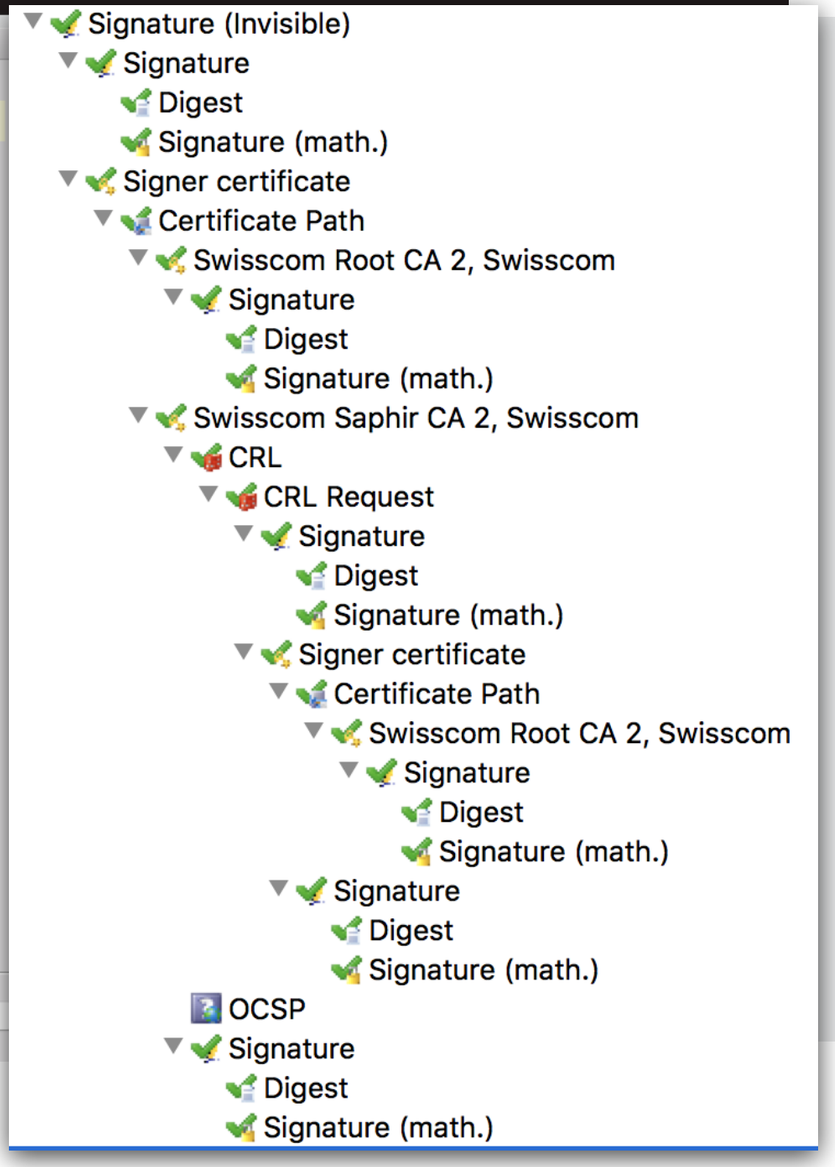
- **TS 319 102-1** Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- **EN 319 122-1** CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
- **EN 319 122-2** CAdES digital signatures; Part 2: Extended CAdES signatures
- **TS 319 122-3** CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) in CAdES
- **EN 319 132-1** XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
- **EN 319 132-2** XAdES digital signatures; Part 2: Extended XAdES signatures
- **EN 319 142-1** PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- **EN 319 142-2** PAdES digital signatures; Part 2: Extended PAdES signatures
- **EN 319 142-3** PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- **EN 319 162-1** Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers
- **EN 319 162-2** Associated Signature Containers (ASiC); Part 2: Other ASiC containers
- **TS 119 172-1** Signature policies; Part 1: Framework

ISO 32000-2 and Signing Standards

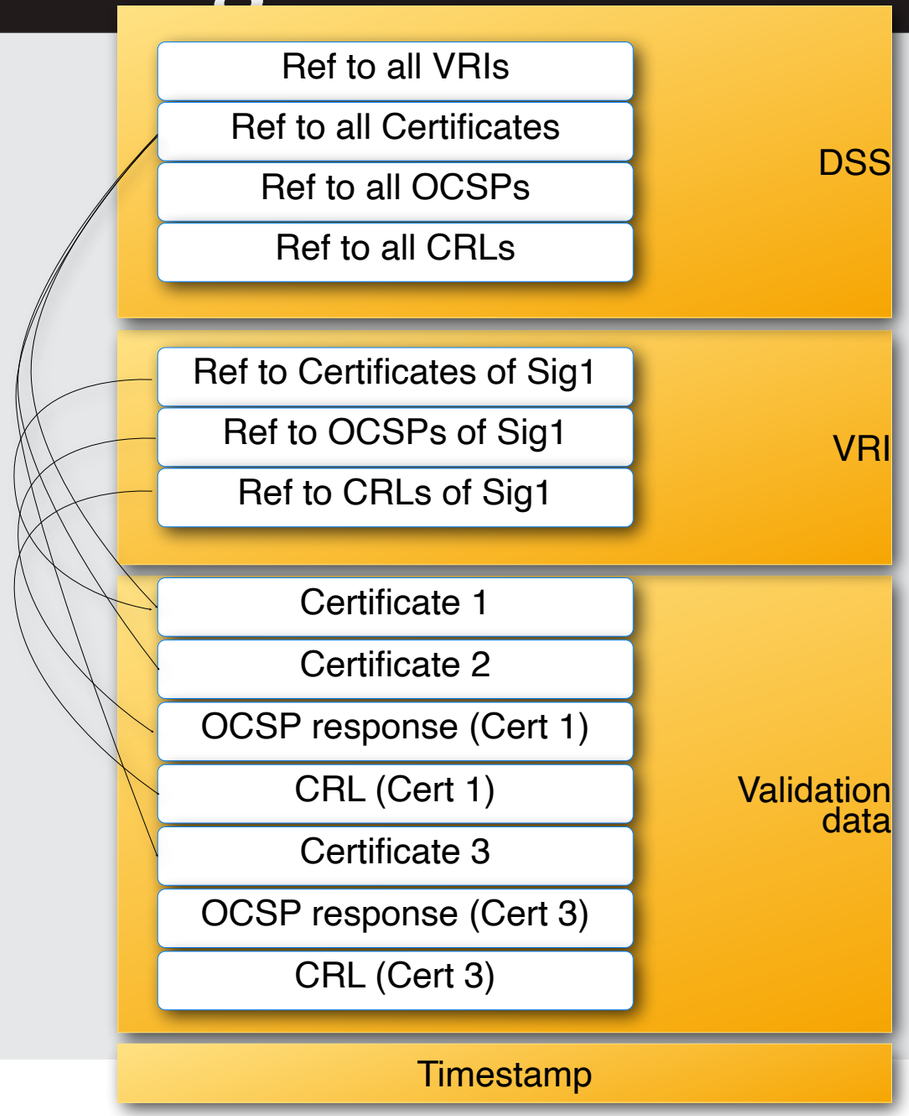


PAdES-LTV


Validation Result
Signature (Invisible)
Signature
Digest
Signature (math.)
Signer certificate
Certificate Path
CRL
OCSP
Signature
LTV
Signature (Invisible)
Overview
Details
Document
Messages
State: Valid
Signed by: intarsys EIDI-V, intarsys consulting GmbH
Signed on May 18, 2015 at 2:26:45 PM
Reference time: May 18, 2015 2:26:45 PM
Trust base: Trust list (CH)
Issuer: intarsys AG
Validity:
The revision comprising this signature was not changed, but there were multiple changes applied to the document.
The signature and corresponding data have not been modified and are valid.
The signer's certificate is valid.
Close


Signature (Invisible)
Signature
Digest
Signature (math.)
Signer certificate
Certificate Path
Swisscom Root CA 2, Swisscom
Signature
Digest
Signature (math.)
Swisscom Saphir CA 2, Swisscom
CRL
CRL Request
Signature
Digest
Signature (math.)
Signer certificate
Certificate Path
Swisscom Root CA 2, Swisscom
Signature
Digest
Signature (math.)
Signature
Digest
Signature (math.)
OCSP
Signature
Digest
Signature (math.)

PAdES Long Term – PAdES-LTA



- **Repeated signature process**
- **No modification of present signatures**
- **PDF document sizes grows with every signature process**
- **Self-contained document**
- **can be validated in offline mode**

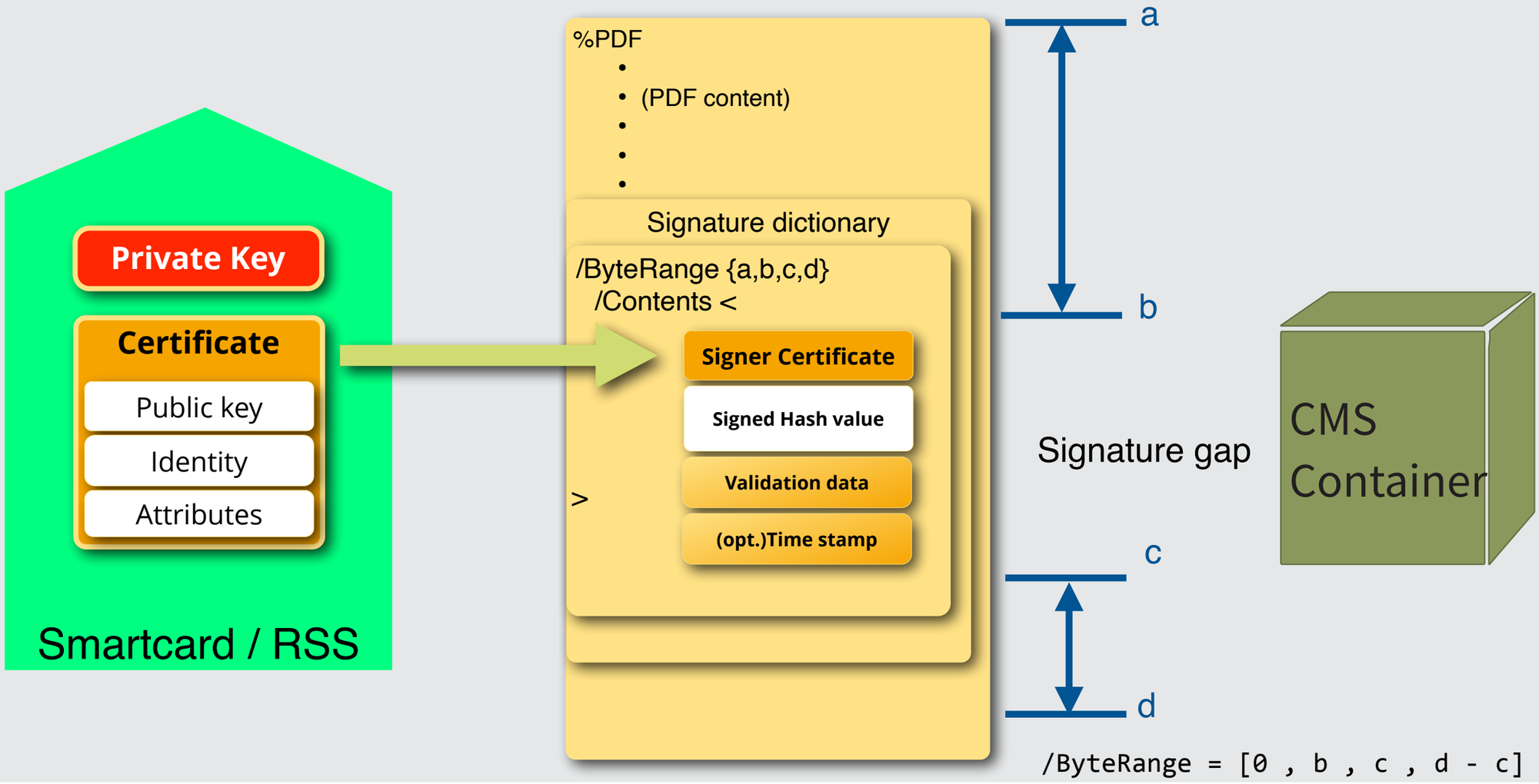
Special signature format

- **Validation information is stored in PDF objects (DSS + VRI dictionaries), not in CAdES or XAdES containers!**
- **No size limitations when extending the signing information**

State of Play in Digital Signing of PDF

- We sign always the whole document (well, except the signing gap …)
- Only serial signing is supported
- Only X.509 based signing certificates are supported
  - Certificate quality is out of scope for the PDF signing
  - Authentication and Identification is out of scope for the PDF signing
- To allow modifications after signing a very complex (and sometimes heuristic) validation policy has been designed

State of Play in digital signing of PDF



PDF and Signature Types

Just to repeat …

- 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

Work at ETSI ESI

- ETSI ESI mostly focused on
  - Revision and updates of existing standards
  - Digital ID and EU Wallet
  - Specification of Validation Services
- No direct changes in PADeS
  - Work on extended validation procedures in PADeS is still ongoing

Work at Cloud Signature Consortium

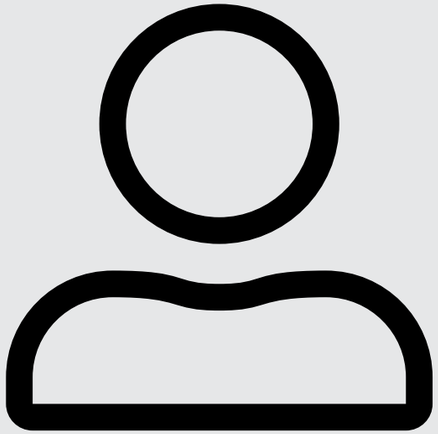
- Publication of Draft CSC API technical specification V2.0.0.0
  - Remote Electronic Signatures and Remote Electronic Seals
  - Focussing on integration of various authentication methods
  - Compliance with EU ID Wallet initiative

My Wishes

working together! PDF
PDF Days Europe 2022

- Wish No. 1: „User friendly validation“
- Wish No. 2: „Signing process aware PDF documents“
- Wish No. 3: „Support of Initialing and notarization“
- Wish No.4: „Support of document part signing“

On Validation



Proofing Identity of Signer

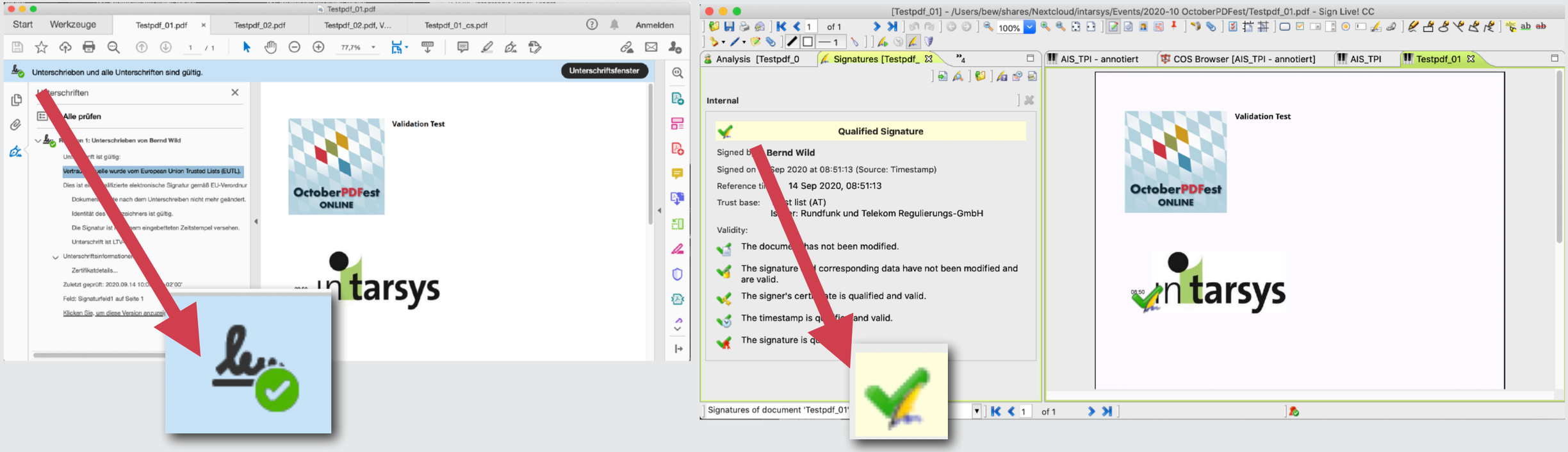
Proofing Integrity of Content

- Much more complex than signing or even PDF/A validation!
- 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 (see 2020)

User Friendly Validation

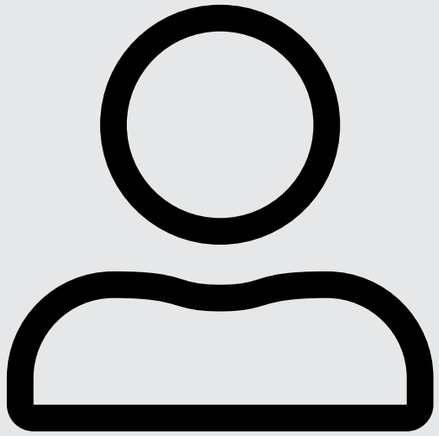
working together! PDF
PDF Days Europe 2022

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



Or if not so, we need a simple and comprehensible explanation!!!

On Validation



Proofing Identity of Signer

- ETSI (CAdES/XAdES/PAdES) standards specify validation of certificates and certificate chains
- Actually, **independent of PDF** —> there's no relationship between Identity Proof and PDF standard
- PDF doesn't have any information about the signer(s)
- Purely technical process
- No signature workflow information

On Validation

Photo by Jeremy Bishop on Unsplash

- There's no „wrong implementation" but standards and specifications allow for some degrees of freedom
  - Validation policies (how to deal with expired certificates in the short-term certificates world)
  - Support of crypto algorithms (in PDF)
  - Different linkage to trusted roots and trusted lists

It's not trivial to assess an ambiguous validation result!

On Validation

- Most PDF Viewer don’t present the information that a PDF is signed at first sight
  - Small info in status bar
  - Appearance of a paper clip or a signing symbol
- PDF Viewers present validation result as a multi-step technical validation procedure (what it is in principal) but not comprehensible for the normal user
  - No Explanation or rating
- Interpretation of „allowed“ modifications is difficult to communicate

On Validation

- Is it easy, to achieve this „OK“?
- Are there only 2 choices „VALID“ or „No VALID“?
- How to handle the validation results between VALID and NO VALID?
- Are there „signed reference documents“ with validation results everybody can agree upon?

User Friendly Validation

- Explanatory component —> remember the first days of AI in the 1980s!!
- Introduction of signature workflow information into PDF data structures
  - Who should sign the document?
  - What signature type (SES, AES, ATS, ASeal, QES, …) should be allowed for signing at least?
  - Which minimum signature quality (Simple, Advanced, Qualified) for which signature step should be required?
- Some sort of Audit trail of the overall signature process
  - Validation is not a purely technical process but has also business and (quite often) legal implications —> minimum signature quality
- Interoperability of market solutions

… and a bit more!

- Some sort of „reference database“ with digitally signed PDF documents which are regarded as to be valid and/or invalid —> the „Isartor Test Suite“ for signed PDFs; —> ETSI Plug-Tests
- A community which discusses validation cases and comes to a common understanding on „valid“ or „not valid“ —> could be the TWG DigSig
- A signed PDF should be validatable without proprietary workflow data stores, i.e. self-contained digital signatures (comparable to PDF/A) —> proposals and discussions in TWG DigSig and PDF Associations communities; standards enhancements
- A recommendation to use LTV informations wherever possible —> self-contained

W2: Signing Process Aware PDF

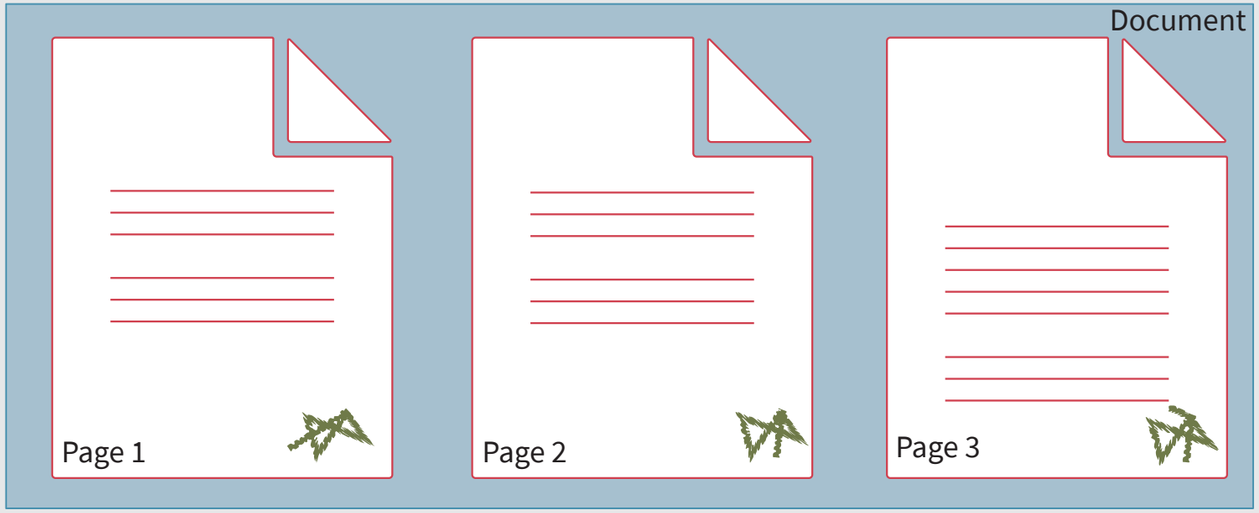
- Proposal on Document-based signing
  - Please, see presentation of Roman Toda, „Interoperable document-based signatures“
- Real business processes show a real need for storing workflow data of the signing workflow
  - What minimum quality of signing certificates is required for signing the document?
  - What type of signature may be used and for which signing step in the process?
  - How many signatures are required for a complete signing?

W3: Support for Initialing and Notarisation

- Some well-established paper-based workflows can’t be digitized using actual PDF Signing standards:
  - Initialing
  - Notarization

W3: Support for Initialing and Notarisation

- **Initialing**

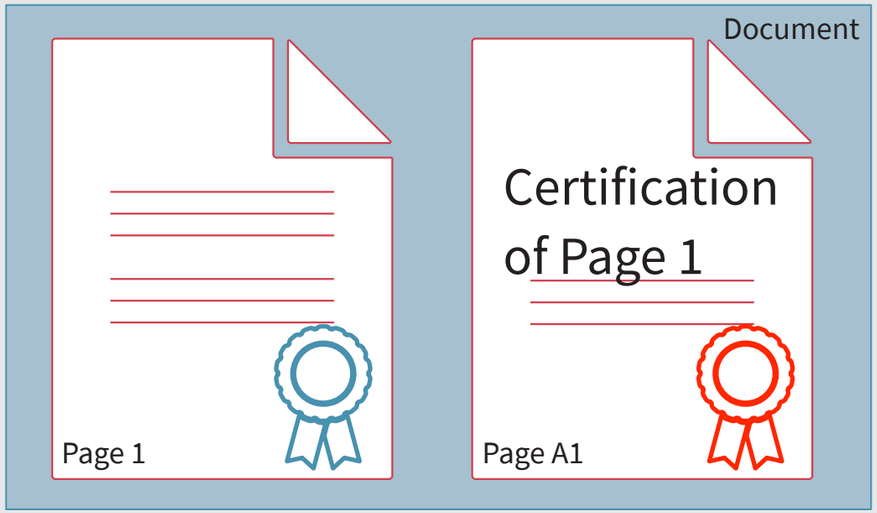


- Problem: There's no page-based signature
- Approaches like the proposal of intarsys

- Documents, that the page was read (by whom?) and the content is OK
- Page-based
  - every page has it's own initial
  - Pages can be exchanged
- No signature meaning
- More integrity check

W3: Support for Initialing and Notarisation

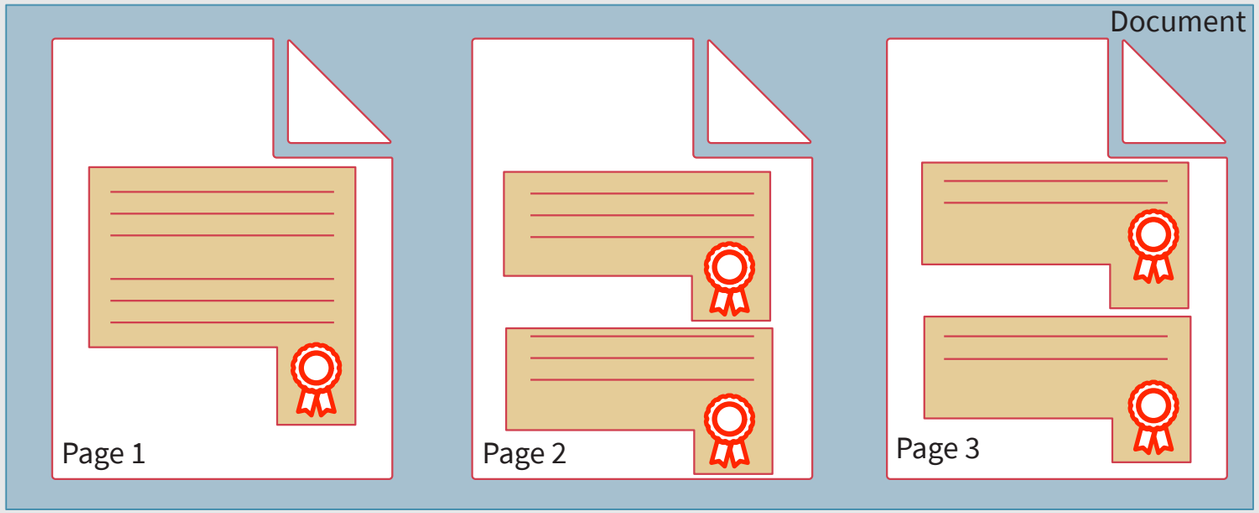
- **Notarization**



- Addition of a notarisation may not affect an already (digitally) signed original
- May be applied much later than the signing of the base document
- Both documents form a unit —> viewer

- Problem: actual PDF signing standards allow for specific modifications in form fields or annotations but no adding of new pages
- Approaches like the proposal of BFO

W4: Support of Document Part Signing



- It should be possible to sign only a well defined part of the document
- Multiple signatures in a document
- Could also solve the initialing and notarisation requirement

News: We not always need a signature

- Enhancement to ISO 32000-2: Integrity protection in encrypted documents in PDF 2.0 (ISO/DTS 32004)
  - If only an integrity protection is needed within a closed user group the HMAC-based approach can provide this cheaper and faster
  - Restrictions:
    - sharing of a symmetrical key
    - Not compatible with PDF/A (due to encryption)

Dr. Bernd Wild
intarsys GmbH
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

- **Since November 2021 member of procilon GROUP**
- ***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**