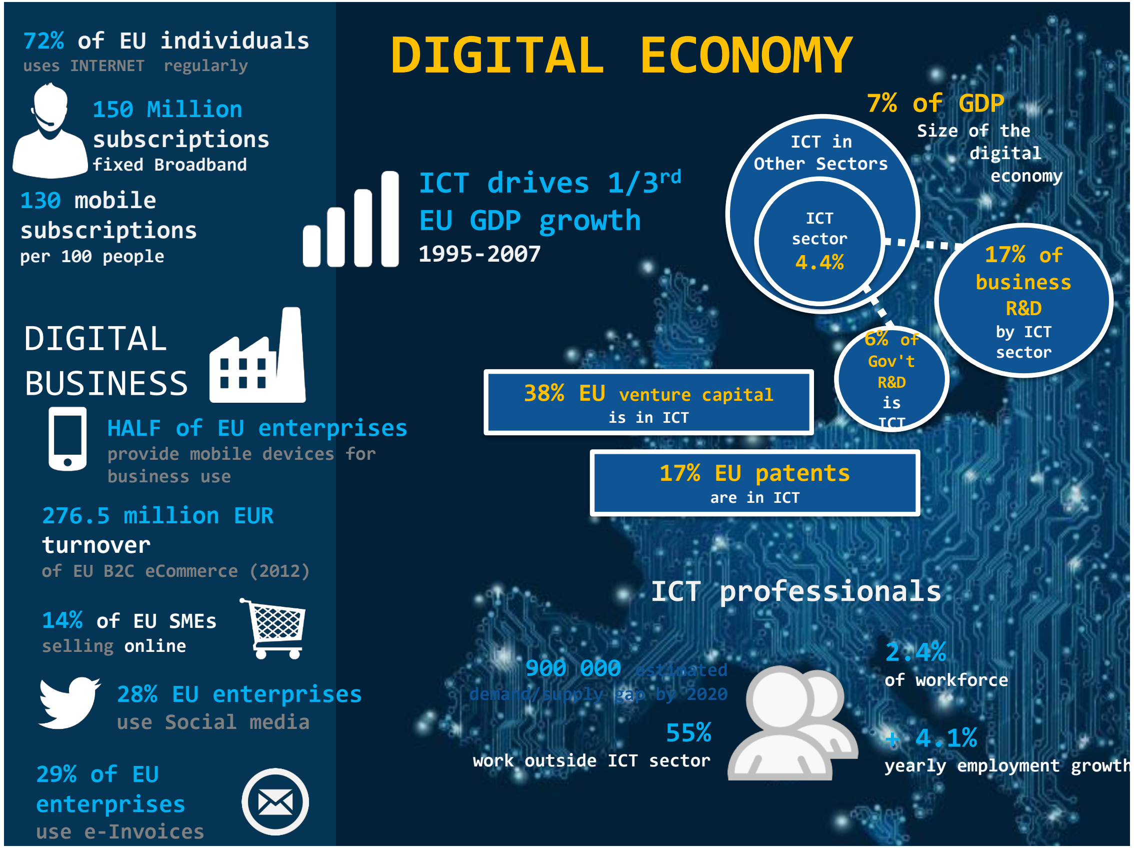
eIDAS-compliant signing of PDF

Technical implications of eIDAS conformance in PDF processing

Bernd Wild
intarsys AG, Member of the Board of PDF Association

Dr. Bernd Wild,
Member of the Board of
PDF Association



DIGITAL ECONOMY

72% of EU individuals
uses INTERNET regularly

150 Million subscriptions
fixed Broadband

130 mobile subscriptions
per 100 people

DIGITAL BUSINESS

HALF of EU enterprises
provide mobile devices for business use

276.5 million EUR turnover
of EU B2C eCommerce (2012)

14% of EU SMEs
selling online

28% EU enterprises
use Social media

29% of EU enterprises
use e-Invoices

ICT drives 1/3rd EU GDP growth
1995-2007

7% of GDP
Size of the digital economy

ICT in Other Sectors

ICT sector 4.4%

17% of business R&D by ICT sector

6% of Gov't R&D is ICT

38% EU venture capital
is in ICT

17% EU patents
are in ICT

ICT professionals

900 000 estimated demand/supply gap by 2020

55%
work outside ICT sector

2.4%
of workforce

+ 4.1%
yearly employment growth

Source: Andrea Servida, DG CONNECT, European Commission, 2016

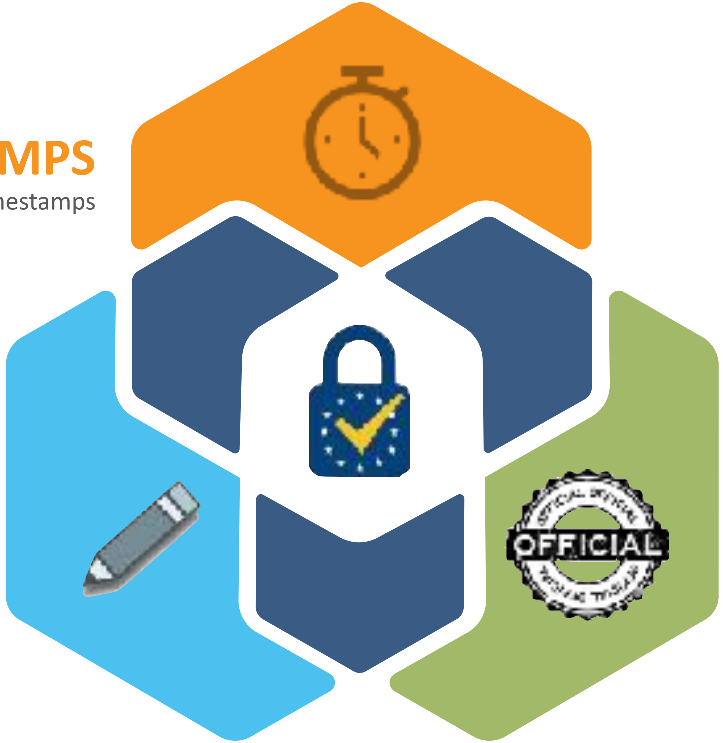
Dr. Bernd Wild, Member of the Board of PDF Association

2018-05-14

eIDAS – electronic Identification and Trust Services

- 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
- Officially published on 28.08.2014

The relevant trust services of eIDAS



TIMESTAMPS

Qualified timestamps

SIGNATURES

Qualified signatures
(person-related)
local and remote signatures

SEALS

Qualified seals
(organization-related)

ELECTRONIC DOCS

Non-discrimination

ELECTRONIC DELIVERY

Secure message delivery services

LTP + VALIDATION

Longterm preservation
Validation of signatures, timestamps and seals

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

The eIDAS Regulation

- **Mutual recognition of e-Identification**
- **Extended Supervision** of „Certification Service Providers“ to „Trust Service Providers“
  - proactive supervision
- **Qualified Electronic Trust Services**
  - Electronic signatures
  - Electronic seals
  - Time stamping
  - Registered delivery service
  - Website authentication
  - Electronic documents

Dr. Bernd Wild,
Member of the Board of
PDF Association

The History of PDF Versions

PDF 1.0 (1992)

Code name „Camelot" and „Carousel"

RGB colour space

Internal hyperlinks

Font embedding

Acrobat 1 costs $50

Distiller costs $695 and $2.495

PDF 1.1 (1994)

Acrobat 2

free Acrobat Reader

Device-independent colours

External hyperlinks

Notes

Security features

Multimedia add-ons

Full text search

Breakthrough comes with US Tax Forms

PDF 1.2 (1994)

Acrobat 3

CMYK colour space

Spot colours

OPI 1.3

Plug-In for Netscape

PDF 1.3 (1999)

Acrobat 4

2-Byte CID Fonts

OPI 2.0

Colour blends

Soft shadows

Annotations

Digital signature

PDF 1.4 (2001)

Acrobat 5

Transparency

Strong encryption

Tagged PDF

JavaScript 1.5

PDF 1.5 (2003)

Acrobat 6

Better compression

JPEG2000

Layers

Improved tagged PDF

Adobe Reader

PDF 1.6 (2005)

Acrobat 7

NChannel enhancement

Improved encryption

OpenType Fonts

File Container

3D data

PDF/A-1 (2005)

PDF 1.7 (2006)

Acrobat 8

Improved 3D embedding

Printer control

ISO32000-1 (2008)

PDF/A-2 (2011)

PDF/A-3 (2012)

ISO32000-2 (2017)

Reference to ETSI concerning DigSig

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

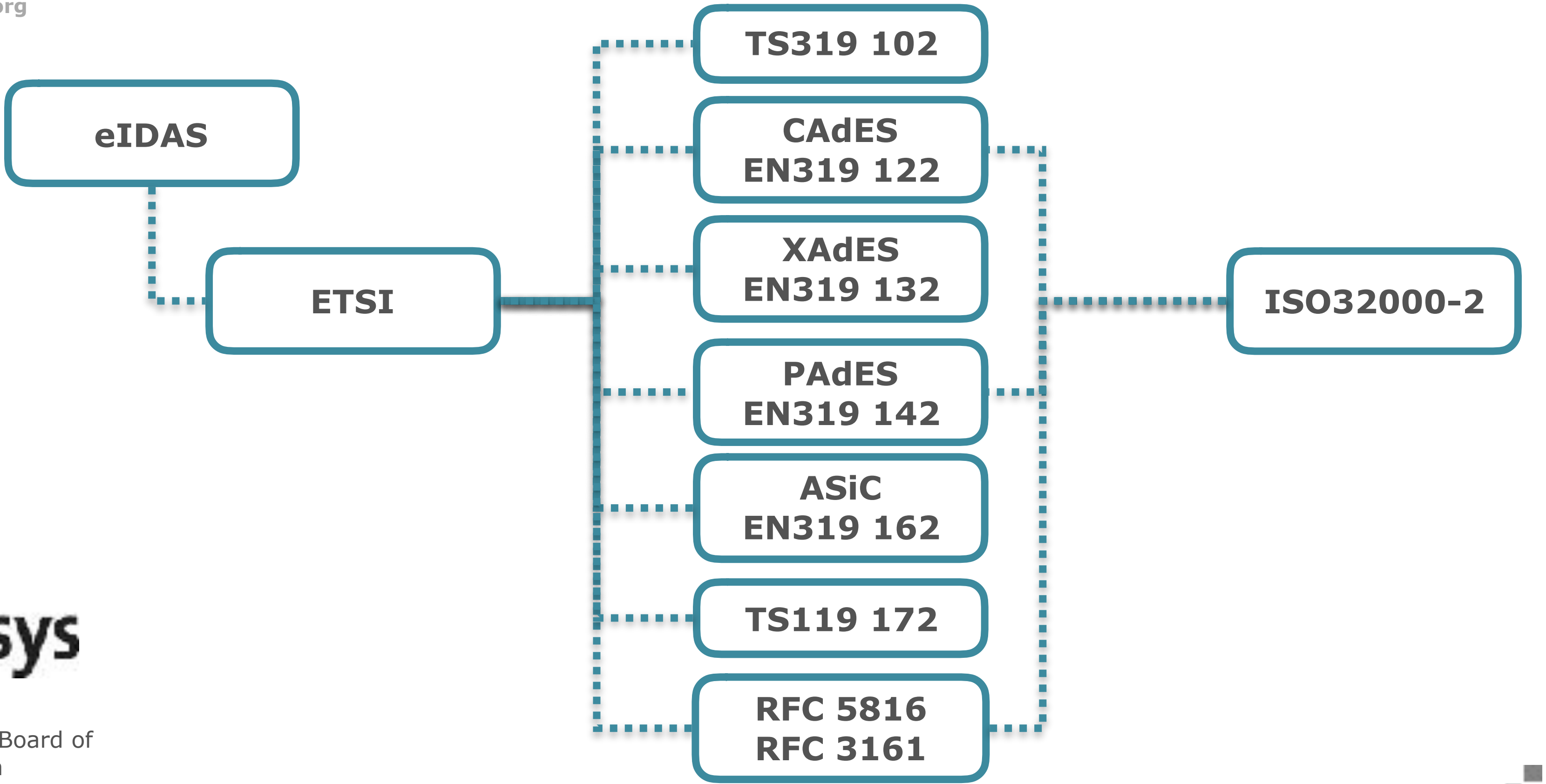
Some ETSI Standards for Signature Creation and Validation

- **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

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

ISO 32000-2 and Signing Standards



intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

2018-05-14

PDF and Signatures

- PDF standard supports only X.509 based digital signatures
- Since PDF 1.3 it‘s possible to embed digital signatures and to visualize them
- PDF viewer with added functionality for signing and verification
  - Problem was compliance to some pre-eIDAS national regulations (e.g. Germany)
- Precaution for multiple signatures (serial signatures)
  - Use of the versioning concept of PDF
  - Adapted validation mode

Signature types	PDF support	Remarks
X.509 based signatures	Yes	
PGP based signatures	No	
Biometric signatures	No	
Hybrid signatures	(Yes)	as long as a X.509 based signature is used

Dr. Bernd Wild,
Member of the Board of
PDF Association

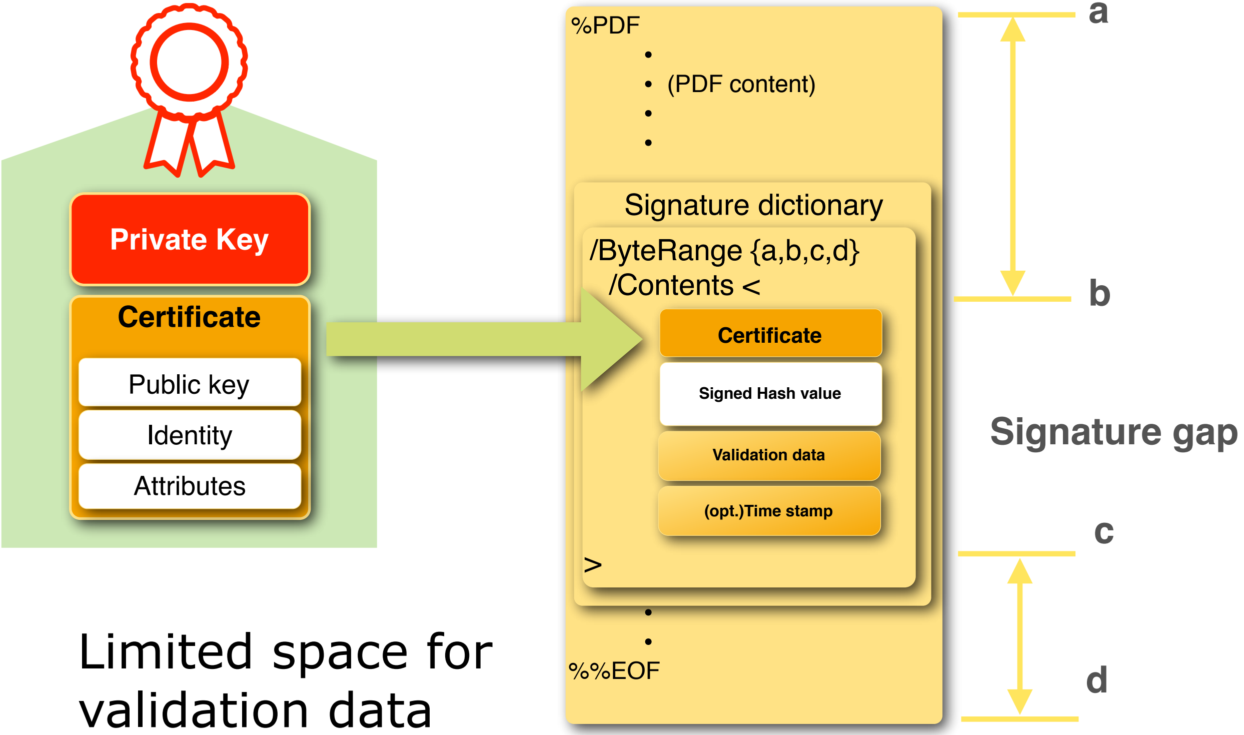
Embedded Signatures in PDF/A

- PDF supports 3 signature types
  - Document signatures (a.k.a. author or certification signatures)
    - can be non-repudiation and legally binding
  - Manipulation Detection & Prevention Signatures (Signing of form fields in a PDF form)
  - Usage Rights Signatures (DRM)
- Document signatures
  - Handled as annotations
  - Must have an appearance stream
    - Defines the visual appearance
    - If appearance stream is empty we have an „invisible" signature ➜ used for mass signing

Only document signatures are allowed in PDF/A

Dr. Bernd Wild,
Member of the Board of
PDF Association

Signing of a PDF Document



Limited space for validation data

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

PAdES Baseline Profiles - ETSI EN 319 142-1

LEVEL	B-B	B-T	B-LT	B-LTA
Use Case	Basic profile	Basic profile with time proof	Longterm validation profile	Longterm validation profile with integrity proof of validation info
signed and unsigned attributes	X	X	X	X
included timestamp		X	X	X
verification information			X	X
additional timestamp				X

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

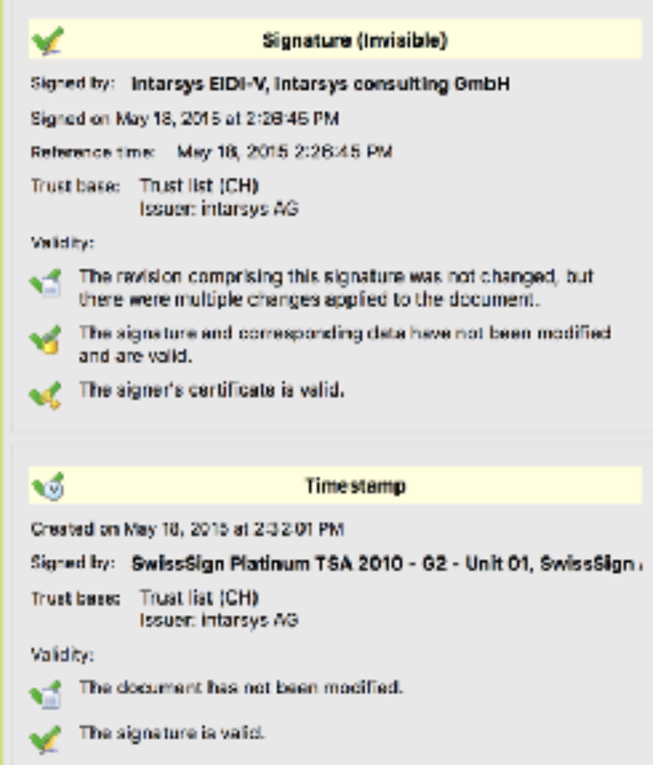
PAdES Extended Profiles - ETSI EN 319 142-2/3

LEVEL	E-BES	E-EPES	E-X-BES E-X-EPES E-X-E-T	E-X-E-C E-X-E-X E-X-XL E-X-E-A	E-X-XFA	DTS
Use Case	Basic profile (Compliance)	Basic profile with signature policy (Compliance)	Basic profile with signature policy and/or timestamp (Compliance)	signed XML embedded in PDF (Basic, Longterm)	signed XFA-Data embedded in PDF (Basic, Longterm)	Timestamp Signature

These profiles are specified due to compliance reasons (except DTS). They are not mentioned by eIDAS!

intarsys
Dr. Bernd Wild,
Member of the Board of
PDF Association

PAdES-LTV



✓ Signature (Invisible)

Signed by: **Intarsys EIDI-V, Intarsys consulting GmbH**

Signed on May 18, 2015 at 2:28:45 PM

Reference time: May 18, 2015 2:28:45 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.

✓ Timestamp

Created on May 18, 2015 at 2:32:01 PM

Signed by: **SwissSign Platinum TSA 2010 - G2 - Unit 01, SwissSign**

Trust base: Trust list (CH)
Issuer: intarsys AG

Validity:

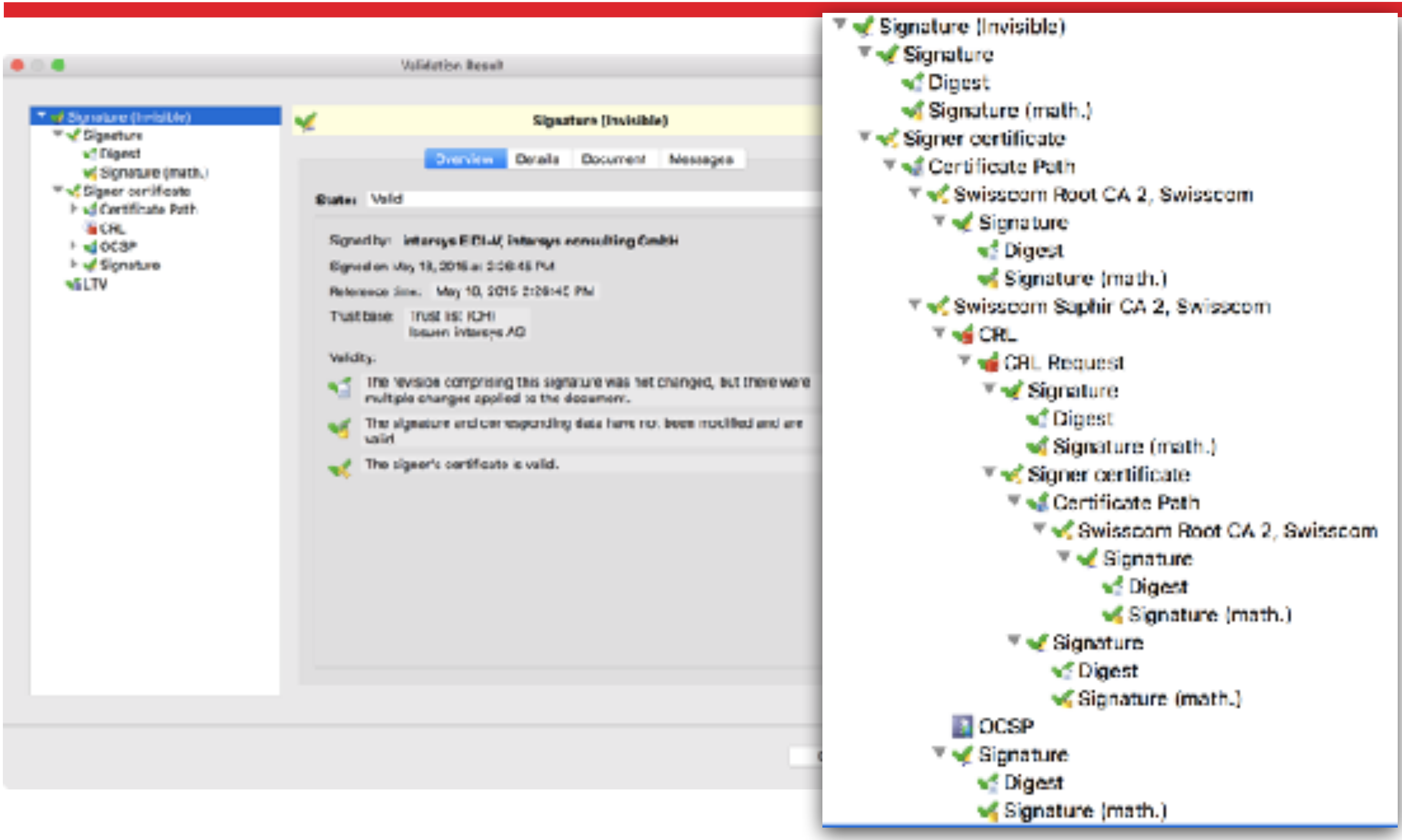
- ✓ The document has not been modified.
- ✓ The signature is valid.

Example PDF document with signature compliant to PAdES-LT profile

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

PAdES-LTV



- Signature (Invisible)
  - Signature
    - Digest
    - Signature (math.)
  - Signer certificate
    - Certificate Path
    - CRL
    - OCSP
    - Signature
  - LTV

Signature (Invisible)

State: Valid

Signed by: **intarsys EBLV, intarsys consulting GmbH**

Signed on May 10, 2016 at 2:08:45 PM

Reference time: May 10, 2016 2:08:45 PM

Trust base: Trust list: KDHI
Issuer: intarsys AG

Validity:

The revision comprising this signature was not changed, but there were multiple changes applied to the document.

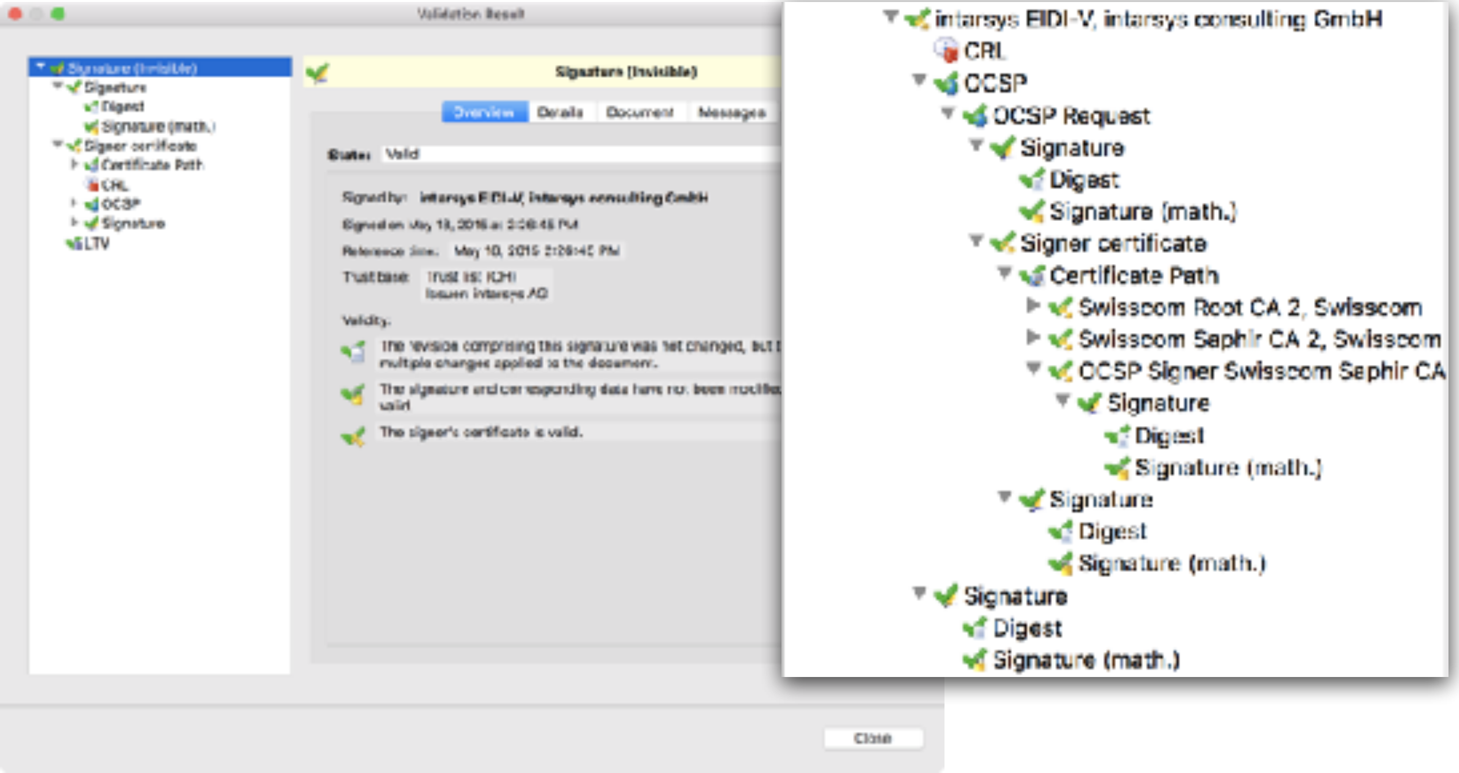
The signature and corresponding data have not been modified and are valid.

The signer's certificate is valid.

- 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.)

Dr. Bernd Wild,
Member of the Board of
PDF Association

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, 2016 at 3:08:45 PM

Reference time: May 18, 2016 2:28:45 PM

Trust base: Trust list: KDH
Issuer: intarsys AG

Validity:

The revision comprising this signature was not changed, but t
multiple changes applied to the document.

The signature and corresponding data have not been modifie
valid

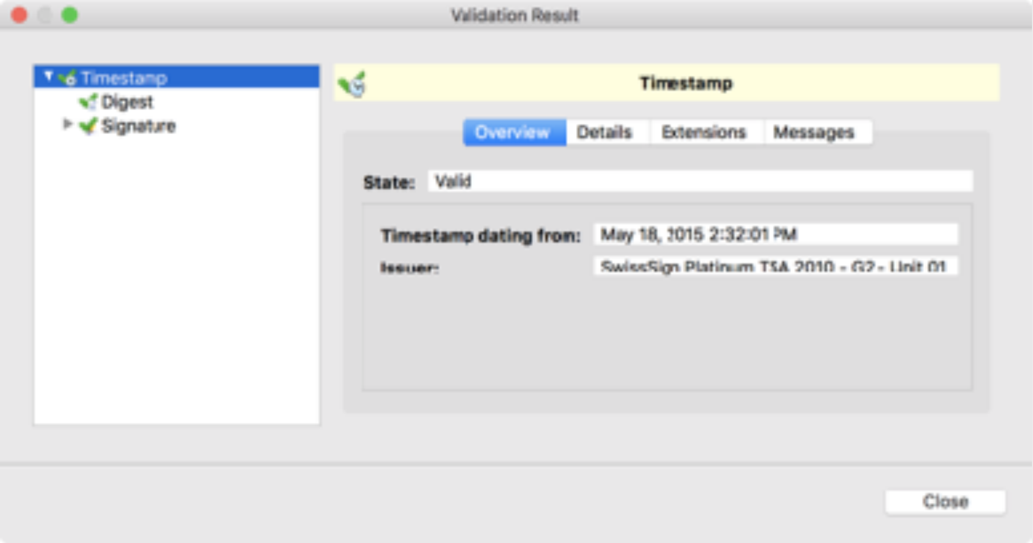
The signer's certificate is valid.

Close

```
▼ intarsys EIDI-V, intarsys consulting GmbH
    CRL
  ▼ OCSP
    ▼ OCSP Request
      ▼ Signature
          Digest
          Signature (math.)
      ▼ Signer certificate
        ▼ Certificate Path
          ▸ Swisscom Root CA 2, Swisscom
          ▸ Swisscom Saphir CA 2, Swisscom
          ▼ OCSP Signer Swisscom Saphir CA
            ▼ Signature
                Digest
                Signature (math.)
        ▼ Signature
            Digest
            Signature (math.)
  ▼ Signature
      Digest
      Signature (math.)
```

Dr. Bernd Wild,
Member of the Board of
PDF Association

PAdES-LTV



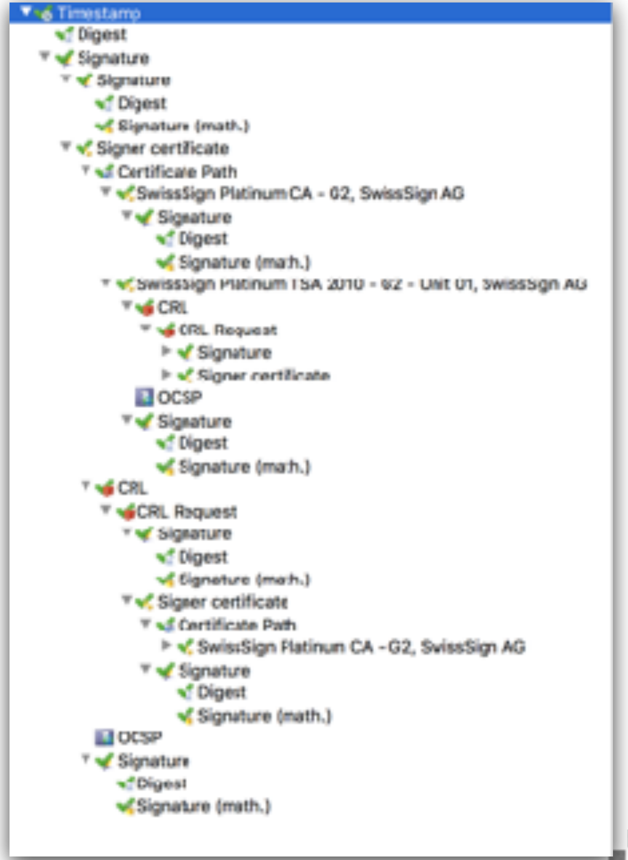
```
▼ Timestamp
    Digest
  ▶ Signature
```

Timestamp

State: Valid

Timestamp dating from: May 18, 2015 2:32:01 PM

Issuer: SwissSign Platinum TSA 2010 - G2 - Unit 01

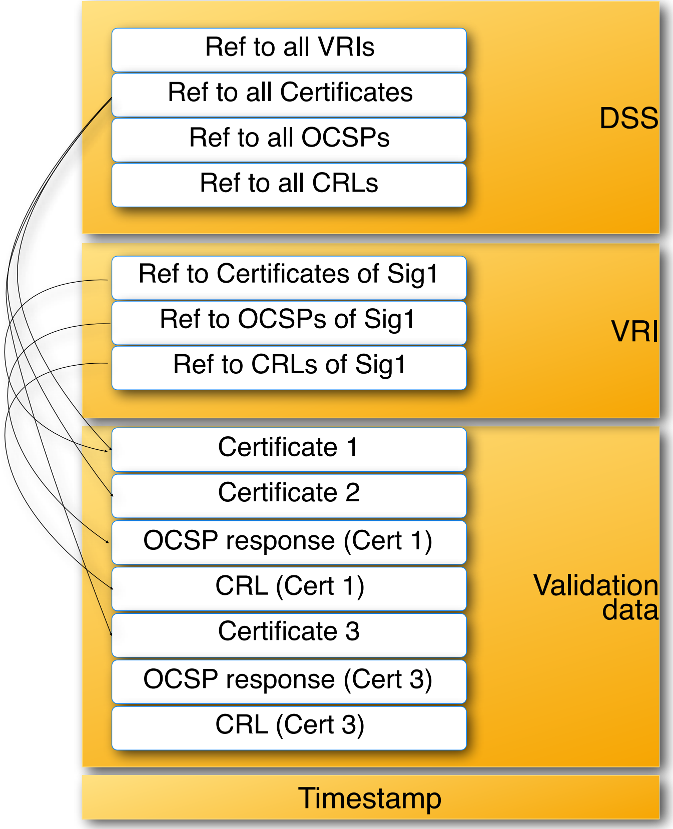


```
▼ Timestamp
    Digest
  ▼ Signature
    ▼ Signature
        Digest
        Signature (math.)
    ▼ Signer certificate
      ▼ Certificate Path
        ▼ SwissSign Platinum CA - G2, SwissSign AG
          ▼ Signature
              Digest
              Signature (math.)
        ▼ SwissSign Platinum TSA 2010 - G2 - Unit 01, SwissSign AG
          ▼ CRL
            ▼ CRL Request
              ▶ Signature
              ▶ Signer certificate
            OCSP
          ▼ Signature
              Digest
              Signature (math.)
      ▼ CRL
        ▼ CRL Request
          ▼ Signature
              Digest
              Signature (math.)
          ▼ Signer certificate
            ▼ Certificate Path
              ▶ SwissSign Platinum CA - G2, SwissSign AG
            ▼ Signature
                Digest
                Signature (math.)
      OCSP
      ▼ Signature
          Digest
          Signature (math.)
```

Dr. Bernd Wild,
Member of the Board of
PDF Association

www.pdfa.org

PAdES Long Term – PAdES-LTA



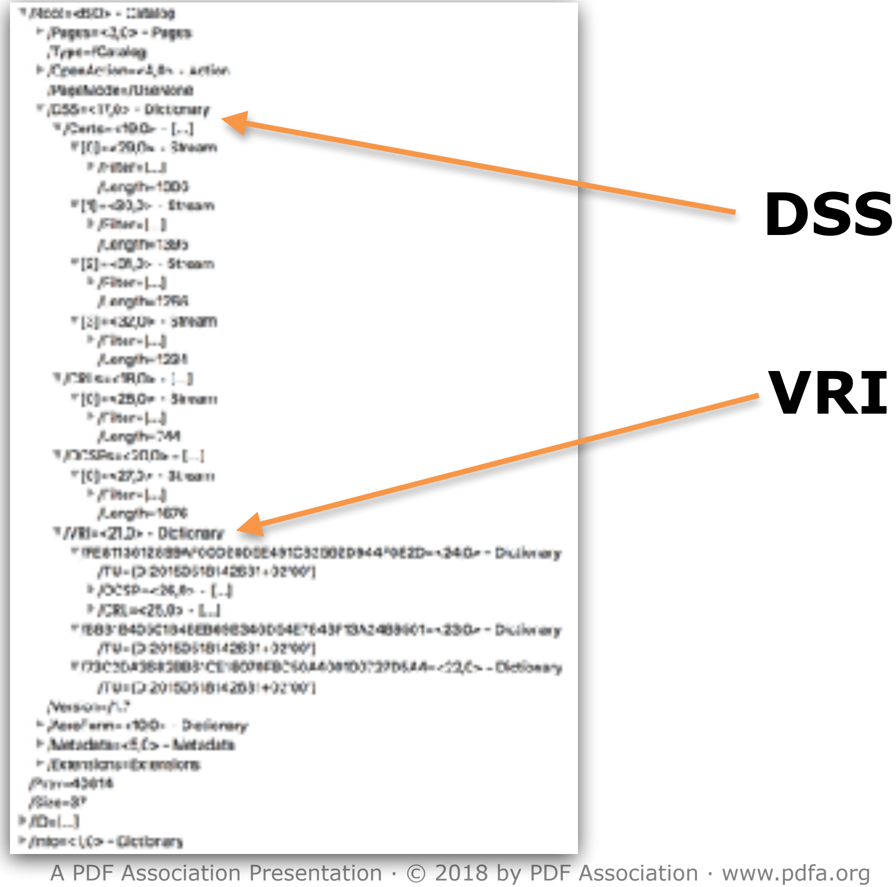
- Repeated signature process
- No modification of present signatures
- PDF document sizes grows with every signature process
- Self-contained document
- can be validated in offline mode

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

Dr. Bernd Wild,
Member of the Board of
PDF Association

PDF Signing Structures

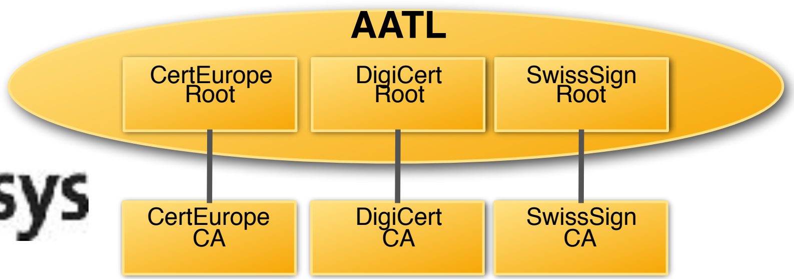


```
▼/Root=<85,0> - Catalog
  ▶/Pages=<3,0> - Pages
   /Type=/Catalog
  ▶/OpenAction=<4,0> - action
   /PageMode=/UseNone
  ▼/DSS=<17,0> - Dictionary
    ▼/Certs=<19,0> - [...]
      ▼[0]=<29,0> - Stream
        ▶/Filter=[...]
         /Length=1303
      ▼[1]=<30,0> - Stream
        ▶/Filter=[...]
         /Length=1385
      ▼[2]=<31,0> - Stream
        ▶/Filter=[...]
         /Length=1266
      ▼[3]=<32,0> - stream
        ▶/Filter=[...]
         /Length=1224
    ▼/CRLs=<18,0> - [...]
      ▼[0]=<28,0> - Stream
        ▶/Filter=[...]
         /Length=744
    ▼/OCSPs=<20,0> - [...]
      ▼[0]=<27,0> - Stream
        ▶/Filter=[...]
         /Length=1676
    ▼/VRI=<21,0> - Dictionary
      ▼/FE8113012689AF0CDE0DDE491C32002D944F0E2D=<24,0> - Dictionary
         /TU=(D:20180518142831+02'00')
        ▶/OCSP=<26,0> - [...]
        ▶/CRL=<25,0> - [...]
      ▼/B831B4D9C1D4EEB69E340D04E7643F13A2488901=<23,0> - Dictionary
         /TU=(D:20180518142831+02'00')
      ▼/73C2DA3B83BB3CE1807EFBC90A4091D0727D5A4=<22,0> - Dictionary
         /TU=(D:20180518142831+02'00')
   /Version=/1.7
  ▶/AcroForm=<10,0> - Dictionary
  ▶/Metadata=<5,0> - Metadata
  ▶/Extensions=Extensions
 /Prev=43816
 /Size=87
▶/ID=[...]
▶/Info=<1,0> - Dictionary
```

Dr. Bernd Wild,
Member of the Board of
PDF Association

Trust Anchor List

- Adobe introduced proprietary „Adobe Approved Trust List“ (AATL); still valid for „advanced electronic signatures“
- With EU TSL validation of pan-euopean qualified certificates is possible
- EU TSL is just a list of „pointers“ to national registries
- EU common understanding of „Qualified“


AATL

CertEurope Root

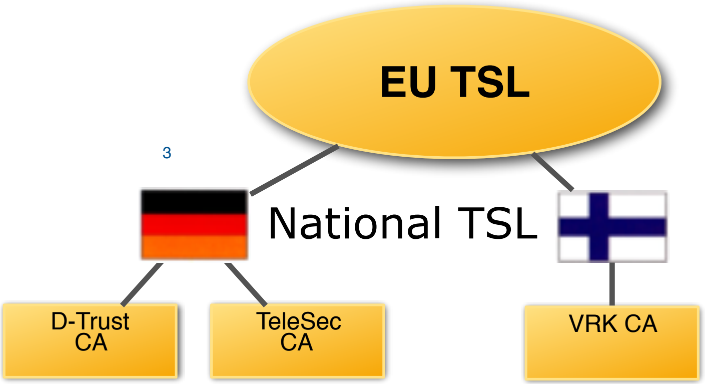
DigiCert Root

SwissSign Root

CertEurope CA

DigiCert CA

SwissSign CA


EU TSL

National TSL

D-Trust CA

TeleSec CA

VRK CA

Dr. Bernd Wild,
Member of the Board of
PDF Association

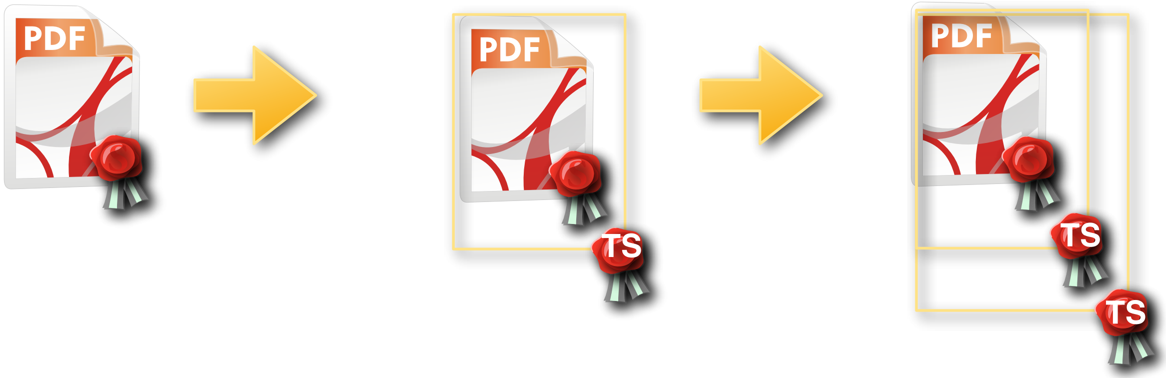
Digitally signing a PDF(/A) still a challenge?

- Problem is not signing but validating the signature, i.e. bringing up the „green checkmark‟ —> compliant to different profiles
- Signing of PDF is well specified (see standards + specifications like PAdES), less freedom of interpretation but many profiles
- eIDAS and EU Trusted List has simplified life for pan-european qualified signatures
- Still no published ETSI/EN standard on correct validation of signatures (—> STFs active at ETSI)
- The distinguishing of „mathematical correctness‟ and „valid signature‟ although the user wants one answer: OK or NOT OK
  - Validation needs proper explanation!

Dr. Bernd Wild,
Member of the Board of
PDF Association

Renewal of Signatures of Signed Documents

- „Fading out“ of trust value
- First Approach: Document level
  - PAdES-LTA
- Second Approach: Document Collection Level
  - based on Evidence Record Syntax ERS and Container format (XAIP, ASiC, prob. PDF/A-3)
  - upcoming Longterm Preservation standard from ETSI



Dr. Bernd Wild,
Member of the Board of
PDF Association

Thank you! Any questions?

intarsys

Dr. Bernd Wild,
Member of the Board of
PDF Association

Get in touch:	bernd.wild@pdfa.org
Web site:	www.pdfa.org
Twitter:	PDFassocation