© Photo by Mick Haupt on Unsplash

PDF

PDF Days Online 2021

Validating Digital Signatures in PDF

About User Experiences And Pitfalls

Agenda

- Again: What’s validation?
- Again: Signing and validating PDFs
- Some Tests
- What we need in validation
- Summary

This is a followup of the OctoberPDFest presentation on validation from 2020!!

What's 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)

What’s Validation?

Proofing Integrity of Content

- Was presented on last year’s session
- Comparison of hash values on byte ranges in PDF
- Handling of revisions

OctoberPDFest
ONLINE

What’s Validation?

Proofing Identity of Signer

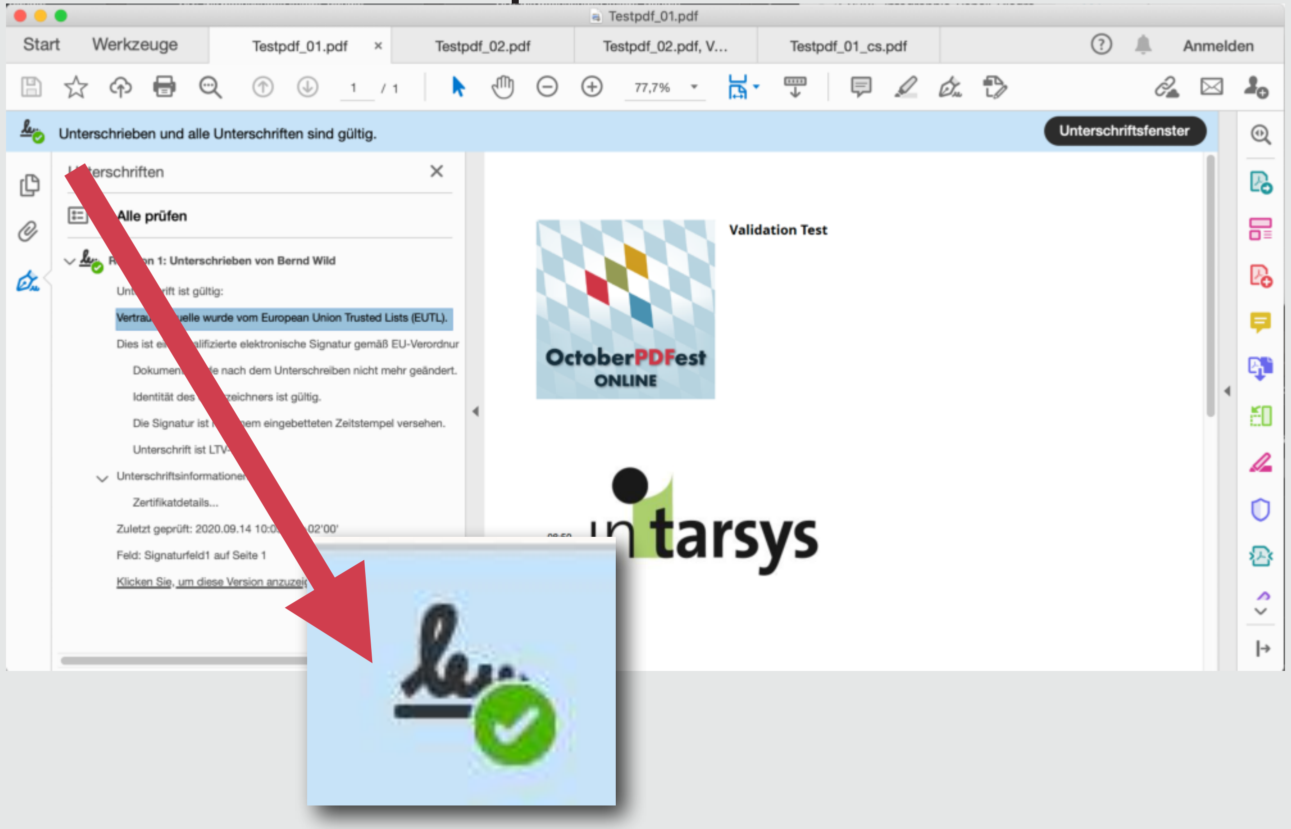
- ETSI (CAdES/XAdES/PAdES) standards specify validation of certificates and certificate chains
- Actually, **independent of PDF** —> there’s no relationship between Identity Proof and PDF standard
- PDF doesn’t have any information about the signer(s)
- Purely technical process
- No signature workflow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

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
  - ETSI EN 319 102-1 V1.2.3 (2021-07) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
  - ISO 32000-1 and ISO 32000-2

What’s Validation?

- User’s Perspective: All what’s necessary to get the „Green Checkmark“



Unterschrieben und alle Unterschriften sind gültig.

Unterschriften

Alle prüfen

R... on 1: Unterschrieben von Bernd Wild

Unt... rift ist gültig:

Vertrau... uelle wurde vom European Union Trusted Lists (EUTL).

Dies ist ei... alifizierte elektronische Signatur gemäß EU-Verordnur

Dokumen... e nach dem Unterschreiben nicht mehr geändert.

Identität des ... zeichners ist gültig.

Die Signatur ist ... em eingebetteten Zeitstempel versehen.

Unterschrift ist LTV-

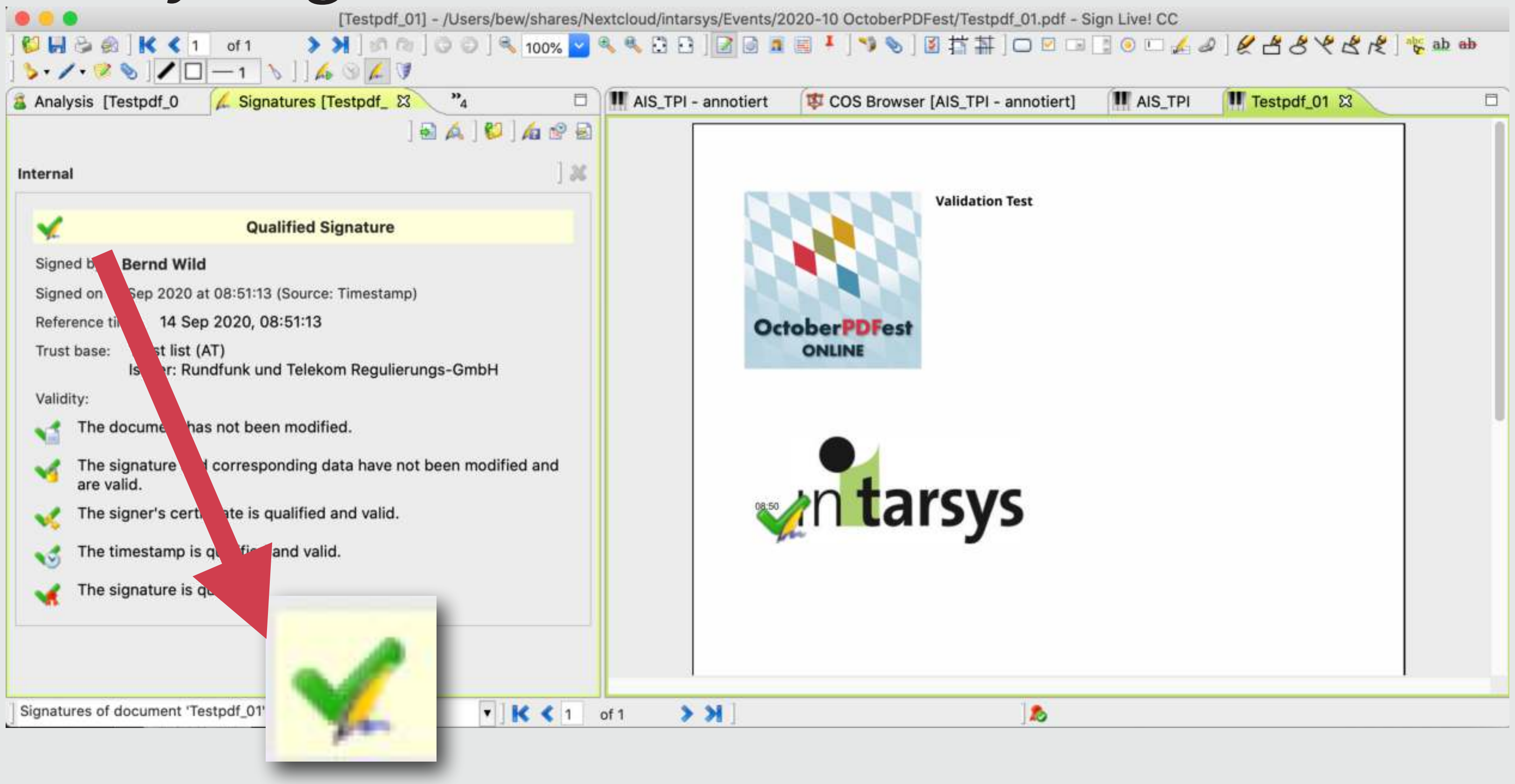
Unterschriftsinformationen

Zertifikatdetails...

Zuletzt geprüft: 2020.09.14 10:0... 02'00'

Feld: Signaturfeld1 auf Seite 1

Klicken Sie, um diese Version anzuzei


[Testpdf_01] - /Users/bew/shares/Nextcloud/intarsys/Events/2020-10 OctoberPDFest/Testpdf_01.pdf - Sign Live! CC
of 1
100%
Analysis [Testpdf_0
Signatures [Testpdf_
AIS_TPI - annotiert
COS Browser [AIS_TPI - annotiert]
AIS_TPI
Testpdf_01
Validation Test
OctoberPDFest ONLINE
intarsys
of 1

Internal

Qualified Signature

Signed b... Bernd Wild

Signed on ... Sep 2020 at 08:51:13 (Source: Timestamp)

Reference ti... 14 Sep 2020, 08:51:13

Trust base: ... st list (AT)
Is... r: Rundfunk und Telekom Regulierungs-GmbH

Validity:

- The docume... has not been modified.
- The signature ... corresponding data have not been modified and are valid.
- The signer's cert... ate is qualified and valid.
- The timestamp is q... fi... and valid.
- The signature is q

Signatures of document 'Testpdf_01'

We always want to end up with a green checkmark!

What’s 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?

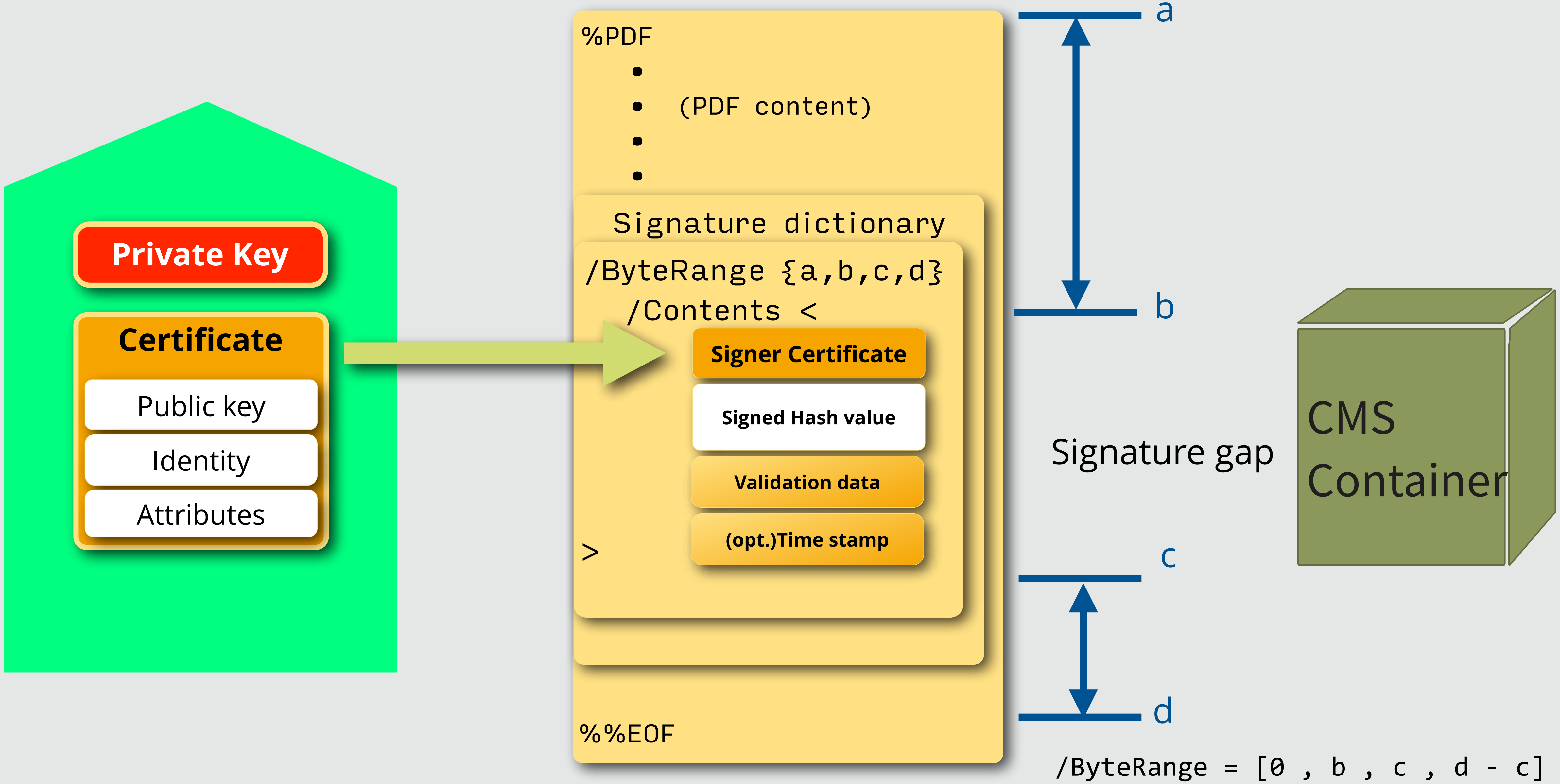
PDF and Signature Types

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

Signing of a PDF Document



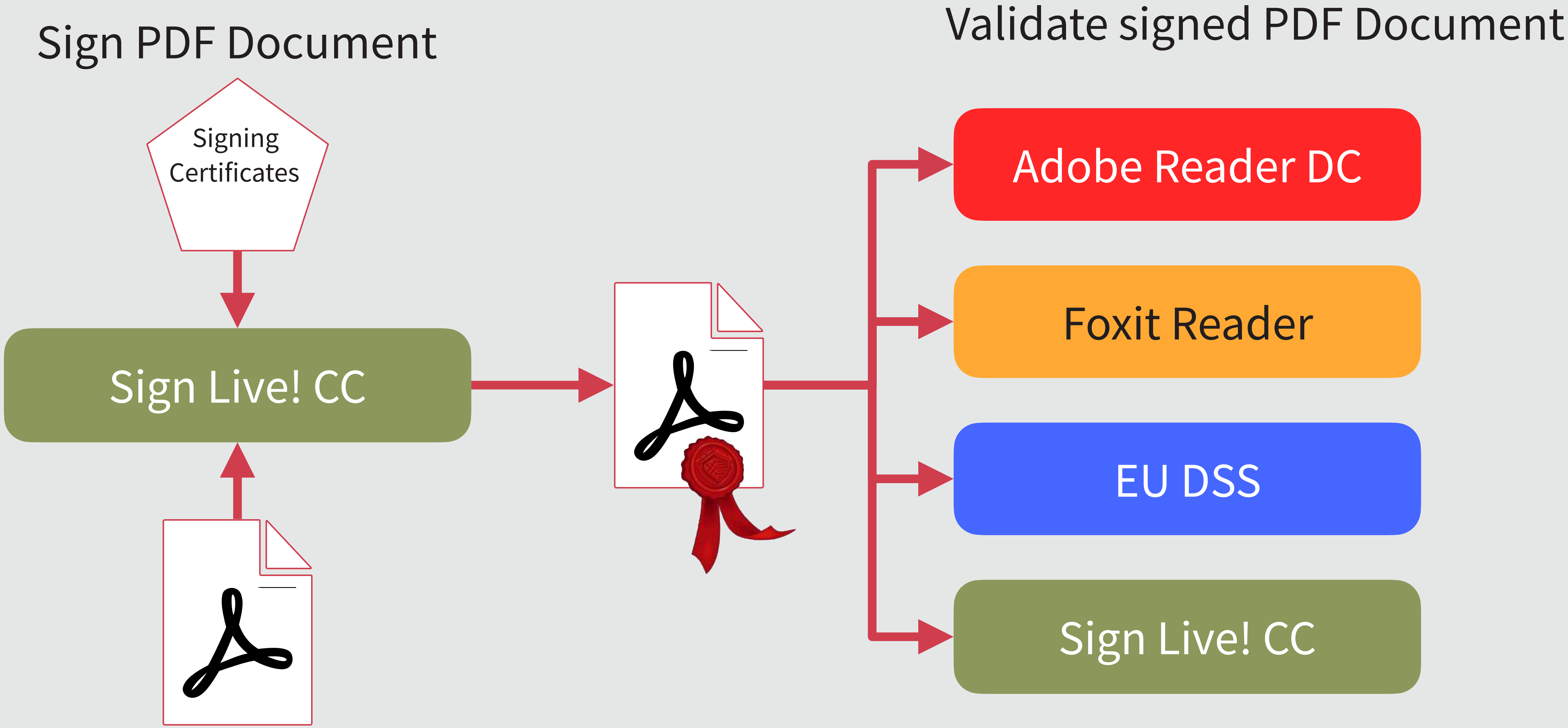
/ByteRange = [0 , b , c , d - c]

Test Setup (I)

User Certificate/Signature Creation Device SCD

Telesec Smartcard QES eIDAS	AIS Remote Signature QES eIDAS	Personal ID AES
Smartcard-based certificate	Ad-hoc (short-term) certificate With/without LTV info	Soft certificate

Test Setup (I)

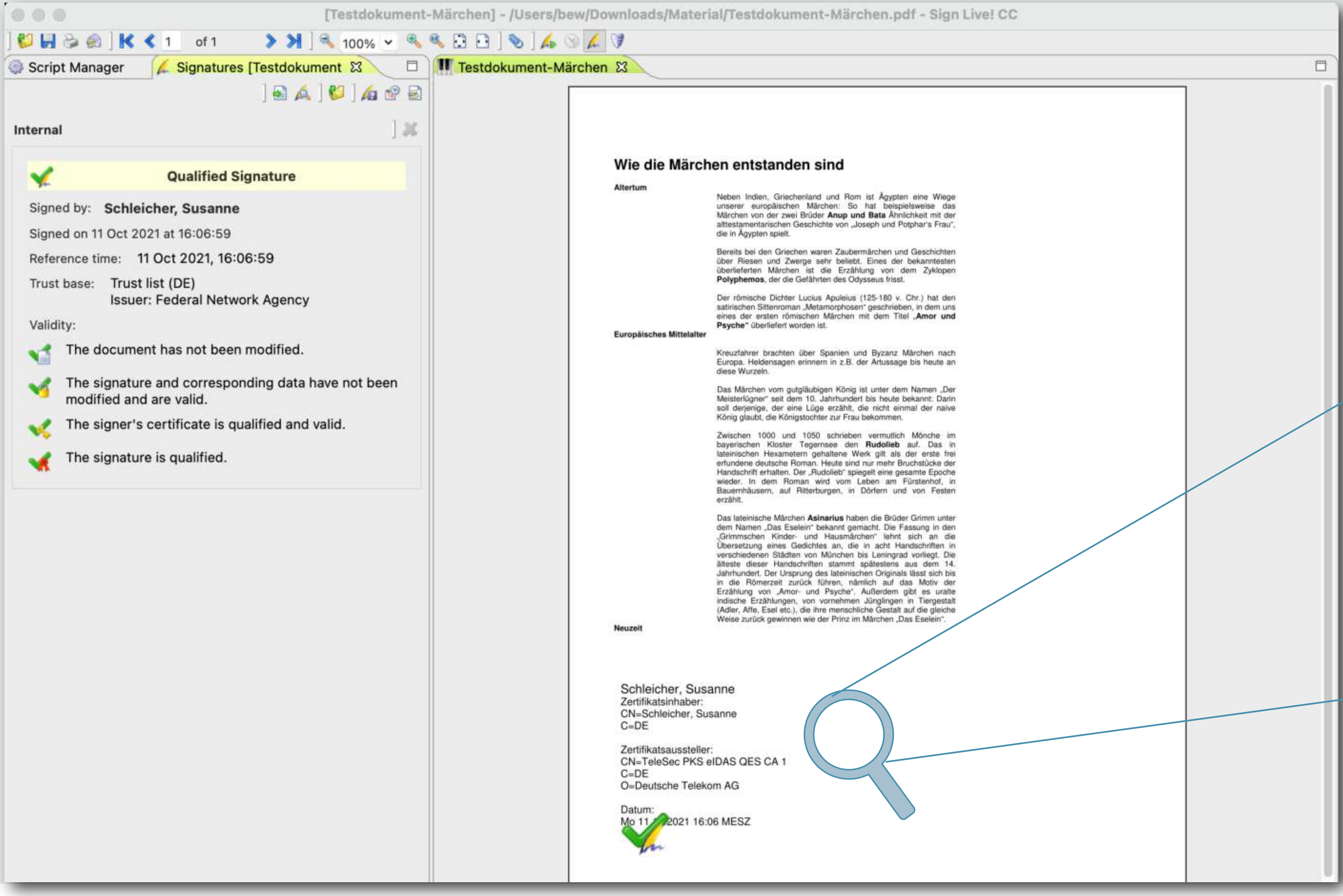


Sign PDF Document

Validate signed PDF Document

Test 1 – Telesec Smartcard QES

Sign Live! CC


[Testdokument-Märchen] - /Users/bew/Downloads/Material/Testdokument-Märchen.pdf - Sign Live! CC
1 of 1 100%
Script Manager
Signatures [Testdokument
Testdokument-Märchen

Internal

Qualified Signature

Signed by: **Schleicher, Susanne**

Signed on 11 Oct 2021 at 16:06:59

Reference time: 11 Oct 2021, 16:06:59

Trust base: Trust list (DE)
Issuer: Federal Network Agency

Validity:

- ✓ The document has not been modified.
- ✓ The signature and corresponding data have not been modified and are valid.
- ✓ The signer's certificate is qualified and valid.
- ✓ The signature is qualified.

Wie die Märchen entstanden sind

Altertum

Neben Indien, Griechenland und Rom ist Ägypten eine Wiege unserer europäischen Märchen: So hat beispielsweise das Märchen von der zwei Brüder **Anup und Bata** Ähnlichkeit mit der alttestamentarischen Geschichte von „Joseph und Potphar's Frau", die in Ägypten spielt.

Bereits bei den Griechen waren Zaubermärchen und Geschichten über Riesen und Zwerge sehr beliebt. Eines der bekanntesten überlieferten Märchen ist die Erzählung von dem Zyklopen **Polyphemos**, der die Gefährten des Odysseus frisst.

Der römische Dichter Lucius Apuleius (125-180 v. Chr.) hat den satirischen Sittenroman „Metamorphosen" geschrieben, in dem uns eines der ersten römischen Märchen mit dem Titel **„Amor und Psyche"** überliefert worden ist.

Europäisches Mittelalter

Kreuzfahrer brachten über Spanien und Byzanz Märchen nach Europa. Heldensagen erinnern in z.B. der Artussage bis heute an diese Wurzeln.

Das Märchen vom gutgläubigen König ist unter dem Namen „Der Meisterlügner" seit dem 10. Jahrhundert bis heute bekannt: Darin soll derjenige, der eine Lüge erzählt, die nicht einmal der naive König glaubt, die Königstochter zur Frau bekommen.

Zwischen 1000 und 1050 schrieben vermutlich Mönche im bayerischen Kloster Tegernsee den **Rudolieb** auf. Das in lateinischen Hexametern gehaltene Werk gilt als der erste frei erfundene deutsche Roman. Heute sind nur mehr Bruchstücke der Handschrift erhalten. Der „Rudolieb" spiegelt eine gesamte Epoche wieder. In dem Roman wird vom Leben am Fürstenhof, in Bauernhäusern, auf Ritterburgen, in Dörfern und von Festen erzählt.

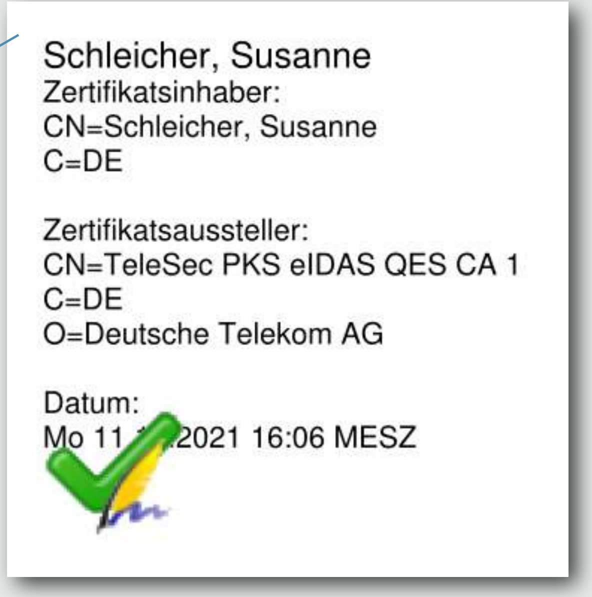
Das lateinische Märchen **Asinarius** haben die Brüder Grimm unter dem Namen „Das Eselein" bekannt gemacht. Die Fassung in den „Grimmschen Kinder- und Hausmärchen" lehnt sich an die Übersetzung eines Gedichtes an, die in acht Handschriften in verschiedenen Städten von München bis Leningrad vorliegt. Die älteste dieser Handschriften stammt spätestens aus dem 14. Jahrhundert. Der Ursprung des lateinischen Originals lässt sich bis in die Römerzeit zurück führen, nämlich auf das Motiv der Erzählung von „Amor- und Psyche". Außerdem gibt es uralte indische Erzählungen, von vornehmen Jünglingen in Tiergestalt (Adler, Affe, Esel etc.), die ihre menschliche Gestalt auf die gleiche Weise zurück gewinnen wie der Prinz im Märchen „Das Eselein".

Neuzeit

Schleicher, Susanne
Zertifikatsinhaber:
CN=Schleicher, Susanne
C=DE

Zertifikatsaussteller:
CN=TeleSec PKS eIDAS QES CA 1
C=DE
O=Deutsche Telekom AG

Datum:
Mo 11 2021 16:06 MESZ



Schleicher, Susanne
Zertifikatsinhaber:
CN=Schleicher, Susanne
C=DE

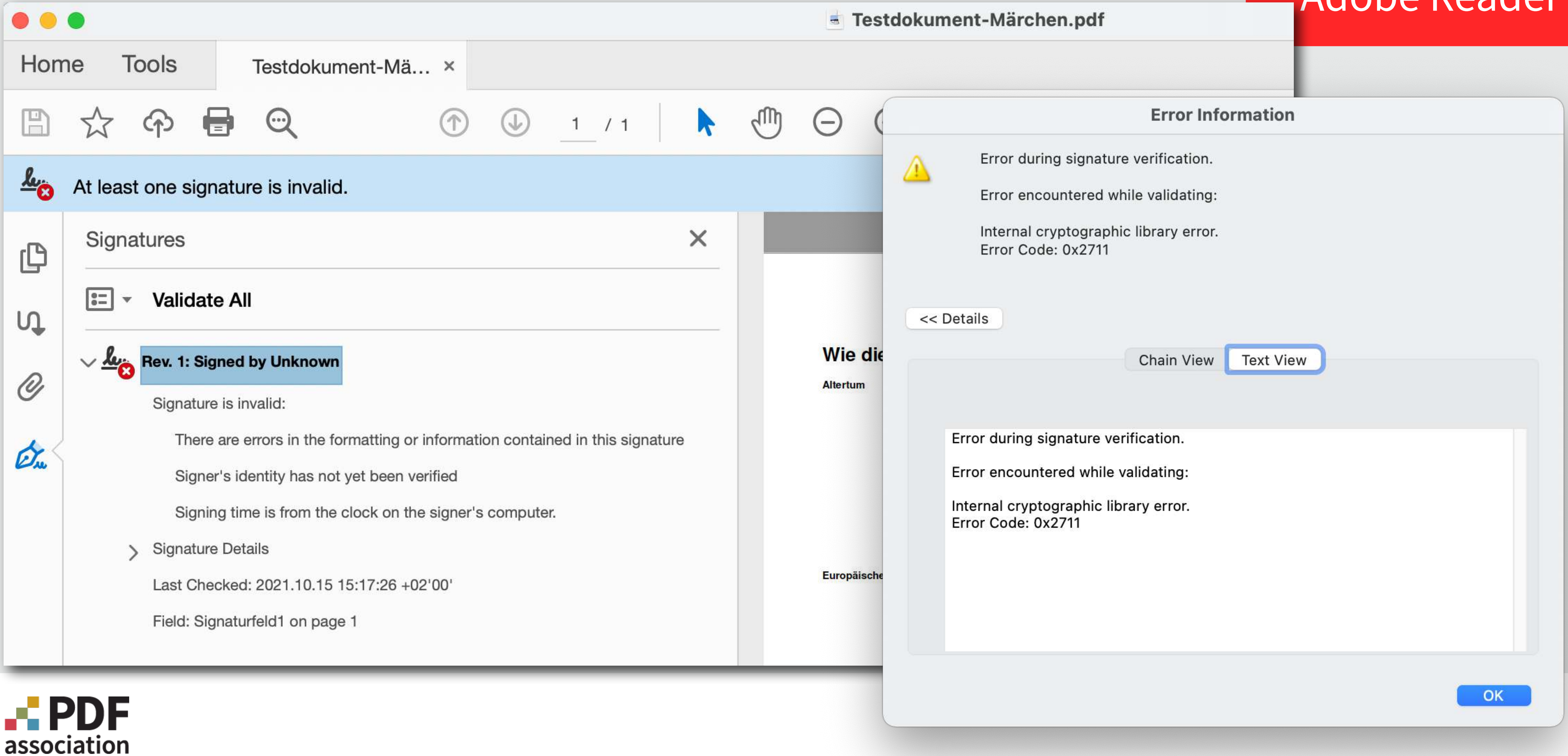
Zertifikatsaussteller:
CN=TeleSec PKS eIDAS QES CA 1
C=DE
O=Deutsche Telekom AG

Datum:
Mo 11 2021 16:06 MESZ

Test 1 – Telesec Smartcard QES

PDF Days Online 2021

Adobe Reader DC



At least one signature is invalid.

Signatures

Validate All

Rev. 1: Signed by Unknown

Signature is invalid:

There are errors in the formatting or information contained in this signature

Signer's identity has not yet been verified

Signing time is from the clock on the signer's computer.

Signature Details

Last Checked: 2021.10.15 15:17:26 +02'00'

Field: Signaturfeld1 on page 1

Error Information

Error during signature verification.

Error encountered while validating:

Internal cryptographic library error.
Error Code: 0x2711

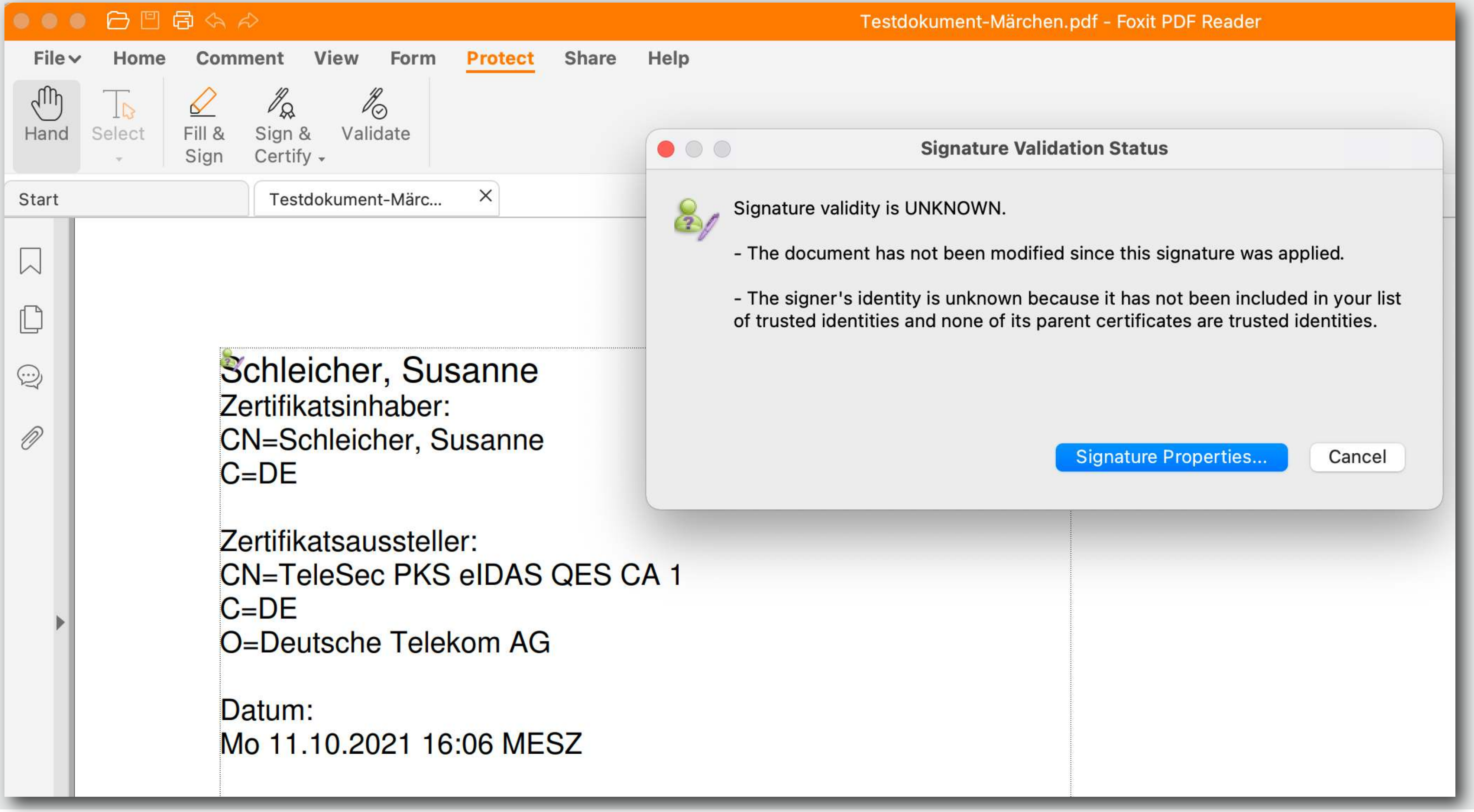
Error during signature verification.

Error encountered while validating:

Internal cryptographic library error.
Error Code: 0x2711

Test 1 – Telesec Smartcard QES

Foxit Reader



Signature validity is UNKNOWN.

- The document has not been modified since this signature was applied.

- The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.

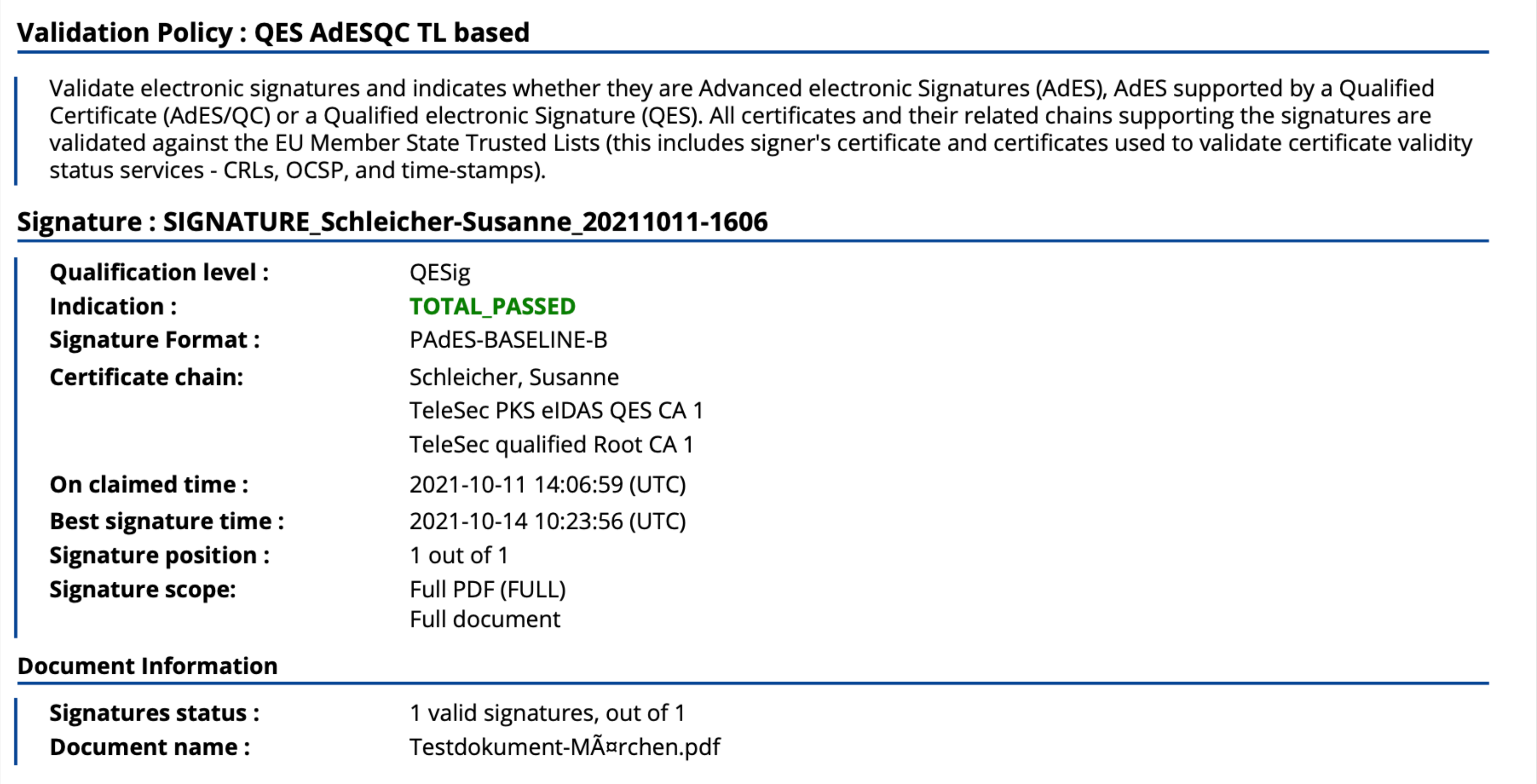
Schleicher, Susanne
Zertifikatsinhaber:
CN=Schleicher, Susanne
C=DE

Zertifikatsaussteller:
CN=TeleSec PKS eIDAS QES CA 1
C=DE
O=Deutsche Telekom AG

Datum:
Mo 11.10.2021 16:06 MESZ

Test 1 – Telesec Smartcard QES

EU DSS



Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature : SIGNATURE_Schleicher-Susanne_20211011-1606

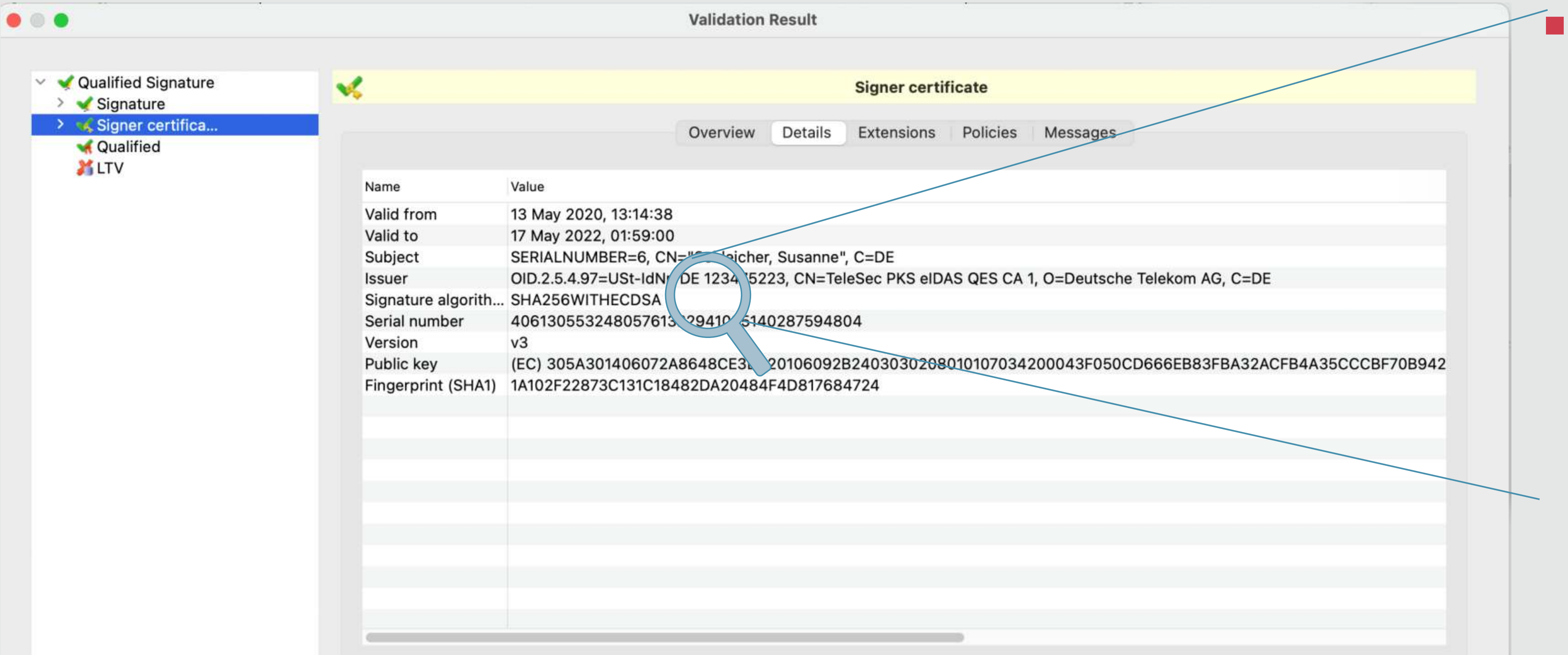
Qualification level :	QESig
Indication :	**TOTAL_PASSED**
Signature Format :	PAdES-BASELINE-B
Certificate chain:	Schleicher, Susanne TeleSec PKS eIDAS QES CA 1 TeleSec qualified Root CA 1
On claimed time :	2021-10-11 14:06:59 (UTC)
Best signature time :	2021-10-14 10:23:56 (UTC)
Signature position :	1 out of 1
Signature scope:	Full PDF (FULL) Full document

Document Information

Signatures status :	1 valid signatures, out of 1
Document name :	Testdokument-MÃ¤rchen.pdf

Test 1 – Telesec Smartcard QES

Sign Live! CC



Name	Value
Valid from	13 May 2020, 13:14:38
Valid to	17 May 2022, 01:59:00
Subject	SERIALNUMBER=6, CN="[illegible]eicher, Susanne", C=DE
Issuer	OID.2.5.4.97=USt-IdN[illegible]DE 1234[illegible]5223, CN=TeleSec PKS eIDAS QES CA 1, O=Deutsche Telekom AG, C=DE
Signature algorith...	SHA256WITHECDSA
Serial number	40613055324805761[illegible]29410[illegible]5140287594804
Version	v3
Public key	(EC) 305A301406072A8648CE3[illegible]20106092B2403030208010107034200043F050CD666EB83FBA32ACFB4A35CCCBF70B942
Fingerprint (SHA1)	1A102F22873C131C18482DA20484F4D817684724

- Signature Algorithm
  - SHA256WITHECDSA
  - Elliptic Curves
  - brainpoolP256r1

Remark: ISO/DTS 32002 will heal this!

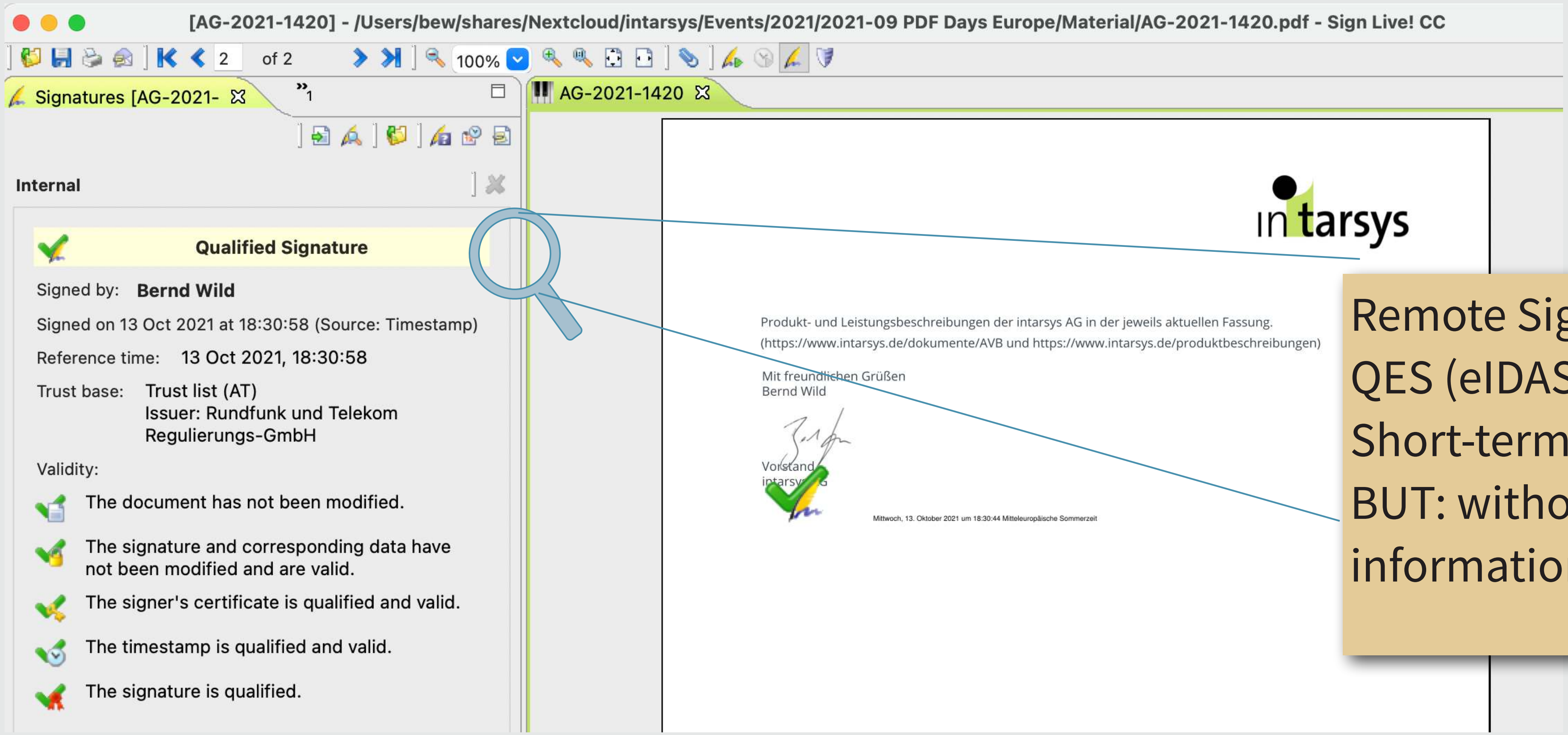
Test 1 – Telesec Smartcard QES

Smartcard-based certificate
eIDAS QES

Validation Application	Overall Result	Remarks
Sign Live! CC	✓	
Adobe Reader DC	✗	Undefined validation result; Does not support the EC algorithm with brainpool parameters
Foxit Reader	✗	Undefined validation result
EU DSS	✓	

Test 2 – AIS QES

Sign Live! CC


[AG-2021-1420] - /Users/bew/shares/Nextcloud/intarsys/Events/2021/2021-09 PDF Days Europe/Material/AG-2021-1420.pdf - Sign Live! CC
2
of 2
100%
Signatures [AG-2021-
AG-2021-1420
Internal
intarsys

Qualified Signature

Signed by: **Bernd Wild**

Signed on 13 Oct 2021 at 18:30:58 (Source: Timestamp)

Reference time: 13 Oct 2021, 18:30:58

Trust base: Trust list (AT)
Issuer: Rundfunk und Telekom
Regulierungs-GmbH

Validity:

- The document has not been modified.
- The signature and corresponding data have not been modified and are valid.
- The signer's certificate is qualified and valid.
- The timestamp is qualified and valid.
- The signature is qualified.

Produkt- und Leistungsbeschreibungen der intarsys AG in der jeweils aktuellen Fassung.
(https://www.intarsys.de/dokumente/AVB und https://www.intarsys.de/produktbeschreibungen)

Mit freundlichen Grüßen
Bernd Wild

Vorstand
intarsy G

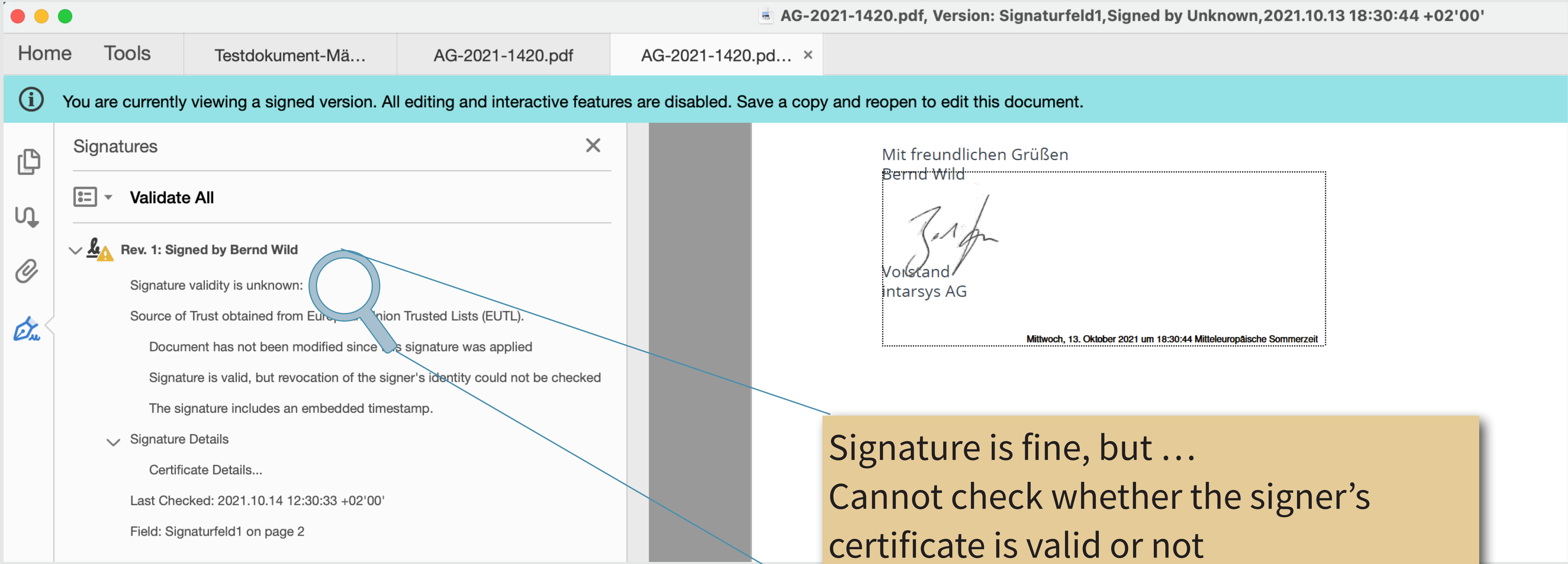
Mittwoch, 13. Oktober 2021 um 18:30:44 Mitteleuropäische Sommerzeit

Remote Signature with SwissCom AIS QES (eIDAS)
Short-term certificates
BUT: without embedding LTV informations

Test 2 – AIS QES

PDF Days Online 2021

Adobe Reader DC



AG-2021-1420.pdf, Version: Signaturfeld1,Signed by Unknown,2021.10.13 18:30:44 +02'00'

You are currently viewing a signed version. All editing and interactive features are disabled. Save a copy and reopen to edit this document.

Rev. 1: Signed by Bernd Wild

Signature validity is unknown:

Source of Trust obtained from Eur[illegible]nion Trusted Lists (EUTL).

Document has not been modified since [illegible]s signature was applied

Signature is valid, but revocation of the signer's identity could not be checked

The signature includes an embedded timestamp.

Signature Details

Certificate Details...

Last Checked: 2021.10.14 12:30:33 +02'00'

Field: Signaturfeld1 on page 2

Mit freundlichen Grüßen
Bernd Wild

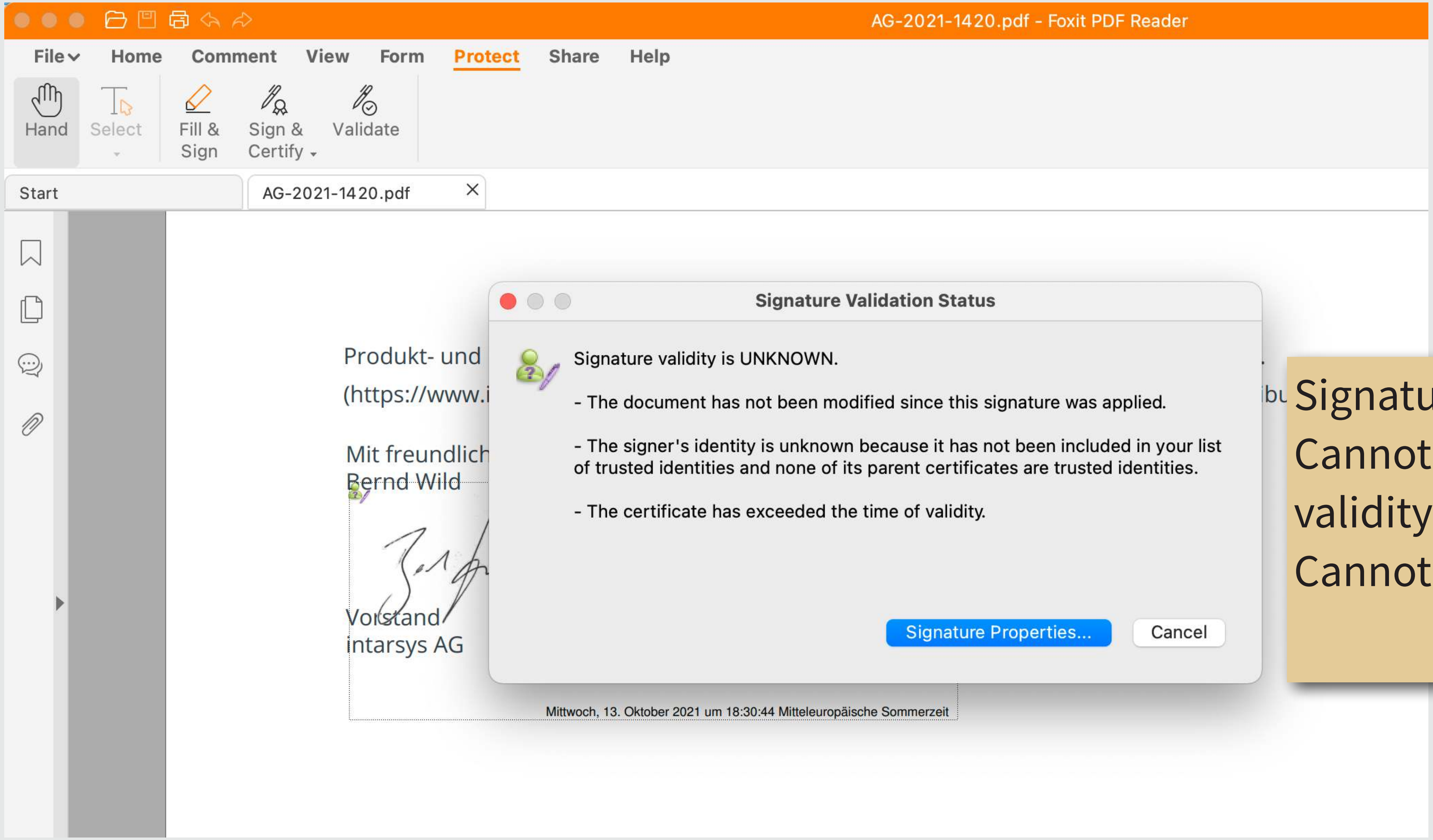
Vorstand
intarsys AG

Mittwoch, 13. Oktober 2021 um 18:30:44 Mitteleuropäische Sommerzeit

Signature is fine, but …
Cannot check whether the signer’s certificate is valid or not

Test 2 – AIS QES

Foxit Reader



Signature Validation Status

Signature validity is UNKNOWN.

- The document has not been modified since this signature was applied.

- The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.

- The certificate has exceeded the time of validity.

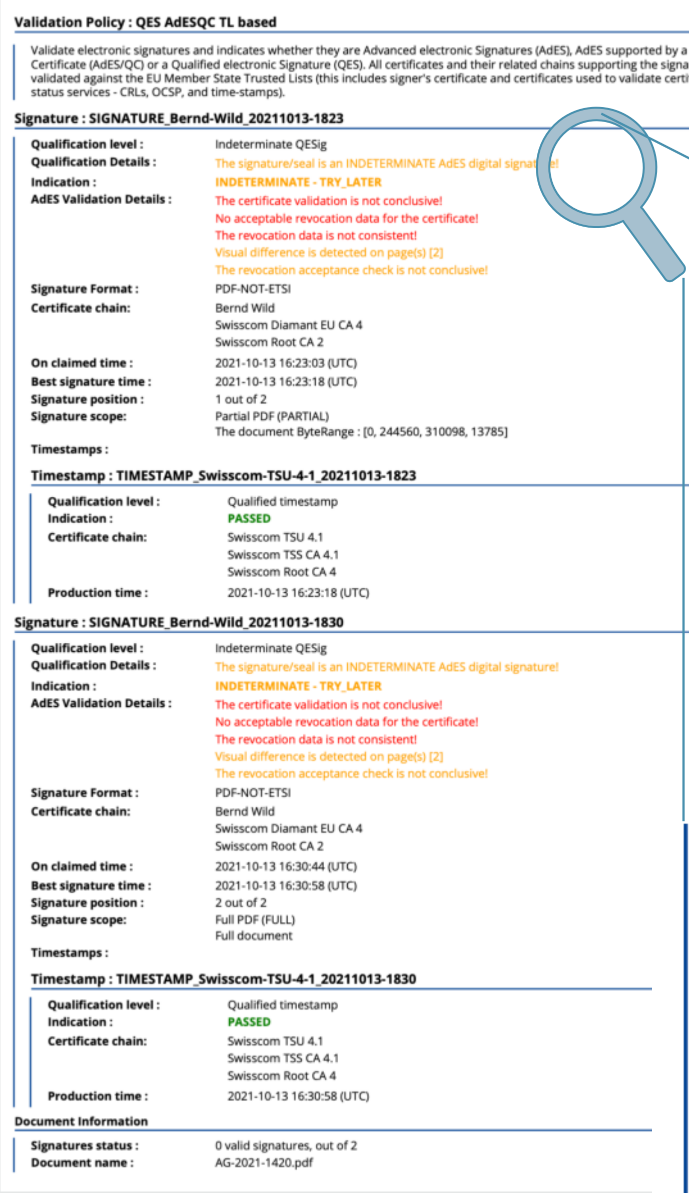
Signature Properties... Cancel

Signature is fine, but …

Cannot check the signer’s identity and validity of certificate

Cannot handle short-term certificates

Test 2 – AIS QES



Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature : SIGNATURE_Bernd-Wild_20211013-1823

Qualification level :	Indeterminate QESig
Qualification Details :	The signature/seal is an INDETERMINATE AdES digital signature!
Indication :	**INDETERMINATE - TRY_LATER**
AdES Validation Details :	The certificate validation is not conclusive! No acceptable revocation data for the certificate! The revocation data is not consistent! Visual difference is detected on page(s) [2] The revocation acceptance check is not conclusive!
Signature Format :	PDF-NOT-ETSI
Certificate chain:	Bernd Wild Swisscom Diamant EU CA 4 Swisscom Root CA 2
On claimed time :	2021-10-13 16:23:03 (UTC)
Best signature time :	2021-10-13 16:23:18 (UTC)
Signature position :	1 out of 2
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 244560, 310098, 13785]
Timestamps :	

Timestamp : TIMESTAMP_Swisscom-TSU-4-1_20211013-1823

Qualification level :	Qualified timestamp
Indication :	**PASSED**
Certificate chain:	Swisscom TSU 4.1 Swisscom TSS CA 4.1 Swisscom Root CA 4
Production time :	2021-10-13 16:23:18 (UTC)

Signature : SIGNATURE_Bernd-Wild_20211013-1830

Qualification level :	Indeterminate QESig
Qualification Details :	The signature/seal is an INDETERMINATE AdES digital signature!
Indication :	**INDETERMINATE - TRY_LATER**
AdES Validation Details :	The certificate validation is not conclusive! No acceptable revocation data for the certificate! The revocation data is not consistent! Visual difference is detected on page(s) [2] The revocation acceptance check is not conclusive!
Signature Format :	PDF-NOT-ETSI
Certificate chain:	Bernd Wild Swisscom Diamant EU CA 4 Swisscom Root CA 2
On claimed time :	2021-10-13 16:30:44 (UTC)
Best signature time :	2021-10-13 16:30:58 (UTC)
Signature position :	2 out of 2
Signature scope:	Full PDF (FULL) Full document
Timestamps :	

Timestamp : TIMESTAMP_Swisscom-TSU-4-1_20211013-1830

Qualification level :	Qualified timestamp
Indication :	**PASSED**
Certificate chain:	Swisscom TSU 4.1 Swisscom TSS CA 4.1 Swisscom Root CA 4
Production time :	2021-10-13 16:30:58 (UTC)

Document Information

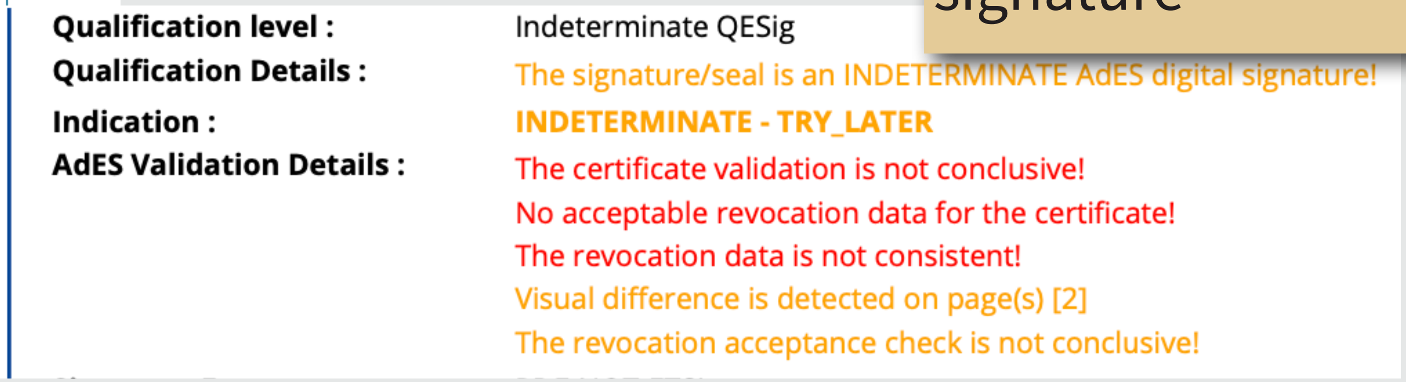
Signatures status :	0 valid signatures, out of 2
Document name :	AG-2021-1420.pdf

EU DSS

Result is … TRY_LATER – INDETERMINATE

Some problems with the revocation data of the short-term certificate

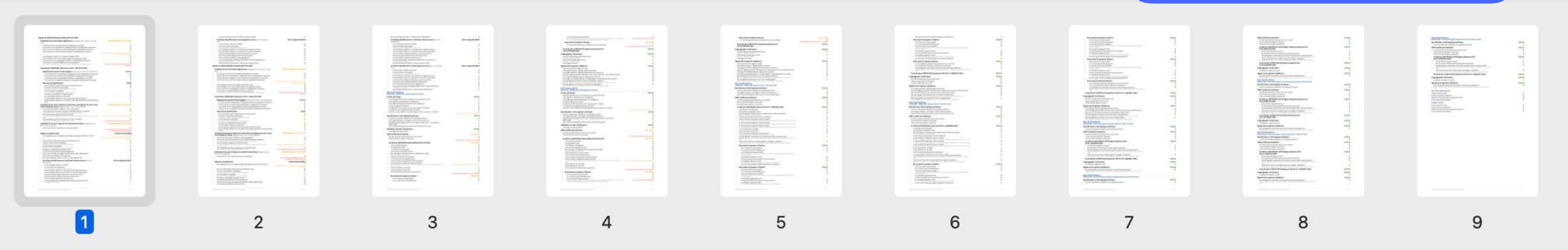
Some information about visual difference —> the overlay image of the handwritten signature



Qualification level :	Indeterminate QESig
Qualification Details :	The signature/seal is an INDETERMINATE AdES digital signature!
Indication :	**INDETERMINATE - TRY_LATER**
AdES Validation Details :	The certificate validation is not conclusive! No acceptable revocation data for the certificate! The revocation data is not consistent! Visual difference is detected on page(s) [2] The revocation acceptance check is not conclusive!

Test 2 – AIS QES

EU DSS



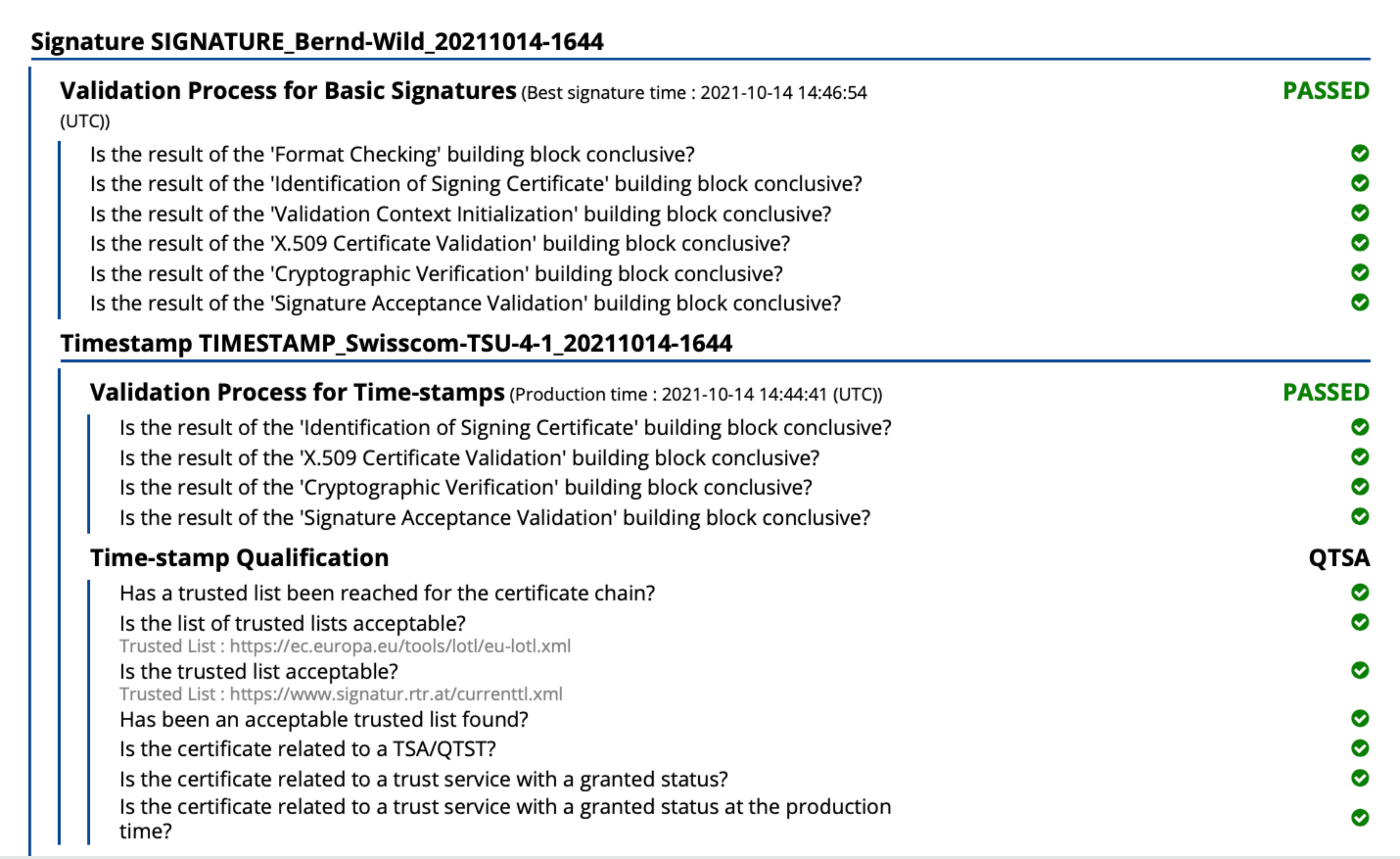
Detailed report is 9 pages long

Shows all checks to be done during the validation process

Illustrates the complexity of the validation process

Test 2 – AIS QES

EU DSS



Signature SIGNATURE_Bernd-Wild_20211014-1644

Validation Process for Basic Signatures (Best signature time : 2021-10-14 14:46:54 (UTC)) **PASSED**

- Is the result of the 'Format Checking' building block conclusive? ✓
- Is the result of the 'Identification of Signing Certificate' building block conclusive? ✓
- Is the result of the 'Validation Context Initialization' building block conclusive? ✓
- Is the result of the 'X.509 Certificate Validation' building block conclusive? ✓
- Is the result of the 'Cryptographic Verification' building block conclusive? ✓
- Is the result of the 'Signature Acceptance Validation' building block conclusive? ✓

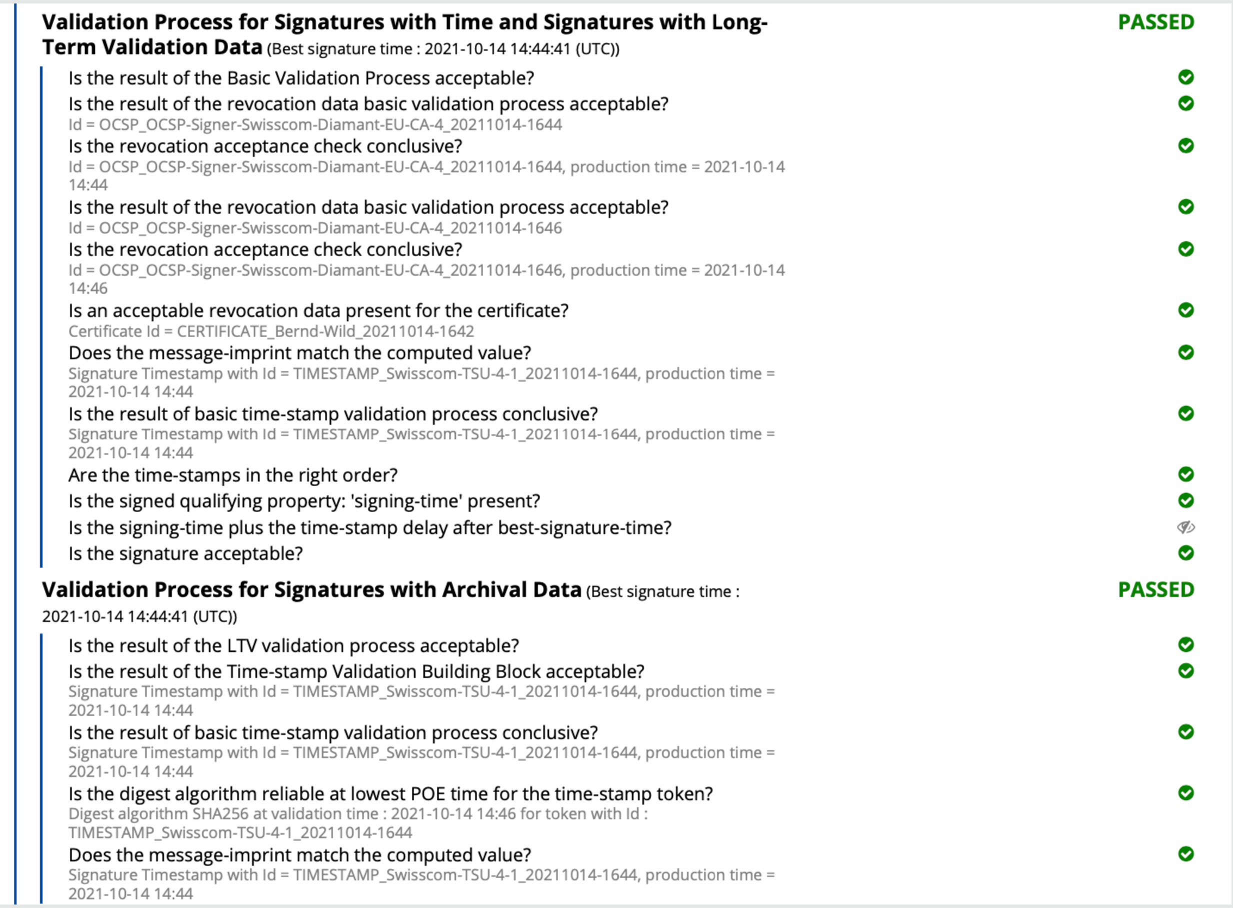
Timestamp TIMESTAMP_Swisscom-TSU-4-1_20211014-1644

Validation Process for Time-stamps (Production time : 2021-10-14 14:44:41 (UTC)) **PASSED**

- Is the result of the 'Identification of Signing Certificate' building block conclusive? ✓
- Is the result of the 'X.509 Certificate Validation' building block conclusive? ✓
- Is the result of the 'Cryptographic Verification' building block conclusive? ✓
- Is the result of the 'Signature Acceptance Validation' building block conclusive? ✓

Time-stamp Qualification **QTSA**

- Has a trusted list been reached for the certificate chain? ✓
- Is the list of trusted lists acceptable? ✓
  Trusted List : https://ec.europa.eu/tools/lotl/eu-lotl.xml
- Is the trusted list acceptable? ✓
  Trusted List : https://www.signatur.rtr.at/currenttl.xml
- Has been an acceptable trusted list found? ✓
- Is the certificate related to a TSA/QTST? ✓
- Is the certificate related to a trust service with a granted status? ✓
- Is the certificate related to a trust service with a granted status at the production time? ✓



Validation Process for Signatures with Time and Signatures with Long-Term Validation Data (Best signature time : 2021-10-14 14:44:41 (UTC)) **PASSED**

- Is the result of the Basic Validation Process acceptable? ✓
- Is the result of the revocation data basic validation process acceptable? ✓
  Id = OCSP_OCSP-Signer-Swisscom-Diamant-EU-CA-4_20211014-1644
- Is the revocation acceptance check conclusive? ✓
  Id = OCSP_OCSP-Signer-Swisscom-Diamant-EU-CA-4_20211014-1644, production time = 2021-10-14 14:44
- Is the result of the revocation data basic validation process acceptable? ✓
  Id = OCSP_OCSP-Signer-Swisscom-Diamant-EU-CA-4_20211014-1646
- Is the revocation acceptance check conclusive? ✓
  Id = OCSP_OCSP-Signer-Swisscom-Diamant-EU-CA-4_20211014-1646, production time = 2021-10-14 14:46
- Is an acceptable revocation data present for the certificate? ✓
  Certificate Id = CERTIFICATE_Bernd-Wild_20211014-1642
- Does the message-imprint match the computed value? ✓
  Signature Timestamp with Id = TIMESTAMP_Swisscom-TSU-4-1_20211014-1644, production time = 2021-10-14 14:44
- Is the result of basic time-stamp validation process conclusive? ✓
  Signature Timestamp with Id = TIMESTAMP_Swisscom-TSU-4-1_20211014-1644, production time = 2021-10-14 14:44
- Are the time-stamps in the right order? ✓
- Is the signed qualifying property: 'signing-time' present? ✓
- Is the signing-time plus the time-stamp delay after best-signature-time?
- Is the signature acceptable? ✓

Validation Process for Signatures with Archival Data (Best signature time : 2021-10-14 14:44:41 (UTC)) **PASSED**

- Is the result of the LTV validation process acceptable? ✓
- Is the result of the Time-stamp Validation Building Block acceptable? ✓
  Signature Timestamp with Id = TIMESTAMP_Swisscom-TSU-4-1_20211014-1644, production time = 2021-10-14 14:44
- Is the result of basic time-stamp validation process conclusive? ✓
  Signature Timestamp with Id = TIMESTAMP_Swisscom-TSU-4-1_20211014-1644, production time = 2021-10-14 14:44
- Is the digest algorithm reliable at lowest POE time for the time-stamp token? ✓
  Digest algorithm SHA256 at validation time : 2021-10-14 14:46 for token with Id : TIMESTAMP_Swisscom-TSU-4-1_20211014-1644
- Does the message-imprint match the computed value? ✓
  Signature Timestamp with Id = TIMESTAMP_Swisscom-TSU-4-1_20211014-1644, production time = 2021-10-14 14:44

Example of an detailed validation report

Test 2 – AIS QES

swisscom

AIS Remote Signature QES eIDAS

Ad-hoc (short-term) certificate

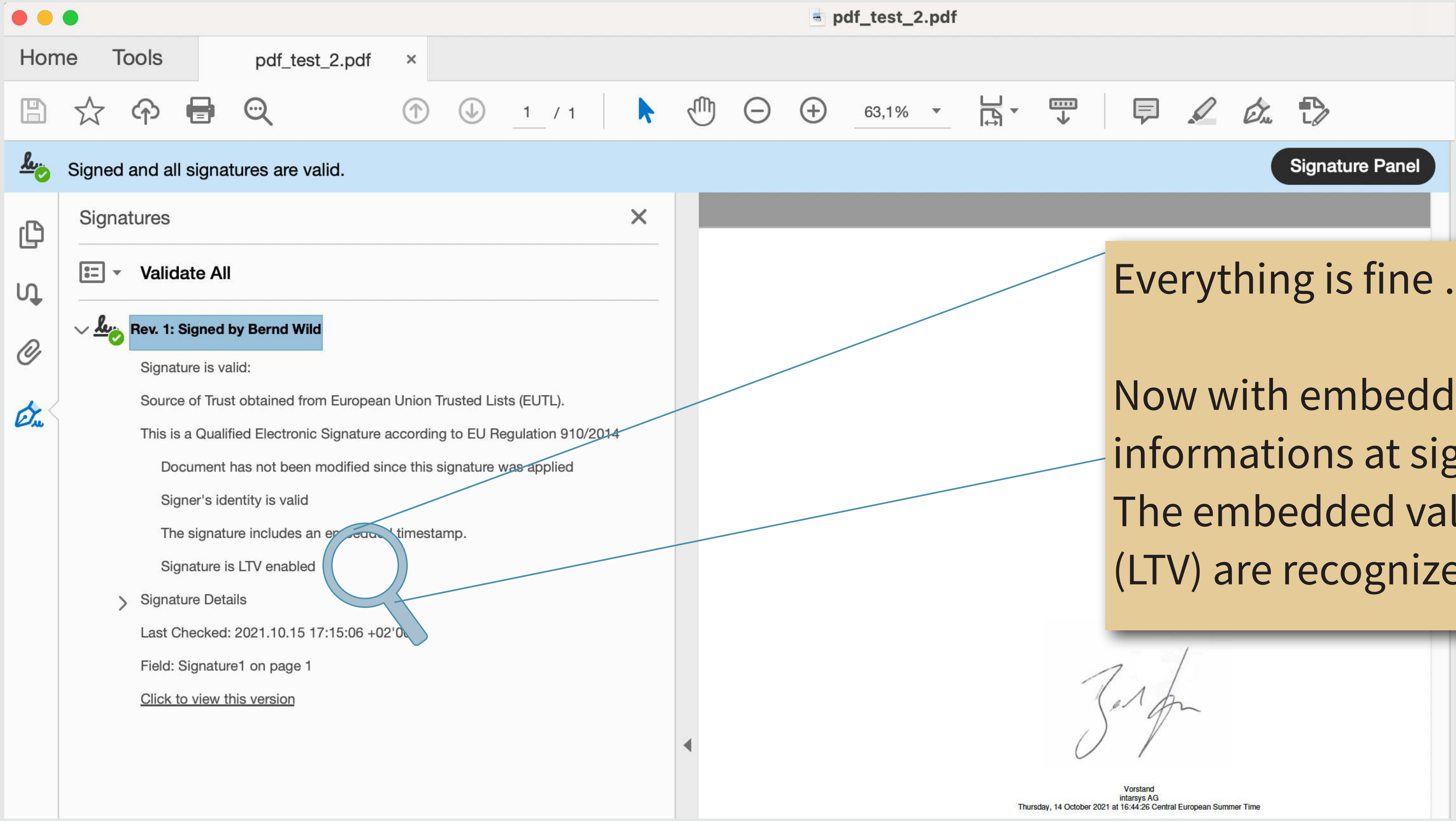
With referenced LTV information

Validation Application	Overall Result	Remarks
Sign Live! CC	✓	Implements draft EN119102-1 v1.2.3
Adobe Reader DC	✓ ?	Signature is OK, but user identity could not be verified due to missing revocation information; OK as it is EN119102-1 v1.1.1 based
Foxit Reader	✓ ?	Signature is OK, but user identity could not be verified due to missing revocation information; OK as it is EN119102-1 v1.1.1 based
EU DSS	✓ ?	Signature is OK, but user identity could not be verified due to missing revocation information; OK as it is EN119102-1 v1.1.1 based

Test 3 – AIS QES (LTV)

PDF Days Online 2021

Adobe Reader DC



Signed and all signatures are valid.

Rev. 1: Signed by Bernd Wild

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

This is a Qualified Electronic Signature according to EU Regulation 910/2014

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Signature Details

Last Checked: 2021.10.15 17:15:06 +02'00'

Field: Signature1 on page 1

Click to view this version

Vorstand
intarsys AG
Thursday, 14 October 2021 at 16:44:26 Central European Summer Time

Everything is fine …

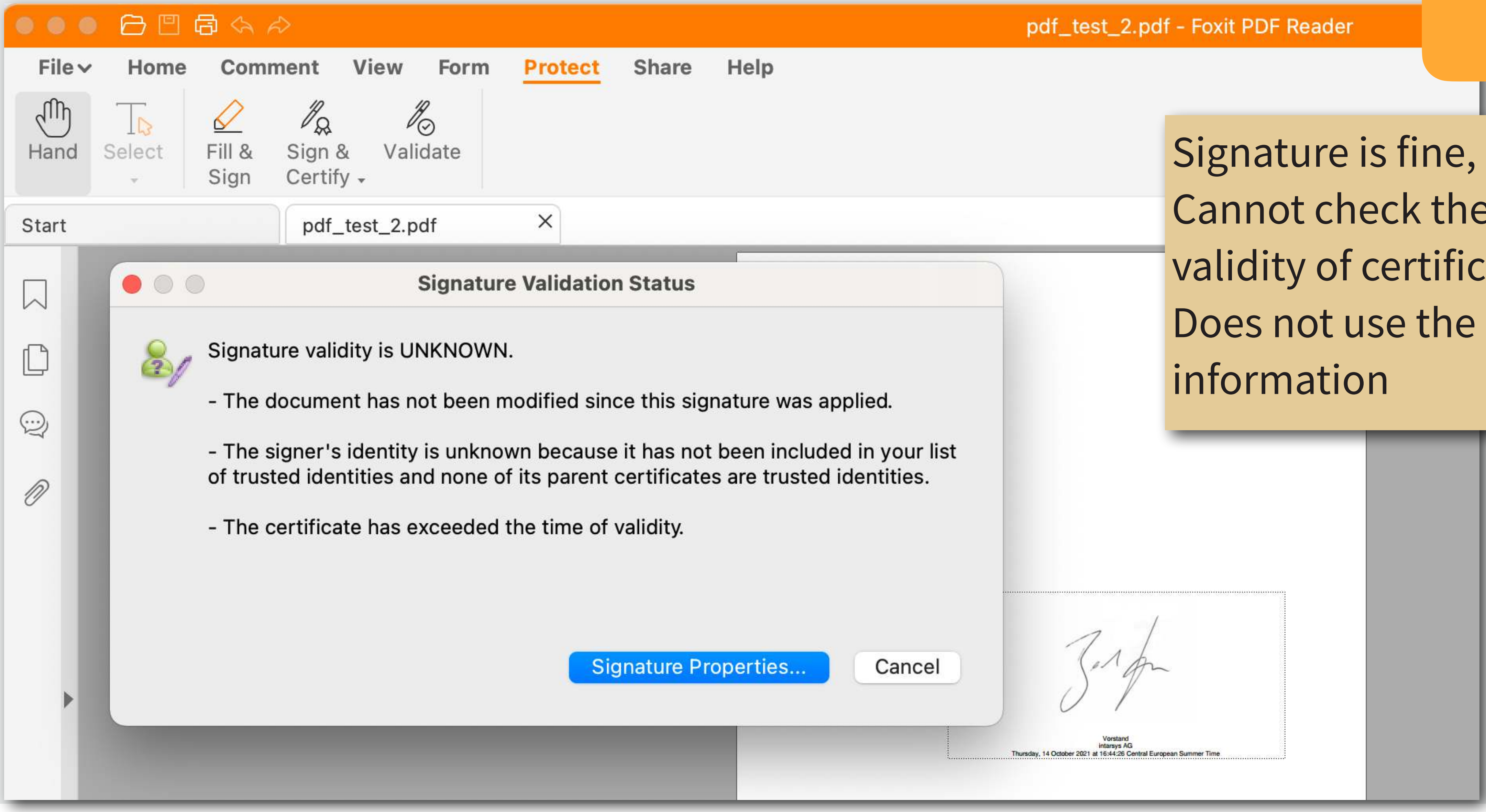
Now with embedded validation informations at signing time
The embedded validation informations (LTV) are recognized and been validated

PDF association

Test 3 – AIS QES (LTV)

PDF Days Online 2021

Foxit Reader



Signature Validation Status

Signature validity is UNKNOWN.

- The document has not been modified since this signature was applied.

- The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.

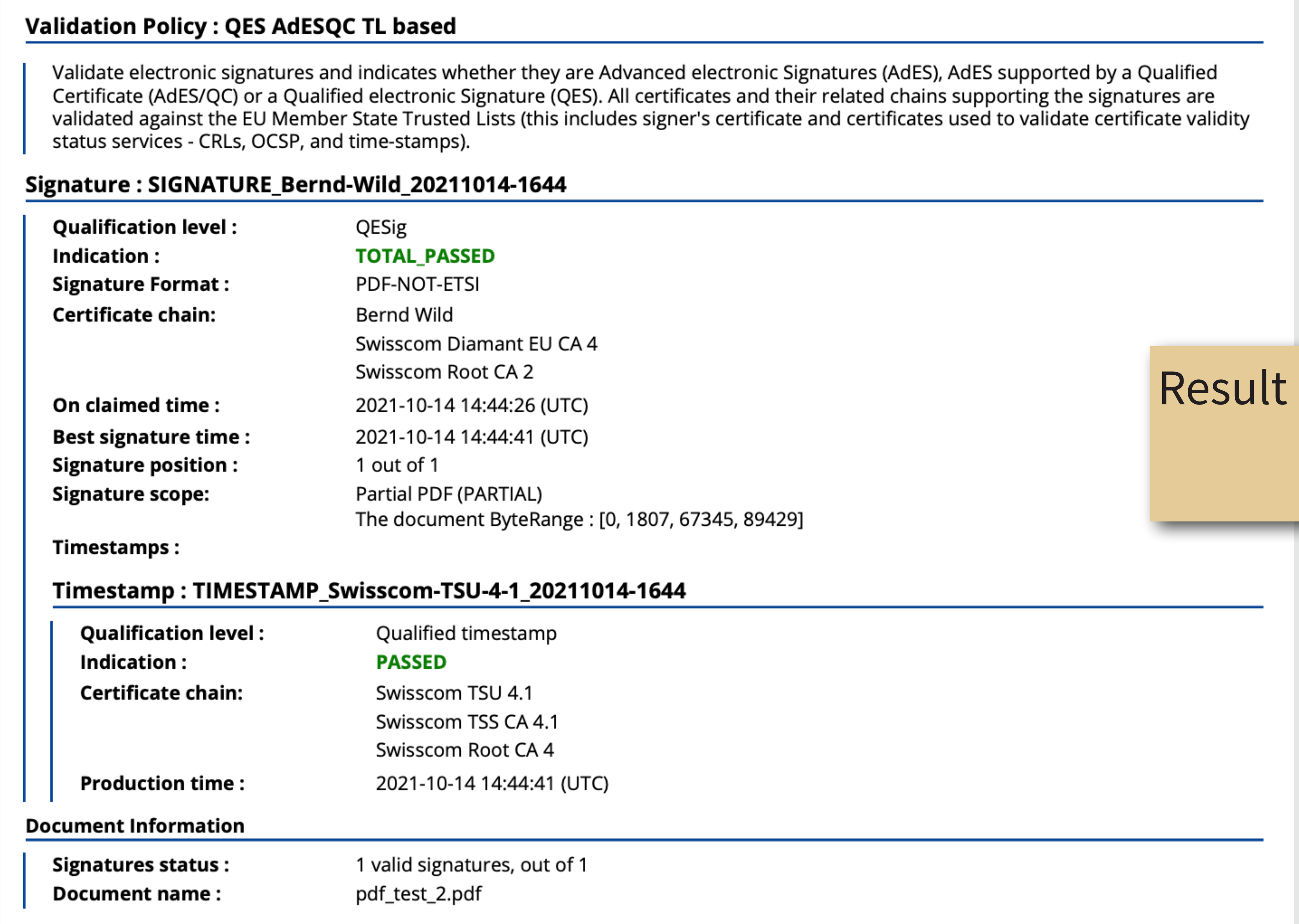
- The certificate has exceeded the time of validity.

Vorstand
intarsys AG
Thursday, 14 October 2021 at 16:44:26 Central European Summer Time

Signature is fine, but …
Cannot check the signer’s identity and validity of certificate
Does not use the embedded LTV information

Test 3 – AIS QES (LTV)

EU DSS



Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature : SIGNATURE_Bernd-Wild_20211014-1644

Qualification level :	QESig
Indication :	**TOTAL_PASSED**
Signature Format :	PDF-NOT-ETSI
Certificate chain:	Bernd Wild Swisscom Diamant EU CA 4 Swisscom Root CA 2
On claimed time :	2021-10-14 14:44:26 (UTC)
Best signature time :	2021-10-14 14:44:41 (UTC)
Signature position :	1 out of 1
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 1807, 67345, 89429]
Timestamps :	

Timestamp : TIMESTAMP_Swisscom-TSU-4-1_20211014-1644

Qualification level :	Qualified timestamp
Indication :	**PASSED**
Certificate chain:	Swisscom TSU 4.1 Swisscom TSS CA 4.1 Swisscom Root CA 4
Production time :	2021-10-14 14:44:41 (UTC)

Document Information

Signatures status :	1 valid signatures, out of 1
Document name :	pdf_test_2.pdf

Result is now OK!

Test 3 – AIS QES (LTV)

swisscom

AIS Remote Signature QES eIDAS

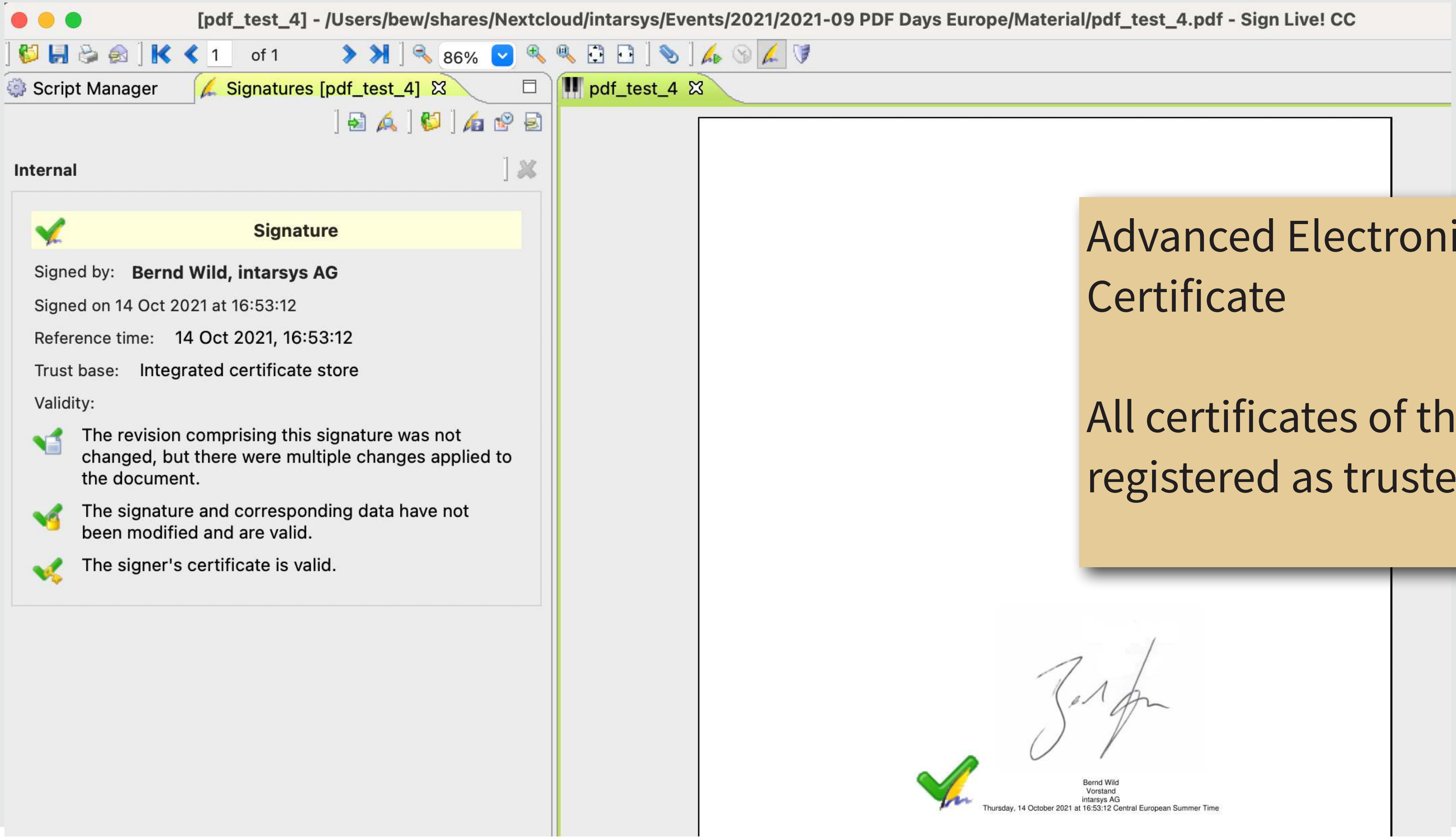
Ad-hoc (short-term) certificate

With embedded LTV information

Validation Application	Overall Result	Remarks
Sign Live! CC	✓	
Adobe Reader DC	✓	
Foxit Reader	✓ ?	Signature is OK, but user identity could not be verified due to certificate expiry
EU DSS	✓	

Test 4 – D-Trust AES

Sign Live! CC


[pdf_test_4] - /Users/bew/shares/Nextcloud/intarsys/Events/2021/2021-09 PDF Days Europe/Material/pdf_test_4.pdf - Sign Live! CC
1
of 1
86%
Script Manager
Signatures [pdf_test_4]
pdf_test_4
Internal

Signature

Signed by: **Bernd Wild, intarsys AG**

Signed on 14 Oct 2021 at 16:53:12

Reference time: 14 Oct 2021, 16:53:12

Trust base: Integrated certificate store

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.

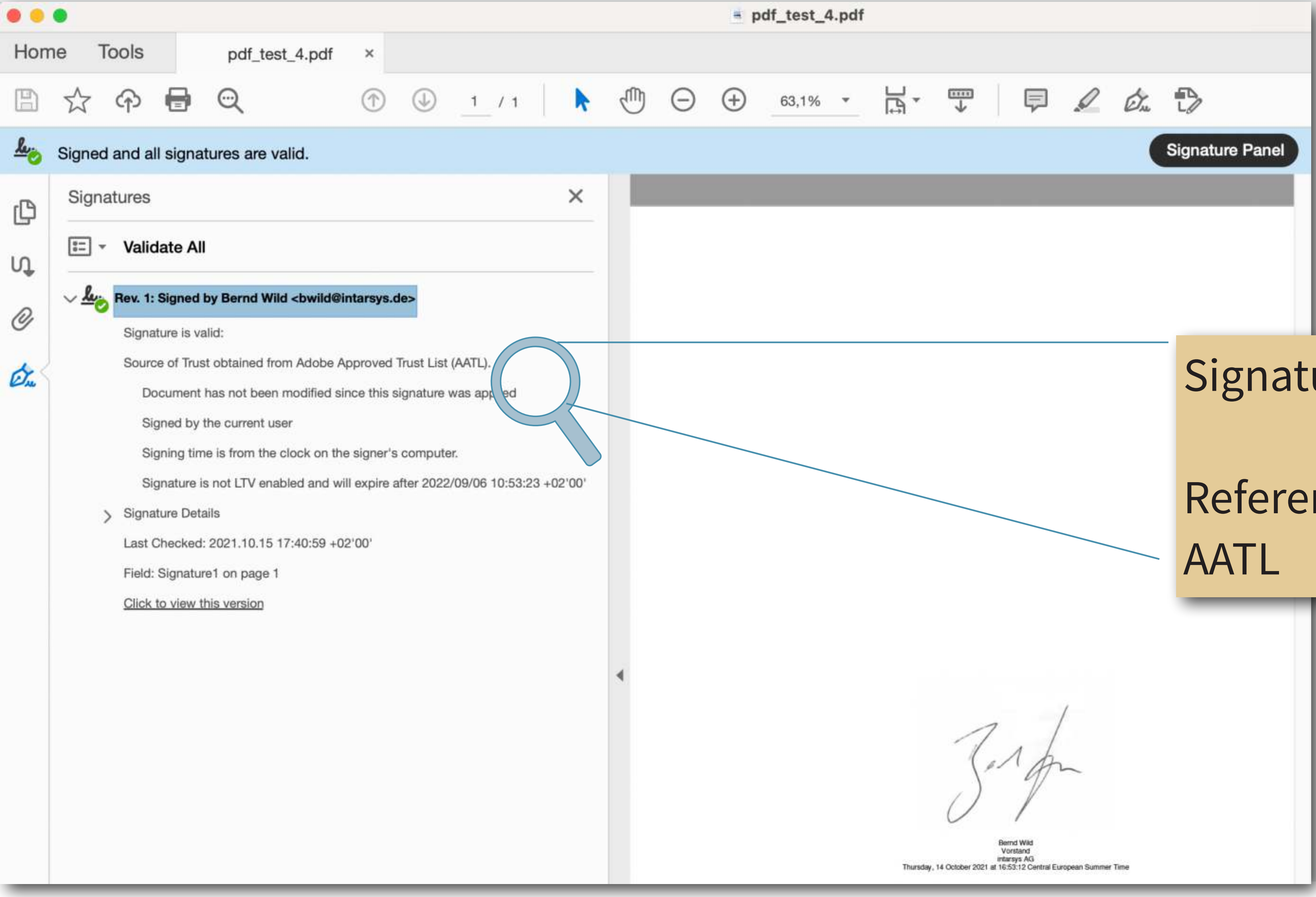
Bernd Wild
Vorstand
intarsys AG
Thursday, 14 October 2021 at 16:53:12 Central European Summer Time

Advanced Electronic Signature with Soft Certificate

All certificates of the certificate chain are registered as trusted

Test 4 – D-Trust AES

Adobe Reader DC



Signed and all signatures are valid.

Rev. 1: Signed by Bernd Wild <bwild@intarsys.de>

Signature is valid:

Source of Trust obtained from Adobe Approved Trust List (AATL).

Document has not been modified since this signature was applied

Signed by the current user

Signing time is from the clock on the signer's computer.

Signature is not LTV enabled and will expire after 2022/09/06 10:53:23 +02'00'

Signature Details

Last Checked: 2021.10.15 17:40:59 +02'00'

Field: Signature1 on page 1

Click to view this version

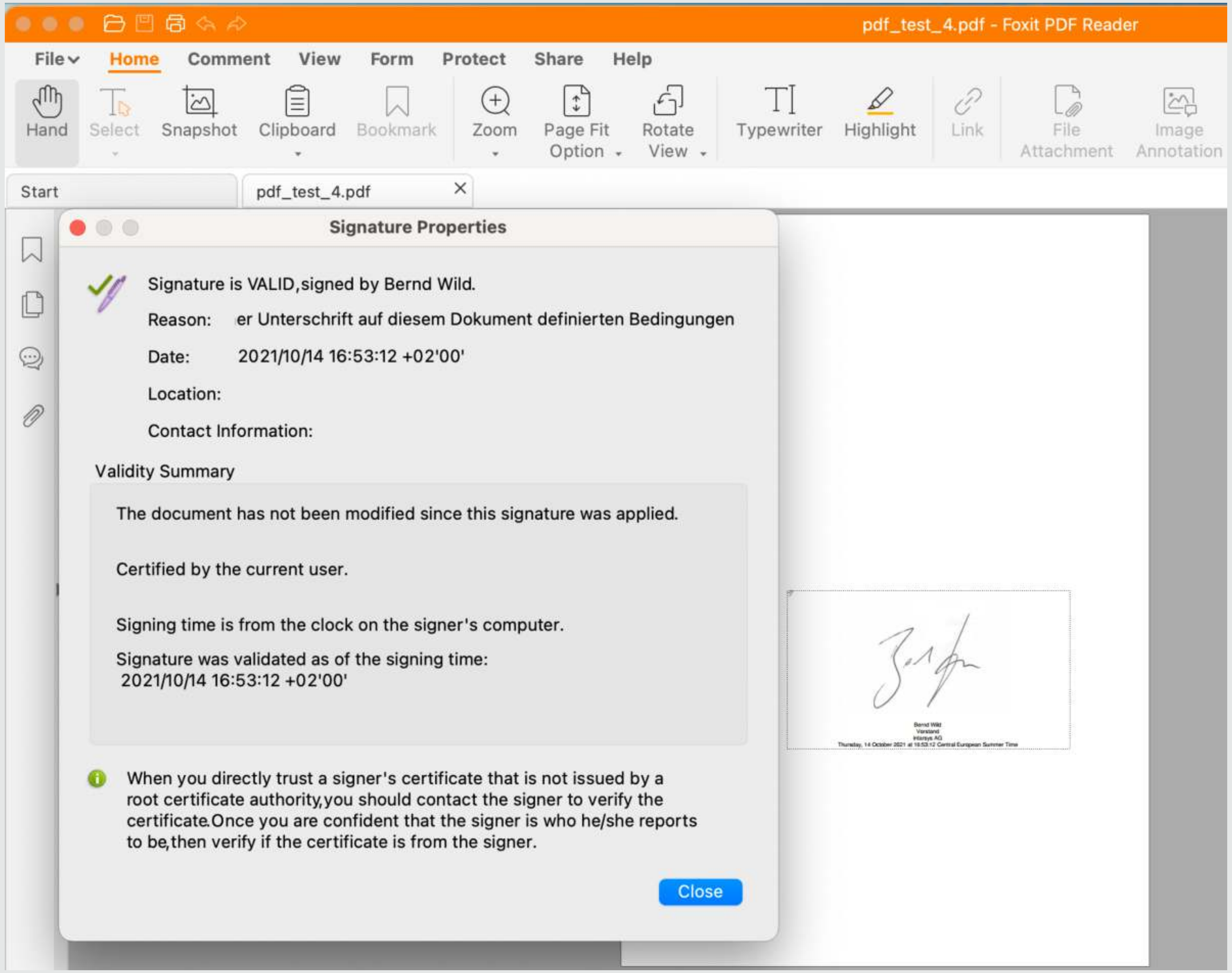
Bernd Wild
Vorstand
intarsys AG
Thursday, 14 October 2021 at 16:53:12 Central European Summer Time

Signature and user certificate are OK

Referenced root certificate is member of AATL

Test 4 – D-Trust AES

Foxit Reader



Signature Properties

Signature is VALID,signed by Bernd Wild.

Reason: er Unterschrift auf diesem Dokument definierten Bedingungen

Date: 2021/10/14 16:53:12 +02'00'

Location:

Contact Information:

Validity Summary

The document has not been modified since this signature was applied.

Certified by the current user.

Signing time is from the clock on the signer's computer.

Signature was validated as of the signing time:
2021/10/14 16:53:12 +02'00'

When you directly trust a signer's certificate that is not issued by a root certificate authority,you should contact the signer to verify the certificate.Once you are confident that the signer is who he/she reports to be,then verify if the certificate is from the signer.

Close

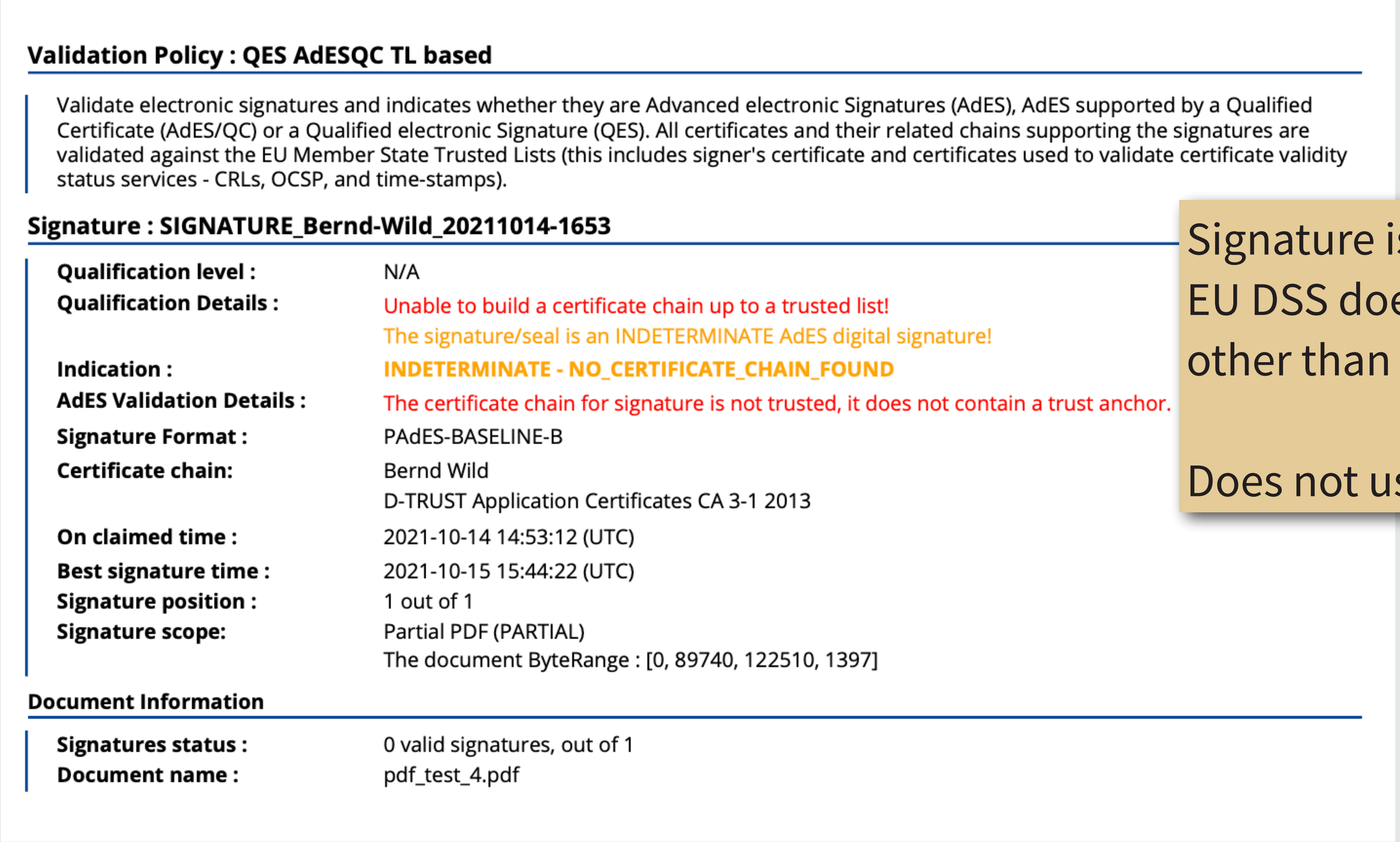
Bernd Wild
Vorstand
intarsys AG
Thursday, 14 October 2021 at 16:53:12 Central European Summer Time

Signature and user certificate are OK

Referenced root certificate is member of AATL

Test 4 – D-Trust AES

EU DSS



Validation Policy : QES AdESQC TL based

Validate electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature : SIGNATURE_Bernd-Wild_20211014-1653

Qualification level :	N/A
Qualification Details :	Unable to build a certificate chain up to a trusted list! The signature/seal is an INDETERMINATE AdES digital signature!
Indication :	**INDETERMINATE - NO_CERTIFICATE_CHAIN_FOUND**
AdES Validation Details :	The certificate chain for signature is not trusted, it does not contain a trust anchor.
Signature Format :	PAdES-BASELINE-B
Certificate chain:	Bernd Wild D-TRUST Application Certificates CA 3-1 2013
On claimed time :	2021-10-14 14:53:12 (UTC)
Best signature time :	2021-10-15 15:44:22 (UTC)
Signature position :	1 out of 1
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 89740, 122510, 1397]

Document Information

Signatures status :	0 valid signatures, out of 1
Document name :	pdf_test_4.pdf

Signature is OK but
EU DSS does not validate certificate chains other than ones ending in the EU TL

Does not use the AATL

Test 4 – D-Trust AES

D-TRUST

Personal ID
AES

Soft certificate

Derived from AATL

Validation Application	Overall Result	Remarks
Sign Live! CC	✓	
Adobe Reader DC	✓	
Foxit Reader	✓	
EU DSS	✓ ✗	Signature is OK, but user identity could not be verified due to missing trusted root

Overall Test Results

- Although we observe different validation results
  - All implementations comply with the existing standards (within the degree of freedom)
  - No false-positives could be seen
- Nevertheless, the user experience in these scenarios could be better …

Why’s Validation So Hard?

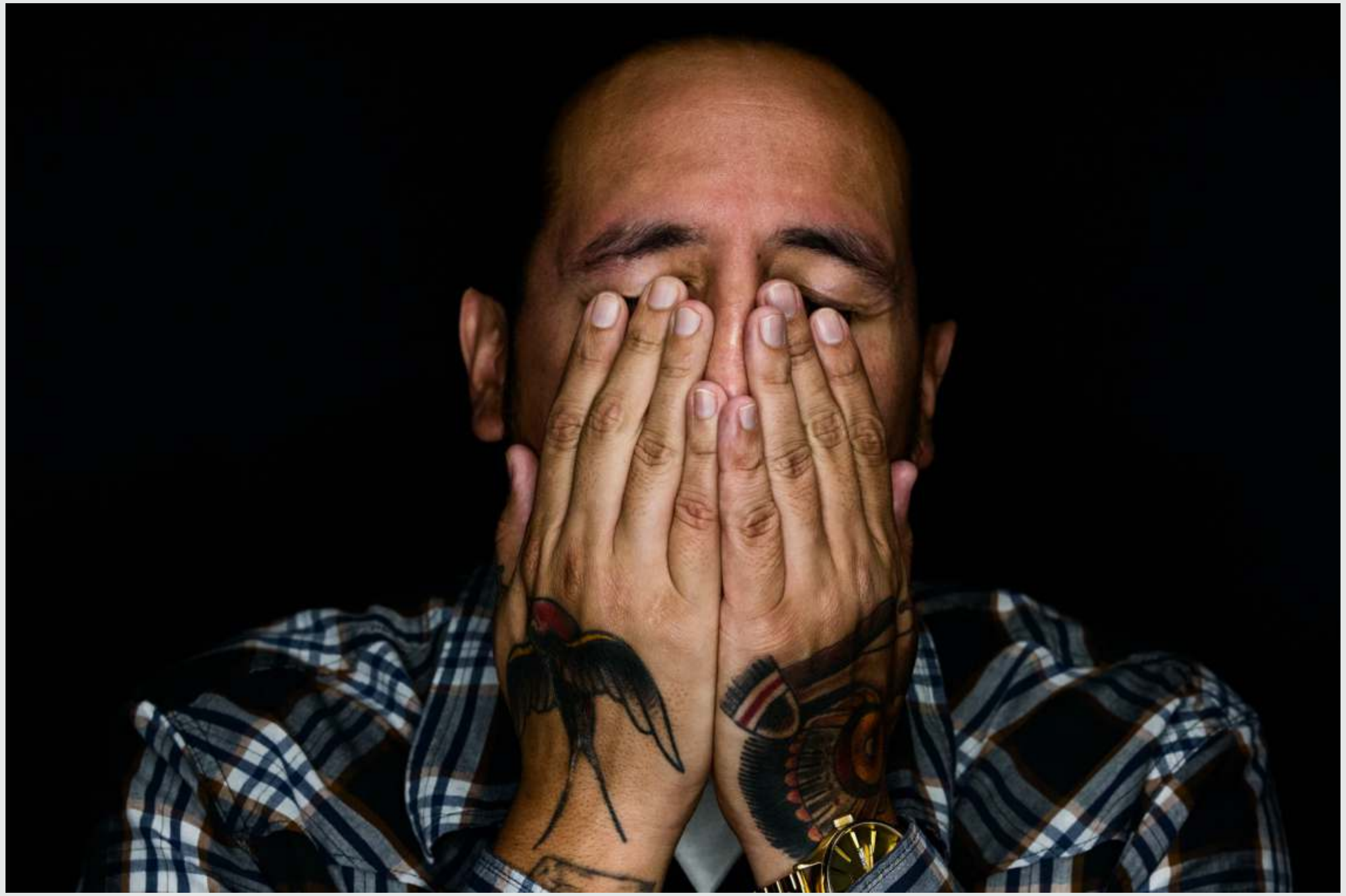


Photo by Jeremy Bishop on Unsplash

- 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!

What We Need in Validation …

- 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

What We Need in Validation …

- Introduction of signature workflow information into PDF data structures
  - Who should sign the document?
  - What signature quality (SES, AES, ATS, ASeal, QES, …) should be allowed for signing?
  - Which minimum signature quality (Simple, Advanced, Qualified) should be used?
- 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

Otherwise …

- Focusing only on technical validation could frustrate PDF users and will lead to a negative attitude to digital signatures and PDF

Finally

- Signature validation is a challenge
- ETSI has intensified work on validation standards
- PDF Association discusses some new concepts on validation of signed PDFs and supporting more real-life signature scenarios

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