TeleTrusT-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Wie man digitale Unterschriften in PDF-Dokumenten unbemerkt fälscht"

Dr. Christian Mainka, Ruhr-Universität Bochum

% whoami

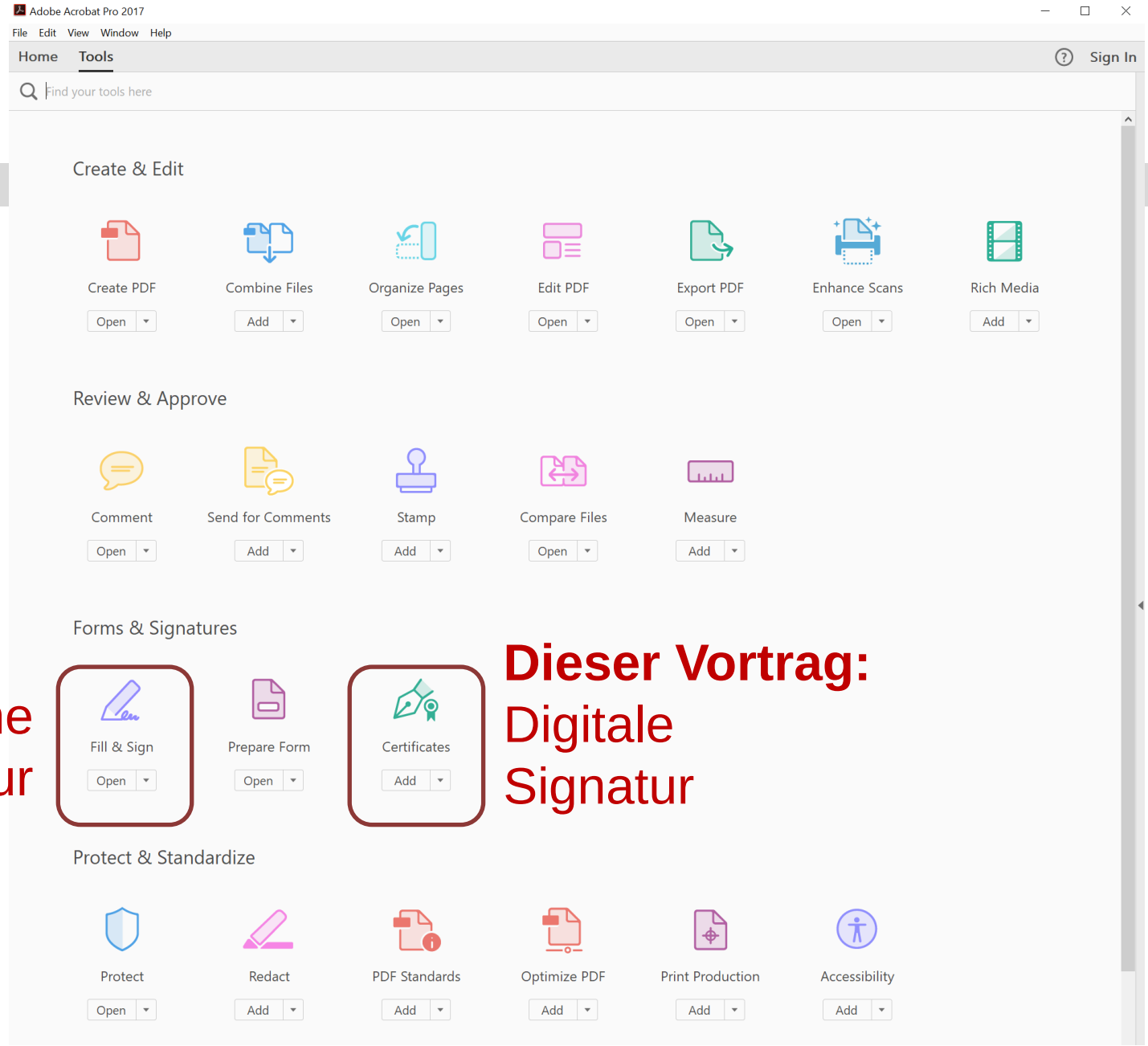
- Christian Mainka

Twitter: @chearix

- PostDoc: Ruhr-Universität Bochum
  - Lehrstuhl Netz-und Datensicherheit
  - Forschung:
    - Dokumentensicherheit (PDF, ODF, MS Office)
    - Single Sign-On (OAuth, OpenID Connect, SAML)

- CTO: HACKMANIT
  - Schulungen, Penetrationstests, Bedrohungsanalysen

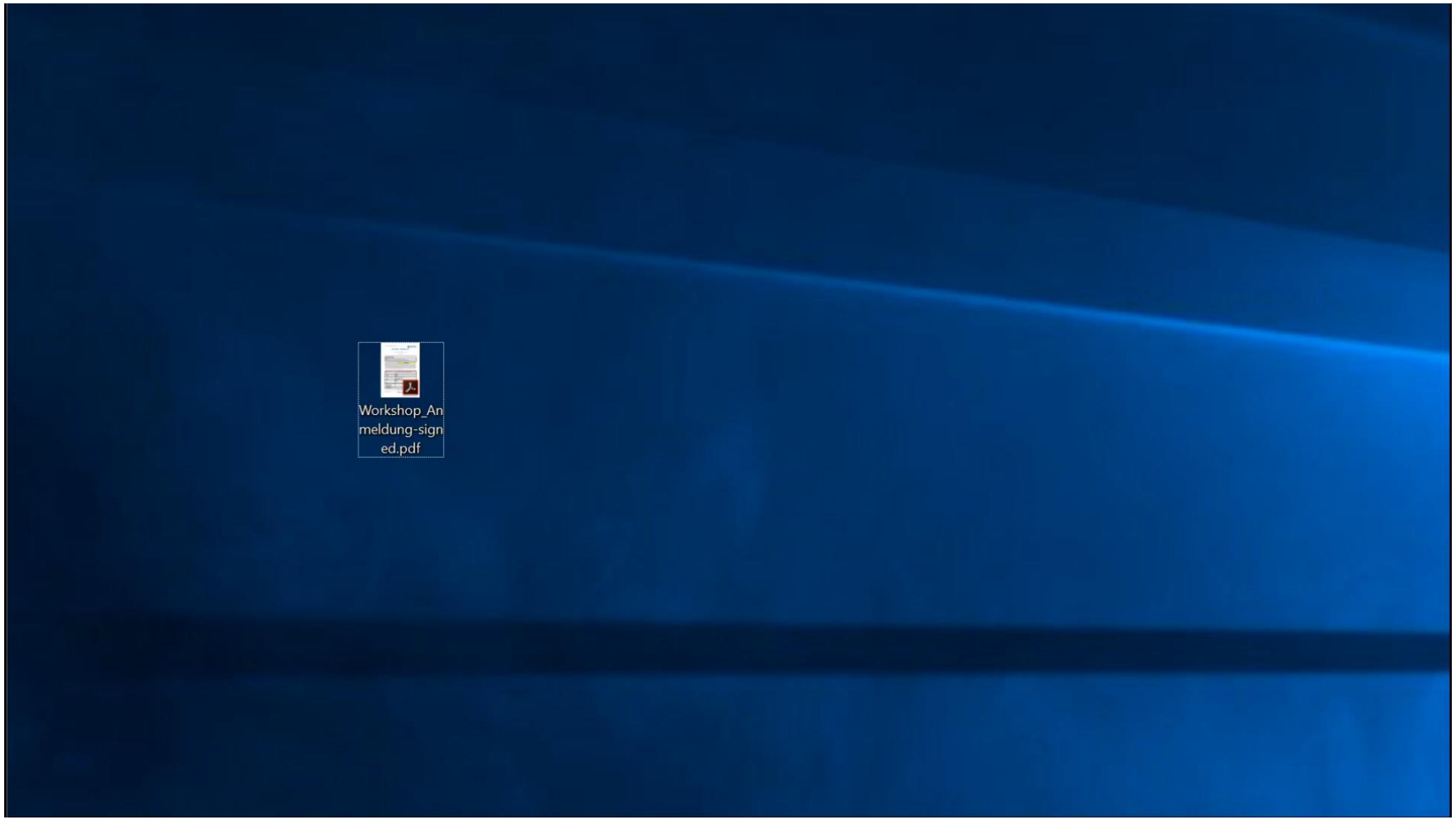
PDF Signieren



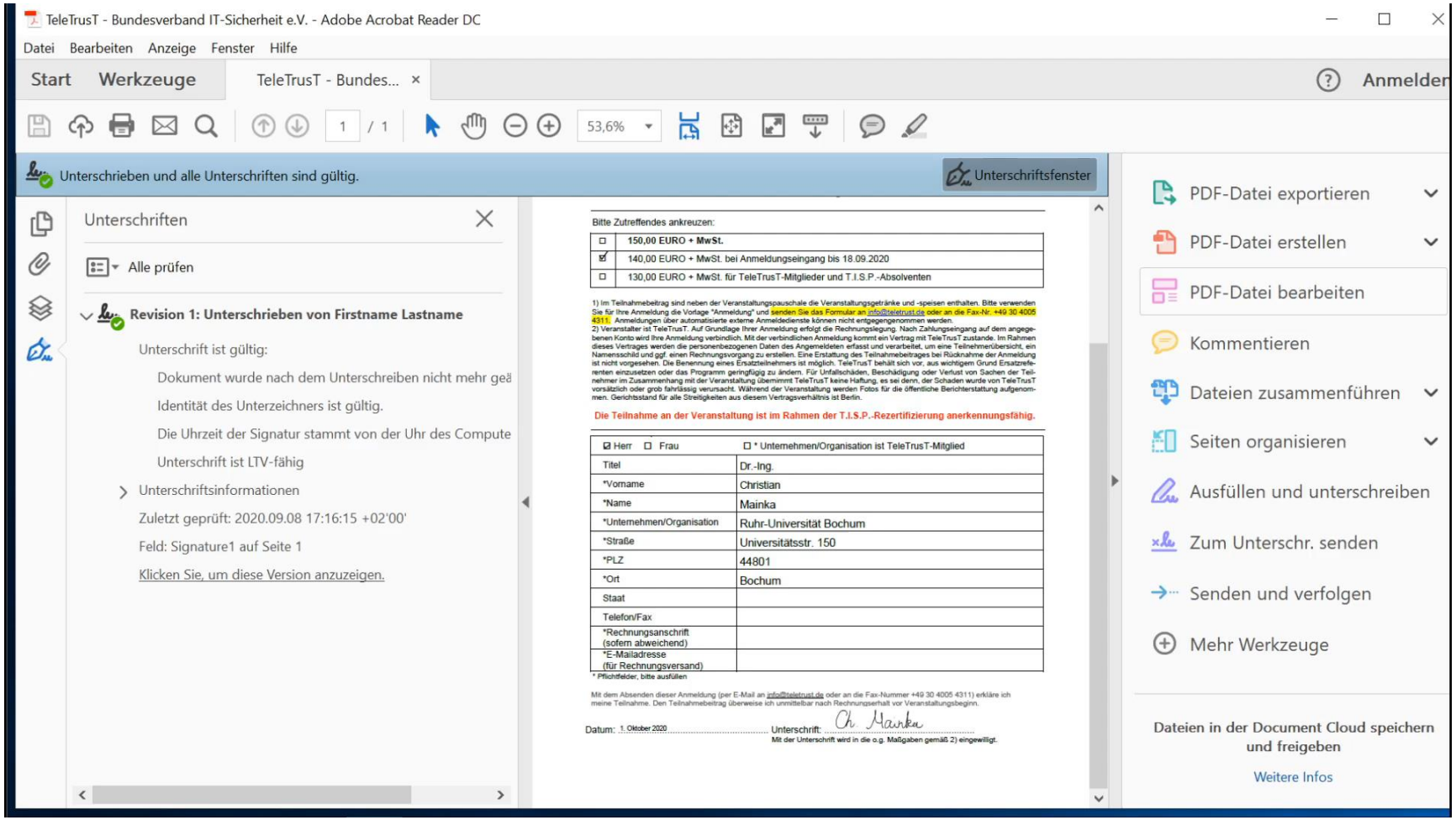
Elektronische Signatur

Dieser Vortrag: Digitale Signatur

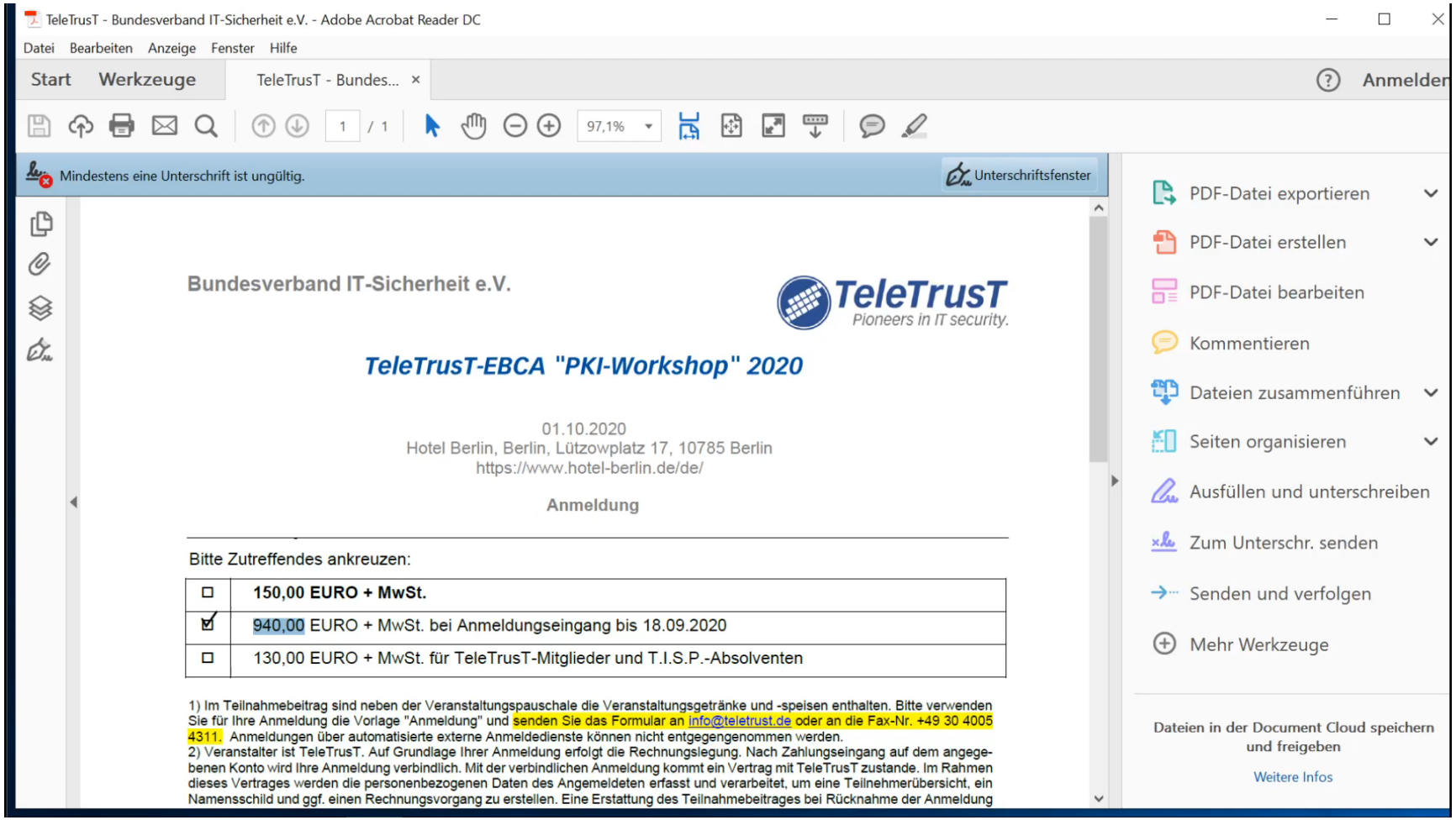
Was ist ein signiertes PDF?



Veränderungen am PDF führen zur ungültigen Signatur



Aber: Wir können sie fälschen!



Februar 2019

SPIEGEL Netzwelt

Gefälschte Dokumente

Forscher tricksen fast alle PDF-Reader aus

Behördenschreiben, Amazon-Rechnungen, Gesetzestexte: Forschern ist es gelungen, populären PDF-Readern manipulierte Dokumente unterzujubeln - mit simplen Mitteln. Warnungen gab es fast nie.

golem.de
IT-NEWS FÜR PROFIS

SICHERHEITSLÜCKEN

PDF-Signaturen fälschen leicht gemacht

Signaturen von PDF-Dateien sind offenbar nicht besonders sicher: Einem Forscherteam der Uni Bochum gelang es, die Signaturprüfung in nahezu all PDF-Programmen auszutricksen.

25. Februar 201

ZDNet

MUST READ: Management skills: Five ways building your network will help you get ahead

Researchers break digital signatures for most desktop PDF viewers

Researchers faked signatures on 21 of 22 desktop PDF viewer apps and 5 out of 7 online PDF digital signing services.

Catalin Cimpanu for Zero Day | February 25, 2019 -- 19:30 GMT (19:30 GMT) | Topic: Security

Signature Panel

amazon.com

Your refund is:

$ 1,000.00

(One Trill

heise

02/2019 › Viele PDF-Viewer begla

-Viewer beglaubige

ung über eine Billion U

itsforscher demonstrieren, wie sie digital unt

ern und die Signatur trotzdem gültig bleibt

Schneier on Security

Blog Newsletter Books Essays News Talks Academic About Me

Blog ›

Digital Signatures in PDFs Are Broken

Researchers have demonstrated spoofing of digital signatures in PDF files.

This would matter more if PDF digital signatures were widely used. Still, the researchers have worked with the various companies that make PDF readers to close the vulnerabilities. You should update your software.

Details are here.

News article.

Tags: academic papers, signatures, spoofing, vulnerabilities

Posted on March 6, 2019 at 6:17 AM • 12 Comments

Search

Powered by DuckDuckGo

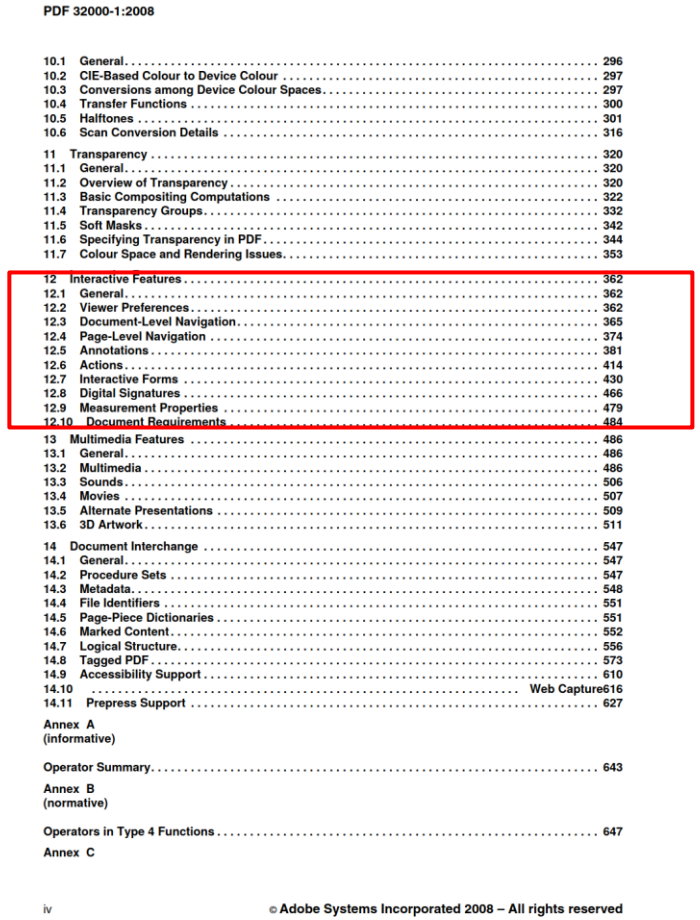
Go

blog essays whole site

Subscribe

About Bruce Schneier

Was war das Problem in 2019?

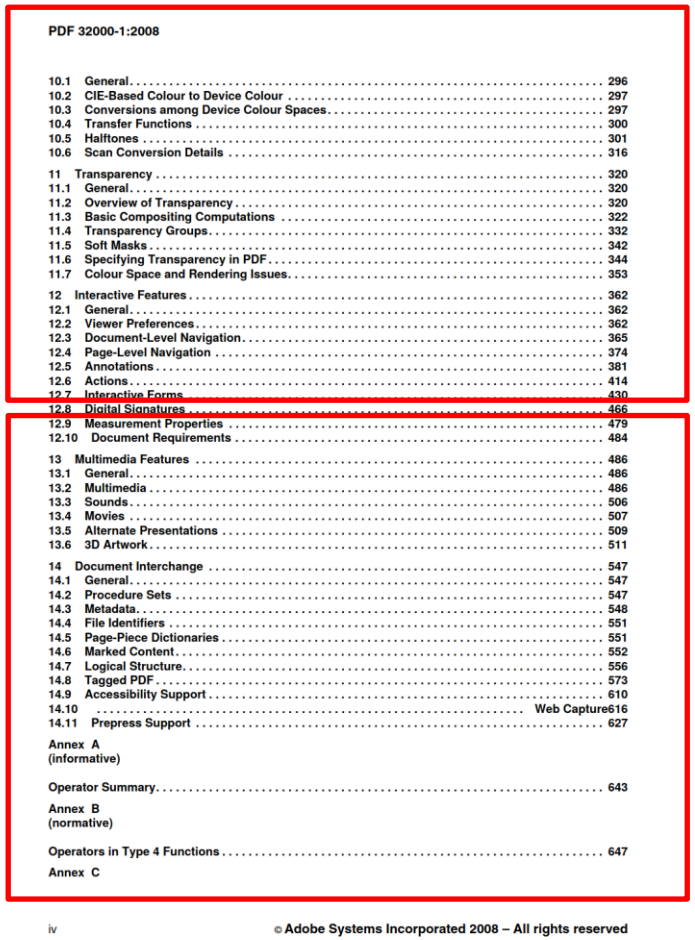


PDF 32000-1:2008

- PDF Signaturen sind nur ein kleiner Teil eines komplexen Standards
- PDF 1.7 (ISO 32000) enthält keine Security Best Practices
- ➔ Implementierungsfehler!

2019… Problem gelöst?

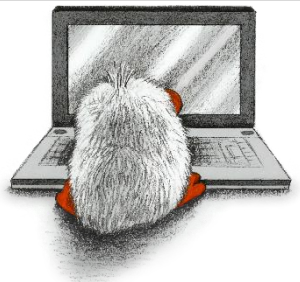
PDF Signaturen



PDF 32000-1:2008

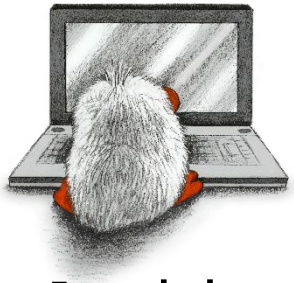
- PDF Signaturen sind nur ein kleiner Teil eines komplexen Standards
- Dafür enthält die restliche Spezifikation umso mehr interessante Features!
- *Bestimmte* Änderungen sind nach dem Signieren erlaubt!

Wie wird ein Vertrag signiert?

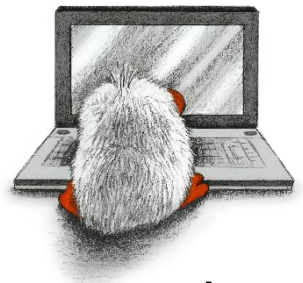


Layout

Partei A

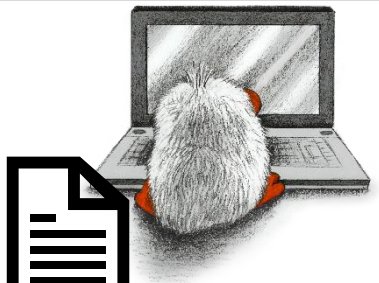


Justiziar

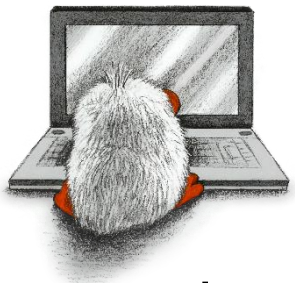


Partei B

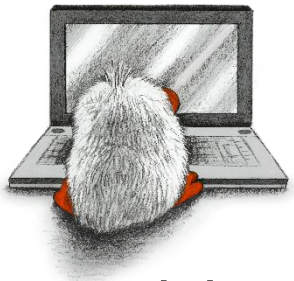
Wie wird ein Vertrag signiert?



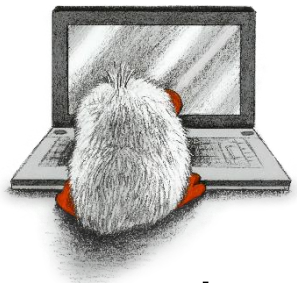
Layout



Partei A

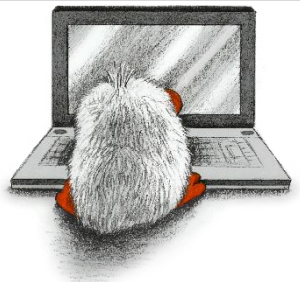


Justiziar

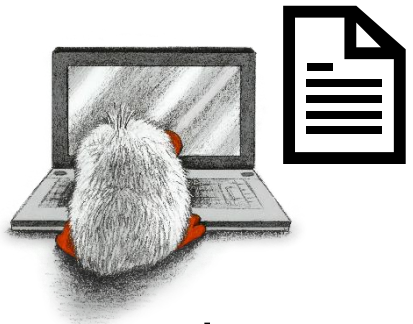


Partei B

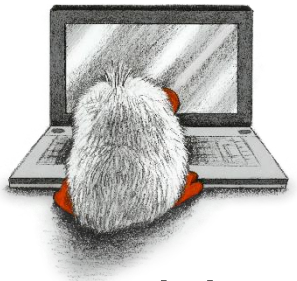
Wie wird ein Vertrag signiert?



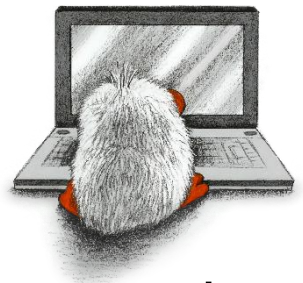
Layout



Partei A

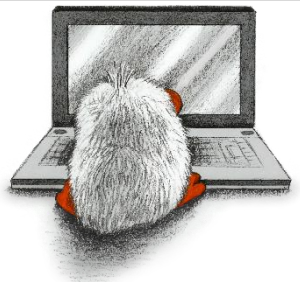


Justiziar

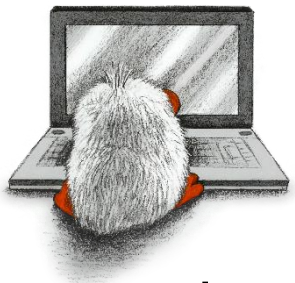


Partei B

Wie wird ein Vertrag signiert?

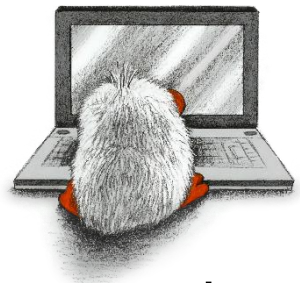


Layout



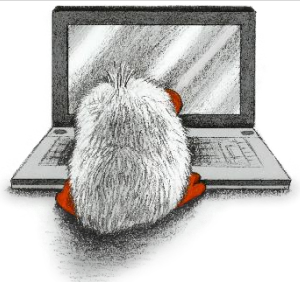
Partei A

Justiziar

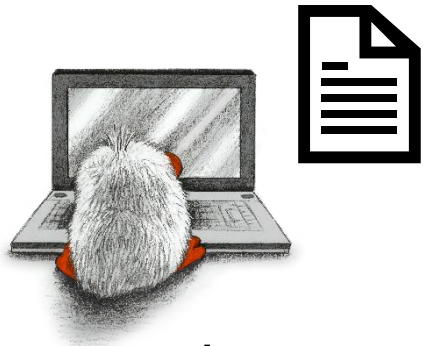


Partei B

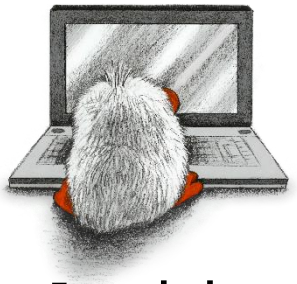
Wie wird ein Vertrag signiert?



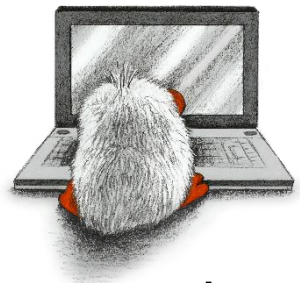
Layout



Partei A

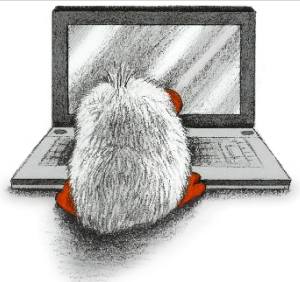


Justiziar

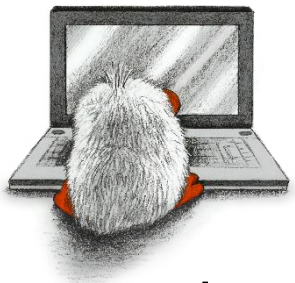


Partei B

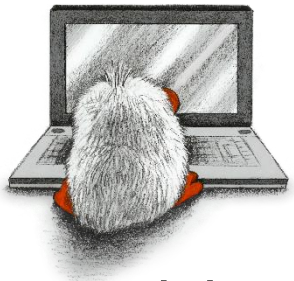
Wie wird ein Vertrag signiert?



Layout



Partei A

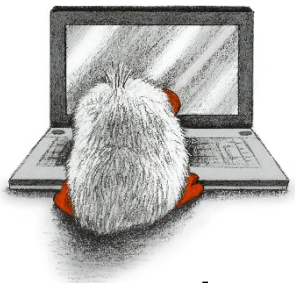


Justiziar

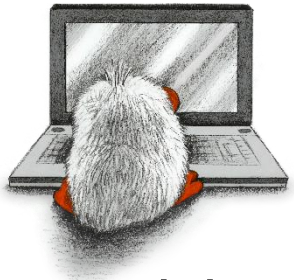
Partei B

Wie wird ein Vertrag signiert?

Angreifer



Partei A



Justiziar

Partei B

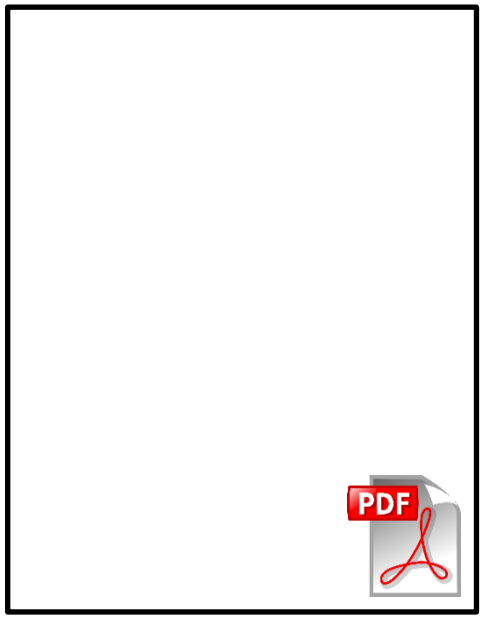
2020: Shadow Attacks

Victim's PDF View

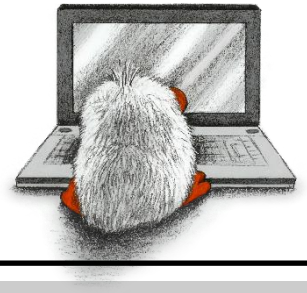
Signer's PDF View

Angriffsklasse 1: Hide

Sign me to get the reward!



Angriffsklasse 1: Hide



Sign me to get the reward!

Signed by Bob

Angriffsklasse 1: Hide

Sign me to get the reward!

Signed by Bob


```
xref
0 5
000000000 00000 f
000000009 00000 n
000000058 00000 n
000000121 00000 n
000000184 00000 n
```

Variante 1

```
xref
0 5
000000000 00000 f
000000009 00000 n
000000121 00000 n
000000121 00000 n
000000184 00000 n
```

Variante 2

```
xref
0 5
000000000 00000 f
000000058 00000 n
000000009 00000 n
000000121 00000 n
000000184 00000 n
```

Variante 3

Angriffsklasse 2: Replace

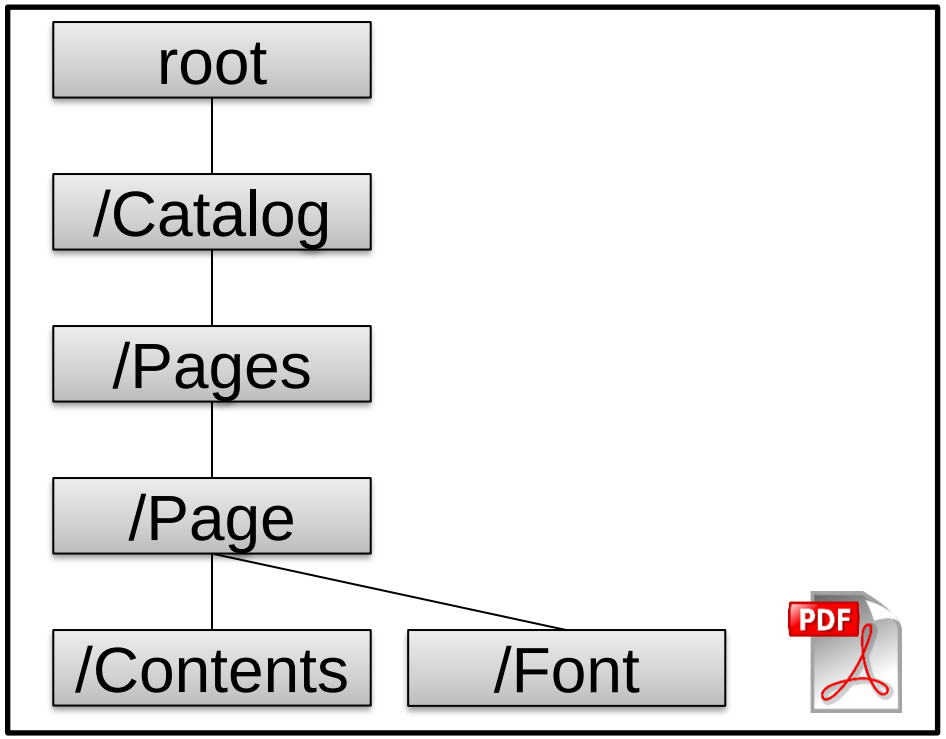
/Font DEF

7999 USD

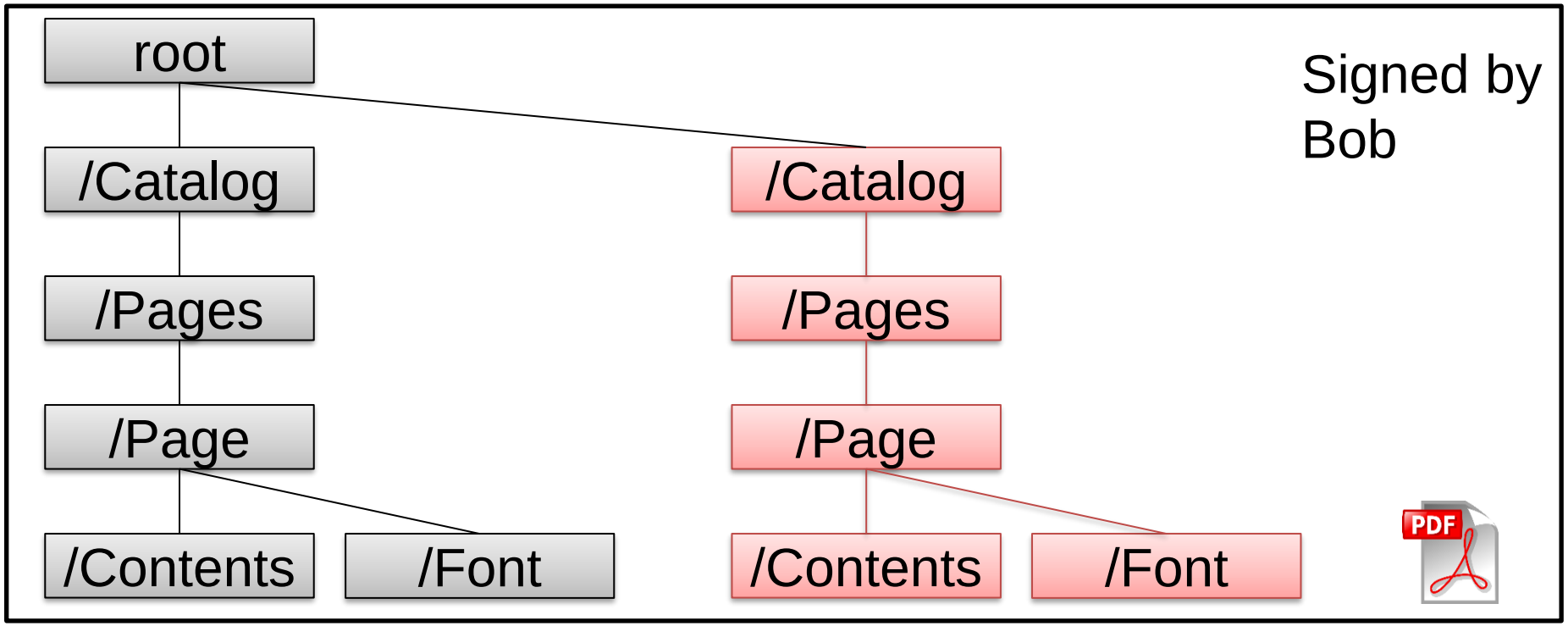
Signed by Bob

- Schriftarten dürfen nach dem Signieren hinzugefügt werden
- Auch eigene Schriftdefinitionen sind möglich

Angriffsklasse 3: Hide-and-Replace



Angriffsklasse 3: Hide-and-Replace



Fazit: Es gibt noch viel zu tun

- Integrität und Authentizität von Dokumenten ist komplex
  - …wenn mehr als ein unveränderliches Dokument benötigt wird.
    - Formulare ausfüllen
    - Kommentieren
- Spezifikation bietet keinerlei Hilfestellung
  - Wir sind Mitglied von ISO/TC 171/SC 2 geworden

Q&A

- Kontakt:
  - Christian.Mainka@rub.de
  - Twitter: @chearix

- https://pdf-insecurity.org/

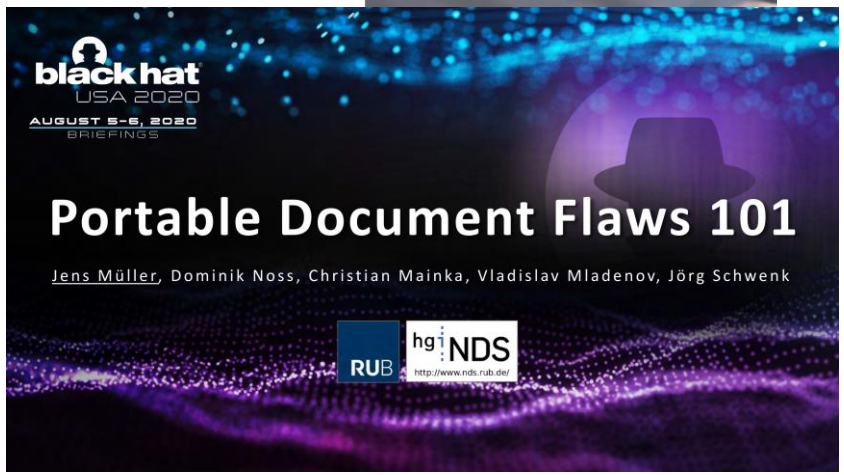

SPIEGEL Netzwelt

Digitale Unterschriften

Forscher täuschen PDF-Reader mit versteckten Text

Wissenschaftler der Ruhr-Universität Bochum haben erneut PDF-Reader überlistet. Mit der Masche können Betrüger ihre Opfer dazu bringen, Dokumente digital zu signieren, in denen später etwas ganz anderes steht.

Von Jörg Breithut
22.07.2020, 08.10 Uhr




golem.de
IT-NEWS FÜR PROFIS
HOME TICKER VIDEOS VORGELESEN FORUM | ANMELDEN
Suchen
TOP-THEMEN: Ifa 2020 Arbeit Auto mehr...
IT-KARRIERE: STELLENMARKT SEMINARE IT-KÖPFE GEHALTSCHECK | SERVICES: PREISVERGLEICH TOP-ANGEBOTE

SICHERHEITSLÜCKE

Angreifer können verschlüsselte PDF-Daten leaken

Passwortgeschützte PDF-Dateien bieten wenig Sicherheit. Ein Angreifer, der die Dateien manipulieren kann, kann dafür sorgen, dass deren Inhalt geleakt wird. Abhilfe gibt es nicht, dafür müsste das Dateiformat geändert werden.

30. September 2019, 12:59 Uhr, Hanno Böck

(Bild: Pixabay / Montage: Golem.de)
PDFex heißt eine Sicherheitslücke, mit der sich die Verschlüsselung von PDF-Dateien austricksen lässt.