

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
- 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

Twitter: @chearix



PDF Signieren

The screenshot shows the Adobe Acrobat Pro 2017 interface with the Tools pane open. The tools are organized into four main categories:

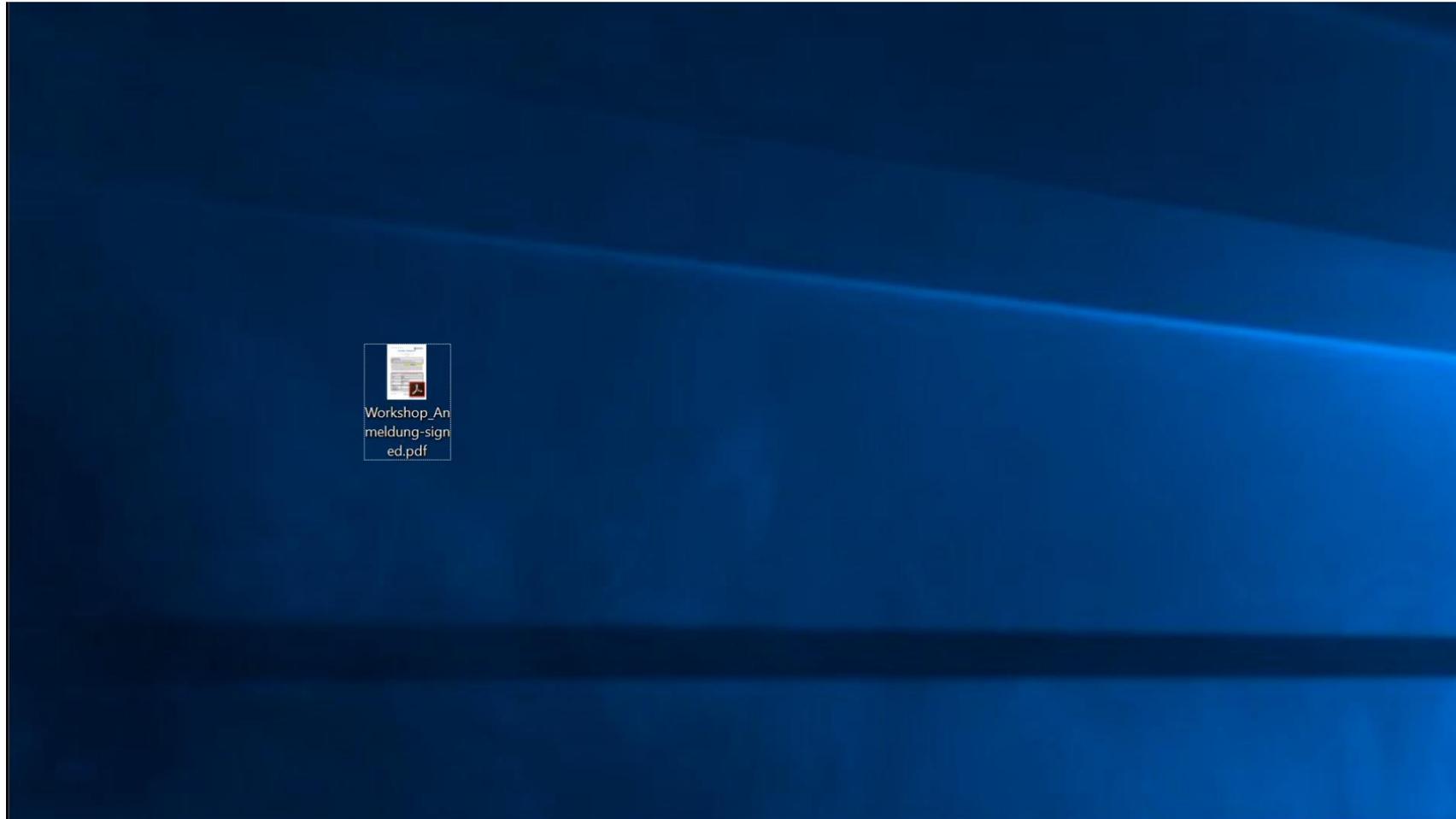
- Create & Edit:** Create PDF, Combine Files, Organize Pages, Edit PDF, Export PDF, Enhance Scans, Rich Media.
- Review & Approve:** Comment, Send for Comments, Stamp, Compare Files, Measure.
- Forms & Signatures:** Fill & Sign, Prepare Form, Certificates.
- Protect & Standardize:** Protect, Redact, PDF Standards, Optimize PDF, Print Production, Accessibility.

The 'Fill & Sign' and 'Certificates' tools in the 'Forms & Signatures' category are highlighted with red boxes.

Elektronische
Signatur

Dieser Vortrag:
Digitale
Signatur

Was ist ein signiertes PDF?



Veränderungen am PDF führen zur ungültigen Signatur

TeleTrust - Bundesverband IT-Sicherheit e.V. - Adobe Acrobat Reader DC

Datei Bearbeiten Anzeige Fenster Hilfe

Start Werkzeuge TeleTrust - Bundes... x

Start 1 / 1 53,6%

Unterschriften und alle Unterschriften sind gültig. Unterschriftsfenster

Unterschriften

Alle prüfen

Revision 1: Unterscriben von Firstname Lastname

Unterschrift ist gültig:

Dokument wurde nach dem Unterscriben nicht mehr geändert

Identität des Unterzeichners ist gültig.

Die Uhrzeit der Signatur stammt von der Uhr des Compute

Unterschrift ist LTV-fähig

Unterschriftsinformationen

Zuletzt geprüft: 2020.09.08 17:16:15 +02'00'

Feld: Signature1 auf Seite 1

Klicken Sie, um diese Version anzuzeigen.

Bitte Zutreffendes ankreuzen:

<input type="checkbox"/>	150,00 EURO + MwSt.
<input checked="" type="checkbox"/>	140,00 EURO + MwSt. bei Anmeldungseingang bis 18.09.2020
<input type="checkbox"/>	130,00 EURO + MwSt. für TeleTrust-Mitglieder und T.I.S.P.-Absolventen

1) Im Teilnahmebetrag sind neben der Veranstaltungspauschale die Veranstaltungstränke und -speisen enthalten. Bitte verwenden Sie für Ihre Anmeldung die Vorlage "Anmeldung" und senden Sie das Formular an info@teletrust.de oder an die Fax-Nr. +49 30 4005 4311. Anmeldungen über automatisierte externe Anmeldekanäle können nicht entgegengenommen werden.

2) Veranstalter ist TeleTrust. Auf Grundlage Ihrer Anmeldung erfolgt die Rechnungslegung. Nach Zahlungseingang auf dem angegebenen Konto wird Ihre Anmeldung verbindlich. Mit der verbindlichen Anmeldung kommt ein Vertrag mit TeleTrust zustande. Im Rahmen dieses Vertrages werden die personenbezogenen Daten des Angemeldeten erfasst und verarbeitet, um eine Teilnehmerübersicht, ein Namensschild und ggf. einen Rechnungsvorgang zu erstellen. Eine Erstattung des Teilnahmebetrages bei Rücknahme der Anmeldung ist nicht vorgesehen. Die Benennung eines Ersatzteilnehmers ist möglich. TeleTrust behält sich vor, aus wichtigem Grund Ersatzteilnehmer einzusetzen oder das Programm geringfügig zu ändern. Für Unfallschäden, Beschädigung oder Verlust von Sachen der Teilnehmer im Zusammenhang mit der Veranstaltung übernimmt TeleTrust keine Haftung, es sei denn, der Schaden wurde von TeleTrust vorsätzlich oder grob fahrlässig verursacht. Während der Veranstaltung werden Fotos für die öffentliche Berichterstattung aufgenommen. Gerichtsstand für alle Streitigkeiten aus diesem Vertragsverhältnis ist Berlin.

Die Teilnahme an der Veranstaltung ist im Rahmen der T.I.S.P.-Rezertifizierung anerkennungsfähig.

<input checked="" type="checkbox"/>	Herr	<input type="checkbox"/>	Frau	<input type="checkbox"/>	* Unternehmen/Organisation ist TeleTrust-Mitglied
Titel		Dr.-Ing.			
*Vorname		Christian			
*Name		Mainka			
*Unternehmen/Organisation		Ruhr-Universität Bochum			
*Straße		Universitätsstr. 150			
*PLZ		44801			
*Ort		Bochum			
Staat					
Telefon/Fax					
*Rechnungsanschrift (sofern abweichend)					
*E-Mailadresse (für Rechnungsversand)					

* Pflichtfelder, bitte ausfüllen

Mit dem Absenden dieser Anmeldung (per E-Mail an info@teletrust.de oder an die Fax-Nummer +49 30 4005 4311) erkläre ich meine Teilnahme. Den Teilnahmebetrag überweise ich unmittelbar nach Rechnungserhalt vor Veranstaltungsbeginn.

Datum: 1. Oktober 2020 Unterschrift: *Ch. Mainka*

Mit der Unterschrift wird in die o.g. Maßgaben gemäß 2) eingewilligt.

PDF-Datei exportieren

PDF-Datei erstellen

PDF-Datei bearbeiten

Komentieren

Dateien zusammenführen

Seiten organisieren

Ausfüllen und unterschreiben

Zum Unterschr. senden

Senden und verfolgen

Mehr Werkzeuge

Dateien in der Document Cloud speichern und freigeben

Weitere Infos

Aber: Wir können sie fälschen!

TeleTrust - Bundesverband IT-Sicherheit e.V. - Adobe Acrobat Reader DC

Start Werkzeuge TeleTrust - Bundes... x

Mindestens eine Unterschrift ist ungültig. Unterschriftsfenster

Bundesverband IT-Sicherheit e.V.



TeleTrust-EBCA "PKI-Workshop" 2020

01.10.2020
Hotel Berlin, Berlin, Lützowplatz 17, 10785 Berlin
<https://www.hotel-berlin.de/de/>

Anmeldung

Bitte Zutreffendes ankreuzen:

<input type="checkbox"/>	150,00 EURO + MwSt.
<input checked="" type="checkbox"/>	940,00 EURO + MwSt. bei Anmeldungseingang bis 18.09.2020
<input type="checkbox"/>	130,00 EURO + MwSt. für TeleTrust-Mitglieder und T.I.S.P.-Absolventen

1) Im Teilnahmebeitrag sind neben der Veranstaltungspauschale die Veranstaltungsgetränke und -speisen enthalten. Bitte verwenden Sie für Ihre Anmeldung die Vorlage "Anmeldung" und **senden Sie das Formular an info@teletrust.de oder an die Fax-Nr. +49 30 4005 4311**. Anmeldungen über automatisierte externe Anmeldedienste können nicht entgegengenommen werden.

2) Veranstalter ist TeleTrust. Auf Grundlage Ihrer Anmeldung erfolgt die Rechnungslegung. Nach Zahlungseingang auf dem angegebenen Konto wird Ihre Anmeldung verbindlich. Mit der verbindlichen Anmeldung kommt ein Vertrag mit TeleTrust zustande. Im Rahmen dieses Vertrages werden die personenbezogenen Daten des Angemeldeten erfasst und verarbeitet, um eine Teilnehmerübersicht, ein Namensschild und ggf. einen Rechnungsvorgang zu erstellen. Eine Erstattung des Teilnahmebeitrages bei Rücknahme der Anmeldung

PDF-Datei exportieren
PDF-Datei erstellen
PDF-Datei bearbeiten
Kommentieren
Dateien zusammenführen
Seiten organisieren
Ausfüllen und unterschreiben
Zum Unterschr. senden
Senden und verfolgen
Mehr Werkzeuge

Dateien in der Document Cloud speichern und freigeben
[Weitere Infos](#)

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.

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

and all signatures are valid.

ate All

not been modified since the clock on the

id: invoicing@amazon.de

valid

the clock on the

6:18 Z

Signature Panel

heise +

ment Wissen

AUTO SECURITY WINL

02/2019 > Viele PDF-Viewer begla

Viewer beglaubig

ung über eine Billion U

sitsforscher demonstrieren, wie sie digital unt

ern und die Signatur trotzdem gültig bleibt

golem.de IT-NEWS FÜR PROFIS

HOME TICKER VIDEOS VORGELESEN FORUM | ANMELDEN

IT-KARRIERE: STELLENMARKT SEMINARE IT-KÖPFE GEHALTSCHECK | SERVICES: PREISVERGLEICH TOP-ANGEBOTE

SUCHEN

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 allen PDF-Programmen auszutricksen.

25. Februar 2019



Schneier on Security

Blog Newsletter Books Essays News Talks Academic About Me

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

blog essays whole site

Subscribe

About Bruce Schneier



Was war das Problem in 2019?

PDF 32000-1:2008

10.1	General	296
10.2	CIE-Based Colour to Device Colour	297
10.3	Conversions among Device Colour Spaces	297
10.4	Transfer Functions	300
10.5	Halftones	301
10.6	Scan Conversion Details	316
11	Transparency	320
11.1	General	320
11.2	Overview of Transparency	320
11.3	Basic Compositing Computations	322
11.4	Transparency Groups	332
11.5	Soft Masks	342
11.6	Specifying Transparency in PDF	344
11.7	Colour Space and Rendering Issues	353
12	Interactive Features	362
12.1	General	362
12.2	Viewer Preferences	362
12.3	Document-Level Navigation	365
12.4	Page-Level Navigation	374
12.5	Annotations	381
12.6	Actions	414
12.7	Interactive Forms	430
12.8	Digital Signatures	466
12.9	Measurement Properties	479
12.10	Document Requirements	484
13	Multimedia Features	486
13.1	General	486
13.2	Multimedia	486
13.3	Sounds	506
13.4	Movies	507
13.5	Alternate Presentations	509
13.6	3D Artwork	511
14	Document Interchange	547
14.1	General	547
14.2	Procedure Sets	547
14.3	Metadata	548
14.4	File Identifiers	551
14.5	Page-Piece Dictionaries	551
14.6	Marked Content	552
14.7	Logical Structure	556
14.8	Tagged PDF	573
14.9	Accessibility Support	610
14.10		Web Capture616
14.11	Prepress Support	627
Annex A	(informative)	
Operator Summary		643
Annex B	(normative)	
Operators in Type 4 Functions		647
Annex C		

iv © Adobe Systems Incorporated 2008 – All rights reserved



- 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	
10.1	General 296
10.2	CIE-Based Colour to Device Colour 297
10.3	Conversions among Device Colour Spaces 297
10.4	Transfer Functions 300
10.5	Halftones 301
10.6	Scan Conversion Details 316
11	Transparency 320
11.1	General 320
11.2	Overview of Transparency 320
11.3	Basic Compositing Computations 322
11.4	Transparency Groups 332
11.5	Soft Masks 342
11.6	Specifying Transparency in PDF 344
11.7	Colour Space and Rendering Issues 353
12	Interactive Features 362
12.1	General 362
12.2	Viewer Preferences 362
12.3	Document-Level Navigation 365
12.4	Page-Level Navigation 374
12.5	Annotations 381
12.6	Actions 414
12.7	Interactive Forms 430
12.8	Digital Signatures 466
12.9	Measurement Properties 479
12.10	Document Requirements 484
13	Multimedia Features 486
13.1	General 486
13.2	Multimedia 486
13.3	Sounds 506
13.4	Movies 507
13.5	Alternate Presentations 509
13.6	3D Artwork 511
14	Document Interchange 547
14.1	General 547
14.2	Procedure Sets 547
14.3	Metadata 548
14.4	File Identifiers 551
14.5	Page-Piece Dictionaries 551
14.6	Marked Content 552
14.7	Logical Structure 556
14.8	Tagged PDF 573
14.9	Accessibility Support 610
14.10	Web Capture 616
14.11	Prepress Support 627
Annex A (informative)	
Operator Summary 643	
Annex B (normative)	
Operators in Type 4 Functions 647	
Annex C	

iv

© Adobe Systems Incorporated 2008 – All rights reserved

- 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

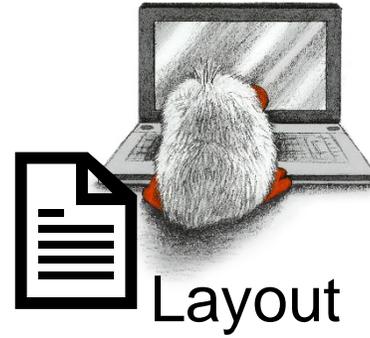


Justiziar



Partei B

Wie wird ein Vertrag signiert?



Partei A



Justiziar

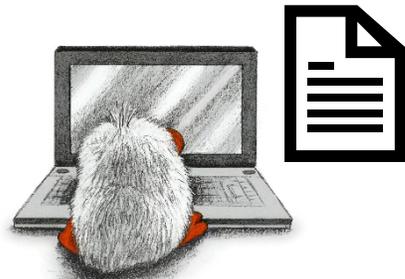


Partei B

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



Partei B



Justiziar

Wie wird ein Vertrag signiert?



Layout



Partei A



Justiziar



Partei B

Wie wird ein Vertrag signiert?



Angreifer



Partei A



Justiziar

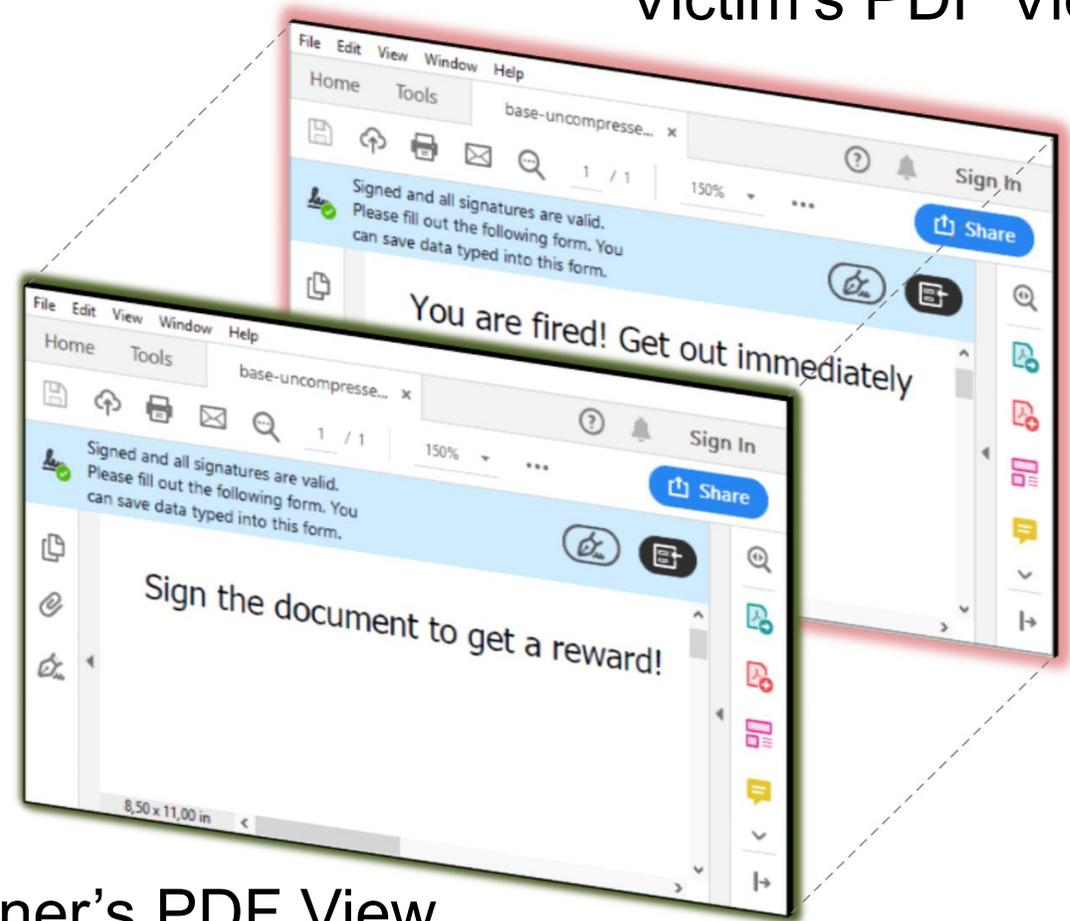


Partei B

2020: Shadow Attacks



Victim's PDF View

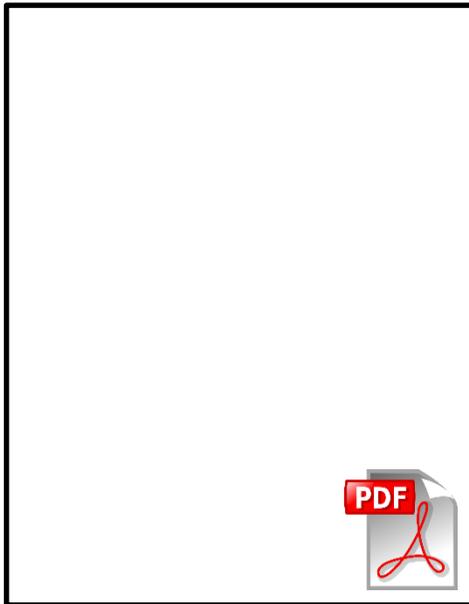


Signer's PDF View

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

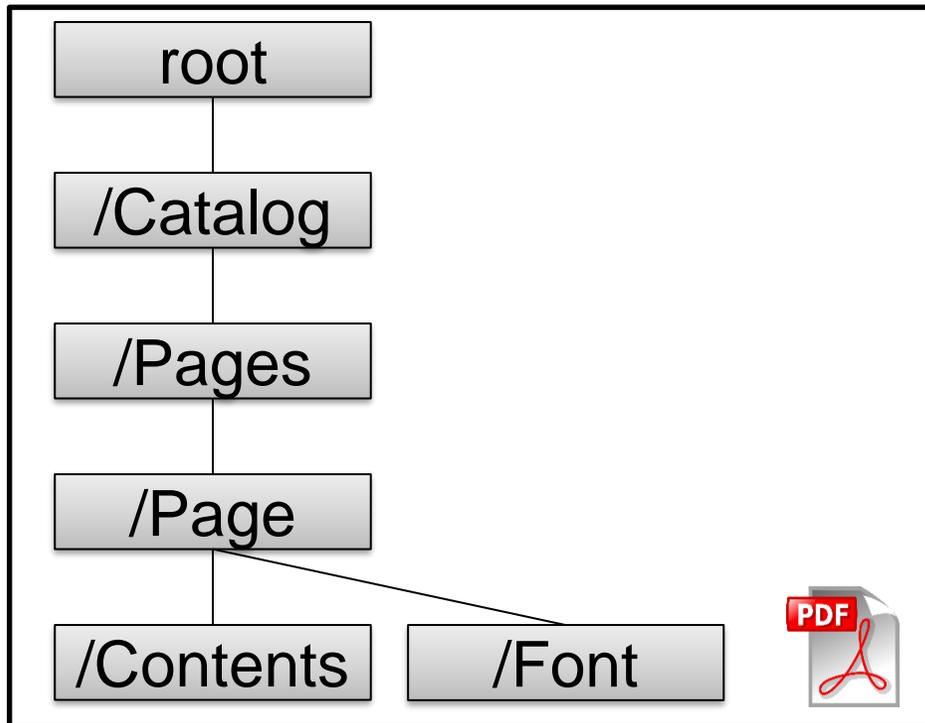
7999 USD

Signed by
Bob

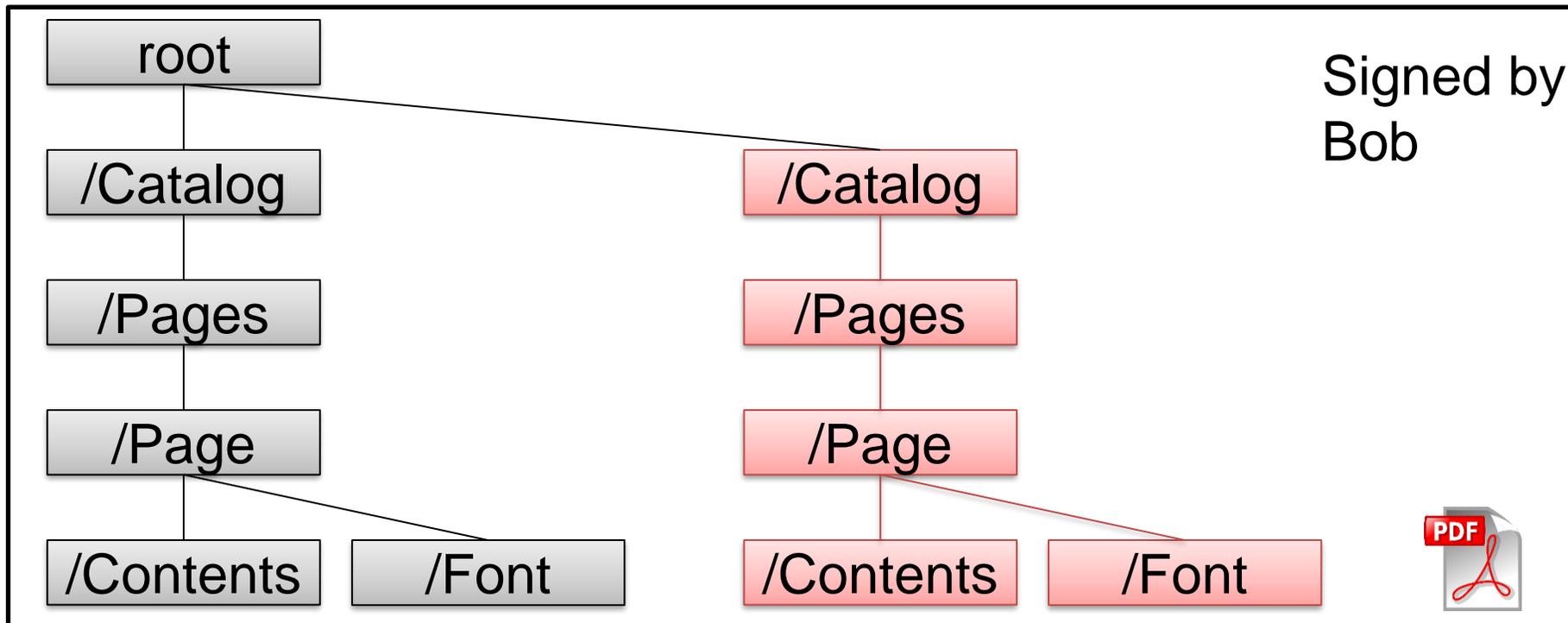


- Schriftarten dürfen nach dem Signieren hinzugefügt werden
- Auch eigene Schriftdefinitionen sind möglich

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

- **Kontakt:**
 - Christian.Mainka@rub.de
 - [Twitter: @chearix](https://twitter.com/chearix)
- <https://pdf-insecurity.org/>

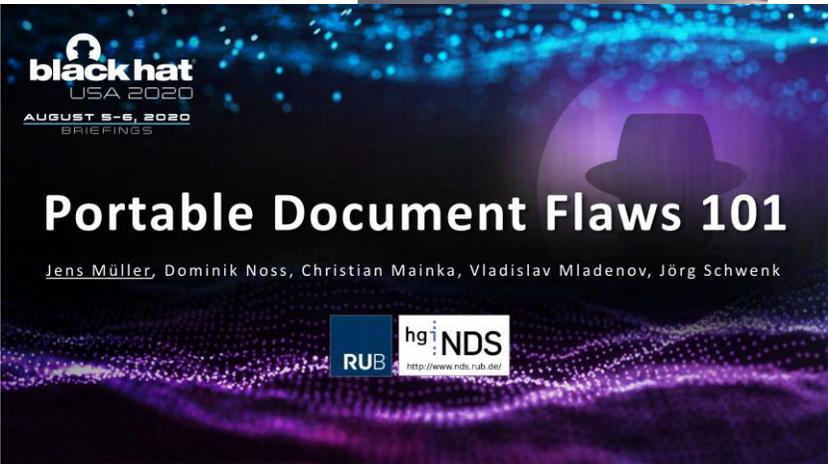


Digitale Unterschriften
Forscher täuschen PDF-Reader mit verstecktem Text
Wissenschaftler der Ruhr-Universität Bochum haben erneut PDF-Reader überlistet. Mit der Masche können Betrüger ihre Opfer dazu bringen, Dokumente digital zu signieren, in denen später etwas ganz anderes steht.
Von **Jörg Breithut**
22.07.2020, 08.10 Uhr



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



black hat
USA 2020
AUGUST 5-6, 2020
BRIEFINGS

Portable Document Flaws 101
Jens Müller, Dominik Noss, Christian Mainka, Vladislav Mladenov, Jörg Schwenk



PDFex

(Bild: Pixabay / Montage Golem.de)