

# **Elektronische Übermittlung im Rahmen der neuen Schweizerischen Zivilprozessordnung**

Bernd Reichert, Geschäftsführer Internet & Recht GmbH, Zürich  
Stephan Stulz, lic. iur., Rechtsanwalt, Zürich/Lenzburg

# Die Referenten

## Bernd Reichert

- Geschäftsführer der Internet & Recht GmbH ([www.internet-und-recht.ch](http://www.internet-und-recht.ch))
- Bis 2005 bei der Züricher Kantonalbank (ZKB) mit Schwerpunkt Technologie Internet-Banking
- 1990 bis 1996 Systems Engineer bei IBM Schweiz
- Masch. Ing. HTL

## Stephan Stulz

- Inhaber Advokaturbüro Stulz ([www.stulz-recht.ch](http://www.stulz-recht.ch)), Konsulent bei Internet und Recht GmbH
- lic. iur., Rechtsanwalt und Masch. Ing. HTL
- wissenschaftl. MA bei der eidg. Wettbewerbskommission, Weko
- Schwerpunkte Immaterialgüterrecht, Internet-Recht, Technikrecht

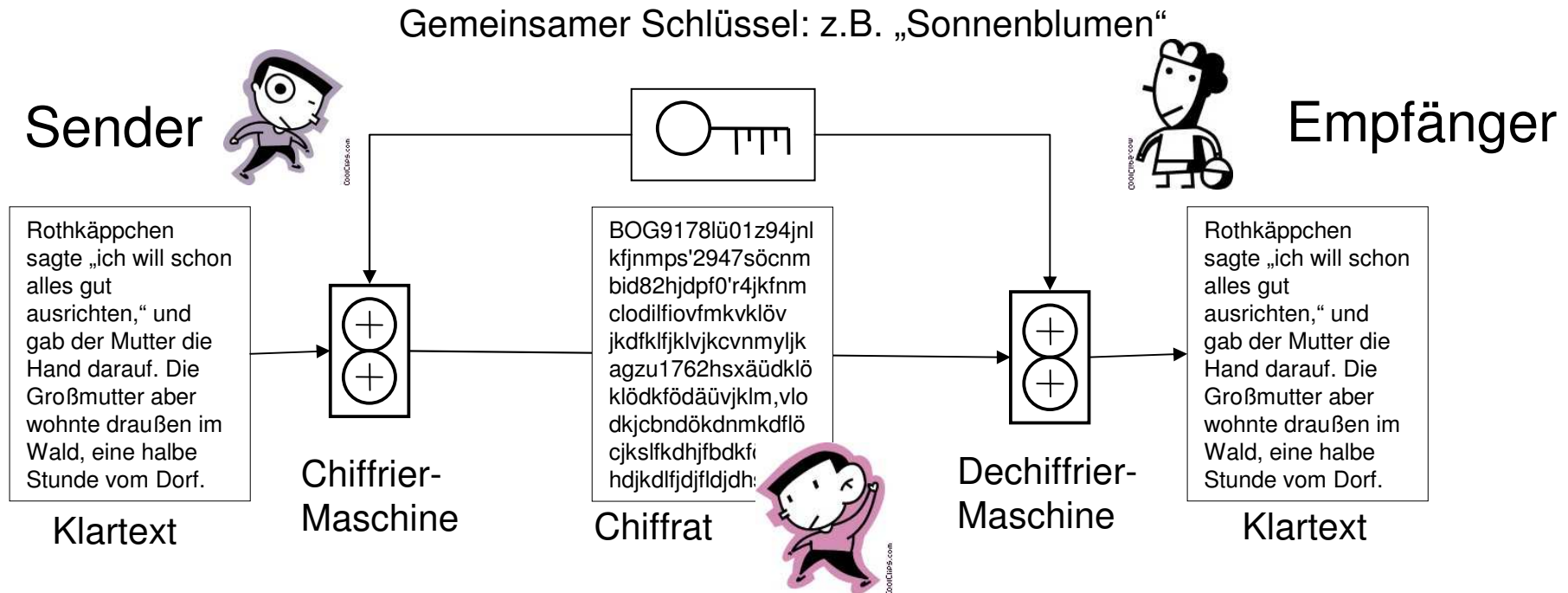
# Übersicht der Themen

1. Basiswissen sichere Internet-Kommunikation, Verschlüsselung
2. Beschaffung und Inbetriebnahme eines Zertifikats
3. Rechtliche Grundlagen, Entwicklung
4. Erzeugen von PDF-Dateien
5. Signieren von PDF-Dateien, Mehrfach-Signaturen,
6. Überprüfen von Signaturen in PDF-Dokumenten
7. Arbeitsmethodik des Anwalts
8. Übermittlung der Eingabe
9. Die Einhaltung von Fristen
10. Sicherer Umgang mit Zertifikaten, Haftung und Verantwortung

# 1. Sichere Internet Kommunikation

- Die heutige Internet-Technologie wurde in den 80er-Jahren für den Austausch von Informationen unter akademischen Einrichtungen entwickelt.
- Die Sicherheit stand nicht im Vordergrund, daher:
  - Keine Vertraulichkeit
  - Keine gesicherte Zustellung
  - Keine gesicherte Identifikation der Teilnehmer
- Diese Einfachheit war aber der Schlüssel für dessen Erfolg.
- Alle Sicherheitsmechanismen für rechtliche Zwecke müssen „aufgesetzt“ werden.

# 1.1 Symmetrische Verschlüsselung

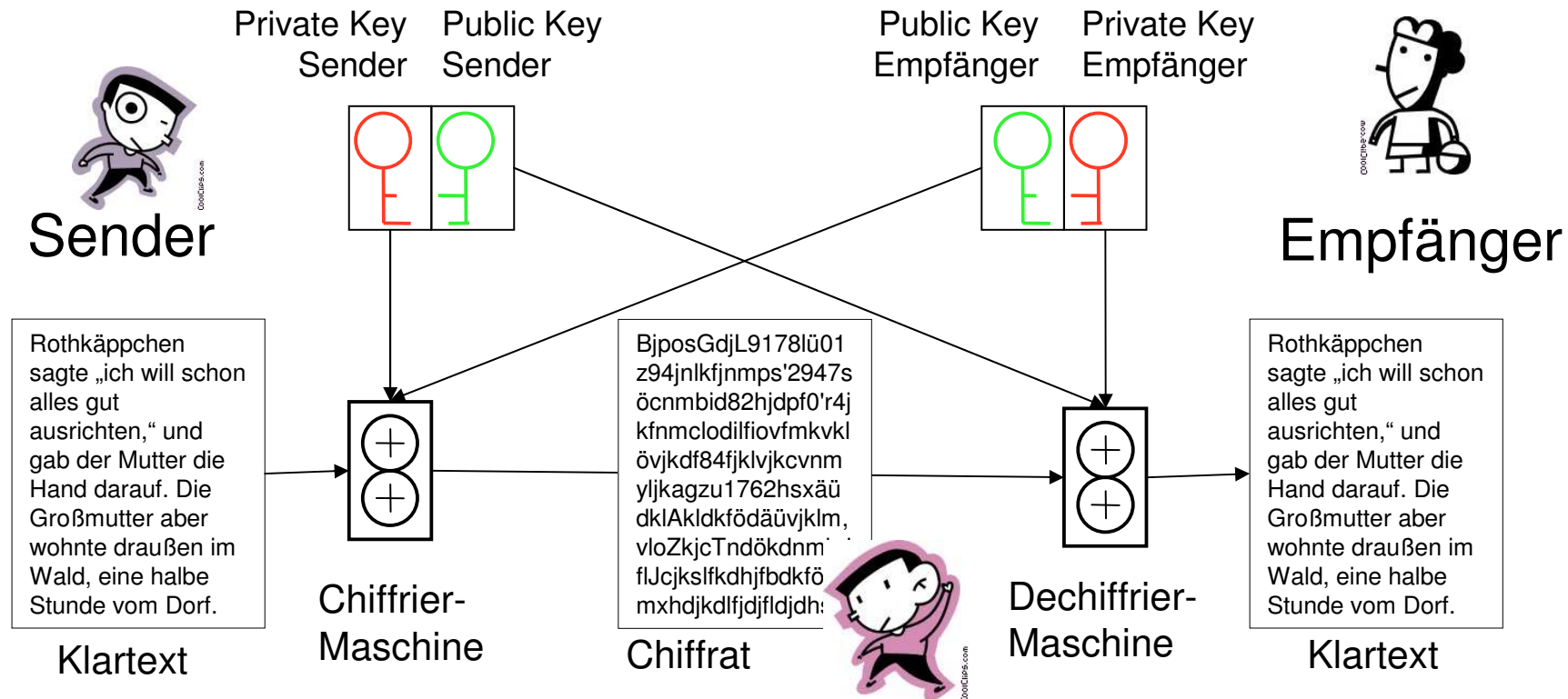


Klartext, Chifftrat und Schlüssel sind Texte. Sie sind als beliebig grosse Zahlen darstellbar

Chiffrierung und Defchiffrierung sind beliebig komplexe mathematische Operationen, die damit beliebig sicher sein können

Schwachstelle ist die Handhabung des gemeinsamen Schlüssels

# 1.2 Asymmetrische Verschlüsselung



Sender und Empfänger haben Schlüsselpaare. Diese bestehen aus einem privaten und einem öffentlichen (public) Schlüssel.

Sie tauschen ihre öffentlichen Schlüssel aus oder veröffentlichen diese.

Nun kann der Sender mit seinem Privaten Schlüssel und dem öffentlichen Schlüssel des Empfängers eine Nachricht für den Empfänger verschlüsseln.

Der Empfänger kann die Nachricht mit dem öffentlichen Schlüssel des Sender und seinem privaten Schlüssel entschlüsseln.

## 1.3 Vom Public Key zum Zertifikat



- Für alle Funktionen, welche mit einer Person zusammenhängen, braucht es eine Instanz, welche glaubwürdig eine Verbindung zwischen Person und Public Key herstellt.
- Von dieser Instanz wird der Public Key signiert. Sie unterschreibt damit, dass dieser einer ausgewiesenen existierenden Person gehört.
- Wie tut sie das? Natürlich auch mit ihrem Private Key.
- Ein signierter Public Key ist ein Zertifikat.
- Die signierende Instanz wird Zertifikats-Aussteller genannt.
- Die Echtheit eines Zertifikats wird mit dem Public Key des Ausstellers geprüft.

## 1.4 Was kann man einem Zertifizierten Schlüsselpaar machen



- Was kann man mit einem solchen Schlüsselpaar machen?
  - Verschlüsseln
  - Eine Identität beweisen
  - Eine Information/Mitteilung unterschreiben



## 1.5 Sicherheitsmassnahmen

Wenn der Private Key verloren geht, ist das Schlüsselpaar und damit das Zertifikat verloren. Deshalb:

- Das Schlüsselpaar mit Zertifikat wird auf einer Smart-Card erzeugt und gespeichert.
- Die Smart-Card wird mit einem PIN freigeschaltet
- Alle Operationen finden auf der Smart-Card und nicht auf dem PC statt.
- Wenn der Verdacht besteht, dass der PIN und die Smart-Card in fremde Hände geraten ist, muss das Zertifikat beim Aussteller gesperrt = revoziert/zurückgezogen werden.

## 2. Beschaffen des Zertifikats

- 2.1 Technische Voraussetzungen
- 2.2 Aussteller der SuisselD
- 2.3 Was bestellen
- 2.4 Identifikation und Validierung der E-Mail-Adresse
- 2.5 Inbetriebnahme
- 2.6 Weitere „Pflege“ des Zertifikats
- 2.7 Was befindet sich auf dem Kärtchen
- 2.8 Vorsicht

## 2.1 Technische Voraussetzungen

- PC mit Windows XP SP2, Vista oder 7  
oder
- Apple Mac mit OS X ab 10.5 (Intel-Prozessor-Generation)  
oder
- PC mit Linux, zum Beispiel Ubuntu (nur Post)  
und
- Smart-Card-Reader, wenn nicht vorhanden mit Zertifikat bestellen
- USB-Anschluss (ab 1.0) für Smart-Card-Reader
- Zuverlässige Internet-Verbindung

## 2.2 Aussteller der SuisseID

- Übersicht aller Anbieter:
  - <http://www.suisseid.ch>
- Schweizerische Post / SuisseSign
  - <http://www.post.ch/suisseid>
- Quovadis Trustlink Schweiz AG und Trüb AG
  - <http://www.suisseid-shop.ch>
- Schweizerischer Anwaltsverband = Quovadis
  - <http://www.swisslawyers.ch>
  - <https://suisseid-shop.ch/index.cfm?content=sav>



## 2.3 Was bestellen?

### Empfehlung

- SuisseID mit 3 Jahren Gültigkeit
- Kartenleser bzw. Smart-Card-Reader



- Persönliche Angaben bei der Bestellung genau so wie in der ID oder im Pass aufgeführt angeben.
- Längerfristig gültige E-Mail-Adresse angeben

## 2.4 Identifikation und Validierung E-Mail

- Identifikation durch eine beglaubigte ID- oder Pass-Kopie für den Aussteller
  - Post: Am Postschalter
  - Quovadis: SBB/Western Union Schalter
  - SAV: Von einem anderen Anwalt beglaubigt
- Validierung der E-Mail-Adresse
  - Aussteller schickt eine E-Mail mit einem Browser Link.
  - Durch Aufrufen des Browser-Links wird die E-Mail-Adresse bestätigt.

## 2.5 Inbetriebnahme

- Inbetriebname des Zertifikats
  - Installation der Software
  - Freischaltung des Zertifikats beim Aussteller
  - Neuen PIN wählen
- Was sie benötigen:
  - Den Brief mit dem PIN
  - Den Kartenleser
  - Die Karte mit der SuisseID
  - Internet-Verbindung
- Anleitung Quovadis: <http://www.quovadis.ch/activation>
- Anleitung Post SwissSign: <http://www.postsuisseid.ch/setup>

## 2.7 Was befindet sich auf dem Kärtchen

- Schlüsselpaar zur Authentifizierung = Nachweis der Identität
  - Private Key
  - Public Key
  - Zertifikat, vom Aussteller signierter Public Key
- Schlüsselpaar zur Signierung (Qualified Signature)
  - Private Key zur Signierung
  - Public Key zur Signierung
  - Zertifikat, vom Aussteller signierter Public Key zur Signierung
- KEIN Schlüsselpaar zur Verschlüsselung/Geheimmachung



## 2.5.1 Wahl des PINs / Passworts

- Quovadis lässt es zu, dass für das Authentication Zertifikat und das Qualified Signature Zertifikat unterschiedliche PINs gesetzt werden.
- Es wird auch von Quavadis empfohlen, beide PINs gleich zu setzen, weil bei der PIN-Abfrage nicht immer ersichtlich ist, welches Zertifikat angesprochen wird.
- Empfehlung für den PIN:
  - Zahlen 0-9
  - Klein- und Grossbuchstaben a-z, A-Z
  - Keine Sonderzeichen

## 2.6 Und nachher

- Installation von zusätzlicher Software
  - Acrobat Reader
  - SuisseSign von der Post
  - eGov Local Signer vom Bundesamt für Justiz (Quovadis und Post)
- Passwort für SuisseID merken
- Brief mit dem PIN aufbewahren falls eine Revozierung mit Feld B nötig wird (Post)
- Daran denken, dass die SuisseID in 3 Jahren abläuft

## 2.8 Wichtig: Es gibt keinen PUK für den Signaturschlüssel!

Nach 3-maliger (Post) oder 4-maliger (Quovadis) Falscheingabe des PIN ist die Karte gesperrt und es muss eine neue SuisseID bestellt werden!



**TIP: Bei der PIN-Eingabe Caps-Lock-Taste im Auge behalten**

## 3. Rechtliche Grundlagen

3.1 Obligationenrecht

3.2 Entwicklung der elektronischen Identifikation im Recht

3.3 Von der (Not-)verordnung zum elektronischen  
Behördenverkehr

3.4 Vereinheitlichung ZPO, StPO

## 3.1 Obligationenrecht

- Art. 13 Abs. 2 Obligationenrecht
  - Erfordernisse bei schriftlichen Verträgen: *eigenhändige* Unterschriften aller Vertragsparteien
  - Gesetzlich vorgeschriebene Schriftlichkeit v.a. für Schutz der schwächeren Vertragspartei (z.B. Mietrecht, Konsumentenrecht, Arbeitsrecht), Übereilungsschutz (z.B. Gerichtsstandsklauseln), zum Schaffen klarer Rechtsverhältnisse (Immobilien- und Gesellschaftsrecht)
- Frühere Fassung von Art. 13 Abs. 2 Obligationenrecht
  - Brief bzw. Telegramm mit Unterschrift desjenigen, der sich verpflichtet (vergangene Zeiten)
- Anpassungsbedarf an technische Entwicklung, elektronische Identifikation

## 3.2 Entwicklung der elektronischen Identifikation im Recht

- Problemstellung
  - Auf welche Art soll die Abgabe eines rechtlich verbindlichen Verpflichtungswillens erfolgen, so dass diese Verpflichtung einer Partei (natürliche oder juristische Person) zuverlässig und problemlos zugeordnet werden kann?
- Lösung
  - Mittels eines eindeutigen, unveränderbaren, individuellen, lesbaren Zeichens
  - Traditionell: Eigenhändige Unterschrift, allenfalls verstärkt durch öffentl., notarielle Beurkundung; BGE 121 II 252 (Bundesgericht schützte 1995 Nichteintretensentscheid, da Unterschrift nur per Fax vorlag)
  - Neue Entwicklung: Elektronisch, d.h. Individualisierung erfolgt mittels elektronischem Algorithmus. Brief bzw. Telegramm mit Unterschrift desjenigen, der sich verpflichtet (vergangene Zeiten)

→ Anpassungsbedarf an technische Entwicklung

## 3.3 Von der (Not-)verordnung zum elektronischen Behördenverkehr

- Zertifizierungsverordnung aus dem Jahre 2000
  - Ohne eigentliche gesetzliche Grundlage, v.a. Vss. für Herausgabe von Zertifikaten
- Bundesgesetz über elektronische Signatur (ZertES)
  - in Kraft seit 1.1.2005
  - Fokus auf Voraussetzungen für die Herausgabe von Zertifikaten, Haftung und Aufsicht der Anbieter von Zertifikaten, Sicherheitsaspekte im Vordergrund
  - Grundsätzliche Anerkennung/Akzeptanz der elektronischen Signatur im Privatrechtsverkehr
  - Einführung von Art. 59a Obligationenrecht, Haftung des Inhabers eines Signaturschlüssels (vgl. sep. Ausführungen)
  - Auswirkung auf den Rechtsalltag: verhältnismässig gering, Scheitern der Firma Swisskey, Ausnahmen zB. Rechtsverkehr mit EIGE für Marken/Patente/Designs, Bundesgericht

### 3.4 Vereinheitlichung ZPO, StPO

- Möglichkeit elektronischer Eingabe, Art. 130 ZPO; Möglichkeit elektronischer Zustellung mit Zustimmung der betroffenen Person (Art. 139); Art. 110 und Art. 87 StPO
- Es bleibt abzuwarten, ob sich der elektronische Behördenverkehr durchsetzt. Immerhin ist es so, dass die Kantone verpflichtet sind, Infrastruktur für sichere Verbindungen und Eingaben zur Verfügung zu stellen.
- Stand Januar 2011



## 4. Erzeugen von PDF-Dateien

- 4.1 Warum PDF-Dateien, Vorteile und Nachteile
- 4.2 PDF/A-Format
- 4.3 Grösse von PDF-Dateien
- 4.4 PDF/A-Dateien aus Textprogrammen
  - 4.4.1 PDF/A-Dateien aus Microsoft Word
  - 4.4.2 PDF/A-Dateien auf Apple OS X
  - 4.4.3 PDF/A-Dateien aus OpenOffice
  - 4.4.4 Andere Lösung: PDF-Drucker
- 4.5 PDF/A-Dateien durch Scannen
- 4.6 Weiterverarbeiten von PDF-Dateien

## 4.1 Warum PDF-Dateien

- Vorteile
  - Anerkannter und weit verbreiteter Standard für unveränderbare Dokumente
  - Grosse Verfügbarkeit von Software zur Erzeugung von PDF-Dateien
- Nachteile
  - Die Information im Dokument ist nicht zwingend strukturiert und kann auch nicht automatisch gelesen werden.
  - Ein XML-Format kann das und wird auch immer wieder diskutiert.

## 4.2 PDF/A-Format

- PDF-Format für die Langzeitarchivierung von Dokumenten
- Genormt nach ISO 19005, Siehe auch [www.pdfa.org](http://www.pdfa.org)
- Eigenschaften:
  - Kein Zugriff auf externe Ressourcen, z.B.
    - Alle verwendeten Schriften sind integriert
    - Keine externen Links z.B. Bilder usw.
  - Keine aktiven Elemente
    - Keine „Actions“, kein Sound, keine Filme
    - Formulare bzw. Eingabefelder
    - JavaScript

## 4.3 Grössen von PDF-Files

- Die Verordnung des Bundes machte keine Angaben über die maximale Dateigrösse der Eingaben
- Dateien grösser als 5 MByte sind allgemein aber auch für den normalen Versand per E-Mail schwer handhabbar
- Für die Eingabepattform Privasphere sind Eingaben mit mehreren Dateien auf 15 MByte limitiert.
- Bei normalem Text ~ 20-50kByte pro Seite ergeben 5 MByte 100–250 Seiten
- Verschiedene Schriftarten und Bilder machen eine PDF-Datei grösser

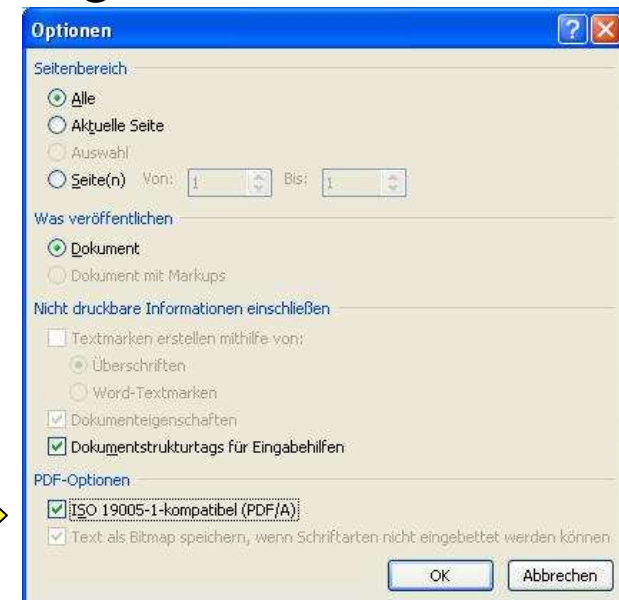
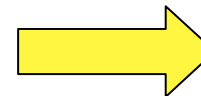
## 4.4.1 PDF/A-Dateien aus Microsoft Word 2007

### Download für Microsoft Office 2007

- Add-In für 2007 Microsoft Office: "Speichern unter – PDF oder XPS" von Microsoft installieren
- Woher: Microsoft-Download-Seite, „Googeln“

### PDF-Option

- ISO 19005-1-Kompatibel (PDF/A)



## 4.4.2 PDF/A-Dateien auf Apple



- Microsoft Word 2008 kann kein PDF
- Es gibt Software von PDF nach PDF/A
- Allgemeine Empfehlung: OpenOffice für OS X verwenden

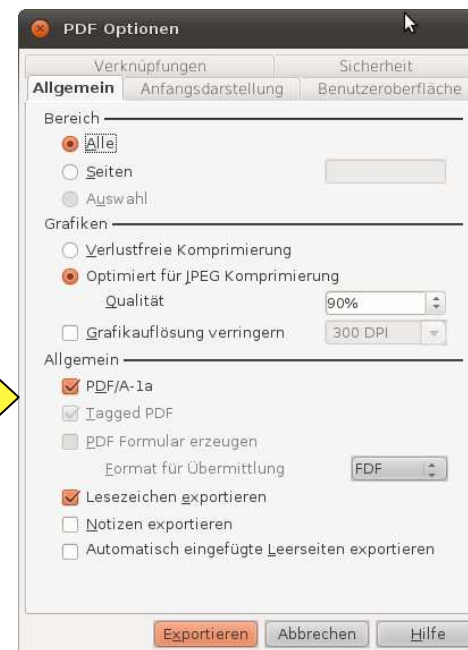
## 4.4.3 PDF/A-Dateien aus OpenOffice

PDF gehört zum Funktionsumfang von OpenOffice.

- Kostenloser Download von OpenOffice unter [www.openoffice.org](http://www.openoffice.org)

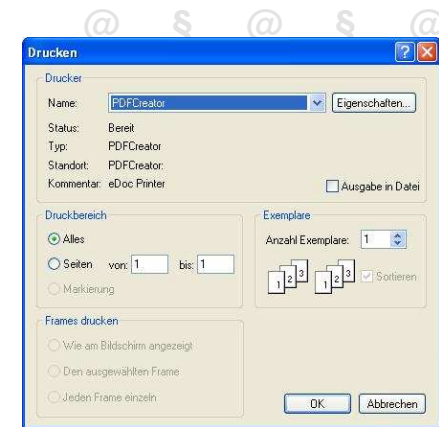
PDF-Option

- Export PDF: PDF/A-1a



## 4.4.3 Andere Lösung: PDF-Drucker

- Download von <http://www.pdfforge.org>
- Installiert einen PDF-Pseudo-Drucker
- Option „Speichern unter“  
“Dateityp „PDF/A-1b Dateien (\*.pdf)“
- Ein PDF-Drucker ist sehr praktisch
  - Erzeugt PDF/A mit alter Word-Version
  - Webseiten mit Browser als PDF/A-Datei speichern
  - E-Mail aus Mail-Programm als PDF/A-Datei speichern
  - PDF-Formular in fixierte PDF/A-Datei umwandeln
  - PDF in PDF/A umwandeln:  
Öffnen mit Acrobat Reader und auf PDF-Drucker ausdrucken





## 4.5. Scannen

- Scann-Programme können direkt PDF-Dateien erzeugen.
- Sie bestehen ohne Texterkennung nur aus Bildern
- Schwarz/Weiss mit maximal 300 DPI Auflösung ist meistens ausreichend
- Max. 100 kByte pro Seite

## 4.6 Weiterverarbeitung von PDF-Dateien

- Meta-Daten ausfüllen
  - Erstellungsdatum und Autor
  - Titel und Stichwörter
- Die Meta-Daten könne später von Dokumentenverwaltungsprogrammen gelesen werden

## 5. Signieren von PDF-Dateien

- 5.1 Was und mit Was signieren
- 5.2 Signieren mit dem eGOV Local Signer: Start
- 5.3 eGOV Local Signer: PDF-Dokument laden
- 5.4 eGOV Local Signer: Signaturfeld
- 5.5 eGOV Local Signer: Signatureinstellungen
- 5.6 eGOV Local Signer: Signaturangaben
- 5.7 eGOV Local Signer: Resultat
- 5.8 Nach dem Signieren
- 5.9 Mehrfache Signatur

## 5.1 Was und Wie signieren?

- Signieren ist das Versehen eines digitalen Dokuments mit einer digitalen Unterschrift
- Was soll signiert werden
  - Alle Dokumente welche auch auf Papier unterschrieben werden
    - Die Rechtsschrift signieren
    - Beilagen bzw. Beweisofferten NICHT signieren oder mit Signatur nur Integrität sicherstellen
- Mit was signieren
  - eGov Local Signer, gratis, im Auftrag des Bundesamts für Justiz entwickelt
  - SwissSigner von der Post
  - Adobe Reader Professional

## 5.2 Signieren mit eGOV Local Signer: Start

- Homepage für Download und Support
  - <http://www.openegov.ch/localsigner>
- Aktueller Adobe Reader muss installiert sein

- Start



## 5.2.1 eGOV Local Signer: PDF-Dokument laden

**Open eGov LocalSigner**

Datei Einstellungen ?

Anzeige des zu signierenden Dokuments

Reichert  
Instrasse 134  
ich

29. Dezember 2010

**EINSCHREIBEN**

Herr  
Sargon Al Bazi  
Hahnrainweg 2  
5400 Baden

E-Mail: [bernd.reichert@bluemail.ch](mailto:bernd.reichert@bluemail.ch)  
Mobile +41 78 561 62 52  
Tel. +41 44 21 29 20  
Fax. +41 44 278 9 21

**Einzahlungsscheine Januar bis Dezember 2011**

Sehr geehrter Herr Al Bazi,

Dokument: C:\Dokumente und Einstellungen\bre\Eigene Dateien\2010\_12\_29\_EZ\_Sargon\_Al\_Bazi.pdf PDF/A-1a Auswählen

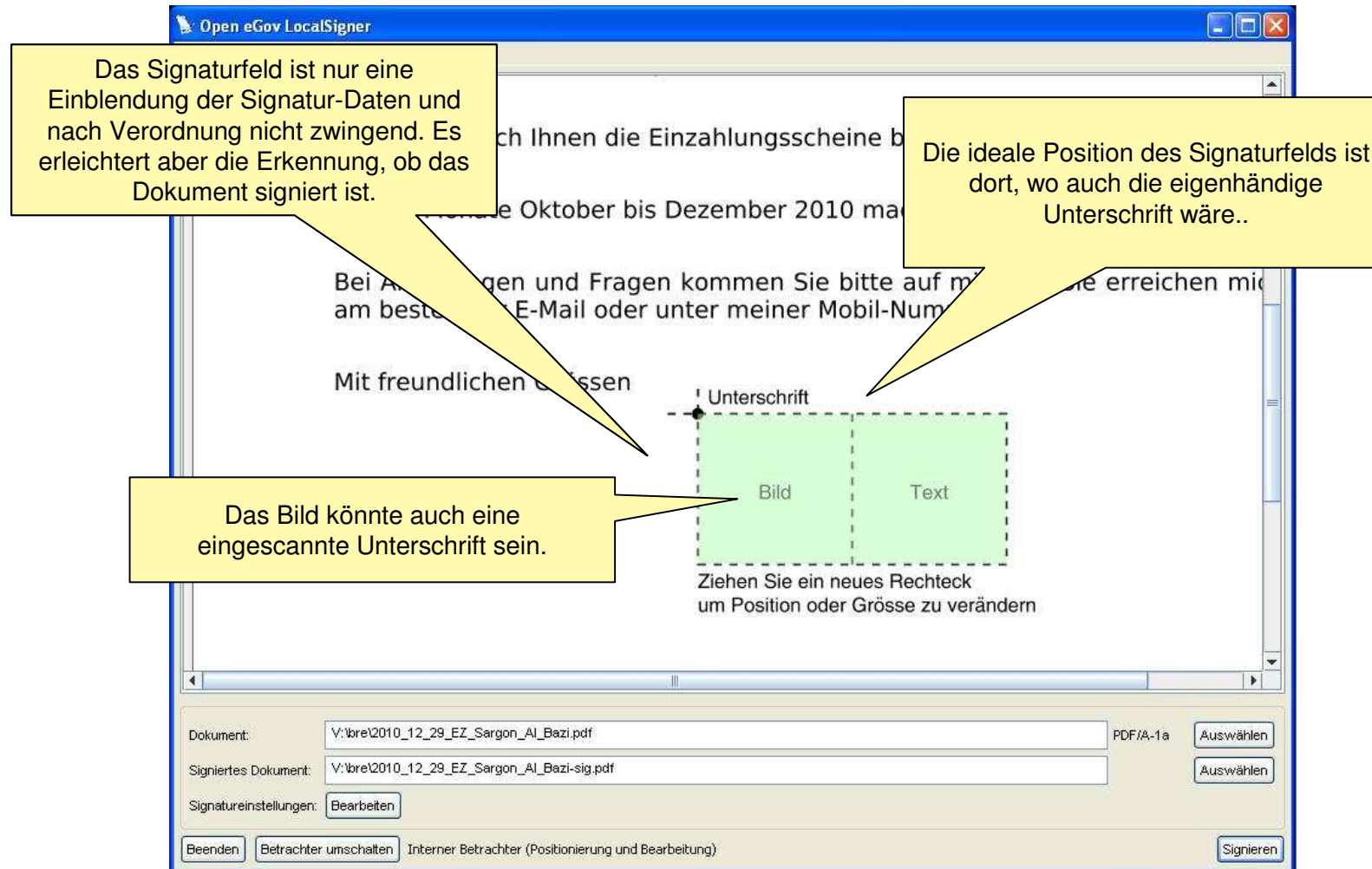
Signiertes Dokument: C:\Dokumente und Einstellungen\bre\Eigene Dateien\2010\_12\_29\_EZ\_Sargon\_Al\_Bazi-sig.pdf Auswählen

Signatureinstellungen: Bearbeiten

Beenden Betrachter umschalten Interner Betrachter (Positionierung und Bearbeitung) Signieren

Bestätigung, dass das geladene Dokument dem PDF/A Standard entspricht

## 5.2.3 eGOV Local Signer: Signaturfeld



## 5.2.4 eGOV Local Signer: Signatureeinstellungen

**Profil bearbeiten**

Datei: C:\Dokumente und Einstellungen\bre\localsigner\profiles\default.properties

Standard Zielverzeichnis wechseln: C:\Dokumente und Einstellungen\bre\Eigene Dateien

PDF Zusatz(seite):

Signaturart: Unterschriften (mehrfach) ☐ Zertifizieren ☒ Dokument nach Signaturvorgang anzeigen: ☒

Signaturort: Zürich

Kontakt:

Signaturerklärung: Ich habe dieses Dokument erstellt

Foto oder Bild: C:\Dokumente und Einstellungen\bre\Eigene Dateien\Eigene Bilder\Snoopy.jpg

Unterschrift/Zertifizierung sichtbar ☒

Abstand von Links (mm): 43 Signaturbreite: 53

Abstand von Oben: 214 Signaturhöhe: 26

Signieren auf: letzter Seite

Zeitstempel einfügen (TSA): TSA QuoVadis

**Voreinstellung: Einzelunterschrift**

**Das Signaturfeld wird normalerweise angezeigt**

**Voreingestellte Signaturerklärung**

**Bild für Signaturfeld**

**Voreinstellung mit Zeitstempel von Quovadis. Auswahl: Kein Zeitstempel, Post, Quovadis, Swiss Admin**



## 5.2.5 eGOV Local Signer: Signaturangaben

### Voraussetzung

- SuissID-Kärtchen im Reader
- Internet-Verbindung aktiv

**Zertifikatsauswahl**

Markieren Sie das Zertifikat, mit dem Sie signieren wollen.

Name	Aussteller	Gültigkeit	Beschreibung
Bernd Reichert (Qualified Signature)	SwissSign Qualified Platinum C	2010 - G2	20.10.2013
Bernd Reichert (Authentication)	SwissSign SuisseID Platinum C	2010 - G2	20.10.2013

Signaturart: ☐ Untersreiben (mehrfach) ☒ Zertifizieren ☒ Unterschrift/Zertifizierung sichtbar

Signaturort/Datum: Zürich 2011-01-07

Kontakt:

Signaturerklärung: Ich habe dieses Dokument erstellt

Zeitstempel einfügen (TSA): TSA QuoVadis

Sprache des Signaturtexts: englisch

Abbrechen Signieren

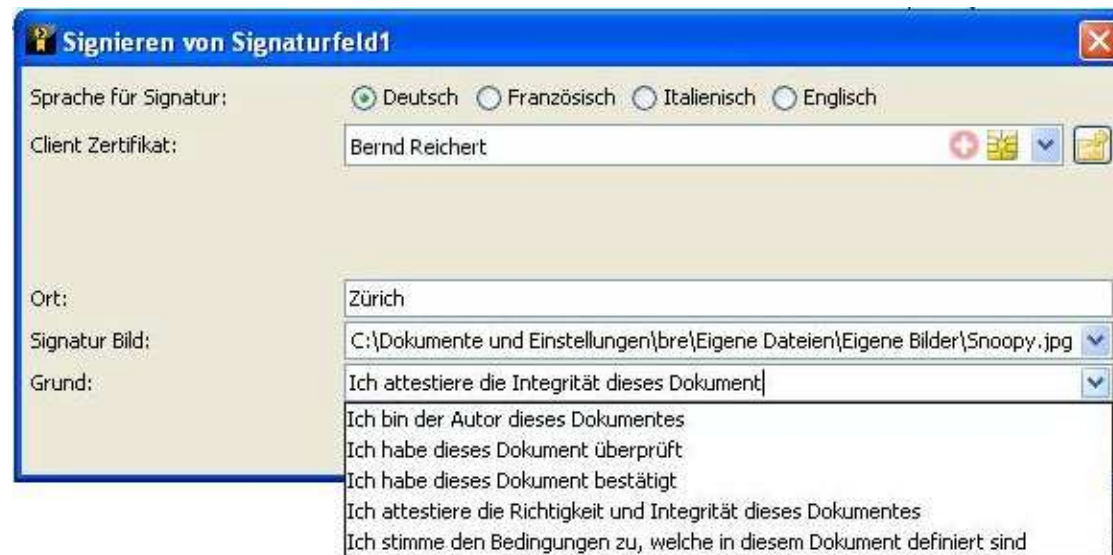
Einfache einzelne Unterschrift

Das Signaturfeld wird im signierten Dokument an der vorher ausgewählten Stelle angezeigt.

Anwendung eines Zeitstempels ist nach Verordnung nicht zwingend aber empfohlen.

## 5.2.6 SwissSigner: Auswahl Signaturerklärungen

- Das Wort „Signaturerklärung“ kommt im ZertES nicht vor.



- Solche Kommentare können je nach Fallkonstellationen massive rechtliche Konsequenzen haben.
- Im Zweifelsfall nur die Unterschrift setzen

## 5.2.7 eGOV Local Signer: Resultat



## 5.8 Nach dem Signieren

- Die PDF-Datei nach dem Signieren nicht mehr verändern.
  - Zum Beispiel mit der Bearbeitungsfunktion im Adobe Reader
- Die signierte elektronisch gespeicherte Datei ist das Original

Wichtig:

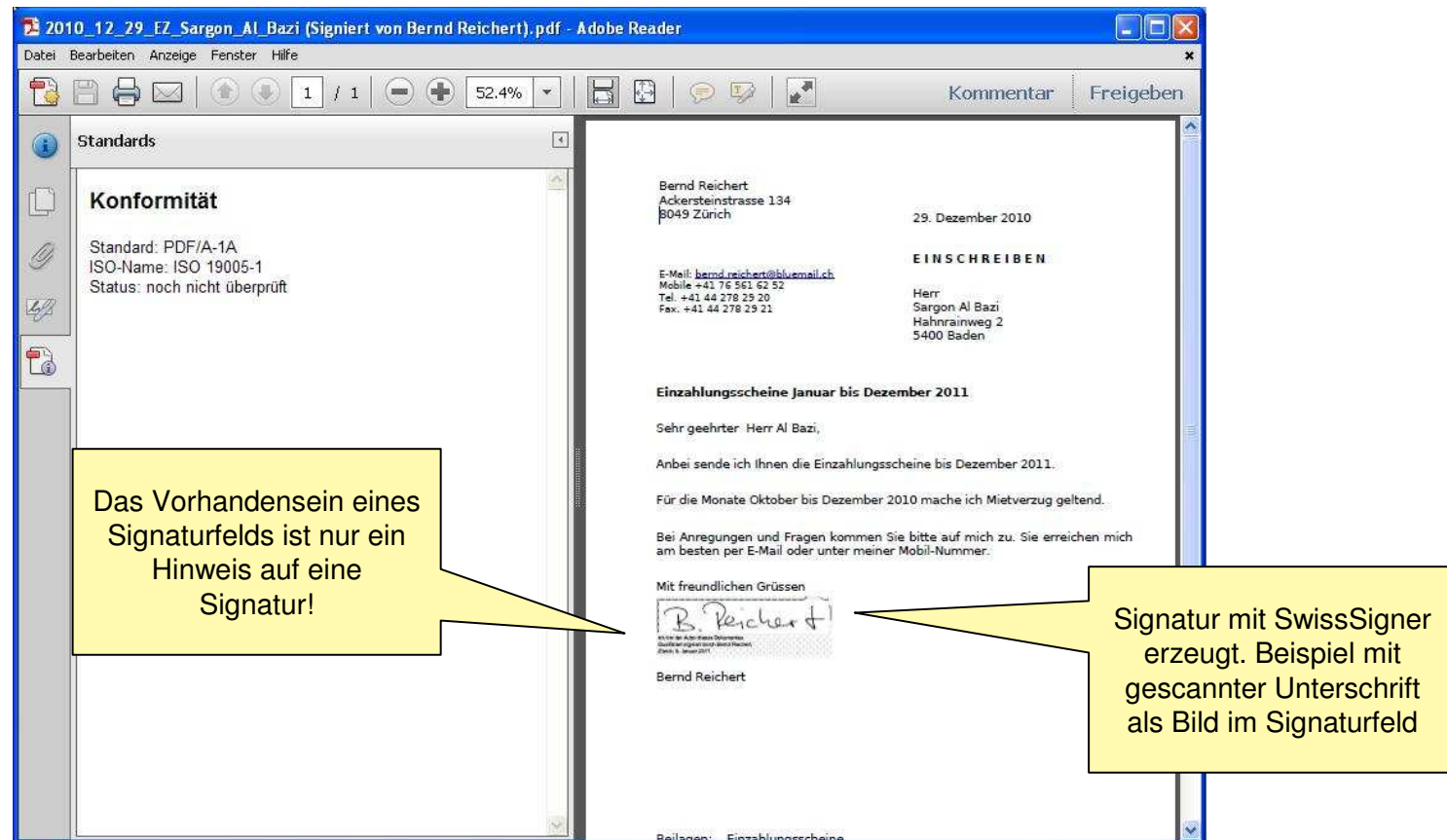
- Die Integrität des elektronisch gespeicherten Dokuments wird durch die Signatur sichergestellt.
- Ausdrücke des Dokuments sind keine Originale
- Auf ausgedruckten Exemplaren ist die Signatur nicht mehr ersichtlich.  
Das Signatur-Feld ist kein Nachweis der Signatur

## 5.9 Mehrfache Signatur

- Eine PDF-Datei kann mehrfach von verschiedenen Personen signiert werden
- Die zu signierende PDF-Datei kann dazu per E-Mail von einer Person zur nächsten verschickt werden
- Beim verifizieren der signierten PDF-Datei sind alle Signaturen ersichtlich

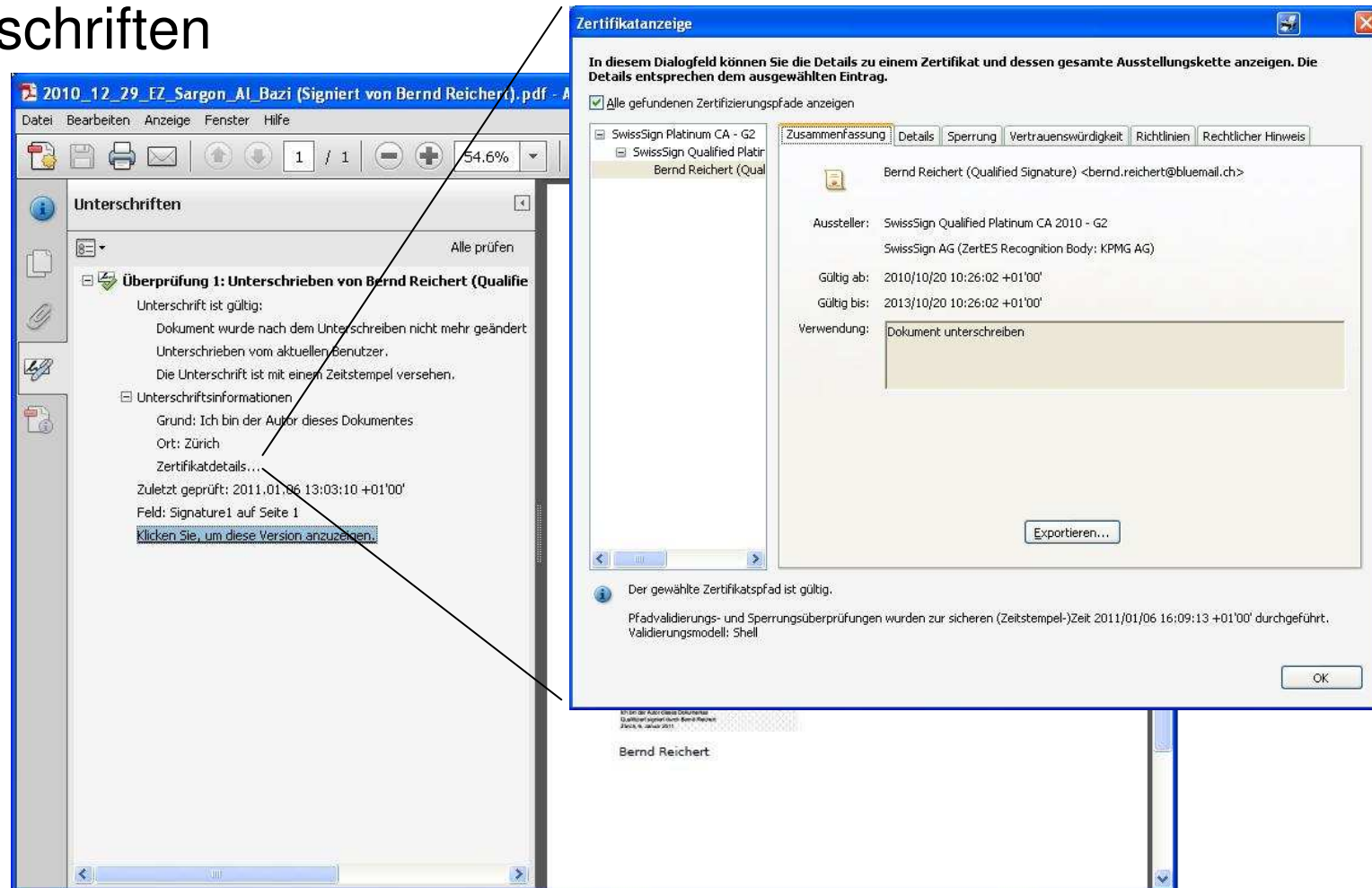
## 6. Überprüfen einer PDF-Datei

- Mit dem Adobe Reader angezeigtes PDF-Dokument



## 6.2 Überprüfen der Signatur im Adobe Reader

Ob ein Dokument signiert ist sieht man erst unter Unterschriften



## 6.3 Validieren eines signierten Dokuments

- Ist das Dokument seit der Signatur unverändert?
- Ist der Unterzeichnende berechtigt?
- Zertifikat des Unterzeichnenden?
  - Gültigkeit jetzt und zum Zeitpunkt der Signatur?
  - Aussteller und Zertifikatskette?
  - Revozierungsstatus
- Wann wurde das Dokument signiert?
- Zeitstempel?



## 7. Arbeitsmethodik, va. im Anwaltsbereich

- Rechtsschrift, Eingabe, Schreiben (Mitteilungen)
  - Mitteilungen in PDF/A-Format mit qualifizierter Unterschrift (vgl. Art. 10 VO zu StPO und ZPO), d.h. Signiert
  - Beilagen in PDF-Format (vgl. Art. 10 VO zu StPO und ZPO), d.h. nicht signiert
- Übermittlungskanal
  - Ausschliesslich anerkannte Zustellplattform der entsprechenden Behörde
    - Derzeit
      - [Www.privasphere.ch](http://www.privasphere.ch) (SG, LU, .....)
      - [Www.post.ch/incamail](http://www.post.ch/incamail) (ZH... )
- Anspruch auf Entscheide und Mitteilungen in elektronischer Form?
  - Mit Einverständnis der betroffenen Person (Art. 139 ZPO, Art. 9 VO zu StPO/ZPO) möglich
  - jedoch **Achtung**: Muss wie Briefkasten regelmässig geleert/betreut werden!
  - Vermutlich sinnvoller, wenn elektronische Eingabe im Einzelfall noch zusätzlich verlangt wird.

## 8. Übermittlung

- 8.1 Behörden, wie finde ich die Adresse
- 8.2 Veröffentlichte Behördenadressen Januar 2011
- 8.3 Kanton Zürich, Stand Januar 2011
- 8.4 Web-Formular oder E-Mail auf einer Plattform
- 8.5 Web-Formulare
- 8.6 Anmeldung auf einer E-Mail-Plattform: Privatsphere
- 8.7 eGov-E-Mail mit Privasphere
- 8.8 Anmeldung auf einer E-Mail-Plattform: IncaMail
- 8.9 eGov-E-Mail mit IncaMail
- 8.10 Wie es funktionieren wird
- 8.11 Stand Januar 2011

## 8.1 Wie finde ich die Adresse einer Behörde

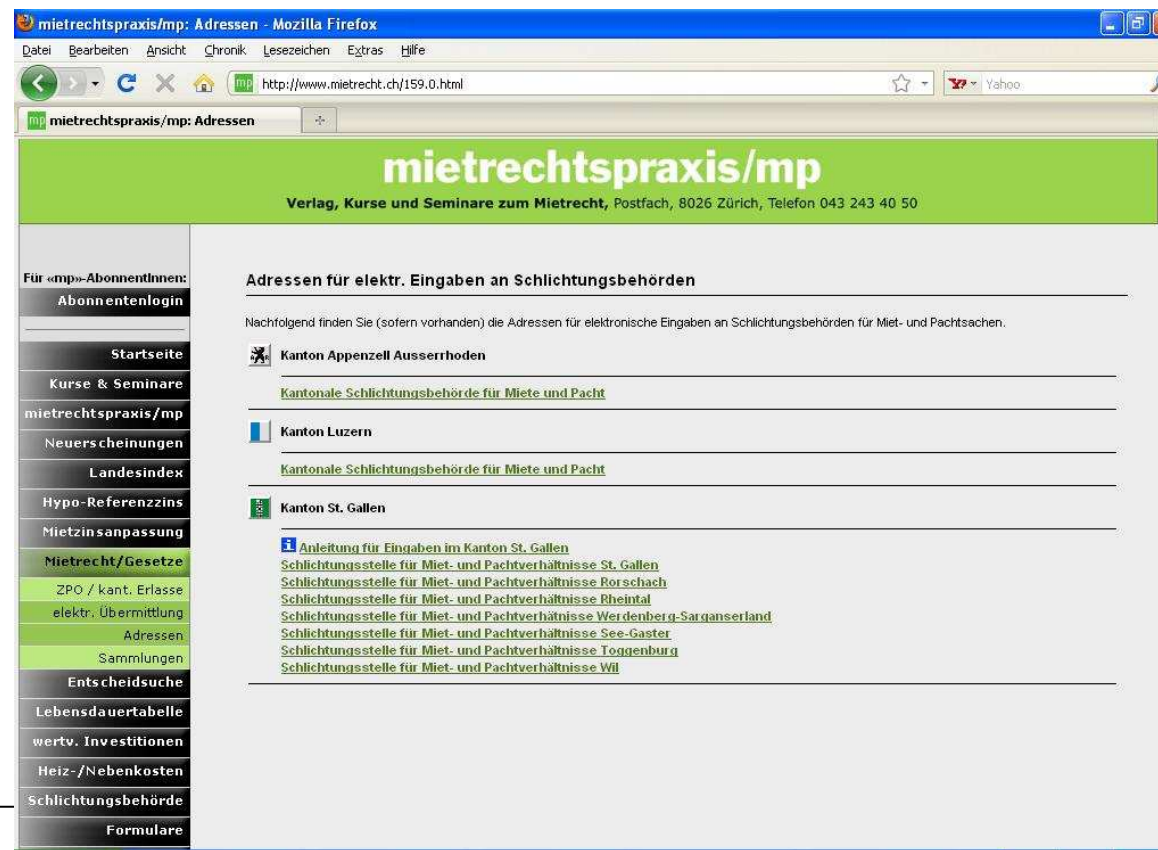
- Offizielle Seite der Bundeskanzlei <http://www.ch.ch>
  - Menü oben: „Über die Behörden“
  - Menü links: „E-Justice“
  - Rechte Seite: Für jeden Kanton eine PDF-Datei



## 8.1.1 Adressen der Schlichtungsbehörden

### Zusammenstellung der Mietrechtspraxis

- <http://www.mietrecht.ch/159.0.html>



## 8.2 Veröffentlichte Behördenadressen Stand Januar 2011

- Für jeden Kanton sollte bekannt sein
  - Gewählte E-Mail- bzw. Eingabeplattform
  - Eine Liste von E-Mail-Adressen für jede Behörde
  - Alternativ zur E-Mail-Adresse Links auf Web-Formulare für jede Behörde
- Was ist wirklich veröffentlicht:
  - Plattform- und Web-Links-Informationen für AR, LU, SG, TI und ZG (alle Privasphere)
  - Plattform und E-Mail Adressen für SH (Privasphere)
  - Nur Plattform: AG, BE, BL, BS, FR, GL, JU, NE, NW, OW, SO, SZ, UR, ZH
  - Keine Angaben: AI, GR, TG, VD, VS

## 8.2.1 Kanton Zürich, Stand Januar 2011

Siehe auch <http://www.gerichte-zh.ch> →Themen

- Der Kanton Zürich hat IncaMail als Plattform gewählt
- Die elektronischen Adressen der Behörden sind der Bundeskanzlei mitgeteilt worden.
- Die Adressen werden aber aus Angst vor SPAM und nicht konformen Eingaben nicht veröffentlicht.
- Es wird auf das Teilnehmerverzeichnis der Plattformen verwiesen:
  - IncaMail hat derzeit kein Teilnehmerverzeichnis
  - Das Plattform-übergreifende Verzeichnis existiert noch nicht

## 8.3 Web-Formular oder E-Mail auf einer Plattform

- Vorteil des Web-Formulars
  - Keine Registrierung auf einer Plattform nötig
  - Validierung der Eingabe auf Pflichtfelder
  - Kostenlos
- Nachteil des Webformulars
  - Keine 2-Weg Kommunikation möglich
- Vorteil der E-Mail auf der Plattform
  - 2-Weg-Kommunikation
- Nachteil der E-Mail auf der Plattform
  - Keine Validierung der Eingaben

## 8.4 Web-Formulare

Unter [http://www.gerichte.sg.ch/home/dienstleistungen/elektronischer\\_rechtsverkehr.html](http://www.gerichte.sg.ch/home/dienstleistungen/elektronischer_rechtsverkehr.html) befindet sich eine Anleitung, welche für alle Web-Formulare von Privasphere, also für AR, LU, SG, TI und ZG gilt.

Beispiel:  
Schlichtungsbehörde  
Miete und Pacht Luzern

PrivaSphere Sicheres Kontaktfo...

KANTON LUZERN

Sicheres Kontaktformular

Schlichtungsbehörde Miete und Pacht

An Luzern Schlichtungsbehörde Miete und Pacht

Von bernd.reichert@bluewin.ch

Betreff

Firma/Organisation

Name\*

Vorname\*

Geburtsdatum\* Tag  Monat  Jahr

Strasse/Nr.  Nr.

PLZ/Ort  Ort

Heimatort\*

Referenznummer

Fallnummer (wenn schon vorhanden)

Sachbearbeiter

Die Eingabe sowie sämtliche Anhänge sind elektronisch zu signieren und im Format PDF einzureichen. Elektronische Eingaben werden während den üblichen Bürozeiten bearbeitet. Bitte beachten Sie: Mit dem Senden dieser Eingabe lösen Sie ein gerichtliches Verfahren aus.

Füllen Sie ihr Formular elektronisch aus. Mit der SuisseID und der Gratissoftware Open eGov LocalSigner können Sie diese mit Ihrer qualifizierten elektronischen Signatur unterzeichnen:

Software  
[Open eGov LocalSigner](#)

Formulare

Spam-Schutz

p<%6a(

Bestätigen Sie diese Zeichenfolge (Gross-/Kleinschreibung beachten).

Anhang   (14.9 MB von max. 15 MB verfügbar)

Fertig



## 8.2.1 Kanton Zürich, Stand Januar 2011

Siehe auch <http://www.gerichte-zh.ch> →Themen

- Der Kanton Zürich hat IncaMail als Plattform gewählt
- Die elektronischen Adressen der Behörden sind der Bundeskanzlei mitgeteilt worden.
- Die Adressen werden aber aus Angst vor SPAM und nicht konformen Eingaben nicht veröffentlicht.
- Es wird auf das Teilnehmerverzeichnis der Plattformen verwiesen:
  - IncaMail hat derzeit kein Teilnehmerverzeichnis
  - Das Plattform-übergreifende Verzeichnis existiert noch nicht

## 8.5 Wenn nur die E-Mail-Adresse der Behörde bekannt ist

- Nicht direkt eine E-Mail an diese Adresse senden
  - Die Behörden dürfen direkte E-Mails nicht entgegen nehmen
- Sichere Zustellplattform verwenden
  - Privasphere
  - IncaMail

## 8.5b Anmeldung auf einer E-Mail-Plattform: Privatsphere

### Identifikation mit dem Authentication-Zertifikat im Browser

Meine Konto-Einstellungen; Bernd's PrivaSphere - Mozilla Firefox

PrivaSphere AG (CH) [https://egov.privasphere.com/userContactForm\\_de.jsp;jsessionid=E88ACFE53F9E802](https://egov.privasphere.com/userContactForm_de.jsp;jsessionid=E88ACFE53F9E802) Yahoo

clientCert PKI authentication by PrivaS... PrivaSphere ist SuisseID Pionierprojekt Meine Konto-Einstellungen; Bern...

**PrivaSphere™**  
Secure Messaging Service

Willkommen,  
**bernd.reichert@bluemail.ch**

D | E | F | I | Hilfe | Abmelden  
Letzter Zugriff: 14:02:57

Meine Mail Meine Kontakte Mein Konto

Konto-Einstellungen Guthaben kaufen Abrechnungs-Log Meine Adresse

Konto-Einstellungen

Übersicht  
Benutzereinstellungen  
Abos und Prepaid  
**Kontaktformular**  
Zertifikateinstellungen  
POP-Einstellungen  
eGov/Einschreiben  
Speicheroptionen  
Ordner Konfiguration  
Berichterstattung

**Kontaktformular**

Entwerfen Sie Ihr eigenes "Sicheres Kontaktformular" und lassen Sie Ihre Kunden und Partner sichere E-Mails auf Ihre Kosten zustellen, ohne dass diese sich anmelden müssen.

Aktivieren ☒

Photo/logo   Laden Sie Ihr Foto/Logo hoch und zeigen Sie es in Ihrem Sicheres Kontaktformular  
Unterstützt sind gif und jpg; max. 50 KB

Hyperlink  Link für Photo/Logo z.B. auf Homepage

Text  Text unter dem Logo

E-Mailadresse unterdrücken ☐ Namen oder E-Mailadresse wird auf Kontaktformular nicht angezeigt

Name unterdrücken ☐

Spam-Schutz ☐

Ihre sichere Kontaktadresse <https://www.privasphere.com/bernd.reichert@bluemail.ch>

[Vorschau \(zuerst speichern\)](#)

## 8.5.1 eGOV-E-Mail mit Privasphere

Meine Mail | Meine Kontakte | Mein Konto

Posteingang | Entwürfe | Gesendet | Umfragen (Beta)

Senden Vertraulich | Zurück | Speichern, kein Senden | E-Mail an

**Erfassen Sie hier Ihre Versandoptionen**

Nicht vertraute PrivaSphere Benutzer benötigen einen Message Unlock Code (MUC) um die E-Mails lesen zu können. Dieser kann mündlich, via SMS oder Fax übermittelt werden.

<b>Von</b>	Bernd Reichert		
<b>Betreff</b>	Test-Mail		
<b>Anhang:</b>	2010_12_29_EZ_Sargon_AI_Bazi (Signie....pdf .. (128k) ?		
<b>An</b>	obergericht@ktsh.ch	Meldung ID: 99D MUC: <b>0g338</b>	Fax Vorlage: <input type="checkbox"/> vertrauen SEND MUC ?
<b>Rückantwort</b>	<input checked="" type="checkbox"/> vorausbezahlen ?		
<b>Beziehungsvertraulichkeit</b>	<input checked="" type="checkbox"/> Absender (E-Mailadresse "bernd.reichert@bluemail.ch") nicht anzeigen ? <input checked="" type="checkbox"/> Betreff nicht anzeigen setzen Sie den Default in "Mein Konto" ?		
<b>Empfangsbestätigung</b>	<input checked="" type="radio"/> Alle ? <input type="radio"/> Keine <input type="radio"/> Letzte nur setzen Sie den Default in "Mein Konto" ?		
<b>Versandart</b>	<input type="radio"/> Vertrauliche E-Mail <input type="radio"/> Einschrieben: Standard E-Mail (S/MIME Format) ? <input checked="" type="radio"/> eGov Einschreiben (Empfang nur mit starker Authentisierung durch identifizierte Empfänger) Mehr Optionen: ?		
<b>Kosten</b>	1 * 0.75 CHF , (erste 1.0M inklusive) CHF 0.75 ? <b>TOTAL CHF 0.75</b> Berechnung aktualisieren		
<b>Guthaben</b>	Ihr Kontostand vor dem Versand beträgt: CHF 10.00		

Vertraulich senden

**E-Mail-Adresse der Behörde** (points to obergericht@ktsh.ch)

**Signierte Eingabe als Anhang** (points to 2010\_12\_29\_EZ\_Sargon\_AI\_Bazi (Signie....pdf .. (128k) ?)

**Nicht Gratis** (points to eGov Einschreiben)

**eGov-Einschreiben** (points to eGov Einschreiben)

## 8.6 Anmeldung auf einer E-Mail-Plattform: IncaMail

Identifikation mit dem Authentication-Zertifikat im Browser

Kontoeinstellungen: Bernd Reichert - Mozilla Firefox

Die Schweizerische Post (CH) https://im.post.ch/run/securehome.app

Kontoeinstellungen: Bernd Reichert

**SWISS POST** IncaMail DE | FR | IT | EN | Hilfe

Willkommen, Bernd Reichert (bernd.reichert@bluemail.ch) [Abmelden](#)

E-Mail schreiben E-Mail lesen **Kontoeinstellungen** Kontakte Logbuch

**Sicherheitsfrage**

Aktuelle Sicherheitsfrage: What was the name of your first teacher? Eigene Frage:

Antwort:

**Passwort ändern**

Aktuelles Passwort:

Neues Passwort:

Neues Passwort bestätigen:

Das Passwort:

- muss mindestens 8 Zeichen lang sein
- muss mindestens zwei der folgenden Zeichentypen enthalten: Grossbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen
- darf nicht Ihren eigenen Namen oder E-Mail-Adresse enthalten

**Sprache ändern** Deutsch

**eGov Einstellungen**

- ☒ Ich will dieses Konto für den schweizerischen Behördenverkehr einsetzen.
- ☒ eGov Einschreiben immer mit SuisseID Identifikation für Empfänger

Der Empfänger muss zum Öffnen eines eGov Einschreibens zwingend ein zugelassenes Zertifikat vorweisen.

**Versandeeinstellungen**

- ☐ Originaltext beim Antworten einfügen
- ☐ Immer Kopie an mich senden

Übermittlungsbestätigung bei vertraulichen E-Mails (gilt nicht für Einschreiben):

☒ Ja ☐ Nein ☐ Nur letzter Empfänger

E-Mail-Signatur:



eGov-Einstellungen

## 8.6.1 eGOV-E-Mail mit IncaMail

Willkommen, Bernd Reichert (bernd.reichert@bluemail.ch)

**E-Mail schreiben** E-Mail lesen Kontoeinstellungen Kontakte Logbuch

Von: Bernd Reichert <bernd.reichert@bluemail.ch> E-Mail-Adresse der Behörde  
obergericht@ktsh.ch

 CHF 0.50  CHF 2.00 Nicht Gratis

☐ CC und BCC anzeigen

Betreff: Test-Mail


Daten:

☒ 2010\_12\_29\_EZ\_Sargon\_Al\_Bazi (Signiert von Bernd Reichert).pdf Signierte Eingabe als Anhang


☐ Weitere Dateien

Signierte Eingabe als Anhang

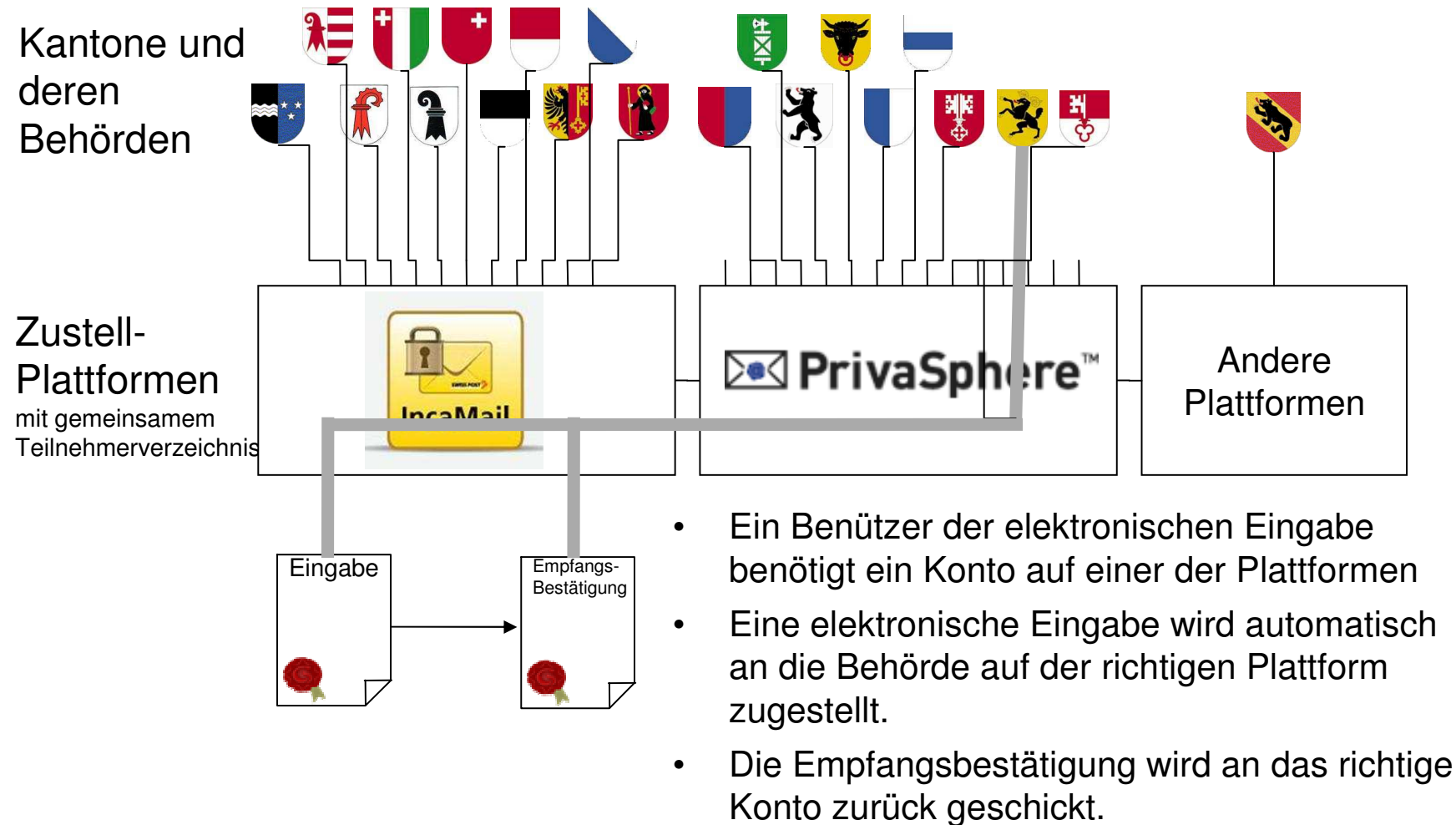
Detaillierte Anleitung unter :  
<http://www.post.ch/post-incamail-anleitung-verordnung.pdf>

Kostenlose Kopie an mich 

☒ Vertrauliche Kopie der Nachricht an mich senden

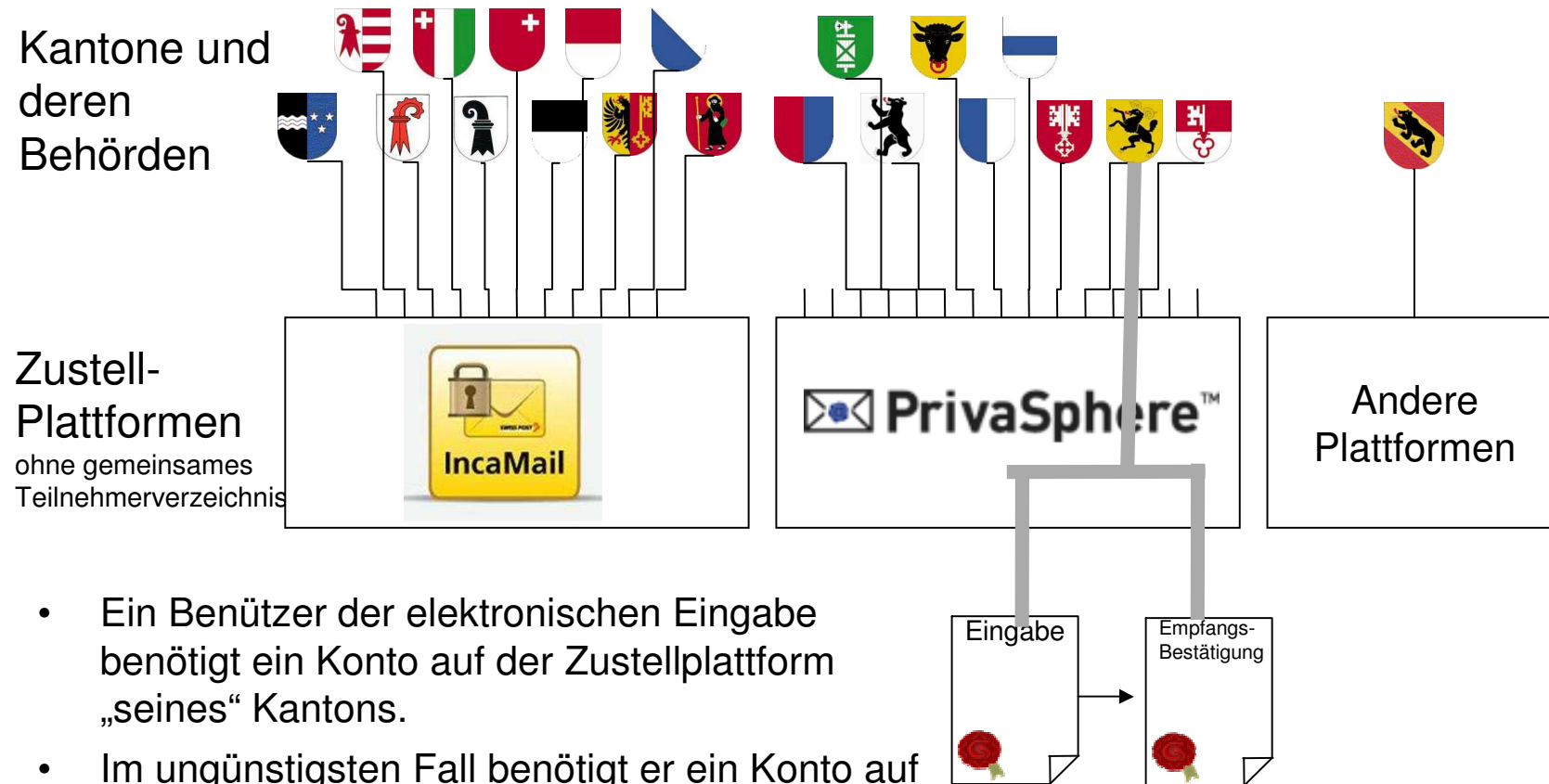
 Senden

## 8.7 Wie es funktionieren wird





## 8.7.1 Stand Januar 2011



- Ein Benutzer der elektronischen Eingabe benötigt ein Konto auf der Zustellplattform „seines“ Kantons.
- Im ungünstigsten Fall benötigt er ein Konto auf allen Zustellplattformen.



## 8.8. Nach erfolgter Eingabe

Es wird empfohlen, folgende PDF(/A)-Dateien auch in digitaler Form aufzubewahren:

- Die Eingabe mit den Beilagen
- Die Sendebestätigung bzw. die Versandquittung
- Die Empfangsbestätigung der Behörden

Man beachte

- Das Original ist die signierte digital gespeicherte Datei
- Art. 957ff und die Geschäftsbücherverordnung (GeBüV)

## 9. Die Einhaltung von Fristen

- 9.1 Sende und Empfangsbestätigung
- 9.2 Einhaltung der Frist nach Art. 143 Absatz 2 ZPO

## 9.1 Sendbestätigung der Plattform oder Empfangsbestätigung des Empfängers?

- Die E-Mail-Plattformen (zur Zeit Privatsphere und IncaMail) liefern eine Sendebestätigung / Versandquittung als signierte PDF-Datei.
- Die empfangende Behörde liefert später eine Empfangsbestätigung, ebenfalls als signierte PDF-Datei

Frage:

Welcher dieser Belege gilt als Nachweis der Fristeinhaltung?

The image shows a screenshot of a 'Versandquittung' (Delivery Confirmation) document from IncaMail. The document is titled 'IncaMail' and 'Versandquittung'. It contains the following information:

Absender		Identifikation	
rnp@kutter@swissign.com		SuiteID	
Versanddatum		Betreff	
Nov 05 2010, 13:00:49 GMT+0100		Eingabe	
Versandart		Nachrichtennummer	
eGov Einschreiben		1288988470.0.17650598261032@incamail.ch	

Empfänger		Identifikation	Status	Datum
rnp@kutter@swissign.com		SuiteID	Eingegangen	Nov 05 2010, 13:00:49 GMT+0100

Original E-Mail:  
Daten (Name, Typ, Größe in Bytes, Hash-Wert)

Die Richtigkeit dieser Quittung bezeugt:  
Die Schweizerische Post  
Datum: Nov 05 2010, 13:00:51 GMT+0100

Powered by © 2010 Swiss Post  
www.incmail.ch

## 9.2 Einhaltung der Frist nach Art. 143 Absatz 2 ZPO

Art. 143 Absatz 2 ZPO lautet:

Bei elektronischer Übermittlung ist die Frist eingehalten, wenn der Empfang bei der Zustelladresse des Gerichts spätestens am letzten Tag der Frist durch das betreffende Informatiksystem bestätigt worden ist.

- Nach der Wortlautauslegung wäre es die Empfangsbestätigung.
- Zählt die Zustellplattform zu den Informatik-Systemen des Gerichts?
- Analogie Postschalter: Beleg der eingeschriebenen Sendung gilt als Beleg der Fristeinhaltung
- Wenn die elektronische Übermittlung einen Nutzen bringen soll, dann muss es die Sendebestätigung der Plattform sein.

Diese Fragestellung ist noch nicht eindeutig geklärt.

## 10. Risiken und sicherer Umgang mit Zertifikaten

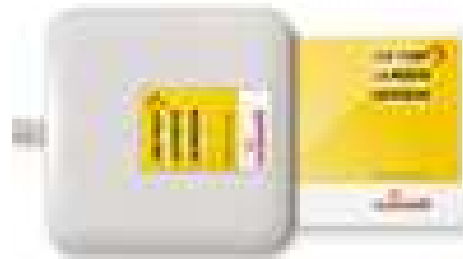
- 10.1 Der sicherste Zustand eines Zertifikats bzw. Schlüsselpaars
- 10.2 Browser und die freigeschaltete SuisselD
- 10.3 Key Katcher und Trojaner
- 10.4 Sicherere Smart-Card-Reader
- 10.5 Haftung und Verantwortung

## 10.1 Der sicherste Zustand eines Zertifikats bzw. Schlüsselpaars

Die Karte befindet sich nicht im Kartenleser



Die Karte erst einsetzen wenn das Zertifikat gebraucht wird



USB-Sticks verleiten dazu,  
dass man sie eingesetzt lässt.

## 10.2 Browser und die freigeschaltete SuisseID

- Wenn das Zertifikat mit dem Browser, zum Beispiel für die Übermittlung einer Eingabe freigeschaltete wurde, bleibt das Zertifikat offen
- Die genaue Identität aus dem Zertifikat wird jeder Webseite mitgeteilt, welche diese Abfragt. Dies geschieht unbemerkt.
- Deshalb
  - SuisseID aus dem Kartenleser nehmen
  - Browser schliessen und wieder öffnen

## 10.3 Key Katcher und Trojaner Software (Malware)

- Der PIN wird mit der Tastatur des PC eingegeben
- Es gibt Hardware, welche zwischen Tastatur und PC eingesetzt wird, die alle Tastatur-Anschläge für eine spätere Abfrage speichert. Diese speichert auch den PIN. Beispiel KeyKatcher



- Es könnte Malware (Trojaner) geben, welche den PIN abfängt und auch Dinge signiert, die sie nicht signieren wollten.



## 10.4 Sicherere Kartenleser

- Dass der PIN auf der Tastatur des PC eingegeben wird gilt als Risiko



– Kartenleser der Sicherheitsklasse 2 haben eine Tastatur für die Eingabe des PIN

- Dass das zu signierende Dokument mit dem PC angezeigt wird, gilt als Risiko



– Kartenleser der Sicherheitsklasse 3 haben zusätzlich eine Anzeige für das, was signiert werden soll

- Sicherere Kartenleser sind für die SuisseID aber noch nicht erhältlich

## 10.5.1 Haftung und Verantwortung: Wichtige Einzelheiten im Gebrauch I

- Grundlage in Art. 59a Obligationenrecht, Milde Kausalhaftung!
  - Haftung entfällt, wenn Inhaber glaubhaft darlegen kann, dass er die nach den Umständen zumutbaren und notwendigen Sicherheitsvorkehrungen getroffen hat, um Missbrauch zu verhindern
  - Art. 59a OR wurde im Rahmen des ZertES geschaffen, Verweis auf Verordnung VZertES
- Wichtigste Pflichten des Inhabers (Art. 11 VZertES)
  - Signaturerstellungseinheit (USB-Stick, Smartcard) darf keiner anderen Person anvertraut werden, wegschliessen oder auf sich tragen!
  - Sofortige Revokationspflicht bei Verlust oder Diebstahl bzw. Verdacht diesbezüglich

## 11.2 Haftung und Verantwortung: Wichtige Einzelheiten im Gebrauch II

- Wichtigste Pflichten des Inhabers (Art. 11 VzertES),  
Fortsetzung
  - Aktivierungsdaten dürfen sich nicht auf die persönlichen Daten des Inhabers beziehen;
  - Was heisst das im Detail? (Namen oder andere Identifikationsmerkmale von Ehepartnern, Kindern, Tieren, Wohnort, Adresse etc.);
  - Aktivierungsdaten sind sicher und getrennt von der Signaturerstellungseinheit (USB-Stick, Smartcard) aufzubewahren;
  - Inhaber hat Aktivierungsdaten zu ändern, wenn Verdacht besteht, dass Dritte Kenntnis von den Aktivierungsdaten genommen hat.

## 11.3 Haftung und Verantwortung: Offene Fragen III

Erlassform Verordnung, Praktikabilität:

- Im ursprünglichen Gesetzesentwurf war noch enthalten, dass der Inhaber seine Sorgfaltspflichten zu beweisen habe!
- Ist es richtig und kann es sein, dass die detaillierten Sorgfaltspflichten zum Erbringen des Entlastungsbeweises auf Verordnungsstufe von heute auf morgen dekretiert werden können.
- Botschaft ZertES: Es ist nichts dagegen einzuwenden, dass mit Wissen und Einverständnis an Dritte weitergeben werden dürfen; allerdings nach heutiger VO stellt dies eine Sorgfaltspflichtsverletzung dar!!!
- Was passiert bei einer Verschärfung der Vorschriften der VO
- Sind die Verhaltensvorschriften der VO abschliessend?
- Vorkehrungen auf Infrastruktur und Betriebsebene gegen Viren, Trojaner und andere Malsoftware
- Etc.?, werfe ich einem Haftungsfall die Signatureinheit am Besten weg?

## 12. Offene Fragen, Zukunft

- Andere Länder
- Ausblick / Zukunft
  - Zustellung von Dokumenten an Privatpersonen
  - Massenbriefe
  - Zustimmung zum elektronischem Geschäftsverkehr inkl. Zulässigkeit der elektronischen Unterschrift via AGB's (va. Mietrecht, Arbeitsrecht aber auch Versicherungsrecht, etc.)
  - Elektronische Unterschriften bei Verträgen und als prov. Rechtsöffnungstitel (z.B. Mietverträge)?