DFN
Deutsches Forschungsnetz

Zeitstempel für digitale Dokumente

Ein neuer Dienst in der DFN-PKI

DFN-Betriebstagung

26. Februar 2008

Gerti Foest (pki@dfn.de)

Was ist ein Zeitstempel?

„**Zeitstempel sind** gemäß [ISO18014-1] **digitale Daten**, **mit denen die Existenz bestimmter Daten vor einem bestimmten Zeitpunkt bewiesen werden kann.**

Häufig, wie z.B. beim Time Stamp Protocol aus [RFC3161], **werden Zeitstempel unter Einsatz digitaler Signaturen erstellt.** Somit sind Zeitstempel elektronische Bescheinigung darüber, dass die mit dem Zeitstempel signierten Daten zum Zeitpunkt der Signatur in der signierten Form vorgelegen haben. …“

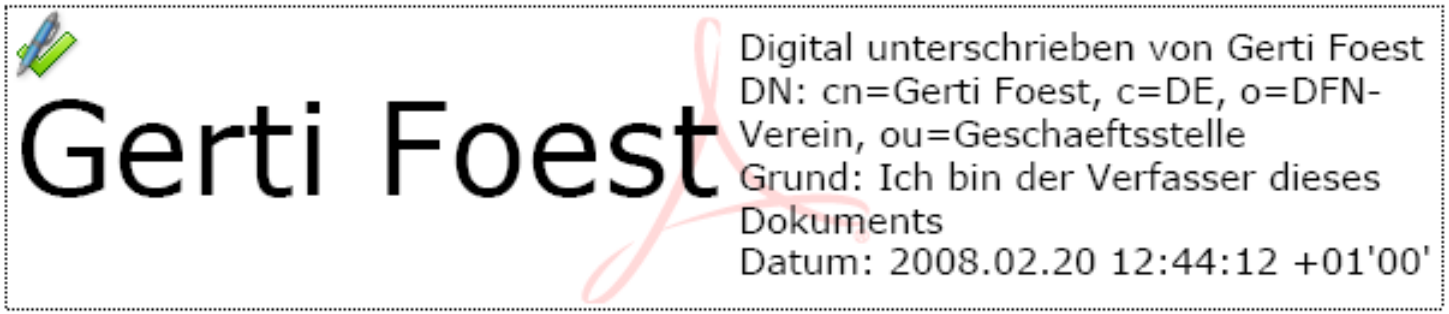
(http://www.bsi.bund.de/esig/glossar.htm)

Warum Zeitstempel?

- Nachweis, dass ein Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form vorhanden war
- Interessant / wichtig für
  - Dokumente mit Fristen, Preisen etc.
  - Prüfungsanmeldungen
  - Zertifikatsperrlisten
  - Programmcodes

Digitale Signatur und Zeitstempel (1)

- Verwendung oft in Zusammenhang mit digitaler Signatur (Zertifikat)
- Mit der digitalen Signatur wird ein Dokument digital „beglaubigt“
- Signatur kann Zeitangabe enthalten (z.B Adobe Acrobat)



Digitale Signatur und Zeitstempel (2)

- Zeitangabe in Adobe Acrobat wird vom Rechner übernommen, sie kann also beliebig verständert werden

  => nicht unbedingt vertrauenswürdig

- Gesucht:

  Vertrauenswürdige Instanz, die eine Zeitangabe durch digitale Signatur bestätigt

Zeitstempeldienst

- Ein **Zeitstempeldienst** erstellt mit Hilfe eines Zeitstempelservers
  - **vertrauenswürdige Zeitstempel**
  - nicht zwingend in Zusammenhang mit digitaler Signatur

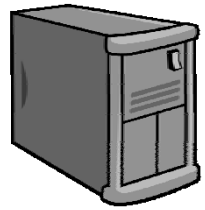
- **Wie funktioniert‘s?**
  - Anwendung schickt Hashwert des Dokuments (+ Nonce) an einen Zeitstempelserver
  - Server ermittelt die aktuelle Zeit (z.B. von Funkuhr)
  - Zeitangabe und Hashwert des Dokuments werden mit Zertifikat des Zeitservers signiert und an die Anwendung zurück gesendet
  - Austausch der Daten nach RFC 3161 (Time Stamp Protocol – TSP)

Funktionsweise Zeitstempeldienst

Ausgangsdokument

Genaue Uhrzeit
(z.B. Funkzeit)

Timestamp-Query
- Hashwert des Dokuments
- Nonce http://de.wikipedia.org/wiki/Nonce



Zeitstempelserver

Timestamp-Response
- Datum, Seriennummer...
- **Signatur**

PKCS#7
Dokument
Signatur

Attribut **timeStampToken**

Privater Schlüssel
für Signatur

DFN Zeitstempeldienst

- **Zeitstempelserver** bei der **DFN-PCA** in Hamburg
- Funktionsweise wie beschrieben
- Ermittlung der aktuellen Zeit über Funkuhr (EMC Professional Net / DCF77)
- Zeitangabe und Hashwert des Dokuments werden mit dem Zertifikat des DFN Zeitstempelservers signiert
  - Zertifikat der DFN-PKI Global Services CA

Nutzung DFN Zeitstempeldienst

- Ab sofort **Pilotbetrieb**
  - keine Formulare, keine Anmeldung, keine Policy
- **Jeder** kann den Dienstes **mit einer geeigneten Anwendung** nutzen
- Geeignete Anwendung
  - Anwendung, die Anfrage an einen Zeitserver stellen und dessen Antwort entgegen nehmen kann, z.B. Adobe Acrobat, OpenTSA, etc.
- Voraussichtlich häufigste Anwendung
  - Signatur mit Zeitstempel in Adobe Acrobat

Zeitstempel in Adobe Acrobat

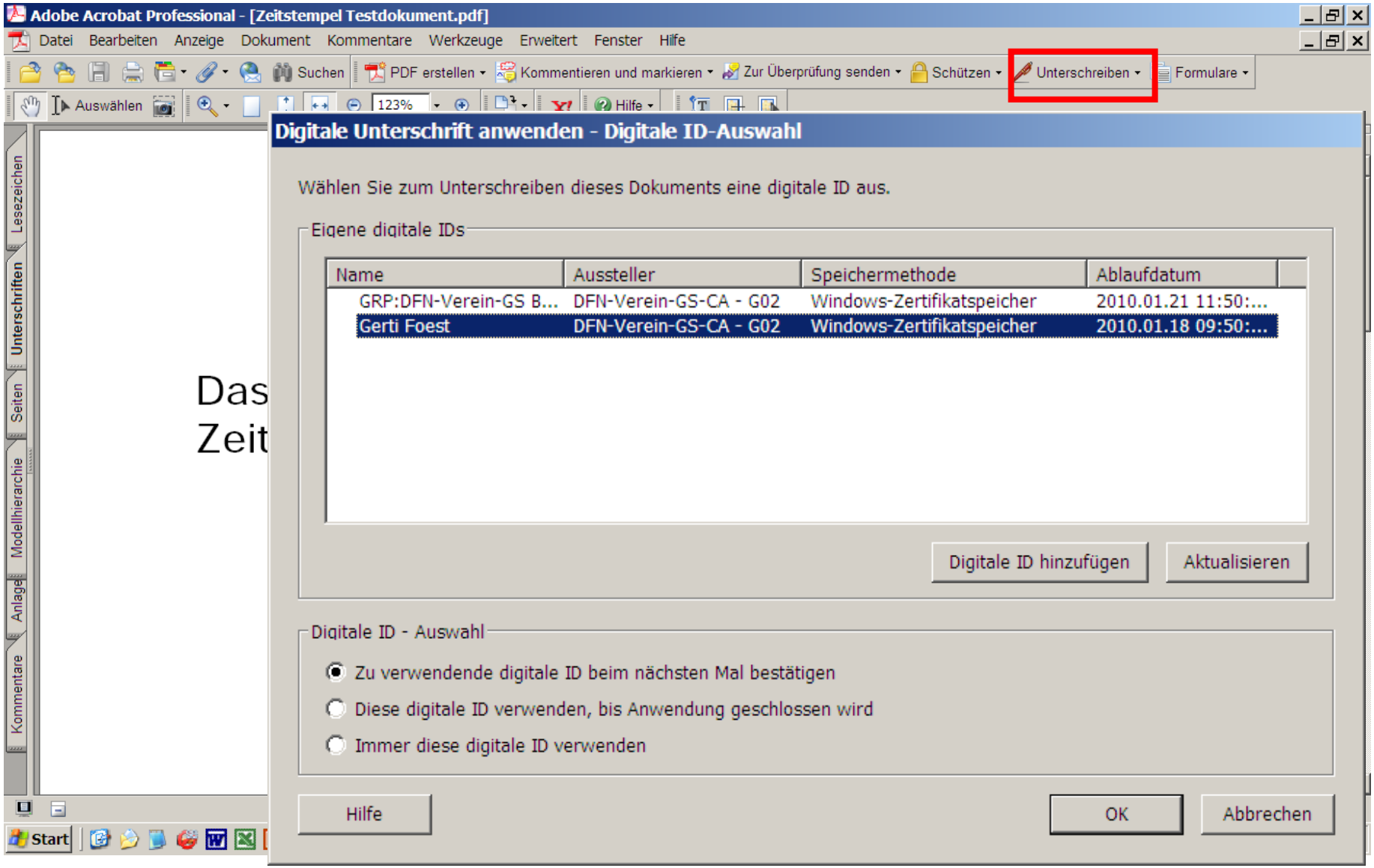
Grundsätzliches

- Bei Adobe ist der Zeitstempel immer mit einer digitalen Unterschrift verbunden
- Unterschreiben eines Dokuments mit Adobe Standard oder Professional
- Prüfen einer Unterschrift auch mit Acrobat Reader möglich
- Unterschiede bei Adobe 7 und 8 (z.B. Einstellungen, Text in Anzeigen)
- In den folgenden Beispielen:
  - Unterschrift erzeugt mit Adobe 7 Professional
  - Unterschrift geprüft mit Adobe 8 Reader

Beispiel 1

Signiertes PDF-Dokument mit Zeitstempel des lokalen Rechners

Dokument unterschreiben

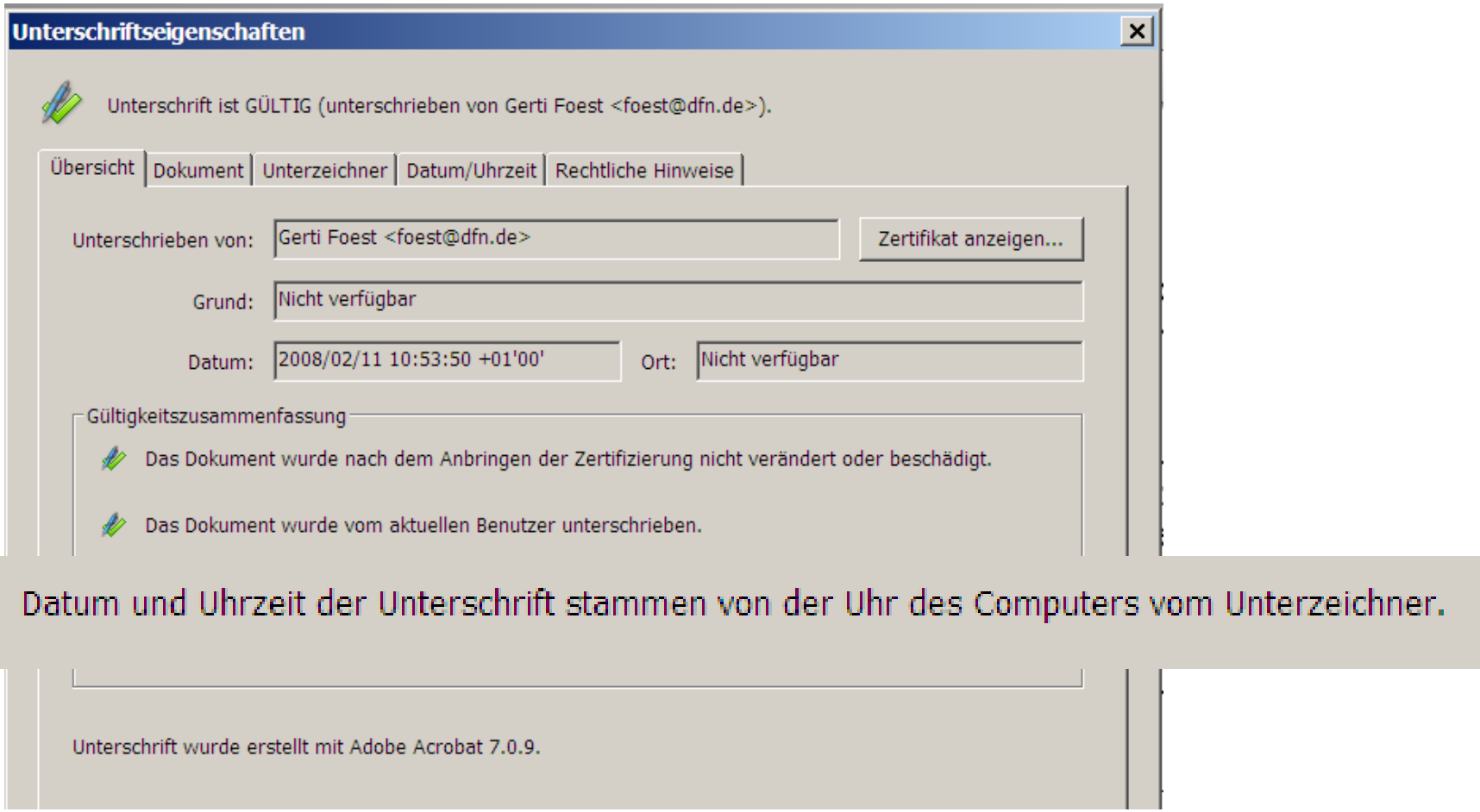


Signatur mit Rechner-Zeitstempel

- Bei Signatur eines Dokuments wird die Zeitangabe standardmäßig vom lokalen Rechner ermittelt
  - Herkunft des Zeitstempels nicht sofort sichtbar

Signatur prüfen (1)

- Empfänger prüft Signatur und wird gewarnt

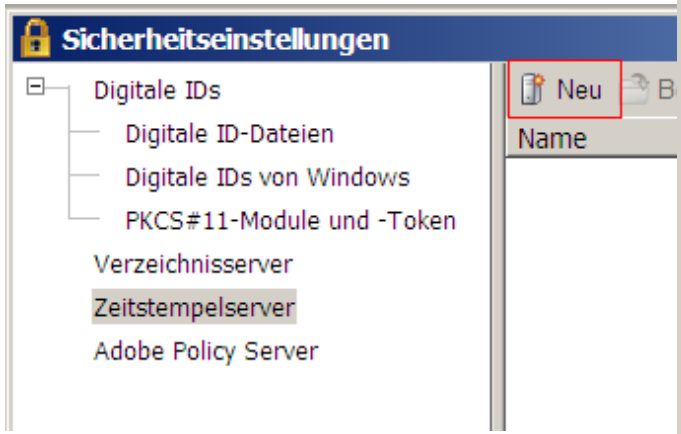


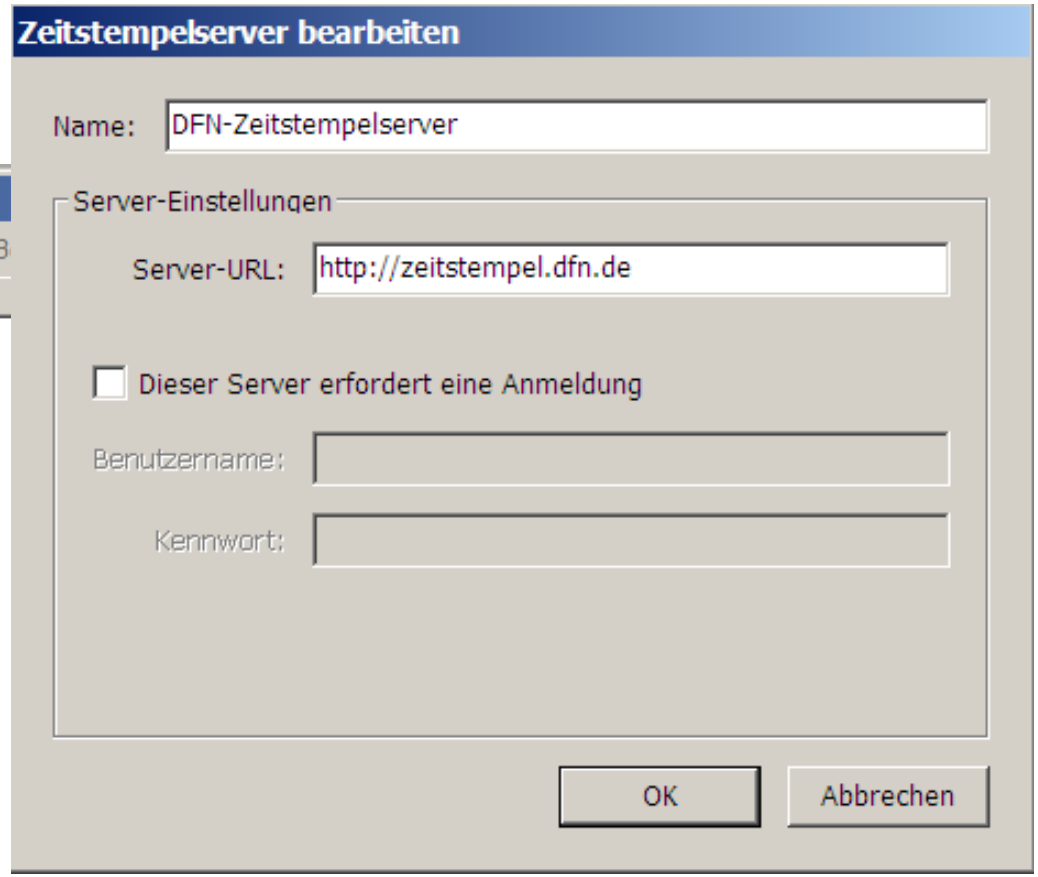
Beispiel 2

Signiertes PDF-Dokument mit DFN Zeitstempel

DFN Zeitstempeldienst einstellen (1)

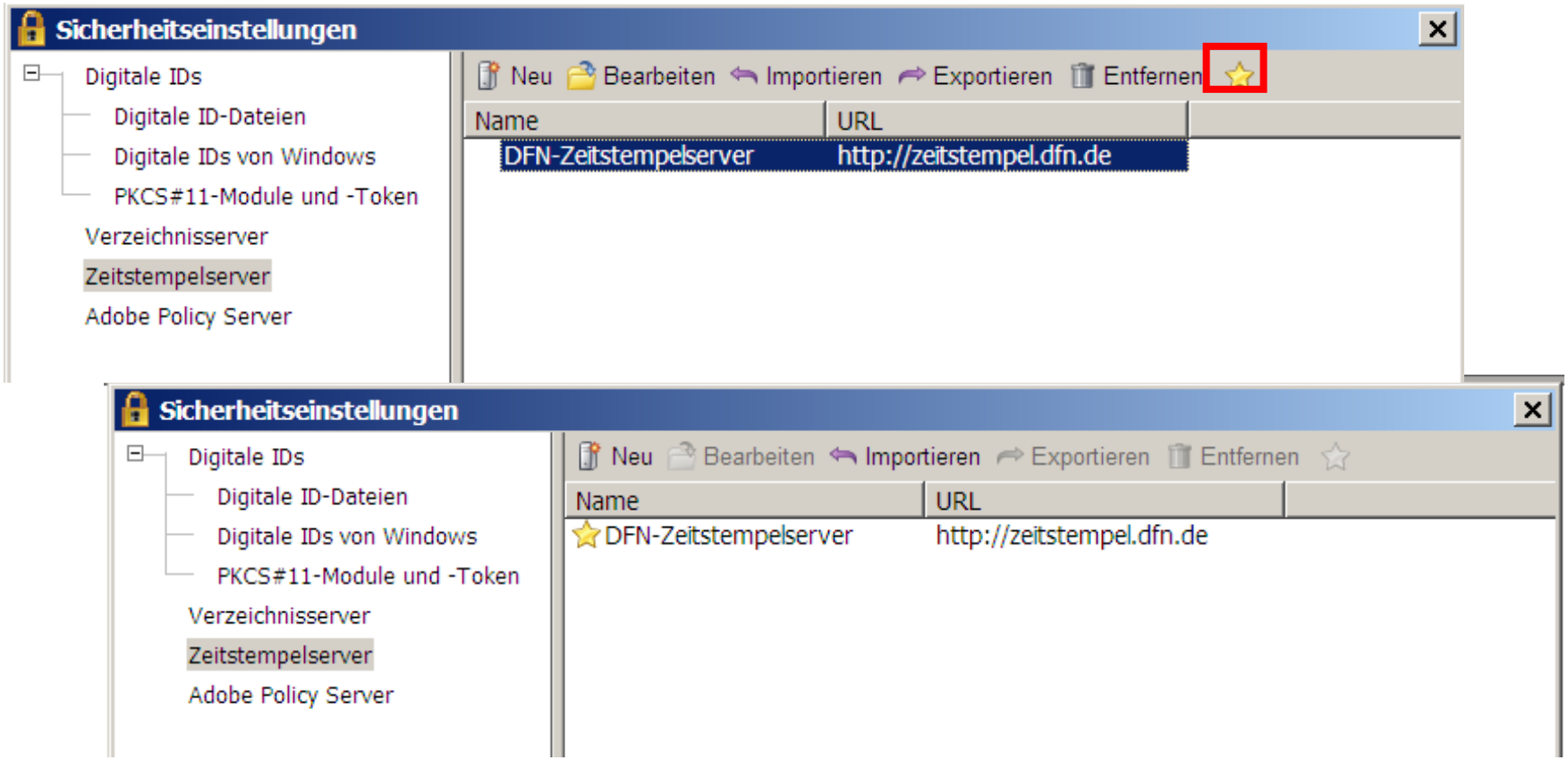
- Externer Zeitstempeldienst kann unter “Sicherheitseinstellungen” konfiguriert werden





DFN Zeitstempeldienst einstellen (2)

- DFN Zeitstempeldienst zum Standard erklären

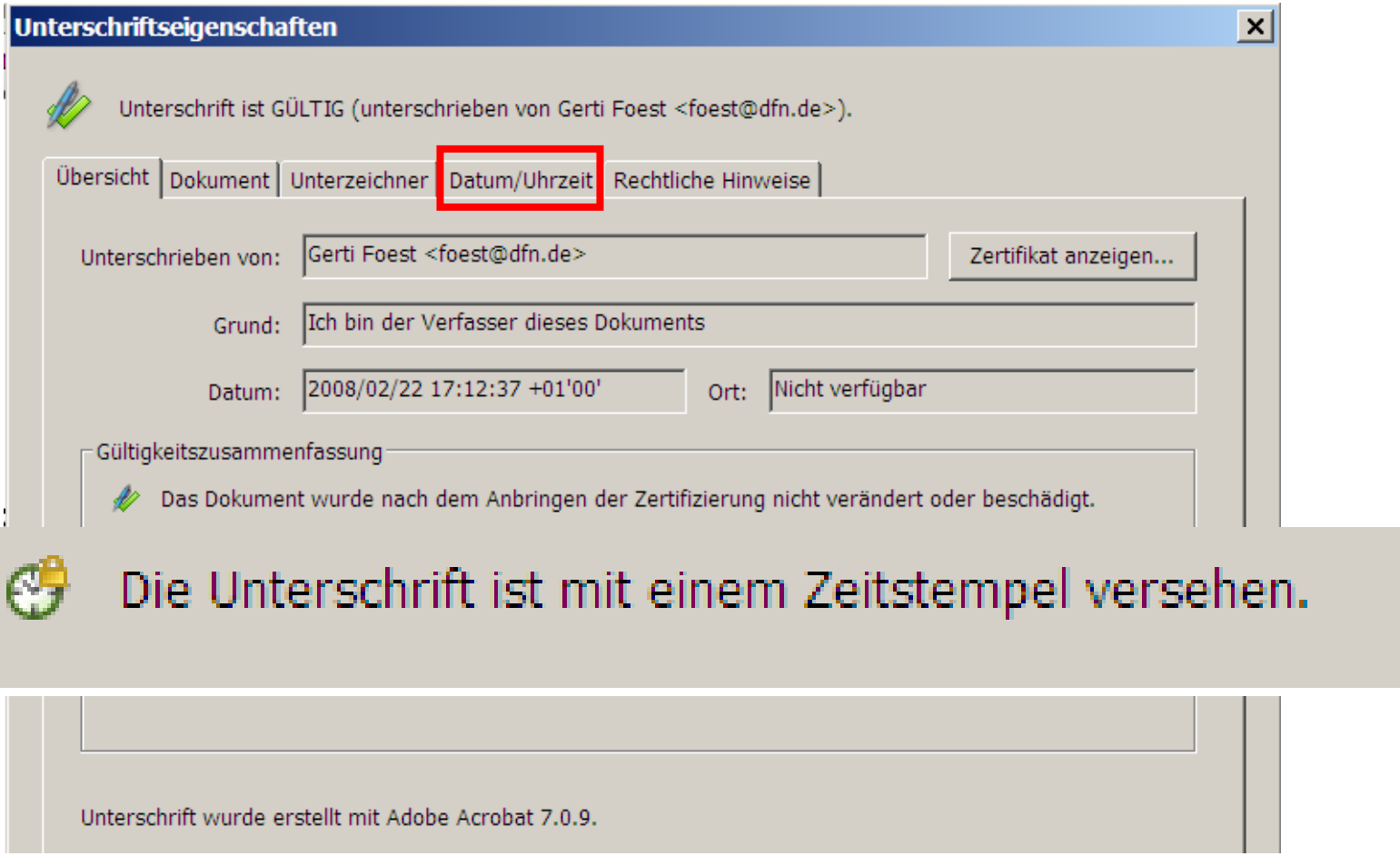


Signatur mit DFN Zeitstempel

- Der DFN Zeitstempeldienst wird nun beim Unterschreiben (Beispiel 1) automatisch kontaktiert
  - Herkunft des Zeitstempels nicht sofort sichtbar

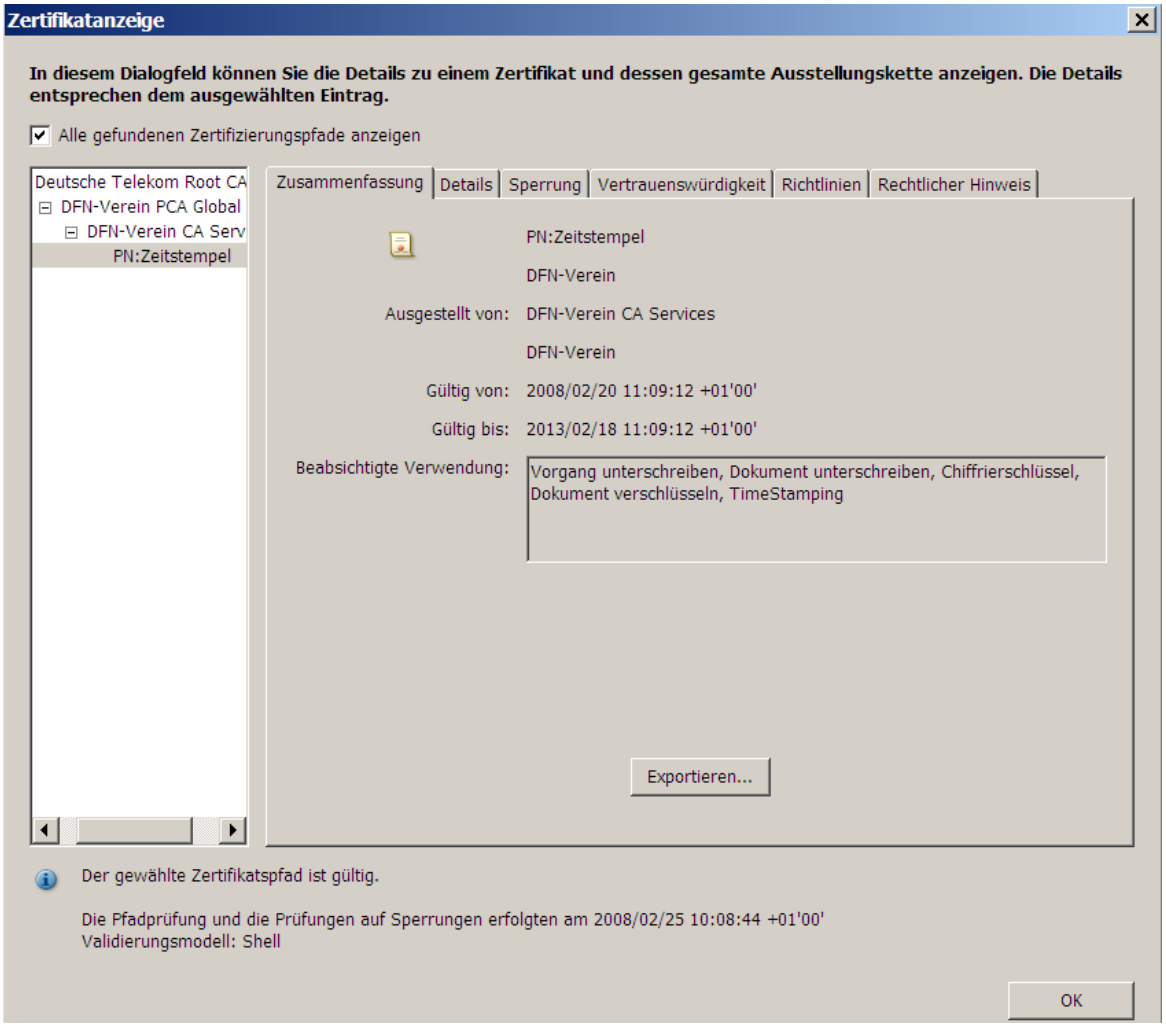
Signatur prüfen (2)

- Empfänger prüft Signatur – Zeitstempelzertifikat ist vertrauenswürdig



Zeitstempel Zertifikat

- Zertifikat des Zeitstempelservers mit Zertifikatkette



Es funktioniert, aber ...

- Mehr "Klicks"/Einstellungen als gezeigt nötig
- Zertifikate aus Global Hierarchie
  - Windows Zertifikatspeicher muss explizit eingeschaltet werden
- Zertifikat des Zeitservers
  - Zertfikatkette wird von Adobe Acrobat nicht erkannt
  - Zertifikat der Global Services CA muss explizit in den Windows Zertifikatspeicher importiert werden
- In Adobe Acrobat 7 noch Übersetzungsfehler (in Version 8 behoben)
  - „Dokument wurde verändert…“ statt
  - „Dokument wurde **nicht** verändert…“

Weitere Anwendungen

OpenTSA und Code Signing

DFN Deutsches Forschungsnetz

- **OpenTSA**
  - Zeitstempel-Client als Erweiterung für OpenSSL
  - Anfragen und Antworten können einzeln als Dateien erzeugt und bezogen werden
  - Open Source-Projekt, Näheres unter http://www.opentsa.org

- Code Signing
  - **signtool** aus dem Microsoft Software Development Kit
  - **jarsigner** aus dem Java Development Kit

Zusammenfassung

- DFN Zeitstempelserver im Pilotbetrieb
- Nutzung (Pilotbetrieb) ohne Anmeldung und Formulare
- Anwendung in erster Linie bei Signatur von PDF-Dokumenten (Adobe Acrobat)
- Weitere Anwendungen möglich (OpenTSA, signtool, jarsign)

Technische Details im Forum Sicherheit!

Informationen und Kontakt

DFN Deutsches Forschungsnetz

Informationen zum Zeitstempeldienst

- ✓ www.pki.dfn.de/zeitstempel
  (mit URL des Zeitstempelservers)

Fragen u. Antworten zum Zeitstempeldienst

- ✓ www.pki.dfn.de/faq-zeitstempel

Kontakt

- ✓ E-Mail: pki@dfn.de