Elektronische Signaturen in PDF/A: Konzept, Einsatz und technische Interoperabilität

OPENLiMiT SignCubes GmbH, Berlin

Armin Lunkeit
Geschäftsführer

PDF/A Competence Center

www.pdfa.org

PDF/A und elektronische Signatur

- Warum elektronische Signatur?
  - Was leistet die elektronische Signatur?
- Konzept der elektronischen Signatur
  - Technische Grundlagen
  - Formate
  - Wie kommt die Signatur in das Dokument?
  - Generierung des Urheberschaftsnachweises
- Interoperabilität
  - Welche Ansätze für interoperable Systeme existieren?
  - Interoperable PDF-Signaturen
- Rechtliche Aspekte
  - Welche Rolle spielt die europäische Richtlinie
  - Was kennzeichnet eine qualifizierte Signatur?
- Typische Anwendungsszenarien

Open Limit
Armin Lunkeit
Geschäftsführer

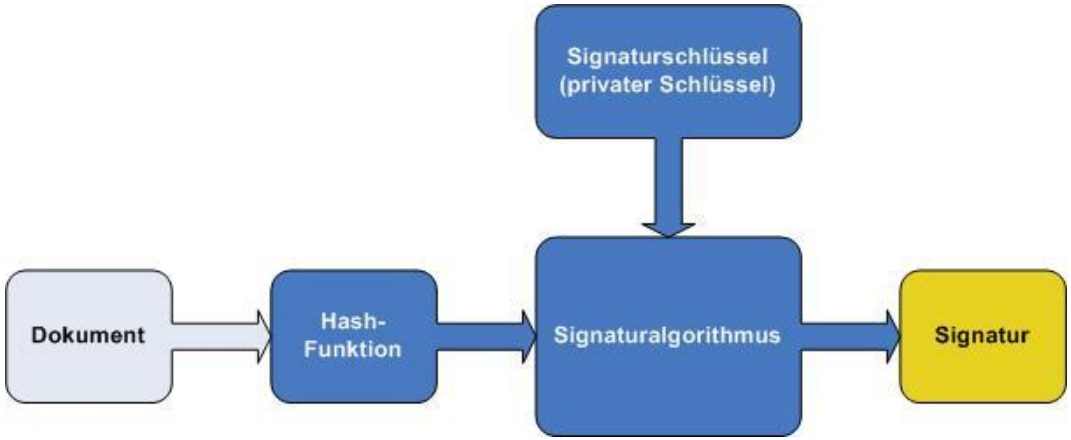
Warum elektronische Signatur?

- **Sicherstellung der Integrität**
  - **Nachweis, dass ein Dokument nicht verändert wurde**
- **Nachweis der Urheberschaft**
  - **In elektronischen (Geschäfts-)prozessen**
- **Beweiswirkung**
  - **Elektronische Unterschriften können die handschriftliche Unterschrift ersetzen**
  - **Nachweis der Urheberschaft bei geeigneten Rahmenbedingungen**

Open Limit
Armin Lunkeit
Geschäftsführer

Konzept der elektronischen Signatur - 1

- **Public Key Algorithmen bilden die technische Grundlage**
  - **Grundlage: Einwegfunktionen (Hashfunktionen) in Verbindung mit asymmetrischen Verfahren**
  - **Verwendung Öffentlicher und Privater Schlüssel**
  - **Bekannte Verfahren:**
    - RSA Signaturen mit SHA Hashwerten
    - ECDSA Signaturen mit SHA Hashwerten



Open Limit
Armin Lunkeit
Geschäftsführer

Konzept der elektronischen Signatur - 2

- **Verschiedene Formate**
  - **„Verbundene Signatur"**
  - **„Abgesetzte Signatur"**
  - **„Eingebettete Signatur (PDF)"**
    - Unsichtbare Signatur
    - Sichtbare Signaturen
  - **Gemeinsamkeit: PKCS#7 Format**
- **Allgemein**
  - **Verbundene und abgesetzte Signaturen sind für alle binären Formate geeignet**
  - **Eingebettete Signaturen liefern Verbindung aus Dokument und Sicherheitsmerkmalen**
  - **Erste Spezifikation in PDF Reference 2nd Edition (PDF 1.3)**
  - **Technische Systeme zur Signaturerzeugung sind identisch**

Open Limit
Armin Lunkeit
Geschäftsführer

Konzept der elektronischen Signatur - 3

- **Wie kommt die elektronische Signatur in das Dokument?**
  - **Anlegen eines neuen Signaturobjektes im PDF Dokument mit optionalen grafischen Elementen (Signature Appearance)**
  - **Verweis auf das Objekt über Formularfeld / Root Dictionary**
  - **Berechnung des Hash-Werts**
  - **Berechnung der Signatur**
  - **Kodierung der Signatur als Hex-String in das Dokument**
  - **Signatur ist ein Fortschreibung des Dokuments!**
- **Mögliche Signaturformate**
  - **PKCS#1 Signatur (rein technische Signatur)**
  - **PKCS#7 Signatur (kompletter Signaturcontainer)**

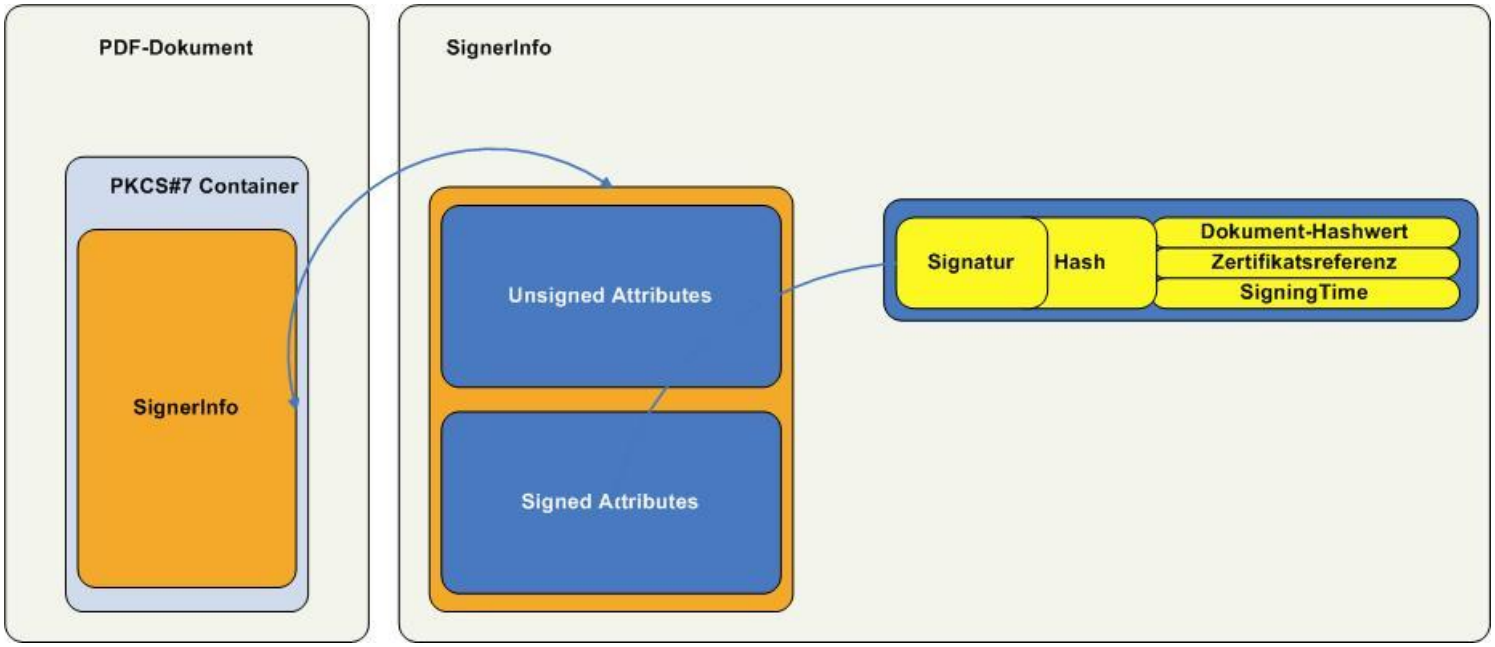
Open Limit
Armin Lunkeit
Geschäftsführer

Konzept der elektronischen Signatur - 4

- **Freiheitsgrade der elektronischen Signatur**
  - **Freie Definition von Unterschriften-Handlern**
    - Filter (Required)
  - **Verwendung zur Definition der Algorithmen und Formate, jedoch nicht zwingend**
    - SubFilter (Optional)
  - **Grafische Abbildungen innerhalb von elektronischen Signaturen möglich**
    - Appearance Stream, Verweis durch Appearance Dictionary (AP)

Open Limit
Armin Lunkeit
Geschäftsführer

Konzept der elektronischen Signatur – 5



SignedData ::= SEQUENCE {
version Version,
digestAlgorithms DigestAlgorithmIdentifiers,
contentInfo ContentInfo,
certificates
[0] IMPLICIT ExtendedCertificatesAndCertificates
OPTIONAL,
crls
[1] IMPLICIT CertificateRevocationLists OPTIONAL,
signerInfos SignerInfos }
DigestAlgorithmIdentifiers ::=
SET OF DigestAlgorithmIdentifier
SignerInfos ::= SET OF SignerInfo

Open Limit
Armin Lunkeit
Geschäftsführer

Nachweis der Urheberschaft

- **Elektronische Signatur im Dokument alleine nicht ausreichend**
  - **Kryptografische Korrektheit generiert keine Aussage zur Gültigkeit**
- **Wie wird die Urheberschaft nachgewiesen?**
  - **Aufbau der Zertifikatskette bis zum Wurzelzertifikat (Root-CA)**
  - **Validierung der Zertifikatskette ebenfalls durch Signaturen**
- **Wann ist eine Prüfung vollständig / die Signatur gültig?**
  - **Nach Prüfung der Sperrlisten liegt kein Sperreintrag vor**
  - **Alternativ: Eine OCSP Abfrage (Online Certificate Status Protocol) ergab eine positive Auskunft (Zertifikat ist bekannt und gültig)**

Open Limit
Armin Lunkeit
Geschäftsführer

Wege in die Interoperabilität -

- **Verschiedene Interoperabilitätsbemühungen**
  - **Internet Working Group**
    - Veröffentlichung entsprechender RFCs
  - **ISO Normierungen**
  - **Arbeitsgruppen zwischen Herstellern**
- **Allgemeines Testbed**
  - **Testbed von TeleTRUST e.v. und T7 e.V.**
  - **Bestandteile:**
    - Zertifikats- und Sperrlistenprofile
    - PKI Management
    - Nachrichtenformate
    - Protokolle
    - Zertifikatspfadvalidierung
    - Kryptografische Algorithmen
  - **Steht allen Herstellern als kostenfreier Service zur Verfügung**

Open Limit
Armin Lunkeit
Geschäftsführer

Einige rechtliche Aspekte

- **Europäische Richtlinie**
  - Liefert die Rahmenbedingungen zur Signaturgesetzgebung in allen EU-Mitgliedsländern – Harmonisierung innerhalb der europäischen Gesetzgebung
  - Mitgliedsländer sind verpflichtet, ein Signaturgesetz zu erlassen
  - Ziel: Definition sicherer und kostensparender Prozesse zur Stärkung der europäischen Wirtschaft
- **Nationale Gesetzgebung**
  - Beispiel Deutschland: Erste Fassung des Signaturgesetzes 1997
- **Relevante Szenarien**
  - Verwendung elektronischer Signaturen im Bereich steuerlich relevante Daten
  - Digitalisierung von Dokumenten zzgl. elektronischer Signatur
  - Anforderungen im Bereich der Langzeitarchivierung

Open Limit
Armin Lunkeit
Geschäftsführer

Was kennzeichnet eine „qualifizierte Signatur"?

- **Europäische Richtlinie**
  - Zertifikat muss auf eine sicheren Signaturerstellungseinheit gespeichert sein
  - Zertifikatsherausgeber muss durch nationale Behörde authentisiert sein
  - (Qualifizierte) Signaturen werden international akzeptiert
- **Nationale Besonderheiten**
  - Nationen implementieren unterschiedliche Zulassungsverfahren
  - Deutschland: Signaturanwendungskomponenten müssen eine Bestätigung nach dem Signaturgesetz aufweisen oder eine Herstellerbestätigung inne haben

Open Limit

Armin Lunkeit
Geschäftsführer

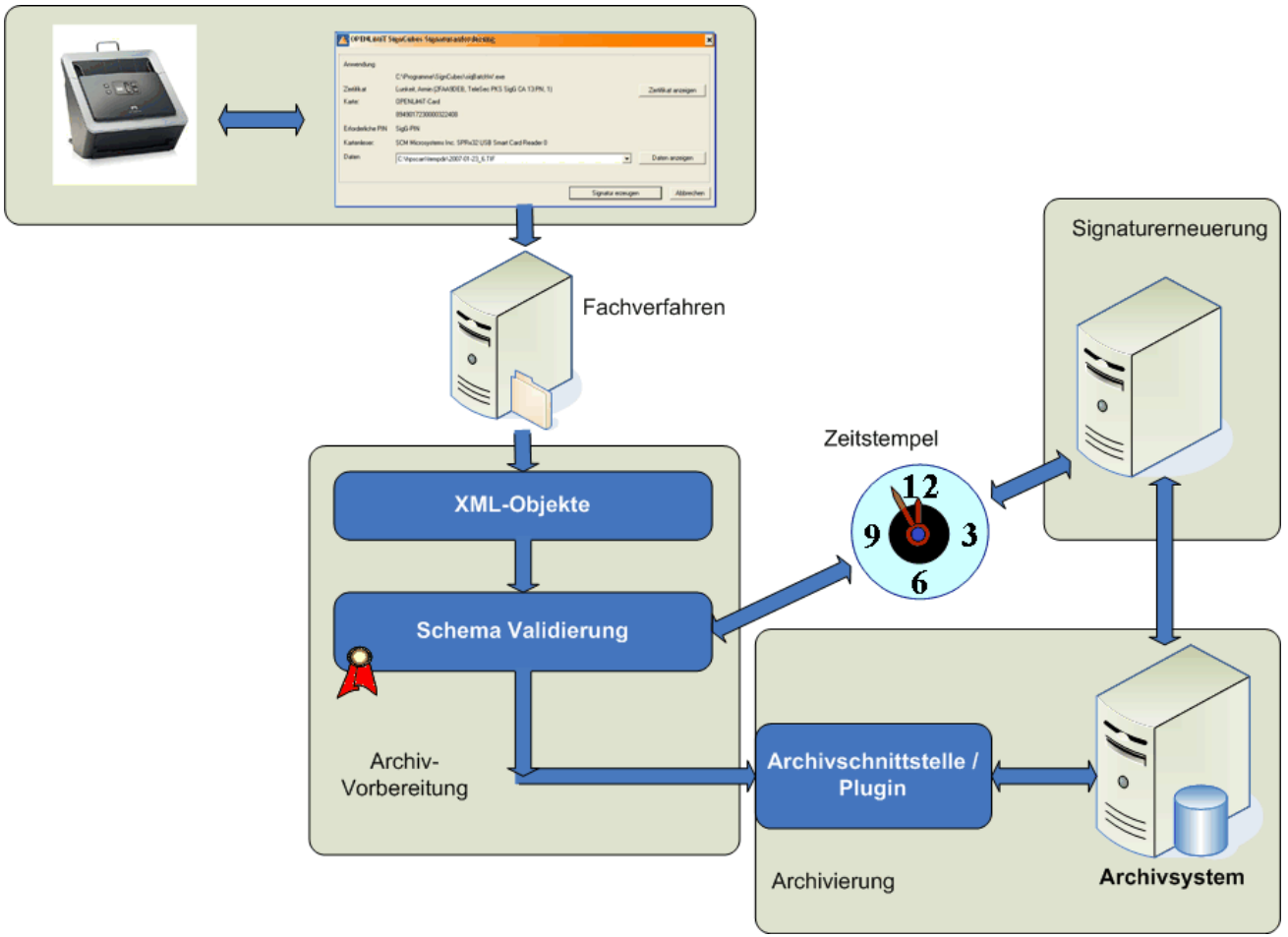
Anwendungsszenarien - 1

- **Archivierung**
  - **PDF/A liefert ISO normiertes Dokumentformat**
  - **Elektronische Signatur stellt die Dokumentintegrität sicher**
- **Elektronischer Geschäftsverkehr**
  - **Elektronisch unterzeichnete Verträge**
  - **Elektronische Arbeitsabläufe mit elektronischen Signaturen**
- **Derzeit in Diskussion**
  - **Implementierung eines einheitlichen Systems / Ansatzes zur Langzeitarchivierung**
  - **Adressierte Aufgaben:**
    - Nachsignatur / Übersignatur
    - Hash-Bäume
    - Einsatz von Zeitstempeln

Open Limit
Armin Lunkeit
Geschäftsführer

Anwendungsszenarien - Langzeitarchivierung

ArchiSafe-Konzept für die Langzeitarchivierung



Armin Lunkeit
Geschäftsführer

Vielen Dank!

OPENLiMiT SignCubes GmbH

http://www.openlimit.com

Armin Lunkeit
Geschäftsführer