

# Aufbewahrung elektronischer und elektronisch signierter Dokumente



© secrept GmbH 2009  
Seite 1

Xinnovations, Berlin

„Archivierung elektronisch unterschriebener Dokumente“

Enrico Entschew, secrept GmbH  
Berlin, 15.09.2009

# Unternehmensprofil

© secrypt GmbH 2009  
Seite 2



Die secrypt GmbH ist spezialisiert auf Lösungen zur Optimierung, Beschleunigung und Sicherung digitaler Geschäftsprozesse mit gesetzeskonformer elektronischer Signatur, Zeitstempel und Verschlüsselung und sorgt so für Authentizität, Manipulationsschutz und Vertraulichkeit von sensiblen elektronischen Daten.

Add-on:

Beweisbar rechtsverbindlicher Ausdruck elektronisch signierter Dokumente auf Papier mittels leistungsstarker 2D-Barcode-Technologie.

Sitz:

Berlin, Deutschland



# Themen



- Aufbewahrungsziele
- Rechtliche Rahmenbedingungen
- Technische Rahmenbedingungen / Aufbau elektronisch signierter Dokumente
- Methode zur Beweiswerterhaltung

# Warum wird archiviert?



## Aufbewahrung

- **... als Gedächtnisstütze und Kommunikationshilfe**

Medizinische Dokumentation nach der ärztlichen Berufsordnung, Verwaltung:  
i.d.R. 10 Jahre nach Abschluss der Verwaltungsverfahrens, ggf. deutlich  
länger (Baugenehmigung)

- **... zur prozessualen Beweissicherung**

Zivilrechtliche Ansprüche § 195 BGB : 3 Jahre; § 197 ff BGB (dingliche  
Ansprüche, Schadensersatz etc.): 30 Jahre

Recht, Berechtigung, Status: Aufbewahrung solange der Zustand besteht  
(Grundstückseigentum)

# Warum wird archiviert?



## Aufbewahrung

- **... zum Zweck der Kontrolle und Rechenschaft**

Handels- und Steuerrecht (GoB, GoBS, HGB, AO), Nachvollziehbarkeit und Kontinuität verwaltungsrechtlichen Handelns

- **... für die Nachwelt**

Archivgesetz (BArchG): Dokumente werden auf Grund ihres besonderen inhaltlichen Wertes archiviert.

- Ohne Signatur: Verfahrensanweisungen, Testfälle und Programmdokumentationen, die die Ordnungsmäßigkeit des elektronischen Archivs nachweisen können

→ Dokumente erbringen nicht aus sich heraus den Beweis ihrer Echtheit !

# Anforderungen an die (papiergebundene) Aufbewahrung



Ziel: Für eine bestimmte Dauer die Rechtmäßigkeit vorgenommener Handlungen oder Unterlassungen nachzuweisen und ihre Nachvollziehbarkeit und Kontinuität zu gewährleisten:

- Unterlagen müssen für die erforderliche Dauer vollständig, jederzeit verfügbar, lesbar und fälschungssicher bleiben
- -> Elektronische Dokumente müssen den gleichen rechtlichen Grundsätzen folgen

Dabei gilt:

- Aufbewahrung = Obliegenheit (eigenes Interesse) -> Anspruchsbegründung
- Aufbewahrung = Rechtspflicht -> evtl. Beweislastumkehr

# Rechtliche Anerkennung elektronisch gespeicherter Dokumente?



Einzug der elektronischen Dokumente (mit qualifizierter elektronischer Signatur) in:

- § § 128 III und 126a BGB (Schriftform)
- § 3a Verwaltungsverfahrensgesetz (Elektronischer Verwaltungsakt)
- § 87a Abgabenordnung (Schriftform)
- § 36a SGB I (Schriftform)

Transformationen in elektronische Dokumente (Beglaubigung)

- § § 39a, 42 BeurkG
- § 33 VwVfG

Beweiserleichterung in § 371a ZPO



# Rechtliche Grundlagen der Aufbewahrung



## Gesetzliche Grundlagen:

- § § 140 ff Abgabenordnung (AO)/GDPdU: Steuerrelevante Unterlagen
- § 257 IV Handelsgesetzbuch (HGB)/GoBS: Kaufmännische Unterlagen
- § 14b Umsatzsteuergesetz (UStG): Rechnungen
- § 9 Geldwäschegesetz (GwG) Aufbewahrung der Identifizierungsdaten



# Rechtliche Grundlagen der Aufbewahrung



## Weitere Grundlagen:

- Grundsätzliche Zulassung der elektronischen Form
- Einbeziehung elektronischer Signaturen nach Signaturgesetz (Authentizität und Integrität)
- Beweisrechtliche Privilegierung elektronisch signierter Dokumente
- Fachspezifische Aufbewahrungsvorschriften (Verwaltung, Medizin, Handels- und Steuerrecht)
- Verwaltung: Aktenordnung; Aktenpläne, GGO (Gemeinsame Geschäftsordnung der Bundesministerien), § § 110 a-d SGB IV (Sozialversicherungsrecht), Justizkommunikationsgesetz

# Gesetzliche Grundlagen der elektronischen Signatur in der EU und Deutschland



Europäische Ebene:

EU-Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

Nationale Ebene:

Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG - Signaturgesetz) vom 16.05.2001 (letzte Änderung 26.02.2007)

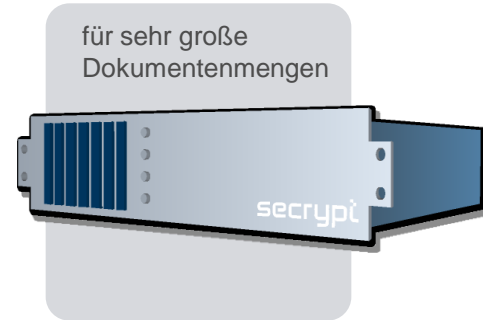
Verordnung zur elektronischen Signatur (SigV – Signaturverordnung) vom 16.11.2001 (letzte Änderung 16.11.2007)

*Der Einsatz der qualifizierten elektronischen Signatur wird in diversen weiteren Gesetzen und Ausführungsbestimmungen, wie z.B. BGB, ZPO, VwVfG konkretisiert.*

# Benötigte Komponenten zum Signieren

## Komponenten

- Signatursoftware
- (Mehrfach-) Signaturkarte mit „qualifiziertem“ Zertifikat von D-Trust GmbH (Trustcenter)
- Kartenlesegerät



# Möglichkeiten der Signaturerzeugung

## Clientbasierte Signaturerzeugung

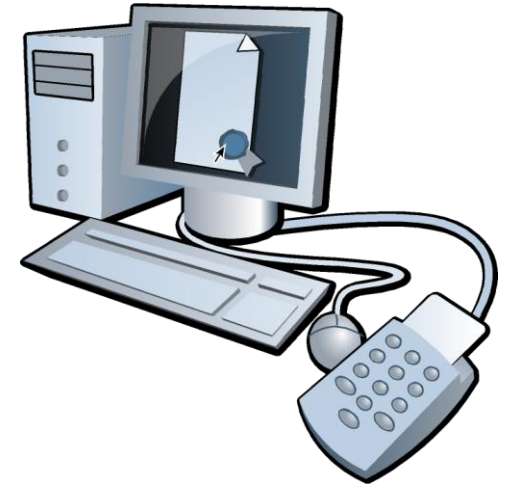
- PIN-Eingabe pro Vorgang

## Clientbasierte Signaturerzeugung (Batch-Signatur)

- Einmalige PIN-Eingabe pro Batch-Vorgang
- Massen-Signaturkarte notwendig
- Begrenzte maximale Signaturanzahl pro Batch

## Serverbasierte automatisierte Signaturerzeugung

- Freischaltung mit einmaliger PIN-Eingabe für bestimmte Anzahl von Signaturen und / oder Signaturzeitfenster
- Massen-Signaturkarte notwendig



# Grundlagen: Aufbau einer signierten Datei

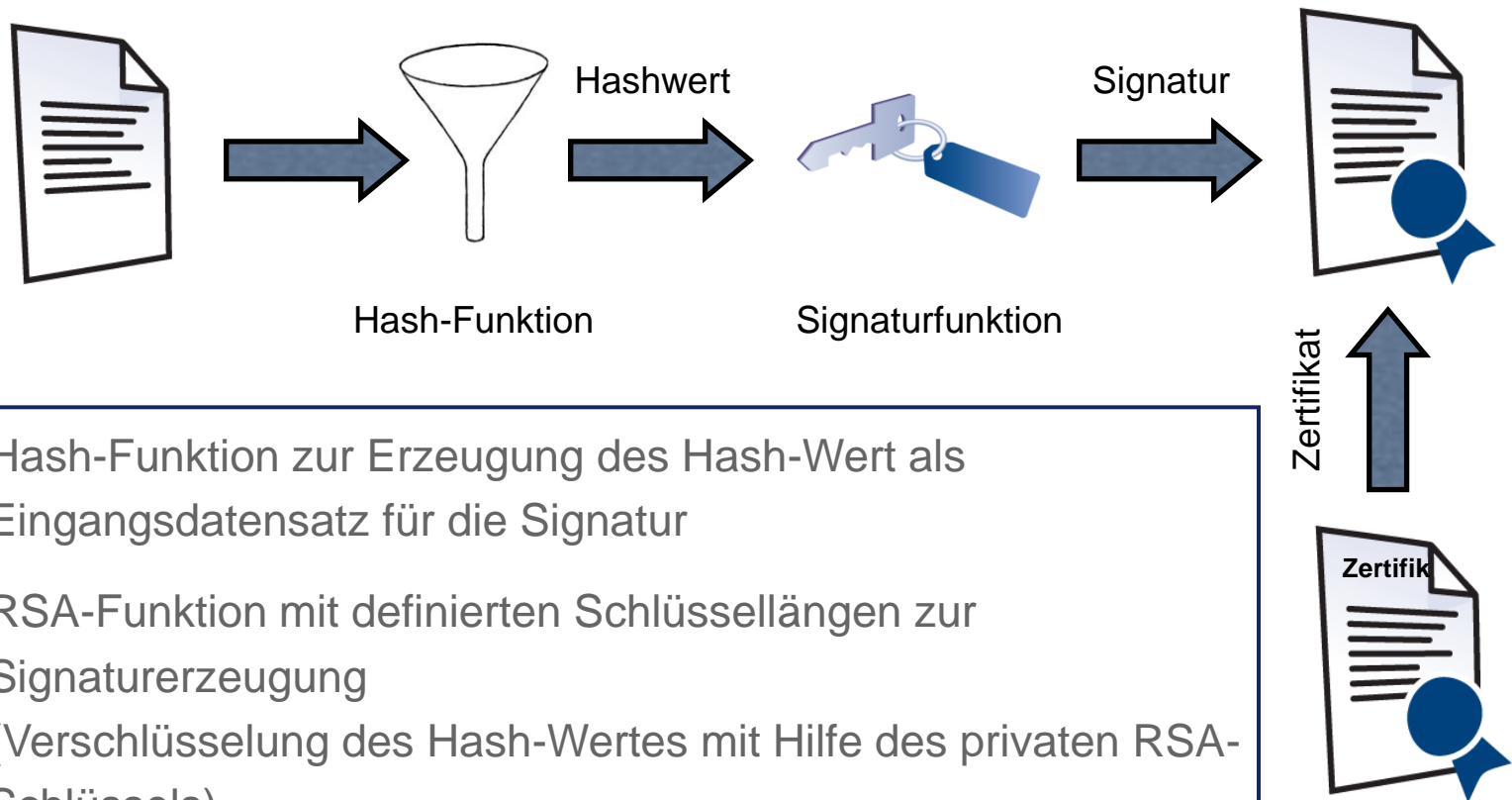


## Drei Bestandteile:

- Ursprungsdatei
- Signatur
- Zertifikat

# Grundlagen: Kryptographischen Algorithmen der Signatur

© secrypt GmbH 2009  
Seite 14





# Grundlagen: Kryptographischen Algorithmen der Signatur



## Hash-Funktionen:

- SHA-1 galt bis Ende Juni 2008
- RIPEMD-160 gilt bis Ende 2010
- SHA-224, SHA-256, SHA-384 und SHA-512 gelten bis Ende 2015

## RSA-Funktionen:

- RSA-Algorithmus mit 1024 Bit-Schlüssellänge galt bis Ende März 2008
- RSA-Algorithmus mit 1280 Bit-Schlüssellänge galt bis Ende 2008
- RSA-Algorithmus mit 1536 Bit-Schlüssellänge gilt bis Ende 2009
- RSA-Algorithmus mit 1728 Bit-Schlüssellänge gilt bis Ende 2010
- RSA-Algorithmus mit 1976 und 2048 Bit-Schlüssellänge gelten bis Ende 2015



# Wird die Signatur ungültig?



# NEIN!

## ABER:

- Die Stärke der kryptographischen Algorithmen nimmt im Zeitverlauf aufgrund des technischen Fortschritts ab

→ Der Beweiswert elektronischer Signaturen kann abnehmen!

# Wie kann der Beweiswert signierter Dokumente erhalten werden?



- Gesetzliche Regelung in Deutschland: § 17 Signaturverordnung (SigV)
- Um den Beweiswert dauerhaft zu erhalten, müssen elektronische Signaturen regelmäßig mittels aktueller „geeigneter“ Algorithmen erneuert werden
- Dieser Vorgang wird als „Übersignieren“ bzw. „Nachsignieren“ bezeichnet
- Unterschiedliche Methoden möglich / Verschiedene Standards im Markt vertreten, z.B. ArchiSig, LTANS/ERS
- Allen gemeinsam → weiterhin volle Beweisführung mit § 371a ZPO

# Methoden der Beweiswerterhaltung



## **Gesetzliche Regelung in Deutschland:**

Aufbringen eines Zeitstempels über die bereits signierte Datei

## **Einfachste Methode:**

- Über jede signierte Datei wird ein Zeitstempel aufgebracht
- Pro: a) Einfache, unkomplizierte Methode für eine sehr geringe Dokumentenmenge und b) jedes Dokument ist autack
- Contra: Bei höheren Dokumentenvolumina a) sehr kostenintensiv und b) sehr zeitaufwendig (Dauer pro Dokument bis zu 3 Sekunden)

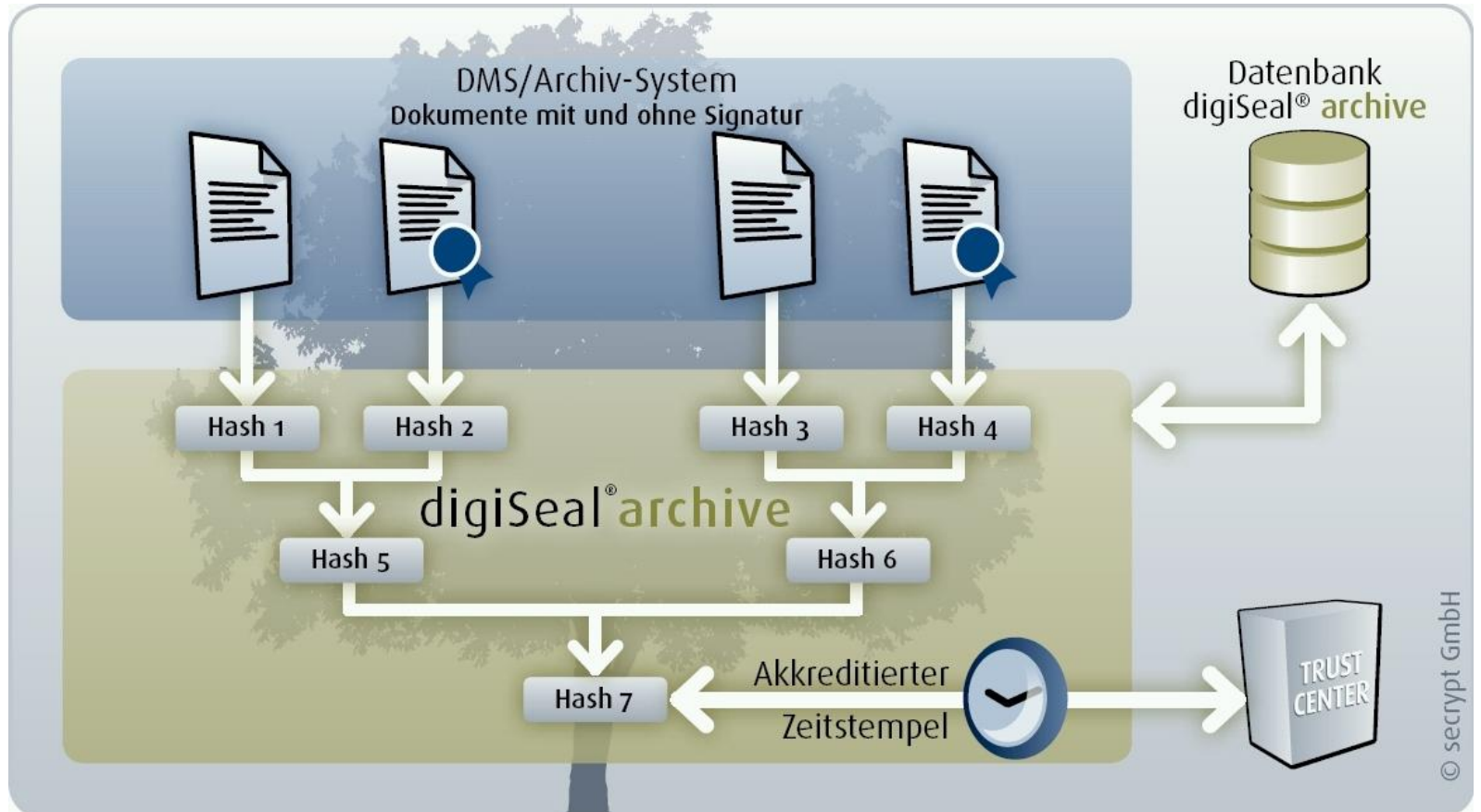
# Methoden der Beweiswerterhaltung



## ArchiSig / LTANS/ERS-Methode:

- Schnelle Verarbeitung großer Dokumentenmengen durch effizientes Hash-Baum-Verfahren:
  - Über jede signierte Datei wird ein Hash-Wert gebildet.
  - Über eine definierte Anzahl von Hash-Werten wird ein neuer Hash-Wert gebildet.
  - Dieser Hash-Wert wird mit einem Zeitstempel versehen.
- Pro: a) sehr gute Methode für mittlere und große Dokumentenmengen, b) kostengünstige Umsetzung möglich und c) internationaler Standard
- Contra: a) gewisser Mindestaufwand bei der Umsetzung und b) eignet sich nur für Empfänger, die den Standard auch beherrschen

# Methode der Beweiswerterhaltung



# Vielen Dank!



Vielen Dank für Ihre Aufmerksamkeit.  
Wir sind jederzeit gerne für Sie da.

E-Mail: [partner@secrypt.de](mailto:partner@secrypt.de)  
Tel.: +49 (30) 756 59 78-42  
Fax: +49 (30) 756 59 78-18  
Internet: [www.secrypt.de](http://www.secrypt.de)