Digitaler Beweiswert im eArchiv mit Kryptographie

conhIT-Satellitenveranstaltung 2015
von GMDS und BVMI

13.04.2015, Berlin

Tatami Michalek, Geschäftsführer secrypt GmbH

secrypt GmbH
Bessemerstr. 82
12103 Berlin
Germany

Tel.: +49 (0)30 756 59 78-0
Fax: +49 (0)30 756 59 78-18
mail@secrypt.de
www.secrypt.de

Medienhype Verschlüsselung

Digitale Transformation

Die digitale Transformation

- zunehmende Umsetzung effizienter elektronischer Geschäftsprozesse im Gesundheitswesen
- Aufbewahrung der zugehörigen Unterlagen / Patientenakten in digitaler Form

→ Vertraulichkeit, Manipulationsschutz, Urhebernachweis und der digitale Beweiswert rücken in das Zentrum der Aufmerksamkeit von IT-Strategie, Compliance und gesellschaftlichem Diskurs.

Digitaler Beweiswert

Schaffung und Erhöhung des digitalen Beweiswerts

durch eine Kombination verschiedener technischer und organisatorischer Maßnahmen, z.B.:

- Dokumentierte Prozesse
- Einsatz von „Write Once, Read Many“-Speichertechnologien (WORM)
- Haftpflichtversicherung
- …

→ Ziel: Schaffung von Fakten und Indizien, um Spielraum für freie Beweiswürdigung im Fall einer rechtliche Auseinandersetzung zu minimieren

Beweiswert mit Kryptographie

Digitale Daten per se ohne Beweiswert

- Zunächst weisen elektronische Daten aus sich heraus keine Anhaltspunkte für Integrität und Authentizität auf
- Integrität und Authentizität sind entscheidende Eigenschaften zum Beweiswert

→ Elektronische Signaturen auf Basis von State-of-the-Art-Kryptographie-Verfahren gemäß dem „Stand der Technik“ sorgen für Integrität und Authentizität

Kryptographische Werkzeuge und Algorithmen

RSA (Rivest, Shamir, Adleman)

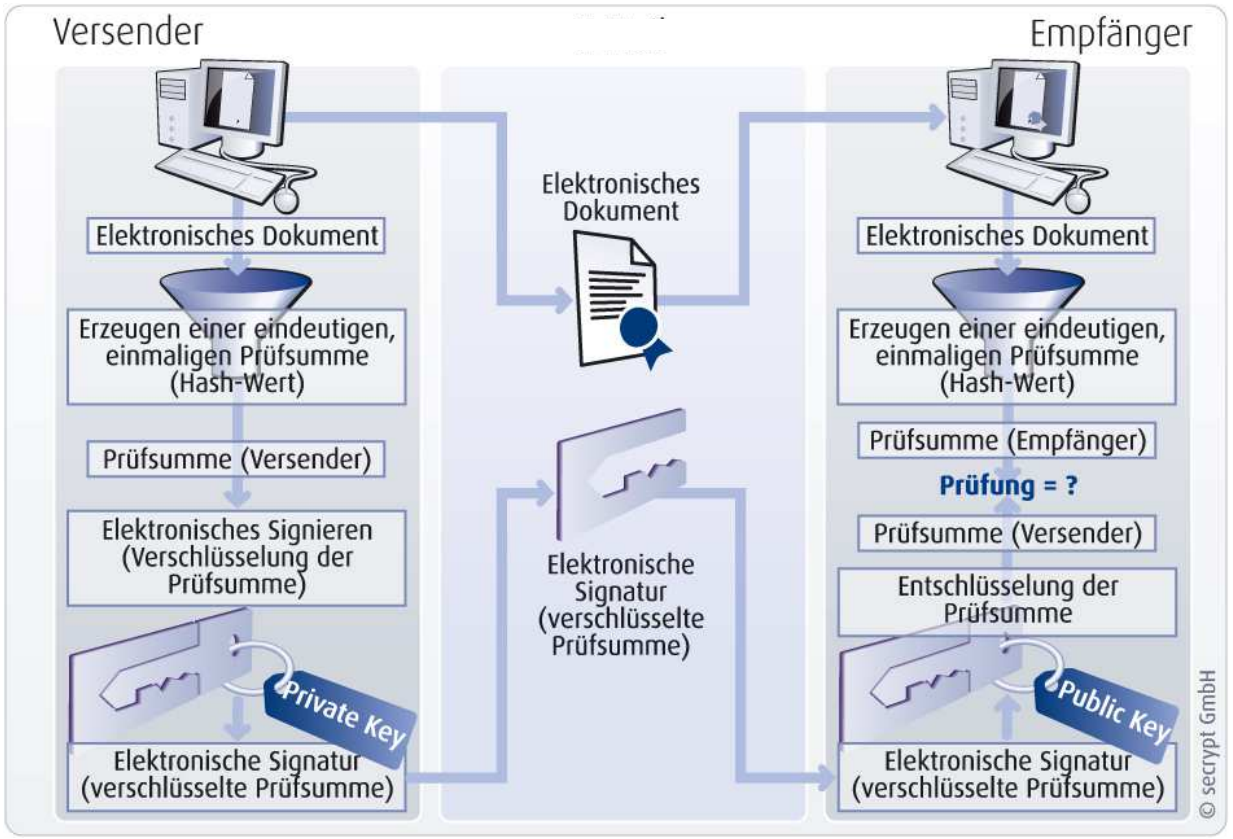
- Asymmetrisches Verfahren für Verschlüsselung und elektronische Signatur auf Basis eines geheimen privaten Schlüssels und eines öffentlichen Schlüssels
- Verwendung in SSL (Secure Socket Layer) und E-Mail-Verschlüsselung (z.B. PGP)
- Verwendung bei eSignatur in Kombination mit Hash-Algorithmus, z.B. SHA (Secure Hash Algorithm)
- Kompensierung der Verdoppelung der PC-Rechenleistung alle 2 Jahre durch Erhöhung der Schlüssellänge
- Entwicklung alternativer Verfahren, bei denen die Schlüssellänge nicht linear von der Rechenleistung abhängt → ECC (Elliptic Curve Cryptography)

Kryptographische Werkzeuge und Algorithmen

Elektronische Signatur

SHA-Algorithmus →

RSA-Algorithmus →



Wie stark sind die Verfahren?

Wie lange benötigt ein aktueller PC, um Schlüssel zu knacken?
(mit Unsicherheiten behaftete Schätzungen)

Beispiel: Intel Core i7 5960X CPU: 336.000 MIPS[1] bei 3,5 GHz (2014)

MIPS-Jahre[2], um Schlüssel zu knacken		Schlüssellänge (Bit)		Kalenderjahre
		RSA	ECC	
10^4	10.000 (10 Tausend)	512	106	0,03 (11 Tage)
10^{11}	100.000.000.000 (100 Milliarden)	1.024	160	297.619 (297 Tausend)
10^{20}	100.000.000.000.000.000.000 (100 Trillionen)	2.048	210	297.619.000.000.000 (297 Billionen)

[1]: MIPS: Million Instructions Per Second: Millionen Instruktionen pro Sekunde, eine Einheit, die die Rechenleistung eines Prozessors beschreibt

[2]: MIPS-Jahr: Rechenleistung eines heute zur Verfügung stehenden PCs, wenn er das gesamte Jahr rechnet

Quellen: Wikipedia, FH Köln, Uni Mainz

Geeignete Algorithmen und Schlüssellängen

Tabelle 1: Geeignete Hashfunktionen

geeignet bis Ende **2015**	geeignet bis Ende **2021**
SHA-224, (SHA-1, RIPEMD-160)*	SHA-256, SHA-384, SHA-512, SHA-512/256

* ausschließlich zur Prüfung qualifizierter Zertifikate, aber nicht zu deren Erstellung oder zur Erzeugung und Prüfung anderer qualifiziert signierter Daten.

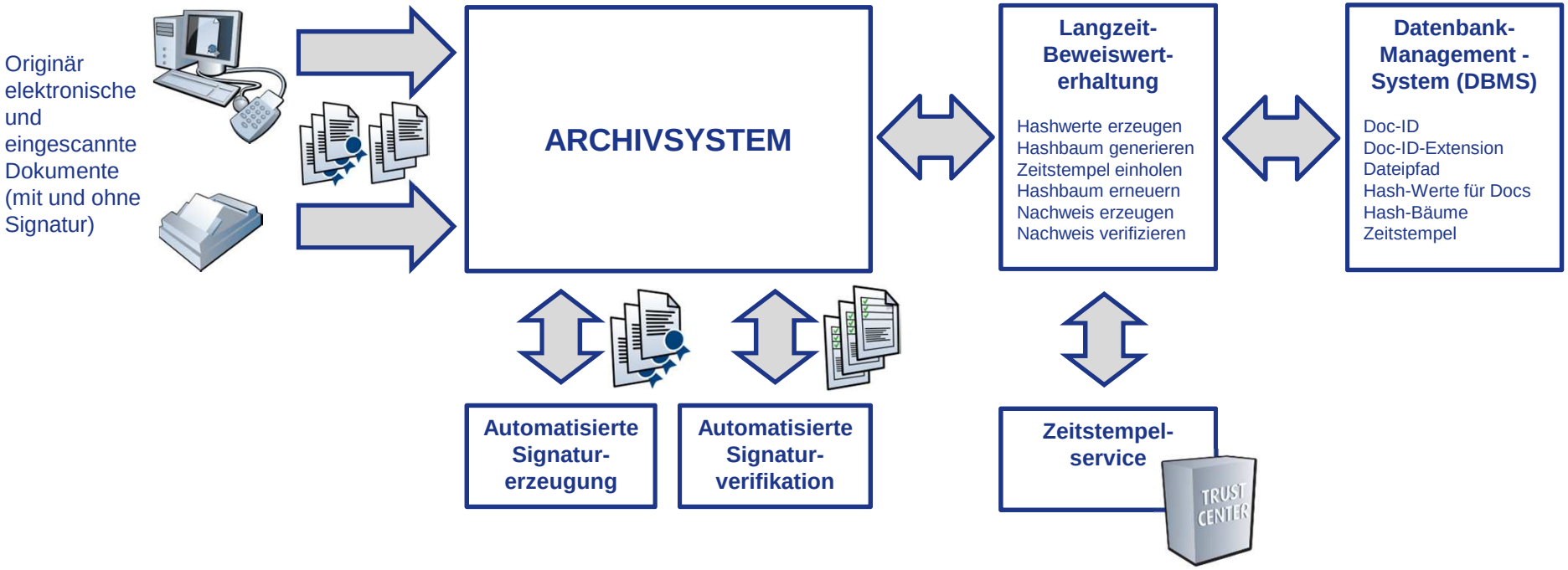
Tabelle 2: Geeignete Schlüssellängen für RSA-Verfahren

Parameter \ Zeitraum	bis Ende **2021**
n	1976 (Mindestwert) 2048 (Empfehlung)

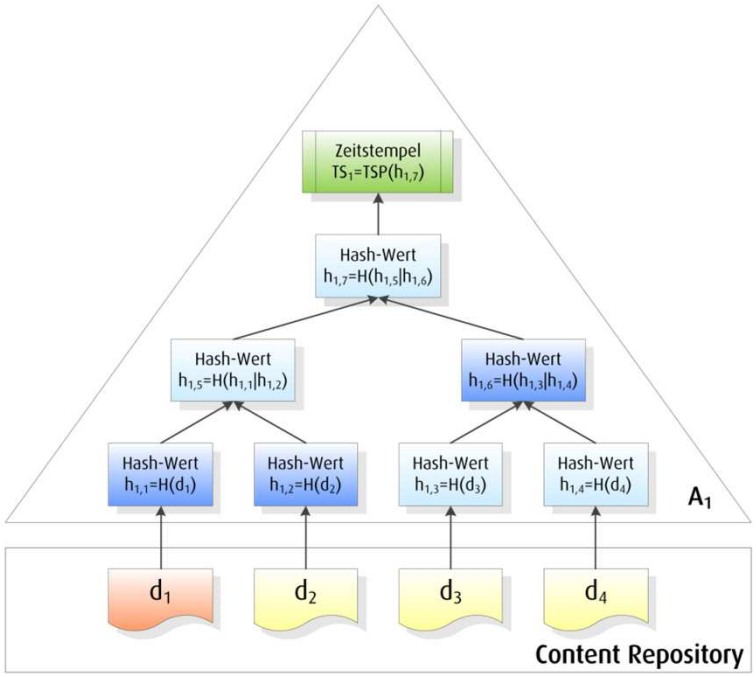
Quelle: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Entwurf – 28.10.2014, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Lösungsschema mit Indizienkette

Zeitnahe Abfolge kryptographischer Verfahrensschritte
zur Erhöhung des digitalen Beweiswerts



Hashbaumverfahren bei Langzeitbeweiswerterhaltung



Standard

LTANS / ERS
(Long-Term Archiving and Notary Service / Evidence Record Syntax)

Ziel

Lückenloser Nachweis in der Zukunft, dass ein Dokument in einem bestimmten Zustand vorgelegen hat.

Abb.: Archivzeitstempel A1 mit seinem Hash-Baum

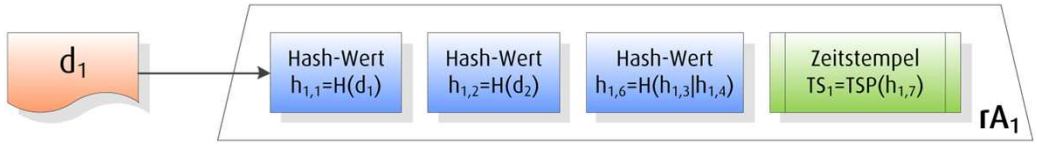


Abb.: Reduzierter Archivzeitstempel rA1

Hinweis: Die Grafiken sind Abbildungen aus dem Buch "Beweiskräftige elektronische Archivierung" von Roßnagel und Schmücker (Verlag: Economica Verlag; Auflage: 1., 2006 (1. Dezember 2005)) entlehnt.

Rechtlicher Rahmen

Gesundheitswesen

- Bundesgesetze (z.B. Arzneimittelgesetz (AMG)), Landesgesetze (z.B. Landeskrankenhausgesetze, Landesdatenschutzgesetze), Verordnungen (z.B. Bundesärzteordnung, Strahlenschutzverordnung), Verträge (z.B. Arztvertrag, Behandlungsvertrag), Regelungen und Richtlinien (z.B. Arzneimittelrichtlinie)
- E-Health-Gesetz (Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen)
- Patientenrechtegesetz

Weiteres

- Signaturgesetz und Signaturverordnung
- Ab Mitte 2016 ersetzt durch: eIDAS (Electronic identification and trust services / Verordnung über die „elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“)

Qualifizierte elektronische Signatur (qeS)

Schriftform gemäß BGB

- § 126 BGB Schriftform:
  (1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift […] unterzeichnet werden.
  (2) Bei einem Vertrag muss die Unterzeichnung der Parteien auf derselben Urkunde erfolgen. […]
- § 126 a BGB Elektronische Form (Bürgerliches Gesetzbuch):
  Gleichstellung von qualifiziert elektronisch signierten Dokumenten mit Papierdokumenten mit Unterschrift (Urkunden)
- Qualifizierte Signatur (gemäß Signaturgesetz und Signaturverordnung) ermöglicht die elektronische Dokumentation, die der Papierdokumentation rechtlich gleichwertig sein soll

Signaturrelevante digitale Dokumente in Krankenhäusern

Aufgrund gesetzlicher Vorschriften sind z.B. folgende Dokumente mit einer qeS zu signieren:

Diagnostik / Therapie: Verschreibung von Betäubungsmitteln, Behandlungsplan, Bestrahlungsplan, Anforderung von Blutkomponenten, Anforderung von Radiologischen Leistungen etc.

Pflege / Maßnahmendokumentation: Anwendung von Blutprodukten, Spenderakte, Anwendung radioaktiver Stoffe und ionisierender Strahlung

Administration: Patienteneinwilligung, Verträge, Blutgruppenausweise, Arbeitsmedizinische Vorsorgeuntersuchungsbescheinigung, Herstellungs- und Prüfprotokolle von Blutgruppen etc.

Quelle: Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. (CCESigG) und Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)

Signaturrelevante digitale Dokumente in Krankenhäusern

Aufgrund von Konventionen oder hoher Dokumentenrelevanz mit qeS zu signieren:

- Arztbriefe
- OP-Berichte und -Dokumentation
- kritische Teile der Intensiv- / Anästhesiedokumentation (ärztliche Dokumentation / Verlaufsbericht)
- kritische / pathologische Befunde

Quelle: Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. (CCESigG) und Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)

Signaturrelevante digitale Dokumente in Krankenhäusern

Für die folgenden Dokumentarten wird ein schwächeres Signaturniveau als ausreichend erachtet:

- unkritische / pathologische Befunde
- unkritische Laborbefunde
- unkritische radiologische Befunde
- große Teile der Intensiv- / Anästhesiedokumentation (pflegerische Dokumentation / Monitoring etc.)

Quelle: Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. (CCESigG) und Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)

Die secrypt GmbH im Überblick

- 2002 gegründet mit Sitz in Berlin, seit 2005 ISO 9001 zertifiziert
- Kernkompetenzen: Lösungen, Produkte und Dienstleistungen zur Einbindung von elektronischer Signatur, Zeitstempel und Verschlüsselung in elektronische Geschäftsprozesse
- Ziele: sichere, effiziente und beschleunigte Dokumenten-Workflows
- Integration der digiSeal®-Produkte in vorhandene Workflows internationaler Anbieter:
  - Standardschnittstellen
  - Programmierschnittstelle (API)
  - standardmäßig eingebunden in DMS, ERP, Output, Scannen und Archiv
- Gesetzeskonformität: Deutsches Signaturgesetz und EU-Signaturrichtlinie
- IT-Security-Consulting: Analysen, Konzepte und Begleitung
- Mitgliedschaften: BITKOM, CCESigG, PDF/A Competence Center, TeleTrust, Sichere Identität Berlin-Brandenburg

Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit.

Wir sind jederzeit gern für Sie da.

conhIT
14.–16. April 2015
Connecting Healthcare IT

Halle 1.2, Stand D-107 (bei synedra)

Themen: Arztbriefsignatur, Patientenaufnahme mit Unterschrift-Tablet, Signatur im KIS und Archiv, ersetzendes Scannen mit eSignatur

www.secrypt.de