Sichere digitale Dokumente in der Patientenaufnahme mit Kombi-Signatur

gmds Berliner Archivtage 2014

03.12.2014, 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

Mengengerüste

Pro Krankenhaus

- ca. 50 Einzelbelege pro stationärem Behandlungsfall
- ca. 1 laufender Meter Dokumentation pro Bett jährlich

Gesundheitsversorgung Deutschland insgesamt

- ca. 5.000.000.000 (5 Milliarden) Dokumente pro Jahr
- ca. 2.500.000.000 € (2,5 Milliarden) Kosten für Archivierung pro Jahr

Quelle: Schmücker, Dujat, Häber (2008)

Ziele

- Vermeidung und Abschaffung kostenintensiver Papierarchive
- Sichere digitale Patientenakte und durchgängig digitale Dokumenten-Workflows
- unabhängig von Zeit und Ort informieren und kommunizieren: schnellere und bessere Durchsuchbarkeit digitaler Archive
- Einhaltung von Compliance-Richtlinien
- Kostensenkungspotentiale heben

Herausforderungen:
Digitale Revisions- und Beweissicherheit

Revisionssicherheit – Begriffsbestimmung

Der Begriff „Revisionssicherheit“

- Begriff bezieht sich auf die revisionssichere Archivierung für elektronische Archivsysteme
- Rechtliche Grundlagen für die Anforderungen in Deutschland:
  - Handelsgesetzbuch (§ § 239, 257 HGB)
  - Abgabenordnung (§ § 146, 147 AO)
  - Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)
  - weitere steuerrechtliche und handelsrechtliche Vorgaben
- Verband Organisations- und Informationssysteme e.V. (VOI) hat den Begriff „Revisionssicherheit“ im Jahr 1996 in einem „Code of Practice“ eingeführt
- Anwendung des Begriffs inzwischen auch außerhalb des handels- und steuerrechtlichen Bereichs

Revisionssicherheit – Kriterien

„Revisionssicherheit“ meint die Erfüllung folgender Kriterien (Basis: HGB-Vorschriften)

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des Gesamtverfahrens
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Nutzung nur durch Berechtigte
- Einhaltung der Aufbewahrungsfristen
- Dokumentation des Verfahrens
- Nachvollziehbarkeit
- Prüfbarkeit

Die detaillierten Anforderungen und deren Umsetzung sind den GoBS zu entnehmen.

Digitale Beweissicherung / Schriftform

Herausforderung „Beweissicherung“ in der digitalen Welt

- § 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

Die qualifizierte elektronische Signatur (qeS)

Die „qualifizierte“ elektronische Signatur ersetzt die handschriftliche Unterschrift (§ 126a BGB Elektronische Form)

- Sie gewährleistet Integrität und Authentizität der signierten Dokumente
- Sie ist ausschließlich dem Signaturschlüsselinhaber zugeordnet
- Sie ermöglicht die Identifizierung des Signaturschlüsselinhabers
- Sie muss mit einer sicheren Signaturerstellungseinheit (Signaturkarte) erzeugt werden
- Sie wird von einem Trustcenter ausgegeben,
  z.B. medisign, D-TRUST etc.
- Grundlage: Signaturgesetz (SigG) und Signaturverordnung (SigV)
  demnächst: neue EU-Signaturverordnung (EiDAS)

Formfreie Verträge in der Papierwelt

- Der Abschluss der meisten Verträge ist grundsätzlich formfrei – das bedeutet, dass auch ein Handschlag reichen würde, um einen wirksamen Vertrag zu schließen.
- In vielen Fällen ist es aber wichtig für die Beteiligten, dass sie auch nachweisen können, dass der Vertrag mit einem bestimmten Inhalt von bestimmten Vertragspartnern abgeschlossen wurde.
- In der Papierwelt dient zu diesem Zweck die Unterschrift, an der sich der Unterschreibende festhalten lassen muss.

Formfreie Verträge in der digitalen Welt

- In der digitalen Welt besteht die Herausforderung, eine ähnlich sichere Beweislage zu schaffen.
- Da in der Regel der Patient nicht Inhaber einer Signaturkarte ist, ist es notwendig, über andere Merkmale ein Dokument dem Patienten zuordnen zu können.

→ Kombi-Signatur: Patient unterschreibt auf Signaturpad, Arzt/Krankenhausmitarbeiter mit Signaturkarte

Kombi-Signatur: Patientenunterschrift

Ablauf in Patientenaufnahme

1. Individuelles Gespräch zwischen Patient und Arzt bzw. Mitarbeiter inklusive Ausfüllen des elektronischen Dokuments,
z.B. Behandlungsvertrag

2. Patient bestätigt, alle Erläuterungen verstanden zu haben

3. Patient unterschreibt auf Unterschrift-Tablet und seine biometrische Signatur (u.a. Schreibdruck, Schreibgeschwindigkeit, Schreibbeschleunigung) wird in das Dokument verschlüsselt eingebettet

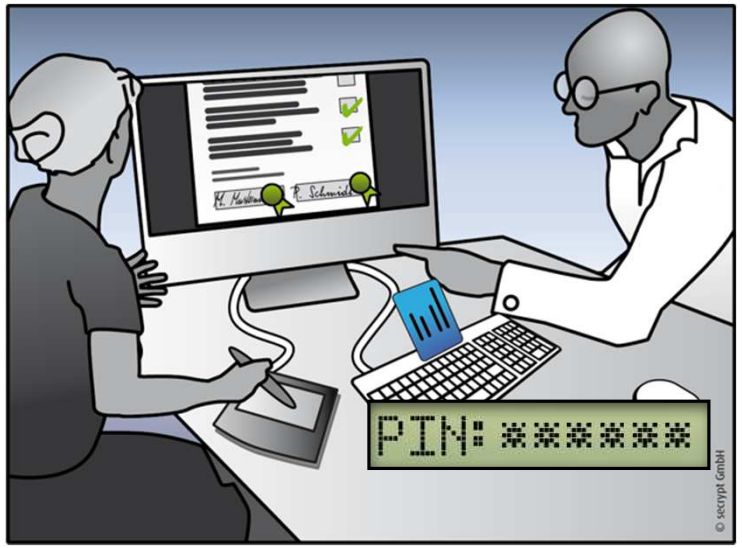
Unterschrift-Tablet

Quelle: Wacom Europe GmbH

Kombi-Signatur: Arzt- / Mitarbeiterunterschrift

4. Arzt bzw. Mitarbeiter signiert unmittelbar anschließend mit Signaturkarte (qualifizierte Signatur), z.B. Heilberufs-ausweis (HBA), und bestätigt, dass Patient in seiner Anwesenheit unterschrieben hat. Das Dokument wird digital ‘versiegelt‘.

5. Ablage des elektronisch signierten Dokuments im digitalen Archiv, wo es z.B. im PDF/A-Format organisationsweit schnell verfügbar ist



Signatur-Datenstruktur im PDF/A

PDF/A

QUALIFIZIERTE SIGNATUR DES ARZTES / MITARBEITERS

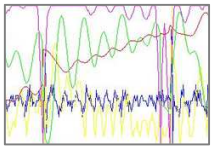
Text

Grafiken

Bilder

INTERNE SIGNATUR

INTERN VERSCHLÜSSELT



Biometrische Unterschriftsdaten des Patienten (Schreibdruck, -geschwindigkeit, -beschleunigung)

+

5E 40 F0 B7 A8 C5 77 3E
BF 00 EB 69 59 C4 E7 1C
E9 73 3E 00 92 83 10 10
2F F6 D7 D1 63 27 67 92

Hashwert / Prüfsumme des Dokuments

Fazit

- Die biometrischen Daten, die mit der Unterschrift aufgenommen und verschlüsselt in dem digitalen Dokument abgelegt werden, erlauben aufgrund der vielen aufgenommenen Parameter den Rückschluss auf den Unterzeichner (Identität).
- Die unzertrennliche Verbindung zwischen Unterschrift und Dokument erfolgt über die eindeutige Prüfsumme (Hashwert) des Dokuments, die gemeinsam mit den Unterschriftsdaten verschlüsselt wird.
  → Dies verhindert, dass die Unterschrift aus einem Dokument herausgenommen und mit dem Inhalt eines anderen Dokuments verbunden werden kann!

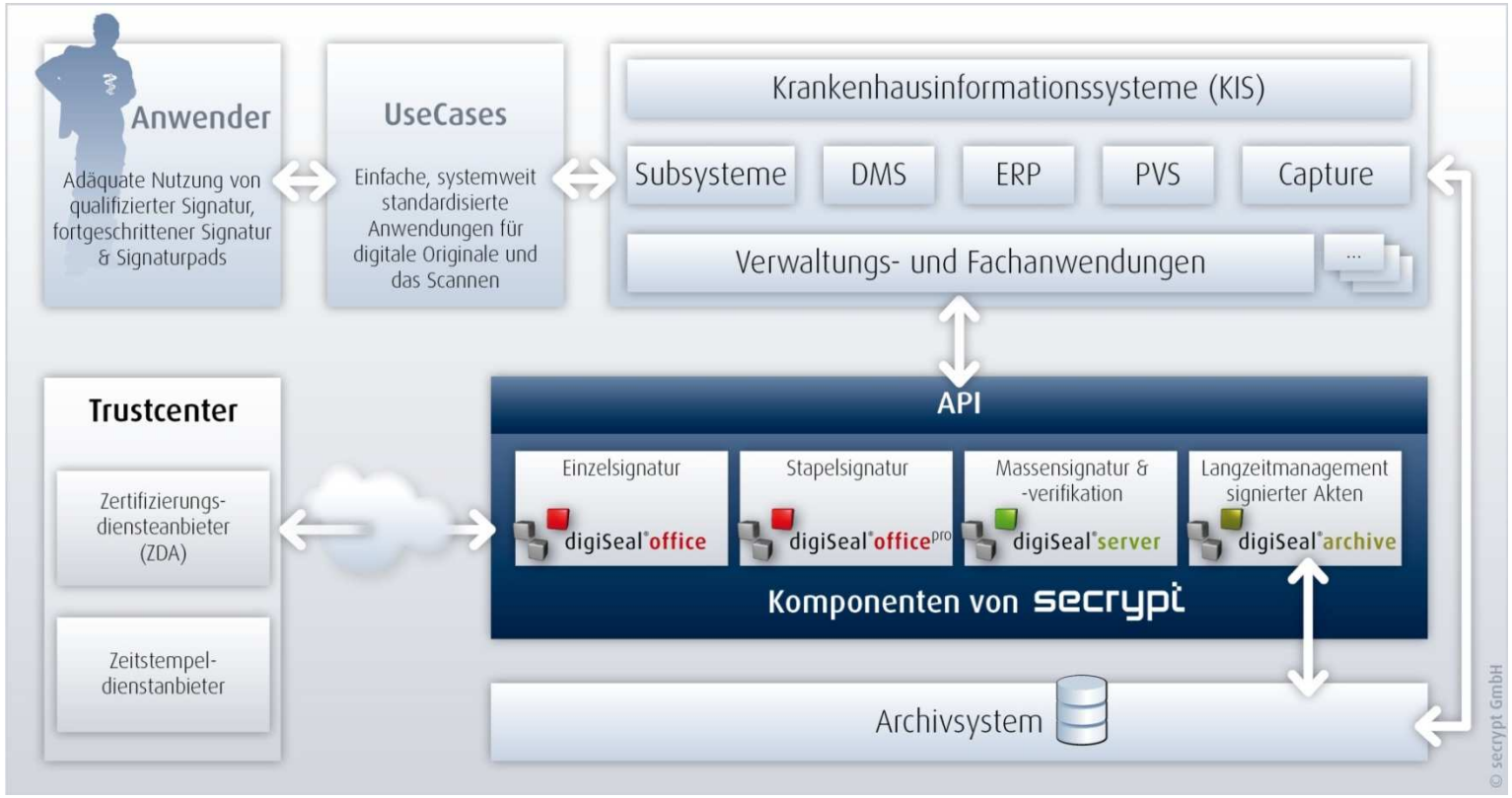
Fazit

- Die Rechtssicherheit wird noch erheblich dadurch gesteigert, dass ein Mitarbeiter nicht nur für das Krankenhaus unterschreibt, sondern dabei mit einer qualifizierten Signatur die Identität des Patienten bestätigt und das Dokument inklusive der erfassten biometrischen Unterschriftsdaten des Patienten digital versiegelt.
- Eine unbemerkte Manipulation des Dokuments ist ausgeschlossen, und der Vertrag ist hinsichtlich der Erklärung des Krankenhausmitarbeiters und des Vorliegens der Unterschriftsdaten des Patienten mit sehr hoher digitaler Beweiskraft ausgestattet.

Die secrypt GmbH im Überblick

- 2002 gegründet mit Sitz in Berlin, seit 2005 ISO 9001 zertifiziert
- Kernkompetenzen: Lösungen und Dienstleistungen zur Einbindung von elektronischer Signatur, Zeitstempel und Verschlüsselung in elektronische Geschäftsprozesse
- Ziel: Digital durchgängige, sichere und effiziente Dokumenten-Workflows
- Signaturprodukte integriert in diverse KIS, DMS, Capture-Lösungen und Archive
- Gesetzeskonformität: Deutsches Signaturgesetz und EU-Signaturrichtlinie
- IT-Security-Consulting: Analysen, Konzepte und Begleitung
- Mitgliedschaften: BITKOM, CCESigG, PDF/A Competence Center, TeleTrusT

Signatur-Integration in Bestandssysteme



Vielen Dank für Ihre Aufmerksamkeit

secrypt GmbH

Bessemerstr.82
D-12103 Berlin
Tel.: +49 30 7565978-0
mail@secrypt.de
www.secrypt.de