provet

Projektgruppe verfassungsverträgliche Technikgestaltung

Beweissicherheit und Beweiswert elektronischer Dokumente

Juristische Simulationsstudie
15. Januar 2014, Kassel

Paul C. Johannes, LL.M.

ITeG Forschungszentrum für Informationstechnik-Gestaltung

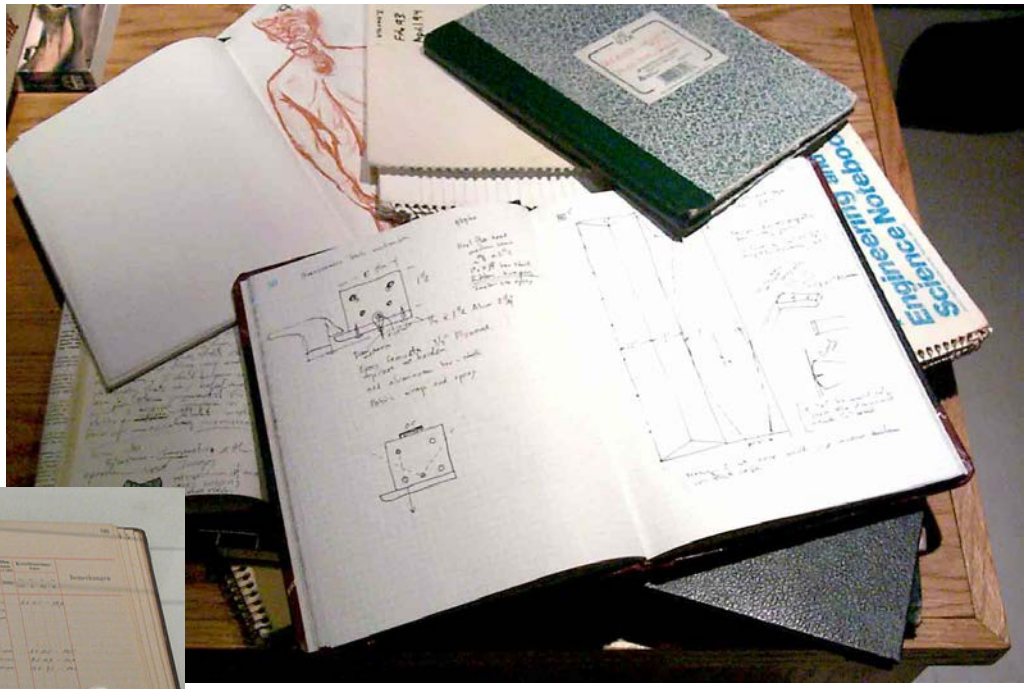
UNIKASSEL VERSITÄT

Überblick

1. Laborbücher
2. Elektronische Laborbücher
3. Beweisrecht
4. Beweiswert elektronischer Dokumente

Laborbücher

Foto: Dale Winters, http://www-personal.umich.edu/~mrwizard/web/labbook.html



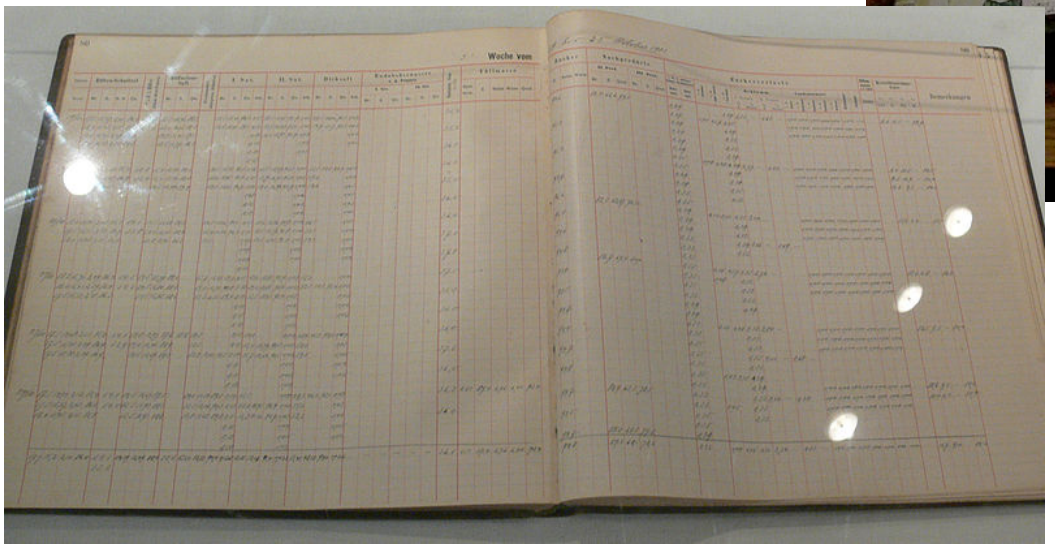


Foto: Laborbuch Zuckerfabrik Tessin 1896-1906, Zucker-Museum

Laborbücher

- Auch genannt Laborjournal, Protokollbuch, Notizbuch u.ä.
- Zweck ist die Dokumentation von Experimenten, Versuchen und Beobachtungen
- Protokollierung von Planung, Durchführung und Auswertung
- Gedächtnisstütze und Arbeitsmittel zugleich
- Dient auch zum Nachweis der Arbeit
- Wissenschaftlicher und analytischer Standard

Gestaltung von Laborbüchern

provet

Keine allgemeingültigen Regeln zur Gestaltung, üblich aber:

- Festes, gebundenes Buch mit durchnummerierten Seiten
- Verwendung dokumentenechter Tinte
- Aufzeichnungen während oder im unmittelbaren Anschluss des Versuches
- Messwerte und Rechnungen direkt eintragen
- Rohdaten in Form von Ausdrucken, Fotografien, Röntgenfilmen u.ä. sollen ins Laborbuch eingeklebt werden
- Schreib- und Rechenfehler sollen durchgestrichen und nicht unkenntlich gemacht werden.
- Seite und oder Versuche sind zu datieren und vom Experimentator zu unterschreiben

→ Zweck: Nachvollziehbarkeit und Nachprüfbarkeit

Bedeutung der Dokumentation im Laborbuch

provet

- Überprüfung kann geführt werden durch inhaltliche Kontrolle (Plausibilität)
- Überprüfung kann geführt werden durch Replikation der Versuche
- Probleme können entstehen, wenn Messungen nicht mit vergleichbaren Ergebnissen wiederholt werden
- Subjektive (Unvermögen) und/oder objektive Gründe (Unmöglichkeit)
- Interesse des Messenden, Echtheit der Messungen zu belegen.

Laborbücher im Rechtsstreit

provet

- Laborbücher können Beweismittel sein
- Zum Beispiel bei
    - Urheberrechtstreitigkeiten,
    - Patenstreitigkeiten,
    - Zulassungs- und Kontrollverfahren,
    - Schul- und Hochschulprüfungen,
    - Arzthaftungssachen,
    - Streit um Arbeitnehmererfindungen
- Aufdecken und Verhindern von wissenschaftlichem Fehlverhalten, wie Erfinden von Daten, Unterdrücken, Löschen, Beseitigen von Daten, Daten schönen/kochen durch Veränderung von Daten (Datenmanipulation)

Grenzen von Laborbüchern aus Papier

Elektronische Laborbücher

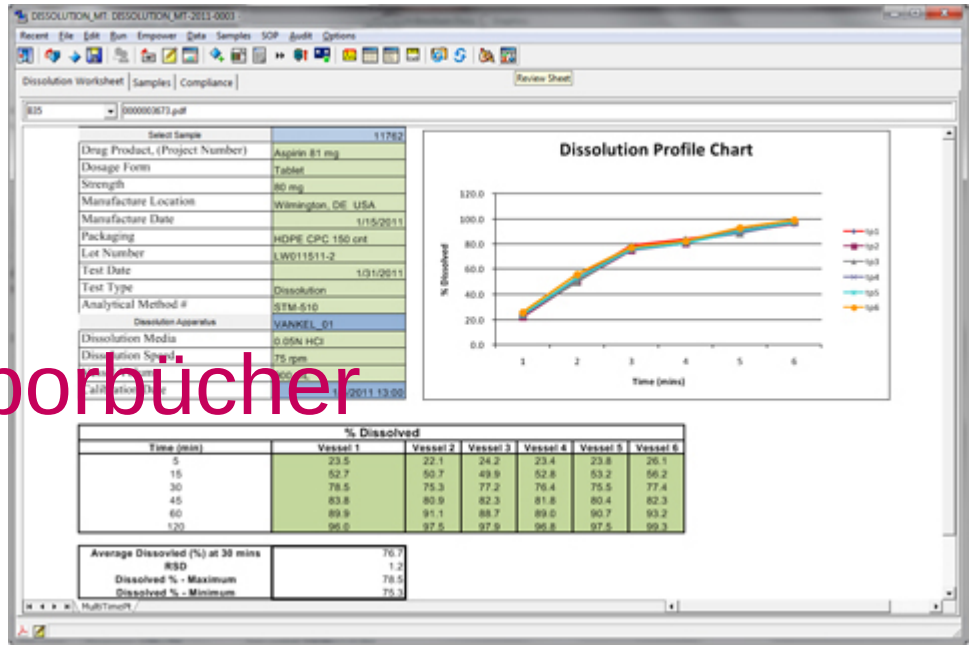


Foto: LabWare Ltd, www.labware.com

Foto: AgileBio SARL, www.labcollector.com

Elektronische Laborbücher

- Abkürzung eLab (englisch ELN für electronic labnotebook)
- Alltag des Labors oft schon digital:
    - elektronische Messgeräte,
    - elektronische Kommunikation,
    - elektronische Recherche
- Teilweise sehr große (Roh-)Datenmengen
- Gute Laborpraxis (ISO-Standard) kann Verwendung indirekt voraussetzen, z.B. bei Reinraumlaboren
- Arbeitserleichterung: Suchfunktion, Kopierfunktion, Eingabemasken usw.
- LIMS bieten auch Kollaborationsmöglichkeiten

Beweiswert elektronischer Laborbücher

provet

- eLab, LIMS und Variationen sind elektronische Dateien aller Art
- Die Echtheit von elektronischen Dateien zu beweisen kann schwierig sein
- Veränderungen können u.U. spurlos vorgenommen werden (Integritätsproblem)
- Der Aussteller ist u.U. nicht sicher feststellbar (Authentizitätsproblem)

Beweisrecht

Beweisrecht

- Beweis = Überzeugung des Gerichts von Wahrheit einer Behauptung
- Beweislast = Risiko des misslungenen Beweises
- Beweislastverteilung = Beweisbelastet ist die Partei, die eine ihr günstige Tatsache behauptet.
- Beweismittel
    - Parteivernehmung,
    - Zeugen,
    - Sachverständige,
    - Urkunden,
    - Augenschein
- Grundsatz freier richterlicher Beweiswürdigung

Freie Beweiswürdigung

- Richter muss von Echtheit des Beweismittels überzeugt sein.
- Richter muss persönlich zur Gewissheit kommen, dass etwas wahr ist und es selbst für wahr *halten.*
- Richter darf sich auf Wahrscheinlichkeiten stützen. Es bedarf keiner absoluten Gewissheit oder gar mathematisch-naturwissenschaftlicher Stringenz.
- Tatsachen, mit denen der Richter von der Echtheit eines elektronischen Dokuments überzeugt werden kann, sind zum Beispiel die Plausibilität des Inhalts der Erklärung sowie das Bestehen von Schutzsystemen und Übertragungsprotokollen.

Beweisrecht

- Wenige Einschränkungen des Grundsatzes der freien Beweiswürdigung
- Urkunden = Urkunden sind als Beweismittel verkörperte Gedankenerklärungen
- Private Urkunden
  - § 416 ZPO (Vermutung der Echtheit der Erklärung)
  - Unterschriebene Privaturkunden bringen den Beweis dafür, dass die in der Urkunde enthaltenen Erklärungen vom Aussteller abgegeben wurden.
- Öffentliche Urkunden
  - §§ 415, 417, 418 ZPO (Vermutung der Echtheit von Erklärungen und bezeugter Tatsachen
  - Öffentliche Urkunden bringen beweis dafür das die enthalten Erklärungen so abgegeben und die bezeugten Tatsachen so wahrgenommen wurden.

Beweisrecht

- Die Urkunde ist schon aufgrund dieser wenigen Beweisregeln das stärkste Beweismittel.

- Beweisregeln der ZPO gelten für Vielzahl anderer Verfahren, z.B.
  - Verwaltungsgerichtsverfahren nach § 98 VwGO,
  - Sozialgerichtsverfahren nach § 118 Abs. 1 SGG,
  - Arbeitsgerichtsverfahren nach § 58, 46 Abs. 2 ArbGG,
  - Patentgerichtsverfahren nach § 99 Abs. 1 PatG, § 82 MarkenG, § 18 Abs. 2 GebrMG, § 23 Abs. 2 GeschmMG, § 36 SortSchG
  - Finanzgerichtsverfahren als allgemeine Rechtsgedanken

Elektronische Dokumente und eLab als Beweismittel

Beweiswert elektronischer Dokumente

- Elektronische Dokumente sind elektronische Dateien aller Art.
- Nach § 371 Abs. 1 S. 2 ZPO sind elektronische Dokumente Objekte des Augenscheins und keine Urkunden.
- Objekte des Augenscheins unterliegen der freien richterlichen Beweiswürdigung.
- Der Richter muss dabei von der Echtheit des Beweismittels überzeugt werden.
- Die Echtheit von elektronischen Dokumenten zu beweisen kann schwierig sein.
- Veränderungen können spurlos vorgenommen werden (Integritätsproblem).
- Der Aussteller ist nicht sicher feststellbar (Authentizitätsproblem).

Beweiswert elektronischer Dokumente

provet

- Wenn Streit über das elektronische Dokument oder dessen Inhalt herrscht, müsste grundsätzlich der Beweisbelaste die Authentizität und die Integrität des elektronischen Dokument beweisen.
- Ist das Dokument unverfälscht?
- Ist es auch von dem, der es angefertigt oder unterschrieben haben soll, angefertigt oder unterschrieben worden?
- Im Zweifel bedarf es dazu eines aufwendigen und teuren Sachverständigengutachtens.

Integritätssicherung

Mittel der Integritätssicherung

- Protokollierung
  - Problem der Sicherung der Protokollierung
  - Manipulationsanfällig
- Authentifizierungs- und Autorisierungskonzept
  - Einschränkung der Nutzer
  - Beschränkung der Nutzerrechte
- Verbot der Datenlöschung
  - Einschränkung der Nutzerechte
  - Möglichkeit der Stornierung
- Elektronischer Zeitstempel einer unabhängigen, dritten Quelle
- Elektronische Signaturen

Signaturrecht

- Nach § 371a ZPO gelten für elektronische Dokumente dann die Beweisregeln für Urkunden, wenn sie mit einer qualifizierten elektronischen Signatur (QES) versehen wurden.
- Private elektronische Dokumente mit QES haben die Beweiskraft einer privaten Urkunde und es besteht ein Anschein der Echtheit.
- Nur durch Tatsachen zu entkräften, die ernstliche Zweifel an der Abgabe der Erklärung durch den Signaturschlüssel-Inhaber begründen.
- Öffentliche elektronische Dokumente haben die Beweiskraft einer öffentlichen Urkunde.
- Mit QES besteht sogar Vermutung der Echtheit der nur durch Gegenbeweis zu widerlegen ist.

Signaturrecht

- Die „digitale Signatur“ ist ein technischer Begriff, der ein kryptografisches Verfahren, beschreibt.
- Das Signaturgesetz (SigG) hat den Zweck, Rahmenbedingungen für elektronische Signaturen zu schaffen.
- Das SigG legt Anforderungen fest für
    - Zertifizierungsdiensteanbieter,
    - Produkte für elektronische Signaturen und
    - Prüf- und Bestätigungsstellen, die die Einhaltung und Umsetzung dieser Anforderungen prüfen,

Technik

- Die elektronische Signatur beruht auf einem Verschlüsselungsverfahren.
- Das Signaturgesetz sieht hierfür ein **asymmetrisches Verschlüsselungsverfahren** vor, in dem jeder Beteiligte einen nur ihm bekannten **privaten Schlüssel** *(private key)* und einen **öffentlichen Schlüssel** *(public key)* hat.
- Der öffentliche Schlüssel ist einem Verzeichnisdienst (einer Art Telefonbuch) des jeweiligen Zertifizierungsanbieters allgemein zugänglich. Der private Schlüssel ist auf einer Signaturerstellungseinheit (§ 2 Nr. 10 SigG) gespeichert.
- Das ist in der Regel eine Chipkarte, die nur mittels einer (nur dem Verwender bekannten) PIN aktiviert werden kann und deren Daten sonst nicht ausgelesen werden können.

Technik

- Die **elektronische Signatur** wird erstellt, indem die mathematische Quersumme des Dokumentes, der sogenannte **Hash-Wert,** mit dem privaten Schlüssel des Absenders verschlüsselt wird.
- Der Empfänger des Dokumentes kann dann mit Hilfe des öffentlichen Schlüssels des Absenders gegenrechnen, ob das ihm übermittelte Dokument denselben Hash-Wert hat, dass heißt ob es nicht verändert wurde und damit von dem signierenden Absender stammt.
- Elektronische Signatur wie Verschlüsselung setzen voraus, dass Absender und Empfänger entsprechende **technisch ausgerüstet** sind, dass heißt der Empfänger jedenfalls die zum Lesen erforderlichen EDV-Programme, der Absender auch ein Lesegerät zur Verwendung der Signaturkarte hat.

Fortgeschrittene elektronische Signaturen (§ 2 Nr. 2 SigG)

Elektronische Signaturen nach § 2 Nr. 1 SigG, die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, die die Identifizierung des Signaturschlüssel-Inhabers ermöglichen und die mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und die mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Qualifizierte elektronische Signaturen (§ 2 Nr. 3 SigG)

Fortgeschrittene elektronische Signaturen nach § 2 Nr. 3 SigG, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat nach § 7 SigG beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden. Zertifikate sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.

eLab als private elektronische Dokumente mit qualifizierter elektronischer Signatur

- Beweisregel nach § 371a Abs. 1 ZPO, die die freie Beweiswürdigung einschränkt.
- Es gelten die Vorschriften über die Beweiskraft privater Urkunden entsprechend.
- Nach § 416 ZPO begründen unterschriebene Privaturkunden vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.
- Die Beweisregel greift bei Privaturkunden aber nur, wenn die Unterschrift echt ist (§§ 439, 440 ZPO).
- Bei elektronischen Dokumenten mit QES ist der Anschein der Echtheit gesetzlich anzunehmen, wenn die Signaturprüfung erfolgreich ist.
- Der Anschein der Echtheit kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

eLab als öffentliche elektronische Dokumente

- Beweisregel nach § 371a Abs. 2 ZPO, die die freie Beweiswürdigung einschränkt.
- Es gelten die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechend, auch ohne qualifizierte elektronische Signatur.
- Gemeint sind die §§ 415, 417, 418 ZPO, wonach öffentliche Urkunden vollen Beweis für die in ihnen enthaltenen Erklärungen, Anordnungen und anderen Inhalte erbringen.
- Diese gelten aber nur soweit eLab innerhalb des zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind.
- Echtheit inländischer öffentlicher Urkunden nach § 437 ZPO gesetzlich vermutet.
- Nach § 371a Abs. 2 S. 2 ZPO gilt dies für öffentliche elektronische Dokumente nur, wenn diese mit einer qualifizierten elektronischen Signatur versehen wurden.

Weitere Mittel der Integritätssicherung

- Frühzeitiges automatisiertes Hashen
- Verzeichnisüberwachung
- Überwachung von Dateien/Datenreihen auf Plausibilität.
- Überprüfung der Hashwerte
- Dateiformatüberwachung
- Erkennen neuer Dateien

Authentizitätssicherung

Authentizitätssicherung

Qualifizierte elektronische Signaturen

- Identifizierung erfolgt durch den Diensteanbieter der Signatur (ZDA).
- Eindeutige Zuordnung einer elektronischen Signatur zu einer natürlichen Person.
- Sichere Authentifizierung der natürlichen Person durch zwei Komponenten: Besitz und Geheimnis.
- Überwachung und Aufsicht.
- Bestimmte Sicherungsmittel, sichere Signaturerstellungseinheit.
- Sehr hohes Sicherheitsniveau und sehr hoher Beweiswert

Authentizitätssicherung

Fortgeschrittene elektronische Signaturen

- Identifizierung erfolgt durch den Diensteanbieter der Signatur (ZDA).
- Eindeutige Zuordnung einer elektronischen Signatur zu einer natürlichen Person.
- Sichere Authentifizierung der natürlichen Person möglicherweise nur durch eine Komponenten: Besitz oder Geheimnis.
- Keine Überwachung und Aufsicht.
- Keine Bestimmte Sicherungsmittel, sichere Signaturerstellungseinheit.
- Keine einheitliches Sicherheitsniveau, Beweiswert einzelfallabhängig.

Authentizitätssicherung

provet

nPA und eID-Funktion

- Identifizierung erfolgt hoheitliche Stelle.
- Eindeutige Zuordnung zu einer natürlichen Person.
- Sichere Authentifizierung der natürlichen Person durch zwei Komponenten: Besitz und Geheimnis.
- Hoheitliche Überwachung und Aufsicht der Infrastruktur.
- Bestimmte, überwachte Sicherungsmittel und Komponenten.
- Hohes Sicherheitsniveau.

Authentizitätssicherung

Beweiswert der eID-Funktion

- Von der erfolgreichen Authentifizierung kann auf die Urheberschaft weiterer Handlungen oder Erklärungen danach geschlossen werden.
- Authentifizierung und Urheberschaft von Handlungen sind aber nicht identisch.
- Wenn nach erfolgreicher elektronischer Identifizierung Daten eingegeben werden, kann der Schluss gezogen werden, dass die Person, die sich authentifiziert wurde.
- Mit Authentisierung könnte ein Anscheinsbeweis für die Urheberschaft unmittelbar damit erfolgter Handlungen begründet sein.
- Parallele zu qualifizierten elektronischen Signaturen.

Authentizitätssicherung

provet

Beweiswert der eID-Funktion

- Integration in den Workflow
- Verbreitung und Verfügbarkeit
- Kollaboration
- Archivierung und Zugriff auf Forschungsdaten
- Pflege von Zugriffsrechten
- Verknüpfung der eID mit den Forschungsdaten
- Integritätssicherung

Zusammenfassung

Zusammenfassung

- Laborbücher und eLab können als Beweismittel in einer Vielzahl von Rechtsstreitigkeiten eine Rolle spielen
- eLab sind schon heute sehr verbreitet; die elektronische Forschungsdokumentation nimmt weiter zu.
- eLab sind elektronische Dokumente im Sinne des Beweisrechts.
- Als solche sind sie in der Regel schlechter gestellt als Urkunden aus Papier.
- Herkömmliche Laborbücher sind in der Regel Urkunden.
- Dieser beweisrechtliche Nachteil kann durch verschiedene Sicherungsmaßnahmen zum Schutz der Integrität und Authentizität versucht aufgefangen zu werden.
- Wichtigste und verlässlichste Werkzeuge sind dafür qualifizierte elektronische Signaturen und elektronische Zeitstempel nach dem SigG.

Vielen Dank

provet

Paul C. Johannes, LL.M.

Universität Kassel
Fachbereich Wirtschaftswissenschaften
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Pfannkuchstr. 1
34121 Kassel

fon +49 (0) 561 804 6083
fax +49 (0) 561 804 6081
paul.johannes@uni-kassel.de
http://provet.uni-kassel.de/