Leibniz-Institut für Pflanzenbiochemie

Signaturen in elektronischen Laborbüchern
Was können wir vom BeLab-Projekt lernen?

Frank Lange

IPB Halle

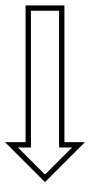
Workshop zu elektronischen Laborbüchern

Leibniz Gemeinschaft

WissenschaftsCampus Pflanzenbasierte Bioökonomie Halle

Agenda

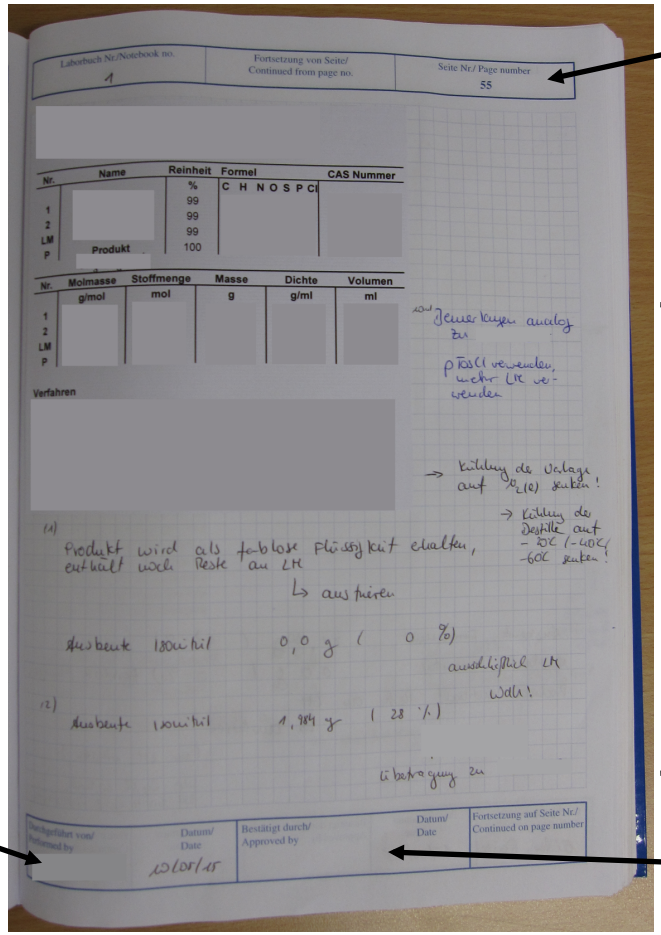
- Unterschriften im Papier-Laborbuch



- elektronische Signatur im ELN
  - Signaturformen
  - Signatur mit asymmetrischen Verschlüsselungsverfahren
- Praxis: Signaturen in ELN-Systemen
- elektronische Signatur und Langzeitarchivierung

Sicherheitsfunktionen im Papier-Laborbuch

gebundenes Buch



nummerierte Seiten

handschriftliche Ausführungen (dokumentenecht)

Unterschrift des Forschenden mit Datum

Unterschrift eines Zeugen

Papier-Laborbuch

Fragen:

Unterschrieben Sie oder Ihre „Stakeholder“ (Forschende) Laborbucheinträge?

Wer lässt gegenzeichnen?

Papier-Laborbuch

Ziel:

Nachweis erbringen,

- **Wer** ⇒ Unterschrift
- **Wann** ⇒ Datum
- **Welches** ⇒ Inhalt

Experiment dokumentiert hat.

Keine Aussage über Korrektheit der Dokumentation!

Grundsätze

Gute wiss. Praxis:

- lege artis arbeiten
- Resultate dokumentieren

} Empfehlung 1

- Laborbucheinträge sind Primärdaten mit 10 Jahren Aufbewahrungspflicht (Empfehlung 7)

Juristisch:

- unterschriebener Laborbucheintrag ist eine Urkunde (=besondere Beweiskraft)
- Urkundendelikte als Straftatbestand

BeLab-Projekt (2010-2014)

juristische Grundsätze:

- ELN-Einträge sind elektronische Dokumente.
- E-Dokument ist keine Urkunde, sondern „Gegenstand des Augenscheins und der freien Beweiswürdigung.“

➢ Beweiswertsteigerung durch **elektronische Signatur** ↔ **Authentizität** und **Integrität** eines E-Dokuments

➢ Beweiswerterhaltung während der Langzeitarchivierung

Was sind elektronische Signaturen?

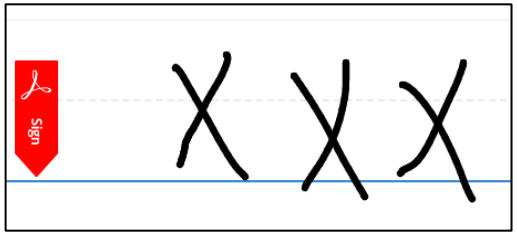
Rechtlicher Rahmen:

- eIDAS-Verordnung
- bis Juli 2017: Signaturgesetz & Signaturverordnung

Definition:

E-Signaturen sind Daten, die einem E-Dokument beigefügt oder logisch mit ihm verknüpft werden und die der Unterzeichner zum Unterzeichnen verwendet.

Nicht verwechseln mit der E-Unterschrift!



Adobe Acrobat Reader

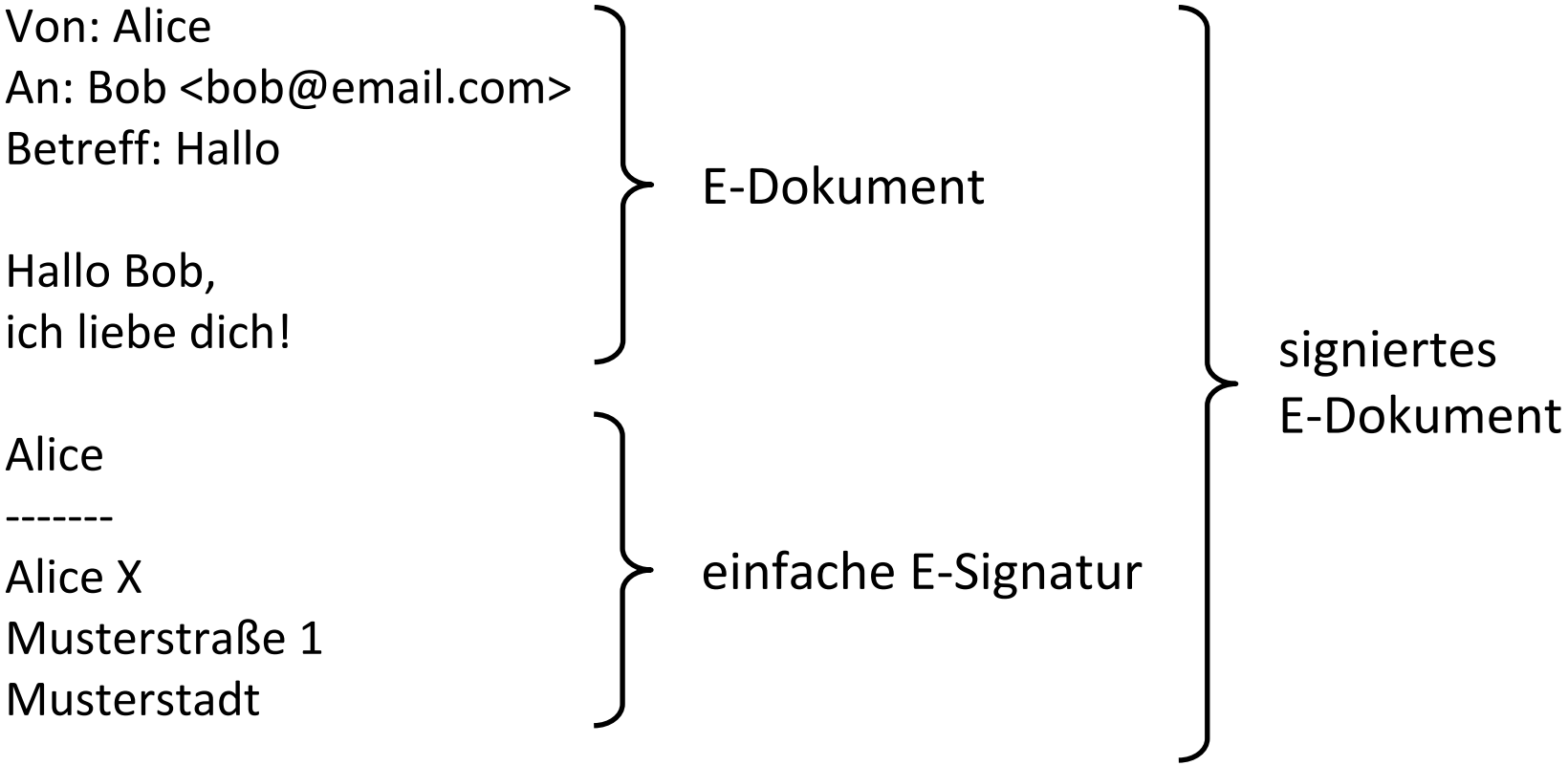
eIDAS = **e**lectronic **ID**entification, **A**uthentication and trust **S**ervices

Signaturstufen

	einfach	fortgeschritten	qualifiziert
Sicherheits-standard	keiner	hoch, z.B. zertifikatsbasiert	sehr hoch, qualifizierte Zertifikate
Beweiswert (jurist.)	**freie Beweiswürdigung**		**äquivalent zur handschriftlichen Unterschrift**

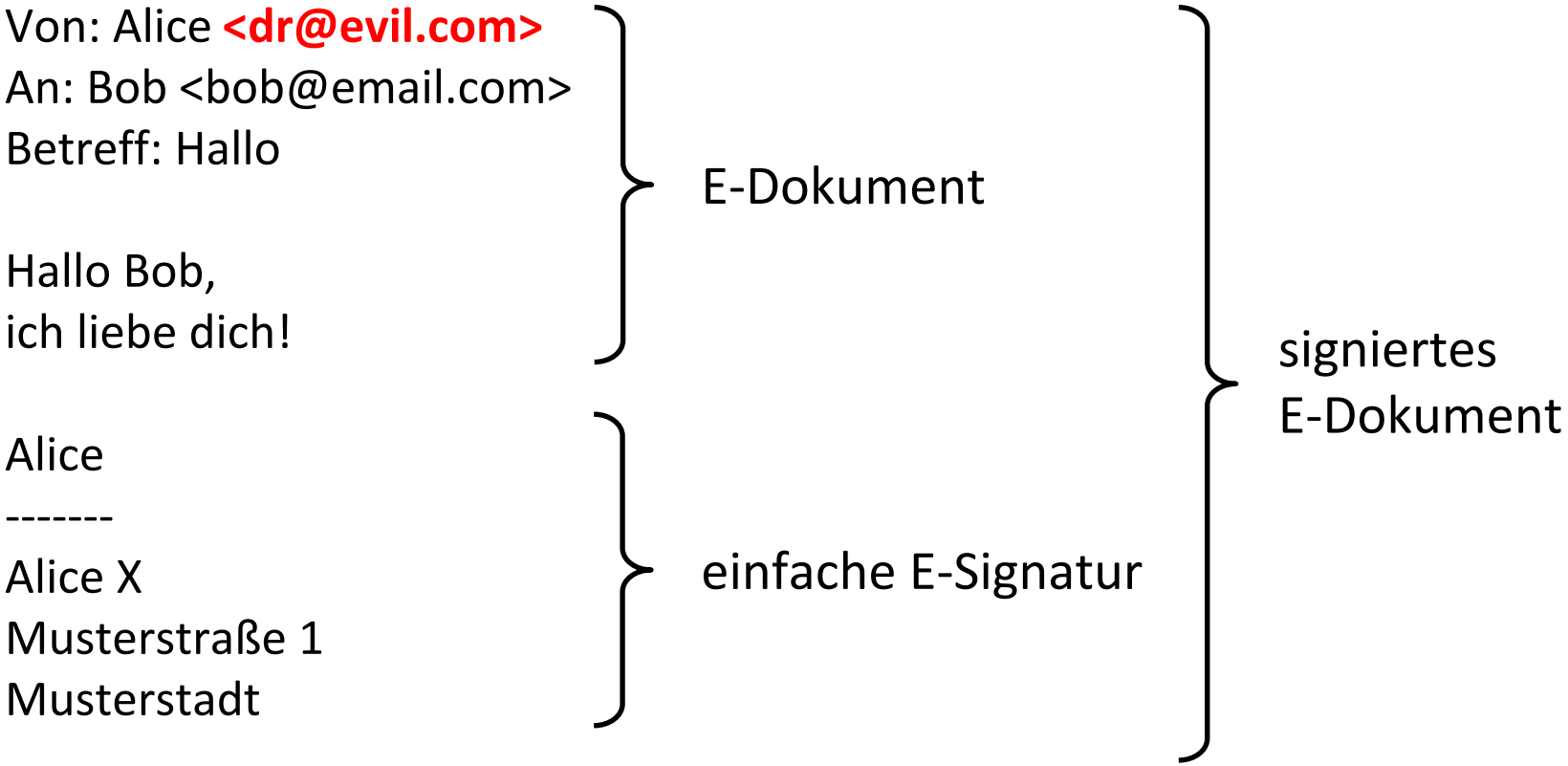
Signaturstufen

einfache E-Signatur: keine Sicherheitsmerkmale



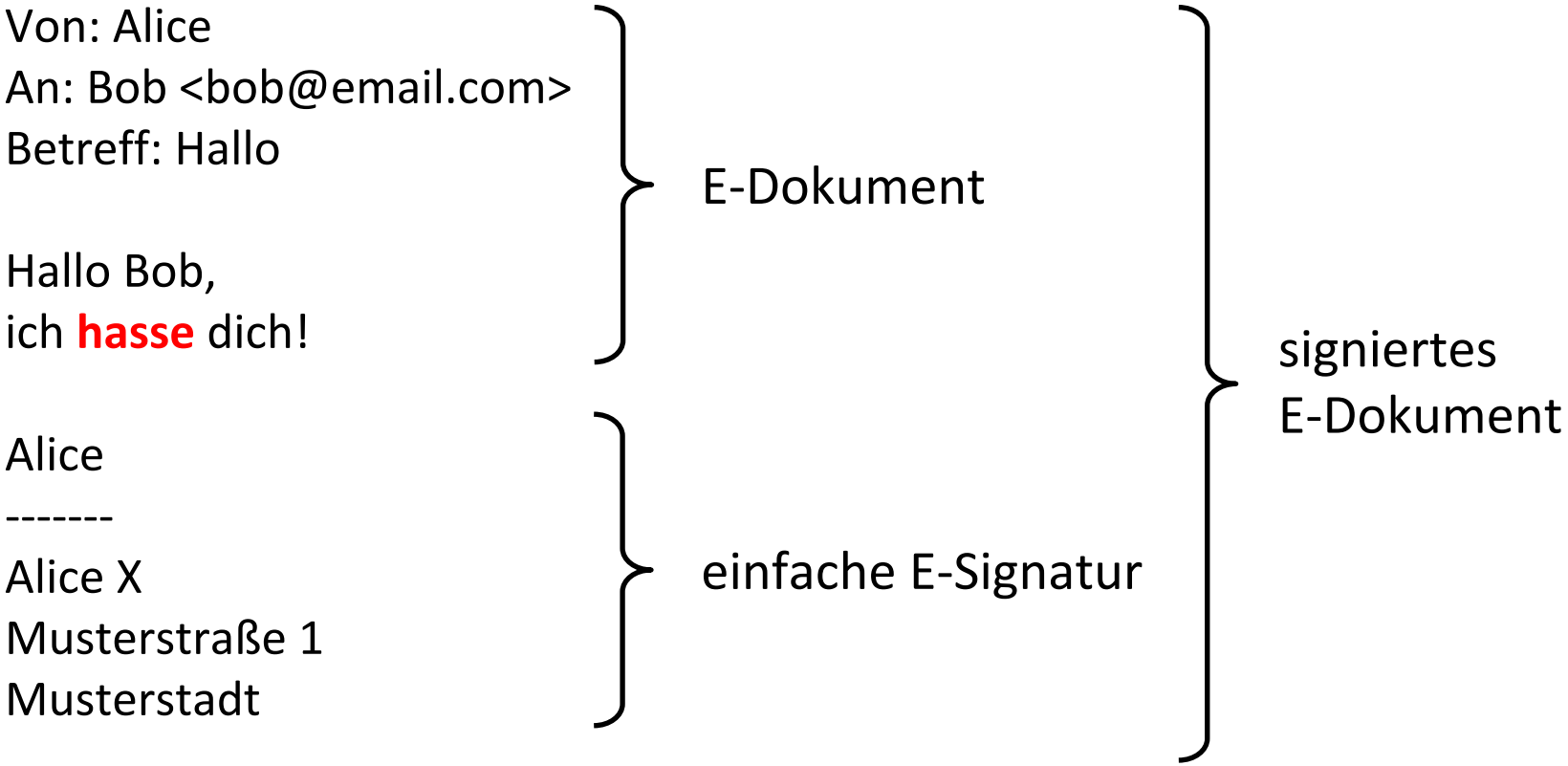
Signaturstufen

einfache E-Signatur: keine Sicherheitsmerkmale



Signaturstufen

einfache E-Signatur: keine Sicherheitsmerkmale



Signaturstufen

fortgeschrittene E-Signatur:

a) ist eindeutig dem Unterzeichner zugeordnet

b) ermöglicht die Identifizierung des Unterzeichners

c) Signaturerstellungsdaten sind unter alleiniger Kontrolle des Unterzeichners

d) Signatur mit dem E-Dokument verbunden, sodass eine nachträgliche Änderung erkannt werden kann

Signaturstufen

qualifizierte E-Signatur

... ist eine fortgeschrittene E-Signatur, die von einer qualifizierten Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht.

z.B.: QES-Funktion des elektronischen Personalausweises

Foto: Bundesdruckerei

Signaturzertifikat: 10€
Gültigkeitsdauer?

Kartenleser: 30 – 120€

Signaturstufen

Zu teuer?

Schlechte Usability/User Experience?

z.B.: QES-Funktion des elektronischen Personalausweises

Foto: Bundesdruckerei

Signaturzertifikat: 10€
Gültigkeitsdauer?

Kartenleser: 30 – 120€

Signaturstufen

fortgeschrittene E-Signatur:

a) ist eindeutig dem Unterzeichner zugeordnet

b) ermöglicht die Identifizierung des Unterzeichners

c) Signaturerstellungsdaten sind unter alleiniger Kontrolle des Unterzeichners

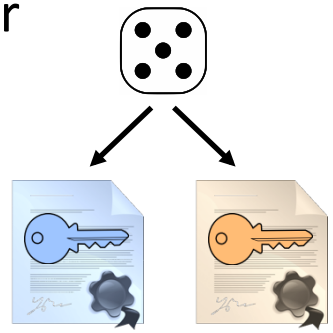
d) Signatur mit dem E-Dokument verbunden, sodass eine nachträgliche Änderung erkannt werden kann

Fortgeschrittene E-Signatur

z.B.: Signierung mit asymmetrischen Verschlüsselungsverfahren

Zutaten:

- persönliches Schlüssel-paar
  z.B. mit Zertifikat



öffentlicher Schlüssel
(Zuordnung und
Identifikation)

privater Schlüssel
(alleinige Kontrolle
des Unterzeichners)

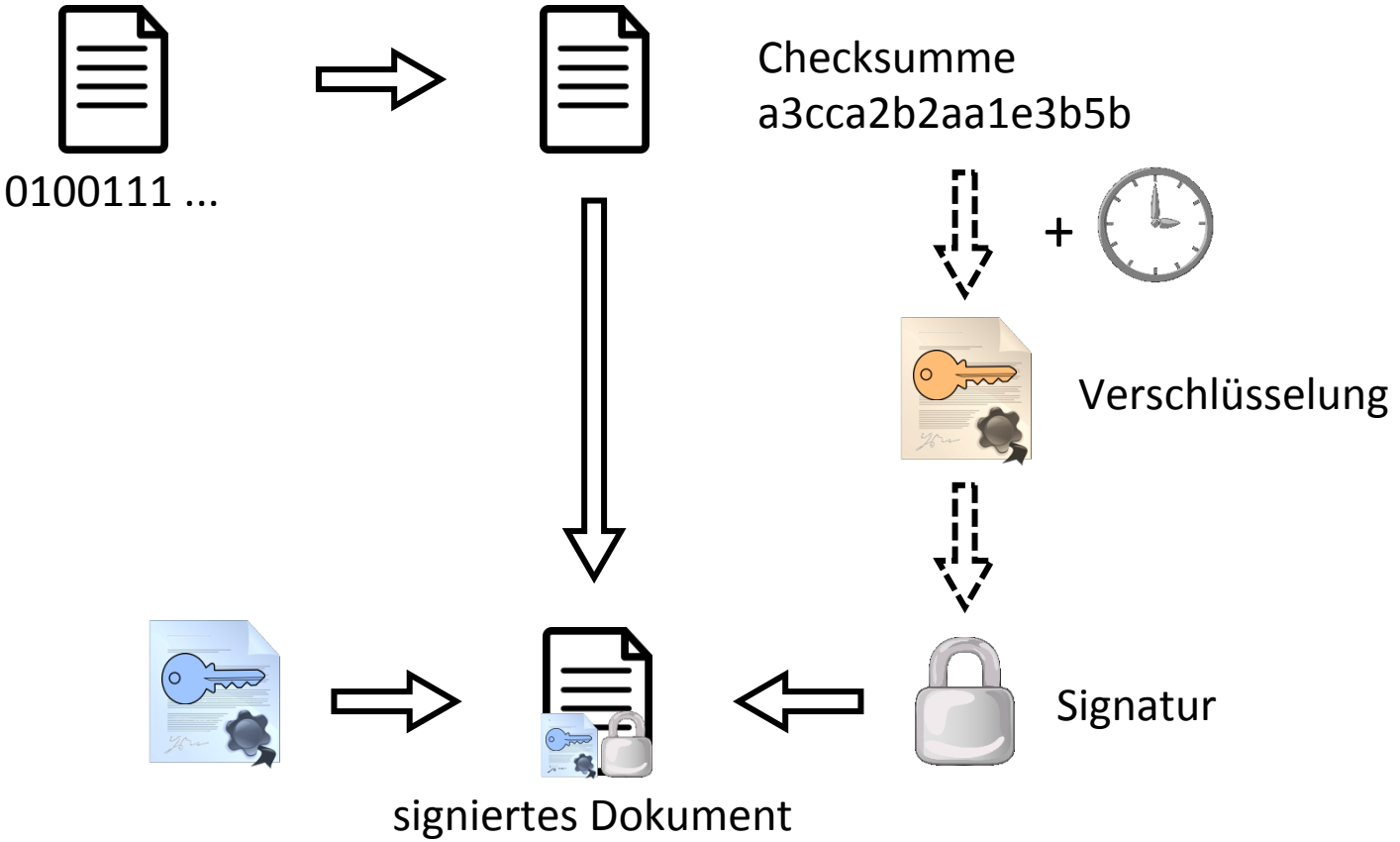
- E-Zeitstempel

- E-Dokument

Fortgeschrittene E-Signatur

z.B.: Signierung mit asymmetrischen Verschlüsselungsverfahren

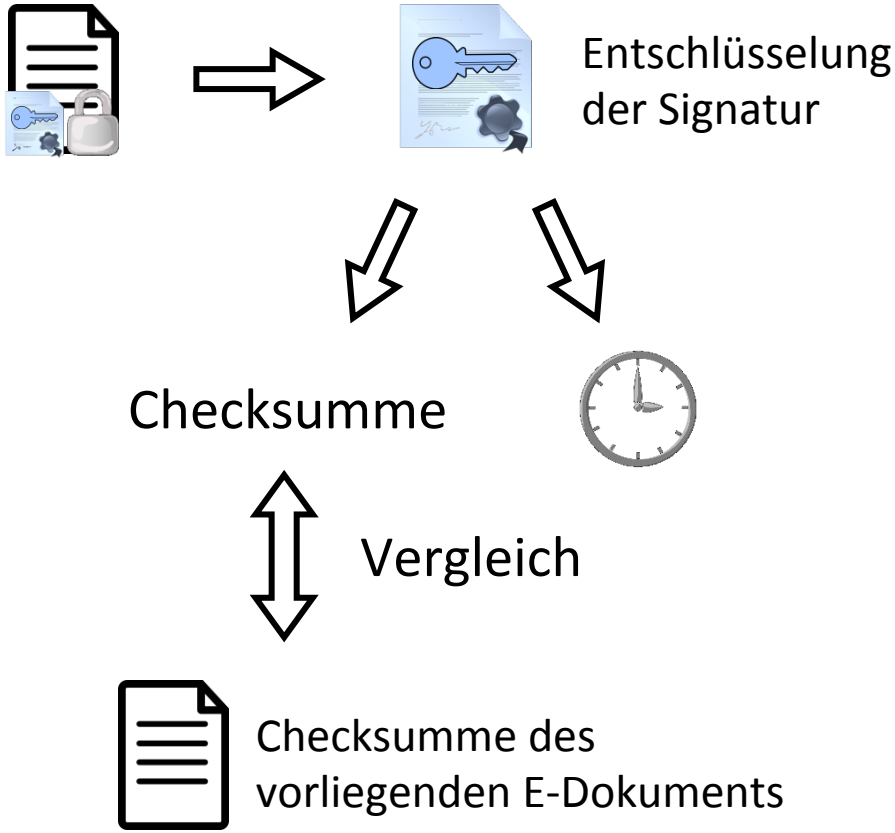
Ablauf:



Fortgeschrittene E-Signatur

z.B.: Signierung mit asymmetrischen Verschlüsselungsverfahren

Validierung:



Fortgeschrittene E-Signatur

Nachweis erbringen,

- **Wer** ⇒ 
- **Wann** ⇒ 
- **Welches** ⇒ Checksumme → Integrität

E-Dokument signiert hat.

Signaturen in ELN-Systemen: Open-Source-ELNs

- i.d.R. keine Signatur-Funktionen
- Ausnahme: Timestamp in eLabFTW

  - keine Passwortabfrage
  - danach ist ELN-Eintrag nicht mehr editierbar

Signaturen in ELN-Systemen: kommerzielle ELNs

- z.T. starker Fokus auf Pharma/Biotech/Servicelabore (GMP, GLP, QM-Normen)

Labfolder

Sign And Witness

Last update: 04.07.2017

You can give a legally binding signature which is equivalent to your handwritten signature in a paper notebook. You can sign your entries with digital signatures compliant to Title 21 CFR Part 11, the standard format for digital signatures in electronic lab notebooks. After signing an entry, you can send it to a colleague who can then witness it by giving his own digital signature. Digital signatures can either be provided by giving a handwritten signature in the signature field or by providing your account password.

Hivebench

ELECTRONIC SIGNATURE

We use electronic signature to warranty the property of your data. It's the first step towards FDA 21 CFR Part 11.

RSpace ELN

Protect IP and maintain compliance

- Full audit trail automatically created by RSpace
- Secure and easily managed signing and witnessing features
- Multiple support for 21 CFR 11

SciNote

CFR 21 Part 11

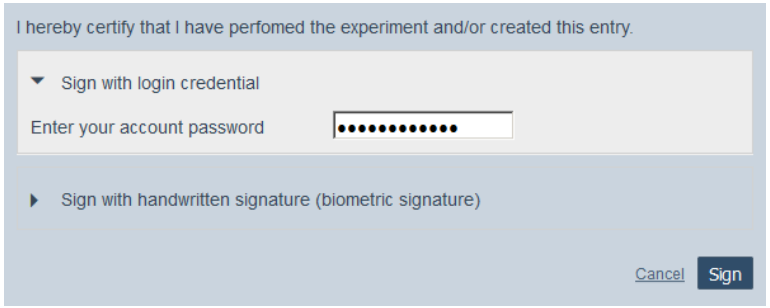
Enables your lab to comply with CRF 21 Part 11 requirements.

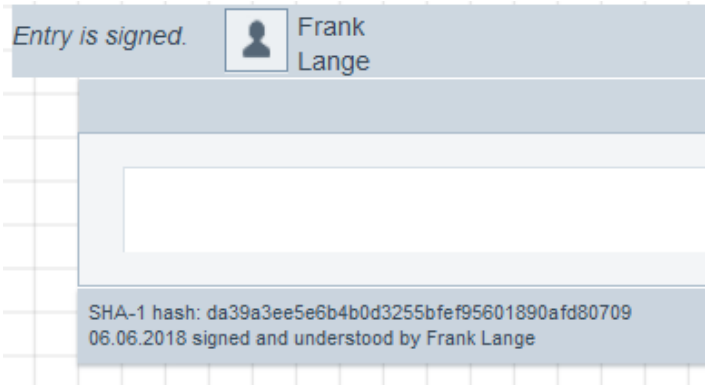
21 CFR Part 11 is FDA's set of instructions and guidelines about the creation, authentication and maintenance of lab's digital records.

This SciNote add-on includes electronic signatures, electronic witnessing, audit trails and advanced user management.

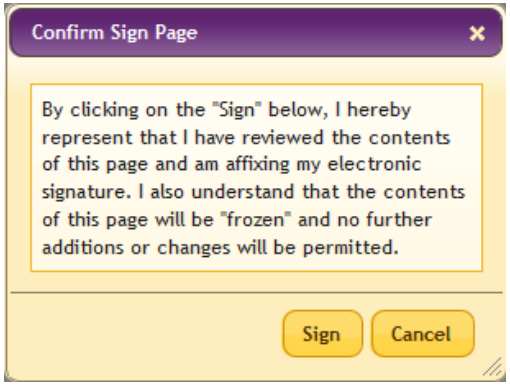
Signaturen in ELN-Systemen: kommerzielle ELNs

Labfolder (Passwort oder E-Unterschirft)





labarchives (kein Passwort)



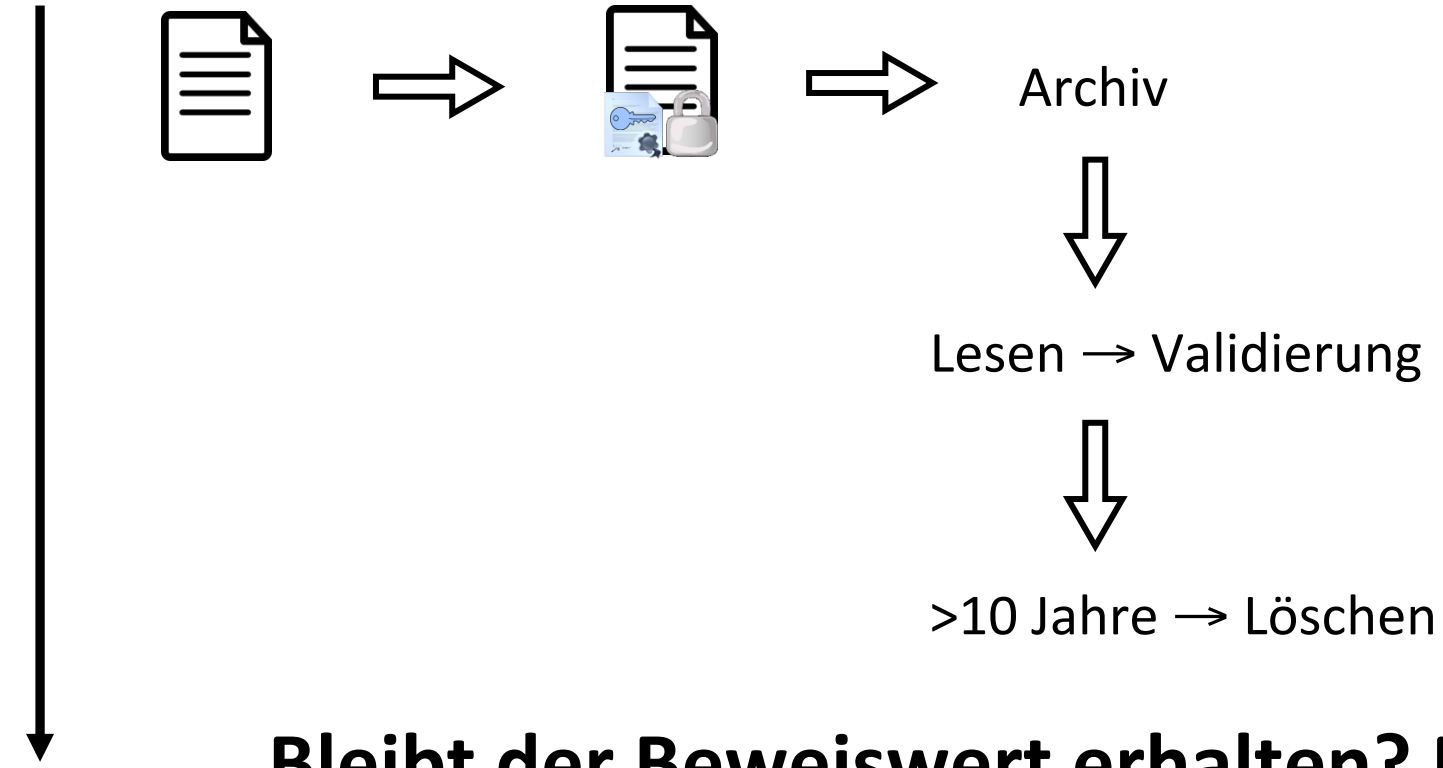
Signaturen in ELN-Systemen: kommerzielle ELNs

- kommerzielle ELNs sind Black-Box-Systeme
- keine Transparenz bei den Signatur-Algorithmen
  - Welche Signaturstufe wird benutzt?
- Wird beim Lesen von ELN-Einträgen die Signatur überprüft?
- Exportfunktionen im ELN:
  - meistens als PDF, html oder xml
  - aber: keine signierten Dokumente

→ Sie werden nicht in der Lage sein, E-Signaturen selbst zu überprüfen.

Archivierung von E-Dokumenten

Lebenszyklus eines signierten E-Dokumentes



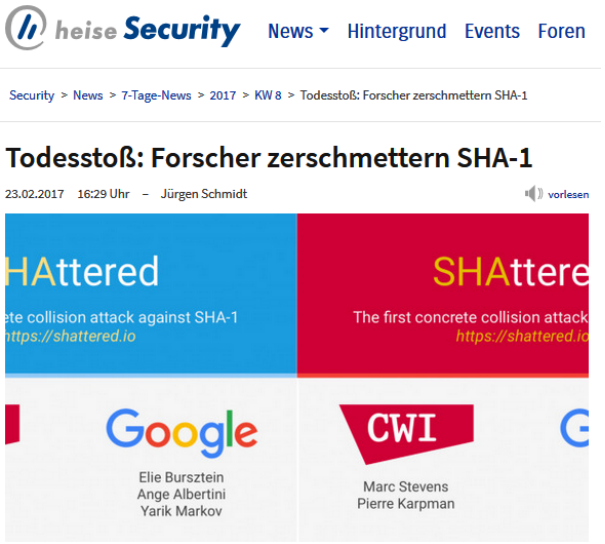
Bleibt der Beweiswert erhalten? Nein!

Archivierung von E-Dokumenten

Problem:

Signatur-Algorithmen werden angreifbar

- Schlüsselpaar
- Hashfunktionen




```
ju@ju-PC:~$ sha1sum shattered-*
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-2.pdf
ju@ju-PC:~$ sha256sum shattered-*
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0  shattered-1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff  shattered-2.pdf
ju@ju-PC:~$
```

„Mehr als 6500 CPU-Jahre und nochmal 100 GPU-Jahre erforderte die Berechnung dieser Kollision“

https://heise.de/-3633589

Archivierung von E-Dokumenten

Lösungen:

- geeignete Algorithmen: Empfehlungen des BSI

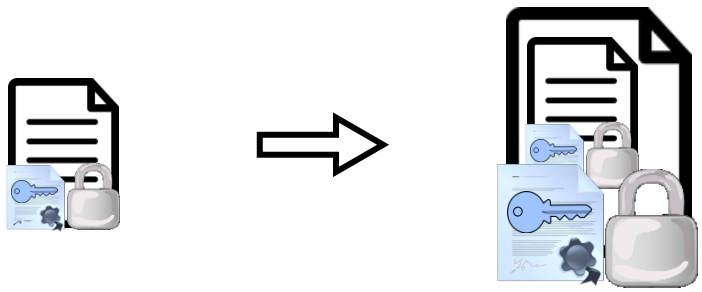
Hashfunktionen

Tabelle 6: Nicht mehr geeignete Hashfunktionen

Hashfunktion	geeignet bis
SHA-1	Ende Juni 2008* Ende 2010** Ende 2015***

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog2017_Entwurf.html

- Übersignieren



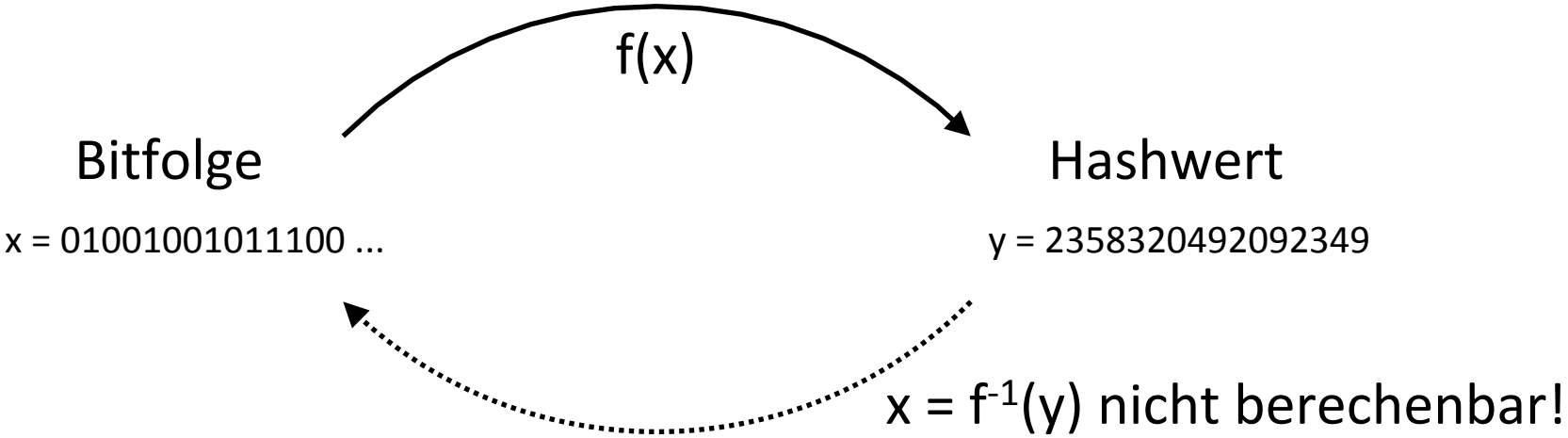
Zusammenfassung

- Unterschriften im Papier-Laborbuch
- juristische und technische Bewertung durch das BeLab-Projekt
- Sicherheits-/Usability-Perspektive: nur fortgeschrittene E-Signatur relevant
- kommerzielle ELN-Systeme sind Black-Boxes
- Langzeitarchivierung: proaktiv handeln

ISBN 978-3-8487-0706-5
http://www.belab-forschung.de

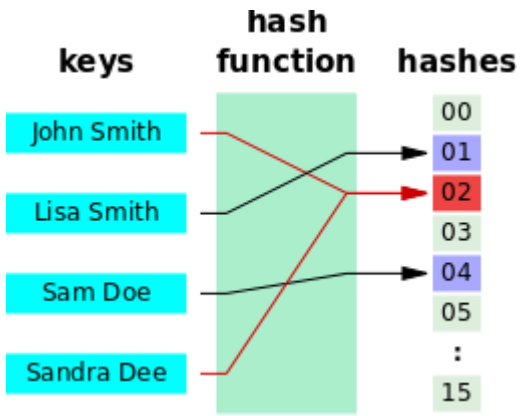
Vielen Dank für Ihre Aufmerksamkeit.

Hashfunktionen



- Kollisionsresistenz
- Chaos/Lawineneffekt:

  md5("Franz jagt im komplett verwahrlosten Taxi quer durch Bayern") = a3cca2b2aa1e3b5b3b5aad99a8529074
  md5("Frank jagt im komplett verwahrlosten Taxi quer durch Bayern") = 7e716d0e702df0505fc72e2b89467910



CC0, public domain

DFN-PKI

Woher bekomme ich persönliche Zertifikate für fortgeschrittene Signaturen?

- https://www.pki.dfn.de

Woher bekomme ich einen Zeitstempel?

- https://www.pki.dfn.de/zeitstempeldienst/
- mit Zertifikat!
- kein qualifizierter E-Zeitstempel

... fragen Sie Ihren IT-Administrator.