Wie können elektronische Siegel und Signaturen langfristig erhalten werden?

Maximilian Maede, Bundesarchiv Referat IT 4

Signatur - klassisch

Erhalt des Trägermediums
des Originals
=
Erhalt des Beweiswerts
durch Unterschrift oder Siegel

Elektronische Signaturen und Siegel verlieren über Zeit ihren Beweiswert.

Warum?

Anstieg der Rechenleistung von Computern

Moorsches Gesetz:

Die Anzahl der Transistoren in Mikrochips verdoppelt sich alle 2 Jahre!

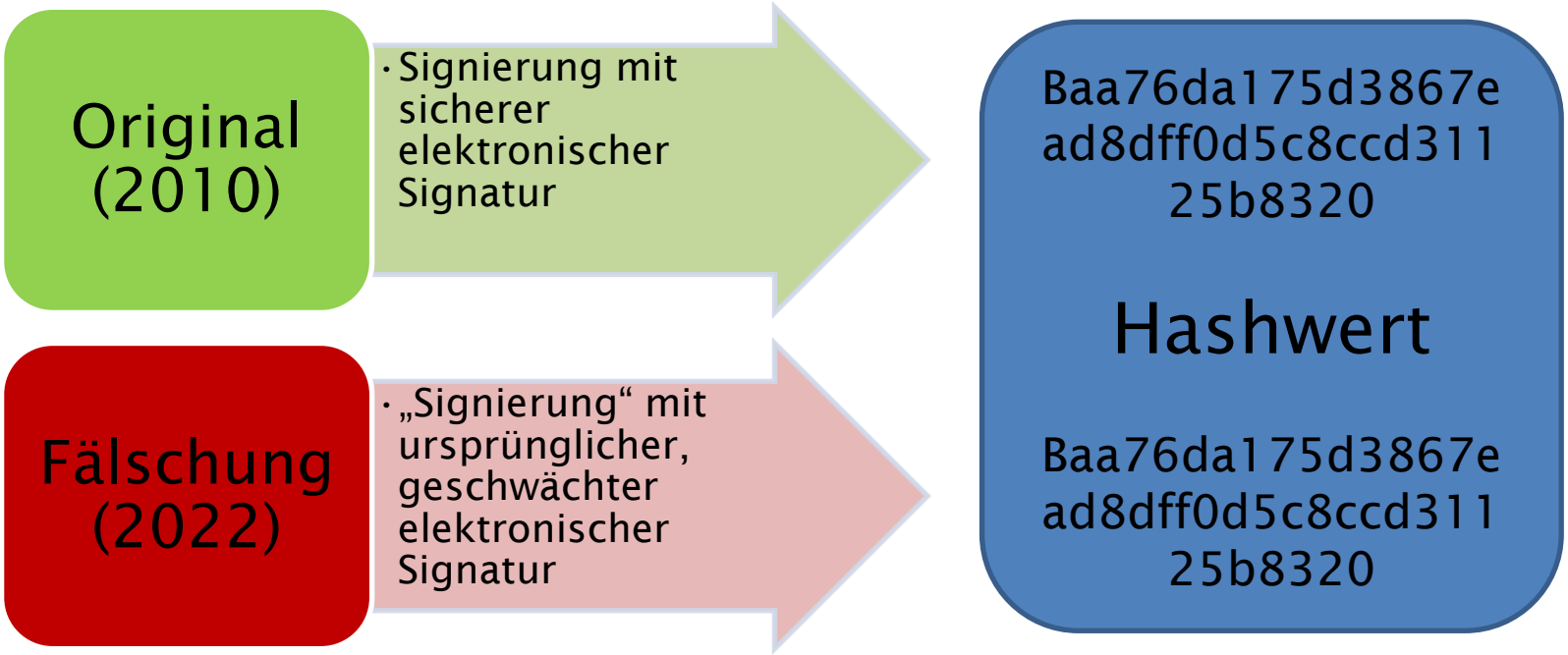
Die Gefahr ist nicht theoretisch!

2017 gab es eine erfolgreiche Kollisionsattacke auf den Hash Algorithmus SHA-1

Resultat: zwei PDF-Dokumente mit dem gleichen Hashwert konnten erzeugt werden.

Der Hashalgorithmus gilt seitdem nicht mehr als sicher und sollte durch einen Nachfolger ersetzt werden!

Folgen von unsicheren Signaturen



Schwächung des Signaturalgorithmus = Verlust der Datenintegrität

Was können wir tun?

Möglichkeiten zum Erhalt des Beweiswerts elektronischer Signaturen/Siegel

Ius Archivi:

Ein Archiv wird als „trusted custodian“ definiert. Aus diesem Archiv vorgelegten Dokumenten wird also grundsätzlich „Echtheit“ in dem Sinne attestiert, dass sie seit der Einlagerung nicht mehr verändert wurden.

Digitale Zeitstempel:

Technisches Mittel um festzustellen, dass ein elektronisches Dokument zu einem bestimmten Zeitpunkt vorgelegen hat.

Warum sind nur Zeitstempel eine Lösung ?

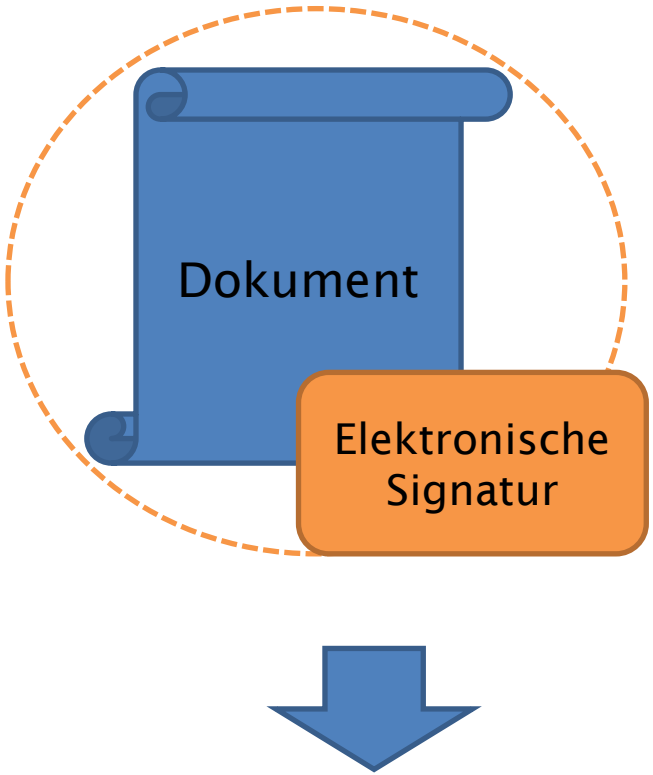
eIDAS – Verordnung Artikel 26

„[Eine elektronische Signatur] ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.“

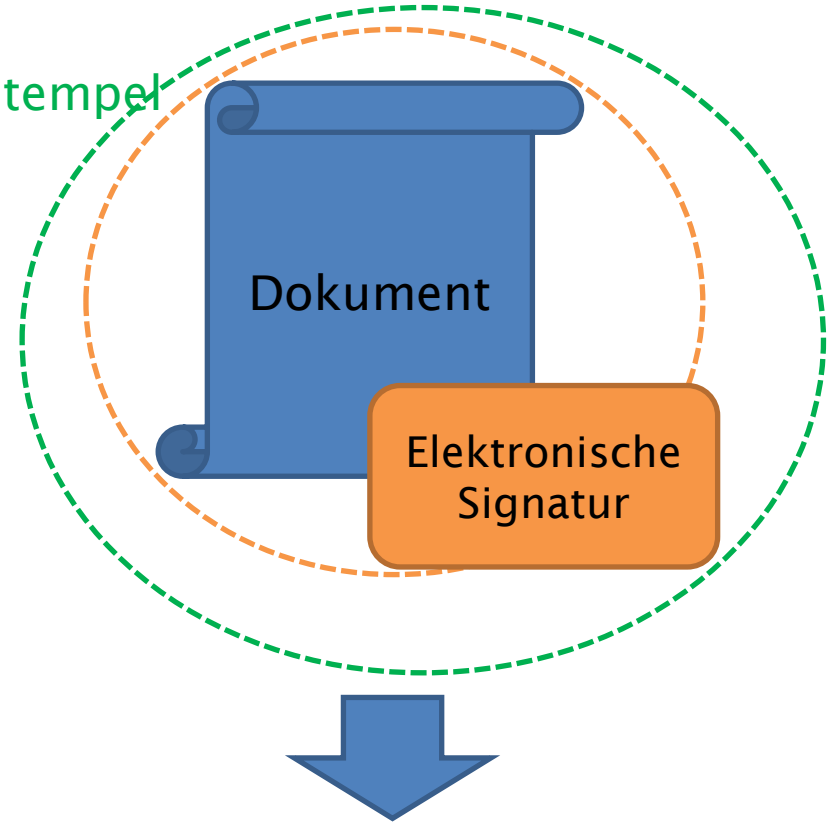
§ 15 Vertrauensdienstegesetz „Langfristige Beweiswerterhaltung“:

„Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen.“

Signatur - elektronisch

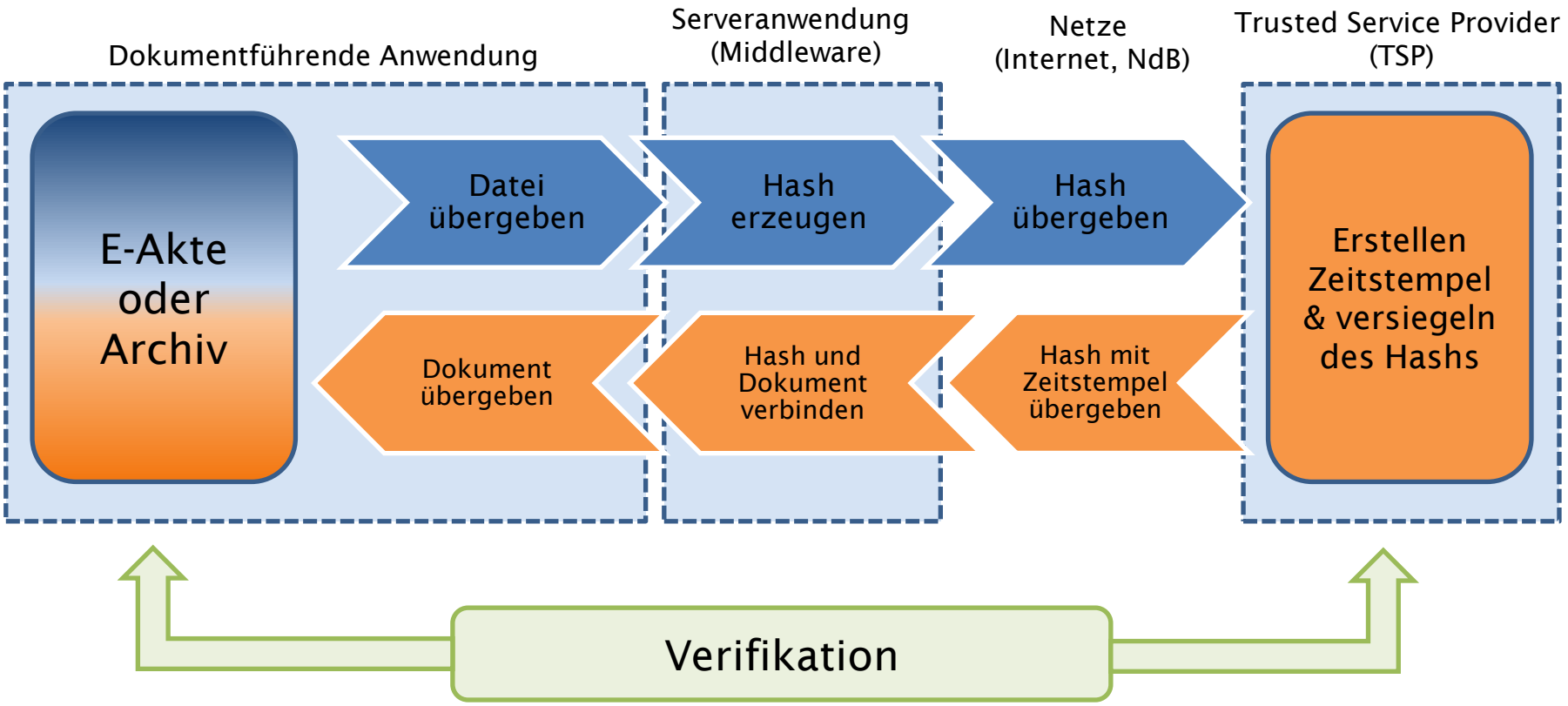


Authentizität und Integrität
(wer hat was unterschrieben)



Dokument und Signatur
haben zu Zeitpunkt X so existiert

Aufbringen eines Zeitstempels (schematisch)



Evidence Record im DZAB

- Evidence Record ist eine Datenstruktur zur Unterstützung der langfristigen Nicht-Abstreitbarkeit der Existenz signierter oder unsignierter Daten bzw. Dokumente.
- RFC 4998 konform (IETF Spezifikation)
- Verfahrensunabhängig

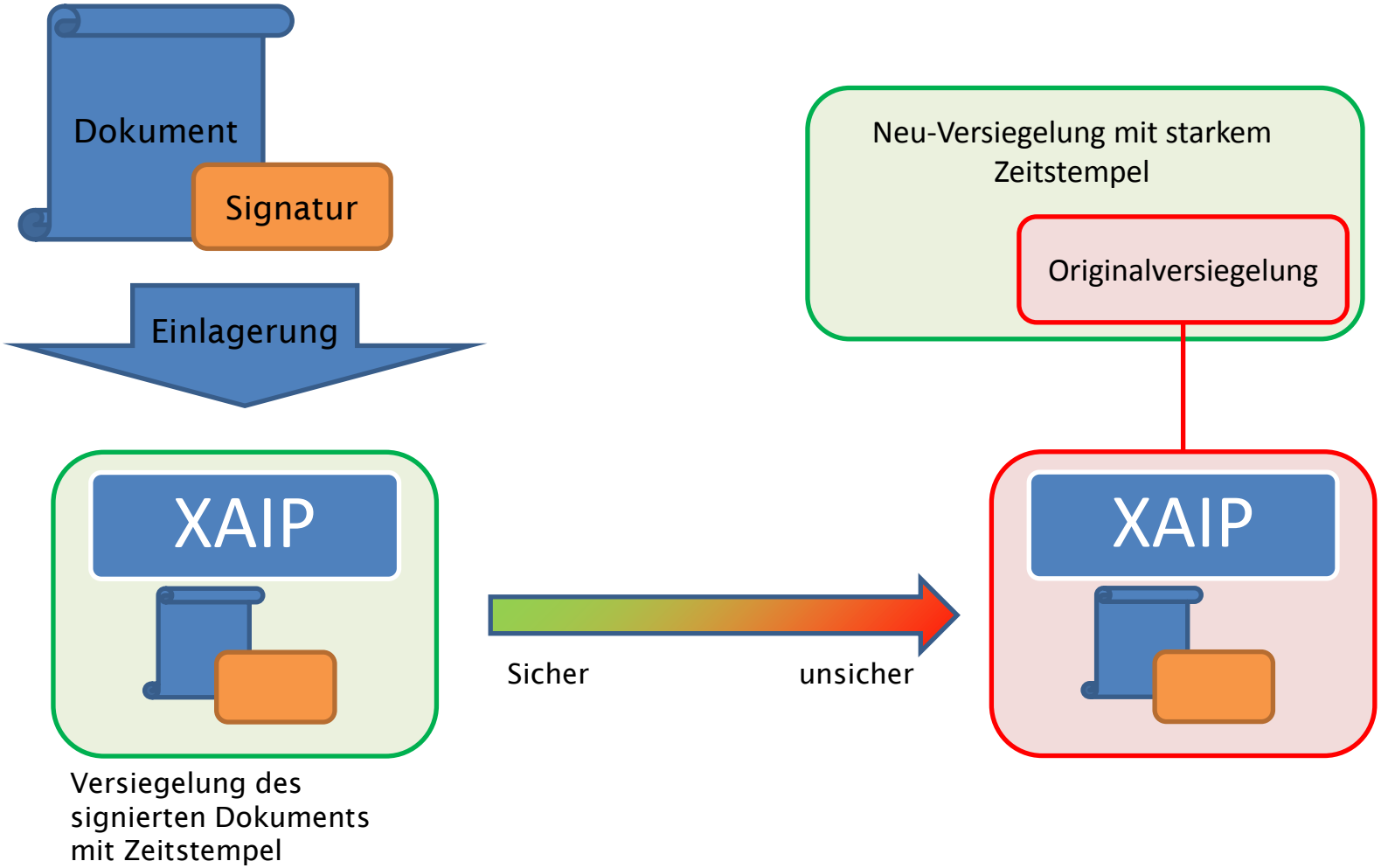
Was stellt er sicher ?

- Eine Zeitstempelkette trägt den Beweiswert (signierter) Inhaltsdateien
- stellt sicher, dass eingelagerte Daten vom Zeitpunkt der Einlagerung bis Zeitpunkt der Prüfung unverändert existiert haben (Langzeitevidenz)

Was stellt er nicht sicher ?

- Beweiswert der Daten an sich (andere Ebene, z.B. ungültig aufgebrachte Signaturen)

→ *„bad in, bad out“* das DZAB kann (fehlenden) Beweiswert nicht nachträglich „heilen“ oder herstellen.


Dokument
Signatur
Einlagerung
XAIP
Versiegelung des signierten Dokuments mit Zeitstempel
Sicher
unsicher
Neu-Versiegelung mit starkem Zeitstempel
Originalversiegelung
XAIP

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen ?

Imprint

Präsentation:

Titel:	Wie können elektronische Siegel und Signaturen langfristig erhalten werden?
vorgetragen von:	Maximilian Maede
vorgetragen am:	30.03.2022

Kontaktdaten:

Ansprechpartner/-in:	Maximilian Maede
Telefon:	0761 47817 848
Email:	m.maede@bundesarchiv.de
Anschrift:	Bundesarchiv Referat IT 4 Wiesentalstr. 10 79115 Freiburg