Beweiswerterhaltung

LTV vs. Beweiswerterhaltung (Übersignatur bei Algorithmen Bruch) – Gegenüberstellung

Die Beweiswerterhaltung elektronisch signierter Dokumente kann auf zwei Arten abgesichert werden:

1. **LTV (Long Term Validation)**
2. **Übersignatur / Resignatur bei Algorithmen Bruch (Beweiswerterhaltung)**

Beide Verfahren dienen dem **Erhalt der Beweis- und Prüfbarkeit**, aber sie adressieren **unterschiedliche Risiken**.

LTV – Schutz gegen den Verlust von Validierungsdaten

Ziel: Sicherstellung, dass eine Signatur auch in vielen Jahren noch prüfbar ist, selbst wenn Zertifikate ablaufen, Widerrufslisten verschwinden oder CAs nicht mehr existieren.

Wie LTV funktioniert:

- Embedding von Validierungsinformationen
  – OCSPAntworten, CRLs, Zertifikatsketten, Qualitätsstufe der Signatur
  – direkt im Dokument.
- Einbindung eines extern signierten Zeitstempels, der beweist, dass das Dokument *zu einem bestimmten Zeitpunkt* existierte

Damit ist das Dokument offline und unabhängig vom Signaturanbieter dauerhaft prüfbar.

Wogegen LTV schützt:

- Ausfall des OCSPServers / CA nicht mehr online
- Ablauf oder Widerruf von Zertifikaten
- Dokument muss Jahrzehnte gültig bleiben (z.B. Verträge, Archivgut)

Wogegen LTV *nicht* schützt:

- Kryptografischer Algorithmenbruch (z.B. RSA wird mathematisch angreifbar)
  Die eingebetteten Validierungsdaten sind dann ebenfalls nicht mehr beweisfähig.

Beweiswerterhaltung - Übersignatur – Schutz gegen einen zukünftigen Algorithmen Bruch

Ziel: Absicherung des Beweiswertes durch erneutes Signieren des Dokuments mit stärkeren oder neuen kryptografischen Verfahren, bevor das alte Verfahren kompromittiert wird.

Diese Maßnahme wird empfohlen, um die Signatur gegen einen zukünftigen kryptografischen Angriff zu „verlängern“ oder auf ein neues Sicherheitsniveau zu heben.

Warum nötig?

- LTV erhält nur die Validierungsdaten – aber wenn der Algorithmus selbst gebrochen wird, sind:
  - die ursprüngliche Signatur
  - die eingebetteten OCSPDaten
  - die Zertifikatsketten

> *kryptografisch nicht mehr vertrauenswürdig, eine erneute Signatur (Übersignatur) mit einem neuen, sicheren Verfahren stellt den Beweiswert wieder her.*

Verantwortlichkeit:

- Diejenige Stelle, die archiviert, ist auch verantwortlich dafür, rechtzeitig eine Übersignatur anzubringen.
  (Dies ergibt sich folgerichtig aus Archivanforderungen; die Quellen sagen dies nicht explizit, aber die Archivpraxis und LTVStandards setzen diese Rolle voraus.)

Direkte Gegenüberstellung

Aspekt	LTV (Long-Term Validation)	Übersignatur bei Algorithmen Bruch
Primäres Ziel	Prüfbarkeit über Jahrzehnte trotz Ablauf/Fehlen von Zertifikatsdaten	Erhalt der Krypto Sicherheit bei neuen Bedrohungen (z.B. Algorithmen Bruch)
Schützt gegen	Ablauf der Zertifikate, Ausfall der CA/OCSP, Widerrufsinformationen	Kryptografische Angriffe auf das ursprüngliche Signaturverfahren
Technik	Einbettung von Zertifikatsketten, OCSP, CRL, Zeitstempel ins Dokument	Neue Signatur mit stärkerem Algorithmus bzw. neuem Zertifikat
Aktiviert durch	Signatursoftware nach definierten ETSI Standards (z.B. PAdES LT)	Archivverantwortliche, sobald ein Verfahren als gefährdet gilt
Quellenbasis	LTV speichert Validierungsinfos im Dokument, Zeitstempel stützen LTV	Empfehlung im Kontext kryptografischer Sicherheit allgemein; nicht Bestandteil von LTV, daher zusätzliche Maßnahme

Fazit

LTV
stellt sicher, dass ein Dokument geprüft werden kann, weil alle Validierungsinformationen eingebettet sind. Es schützt jedoch *nicht* davor, dass der zugrunde liegende kryptografische Algorithmus irgendwann unsicher wird.

Übersignatur (Beweiswerterhaltung)
ist die notwendige Maßnahme, um genau dieses Risiko abzufangen:
Bevor ein Algorithmus bricht, muss das Dokument mit einem neuen, sicheren Verfahren erneut signiert werden.

Beide Maßnahmen ergänzen sich – LTV Schutz vor Algorithmen Bruch.