Bundesnetzagentur

Das dauerhaft prüfbare Verzeichnis für elektronische Vertrauensdienste (DAVE)

Dr. Axel Schmidt, Referent Elektronische Vertrauensdienste

eIDAS Summit

Berlin, 22.03.2018

Signatur in der analogen Welt

Prüfung einer Unterschrift:

(Beispielunterschrift)

(anno 1900)

Wer kann diese Unterschrift heute noch prüfen?

- → Es fehlt ein Vertrauensanker, der belegen kann, zu wem die Unterschrift gehört!
- → Unterschrift verliert Beweiswert

Prüfung einer elektronischen Signatur:

Das Zertifikat des Unterzeichners ist qualifiziert und gültig.

Die Signatur ist qualifiziert und gültig.

Prüfung derselben Signatur (einige Jahre später):

Das Zertifikat des Unterzeichners konnte nicht auf Gültigkeit überprüft werden.

Die Signatur ist ungültig.

Wo ist lange Prüfbarkeit erforderlich?

Was wird signiert?	Wer hat daran Interesse?
Grundbucheintragung	Eigentümer
Grundschuldeintragung	Bank
Testament	Erben
Handelsregistereintrag	Vertragspartner
eANV: Nachweis über korrekte Entsorgung gefährlicher Abfälle	Betreiber, Allgemeinheit

Erkenntnisse

Langfristige Prüfbarkeit stärkt:

- Dauerhafte Absicherung von Rechtsgeschäften
- Verlässlichkeit von Beurkundungen (z.B. Notar)
- Sicherung von Beweiswerten
- Vertrauen in digitale Transaktionen

Gesetzgeber reagiert:

- BeurkG § 39 a: auf Dauer prüfbares Zertifikat
- StandAG § 38: „Daten und Dokumente (...) dauerhaft gespeichert“
- weitere Fachgesetze (Aufbewahrungsfristen, E-Government)

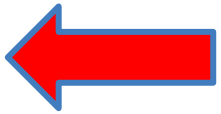
Prüfung einer Signatur:

Anwenderseite

Signatur: mathem. Prüfung

Anbieterseite

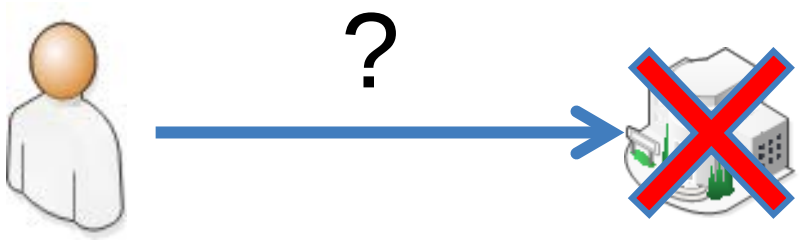
Zertifikat: Existenz, Sperrstatus



Vertrauensliste

Anbieter: Vertrauensstatus

Betriebseinstellung des Anbieters



Anbieterseite

Zertifikat: Existenz, Sperrstatus

→ i.A. keine Prüfung mehr möglich

→ Verlässlichkeit der Unterschrift abhängig von Existenz des Anbieters

DAVE: Dauerhaftes Verzeichnis

Lösungsansatz: DAVE (DAuerhaftes VErzeichnis)

- Sicherung der Vertrauensinfrastruktur betriebseingestellter Anbieter (Datenübernahme)
- Bereitstellung von
  - Zertifikaten
  - Sperrstatus
- Betrieb bei der Bundesnetzagentur
- Staatlicher Vertrauensanker (Ewigkeitsgarantie)
- Ermöglicht dauerhafte Prüfung

DAVE: Rechtliche Grundlage

- SigG/SigV: Aufbewahrung mind. 30 Jahre
- eIDAS: „Dienstekontinuität“ gefordert (Art. 24), aber keine konkreten Vorgaben („Beendigungsplan“)
- VDG: Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit (§ 16)

DAVE: Technische Umsetzung

- Auskunft
  - Zertifikate (via http statt LDAP)
  - Statusauskunft (OCSP) mit statischer Signatur, nach Möglichkeit Erhalt der Anbietersignatur
  - Bei Bedarf werden OCSP-Signaturen neu ausgestellt oder Zeitstempel aufgebracht
  - Weitgehend aufwandlos auf Anwenderseite: Automatische DNS-Umleitung auf DAVE (OCSP)
- Langfristige Sicherheit (Algorithmen)
  - Überwachung der Algorithmen
  - Schutz bzw. Erneuerung der Signaturen
- Sicherer und hochverfügbarer Betrieb im Rechenzentrum der Bundesnetzagentur

DAVE: Technische Herausforderungen

- Automatische Umleitung der Anfragen auf DAVE nicht immer möglich (Unterstützung durch Anwenderkomponenten, Vertrauensliste)
- Konformität zu Standards:
  Prüfung von „fremder“ OCSP-Signatur problematisch (RFC 6960)

→ Mittelfristige Anforderungen:

- Autorisierung über Vertrauensliste
  (service supply point in ETSI TS 119 612)
- Aktuelle ETSI-Standards treffen bereits Vorkehrungen für Übernahme
  (ETSI EN 319 411-2: LastCRL, nextUpdate, ArchiveCutOff)

Ausblick

- Anpassung technischer Standards (ETSI, RFC)
- Elektronischer Algorithmenkatalog
  (auch nutzbar für anwenderseitige Absicherung)
- Auswertung der Praxiserfahrungen
  (u.a. Anwenderkomponenten)
- Neue Technologien

Bundesnetzagentur

Dr. Axel Schmidt
Referent Elektronische Vertrauensdienste

+49 6131 18-0
eidas@bnetza.de