Lösungen im digitalen Binnenmarkt: Siegel, Zeitstempel und Signaturen

BITKOM eIDAS Summit

08.11.2016, Berlin

Tatami Michalek, Geschäftsführer secrypt GmbH

secrypt GmbH
Bessemerstr. 82
12103 Berlin
Germany

Tel.: +49 (0)30 756 59 78-0
Fax: +49 (0)30 756 59 78-18
mail@secrypt.de
www.secrypt.de

Neue Verfahren gemäß eIDAS-VO

u.a.

1. E-Siegel
2. Zeitstempel
3. Fernsignatur

gemäß eIDAS-VO: „Verordnung (EU) über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“
(**e**lektronische **Id**entifizierung, **A**uthentifizierung und **S**ignaturen)

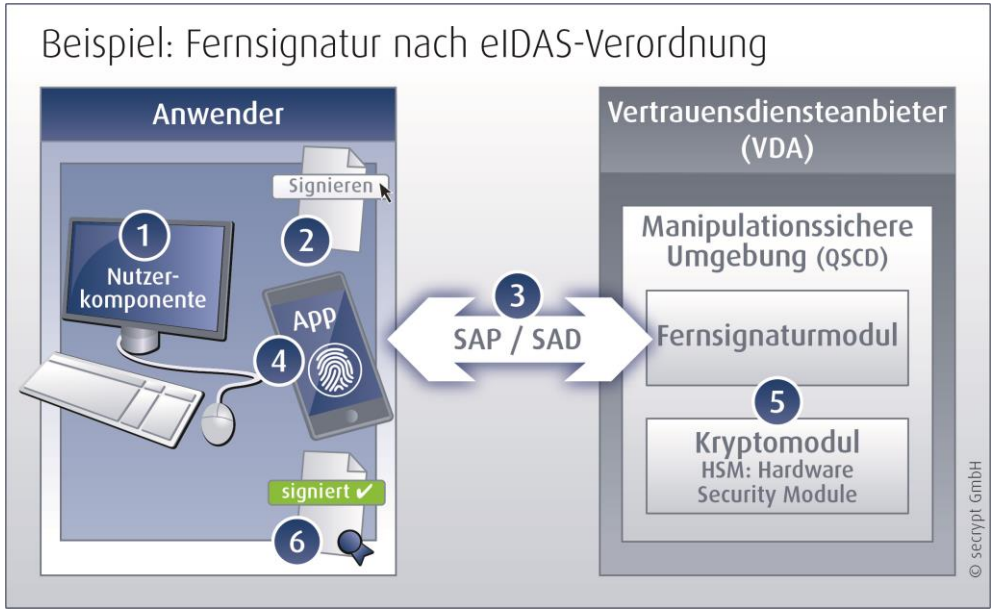
- Seit 18.09.2014 in Kraft, ihre materiellen Vorschriften gelten ab 1. Juli 2016 unmittelbar
- Sie hebt die EU-Signatur-Richtlinie 1999/93/EG auf
- Die eIDAS-VO sorgt für:
  - einheitliche europäische Regelungen für elektronische Signaturen, Siegel und Zeitstempel – sogenannte Vertrauensdienste
  - Interoperabilität im neu geschaffenen digitalen Binnenmarkt und Vertrauensraum

Fernsignatur – Der Rahmen

- Motivation: Realisierung vielfältiger wirtschaftlicher Vorteile
  (siehe Erwägungsgrund Nr. 52 eIDAS-VO)
- Signaturschlüssel wird zentral bei Vertrauensdiensteanbieter (Trustcenter) in einer sicheren Signaturerstellungseinheit (HSM: Hardware Security Module) gespeichert
- Ziel: Steigerung des Komforts durch Verzicht auf Signaturkarte und Lesegerät
- Authentifizierung des Unterzeichners durch zwei Faktoren unterschiedlicher Kategorie (z.B. Besitz, Wissen, Biometrie) und Übertragung über zwei unterschiedliche Interfaces und Kanäle (Normentwurf „Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen DIN CEN/TS 419241-1“)
- Sorgfaltspflicht des Signierenden gewinnt an Bedeutung (z.B. bei Phishing-Angriffen)
- Anwendungen: Online-Vertragsabschlüsse bei Schriftformerfordernis oder hohem Beweiswertbedürfnis, z.B. Kreditverträge, hochvolumige Kaufverträge (Immobilien etc.)

Fernsignatur – Der Rahmen

1. Nutzer öffnet eine Signatur-anwendung (Nutzerkomponente) und meldet sich mit Benutzer-name und Passwort (Faktor 1) an
2. Anschließend markiert er ein Dokument und betätigt Schaltfläche "Signieren"
3. Das Dokument wird zusammen mit weiteren Daten zum Schutz der Transaktion (SAD) über einen sicheren Kommunikationskanal (SAP) an den VDA gesendet



4. VDA startet Authentifizierungsanfrage und Anwender authentifiziert sich z.B. mittels Fingerabdruck (Faktor 2) über eine App auf seinem Smartphone (Kanal 2)
5. Bei erfolgreicher Authentifizierung wird Dokument mit beim VDA hinterlegten Signaturschlüssel signiert und
6. an die Nutzerkomponente des Anwenders gesendet

SAD: Signaturaktivierungsdaten
SAP: Signaturaktivierungsprotokoll

E-Siegel – Der Rahmen

- elektronisches Siegel (Organisationszertifikat, digitaler Unternehmensstempel)
- Inhaber des Siegelzertifikates ist eine juristische Person, z.B. eine GmbH, AG, AöR (eIDAS-VO Erwägungsgrund 59)

(59) Elektronische Siegel sollten als Nachweis dafür dienen, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde, und sollten den Ursprung und die Unversehrtheit des Dokuments belegen.

- Zwei Sicherheitsniveaus: Fortgeschrittenes und qualifiziertes elektronisches Siegel
- Beweiswert qualifiziertes Siegel: Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten“ (Art. 35 Abs. 2 eIDAS-VO)
- Anwendungen: Elektronische Siegelung (ggfs. zzgl. Zeitstempel) z.B. von Kontoauszügen, Gesprächsmitschnitten (Audiofiles), Auskünften, Bescheiden, Beglaubigungen, Urkunden, Zeugnissen, Unternehmenssteuererklärungen, Rechnungen, Angeboten (E-Vergabe), …

Lösungswelt

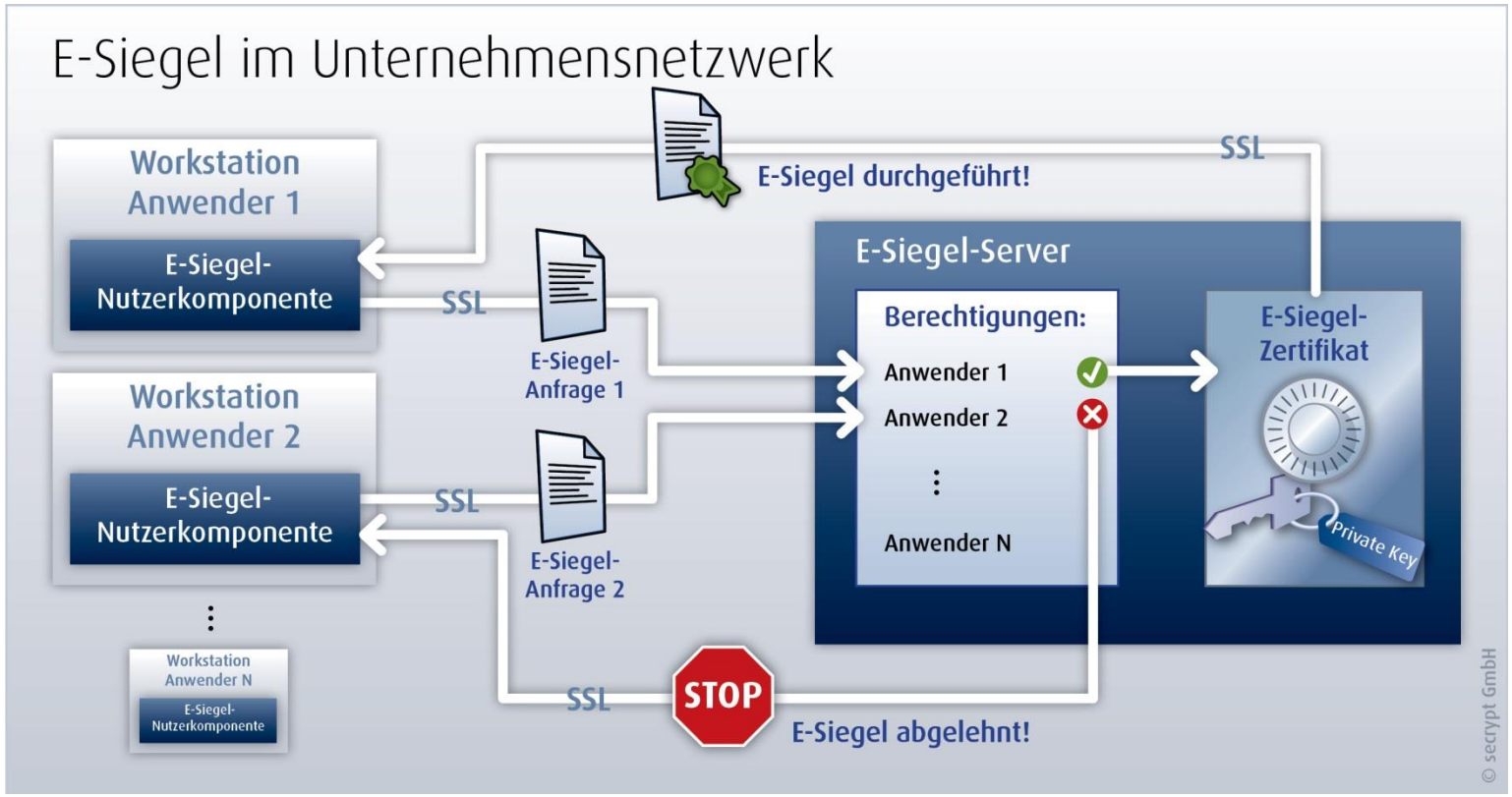
Manuelle Nutzung am Client (Arbeitsplatzrechner, Laptop, Tablet, Mobile Device)

- Stand-alone Clientsoftware für versierte Anwender
  für E-Siegeln (auch auf Karte), Zeitstempeln und Fernsignieren
  bei Bedarf integriert in DMS, Fachsoftware, Archiv etc.

- „Echte“ Web- / Browseranwendungen für Fernsignatur (ohne Plugins)
  bzw. Plattform-Lösungen für das „Signieren auf dem Sofa“
  mit Abbildung der gesamten Prozesskette:
  1. Identifizieren (Video-Ident)
  2. Registrieren
  3. Signaturzertifikat erzeugen (Adhoc oder dauerhaft)
  4. Signieren
  5. Verifizieren
  6. Bezahlen
  7. Archivieren

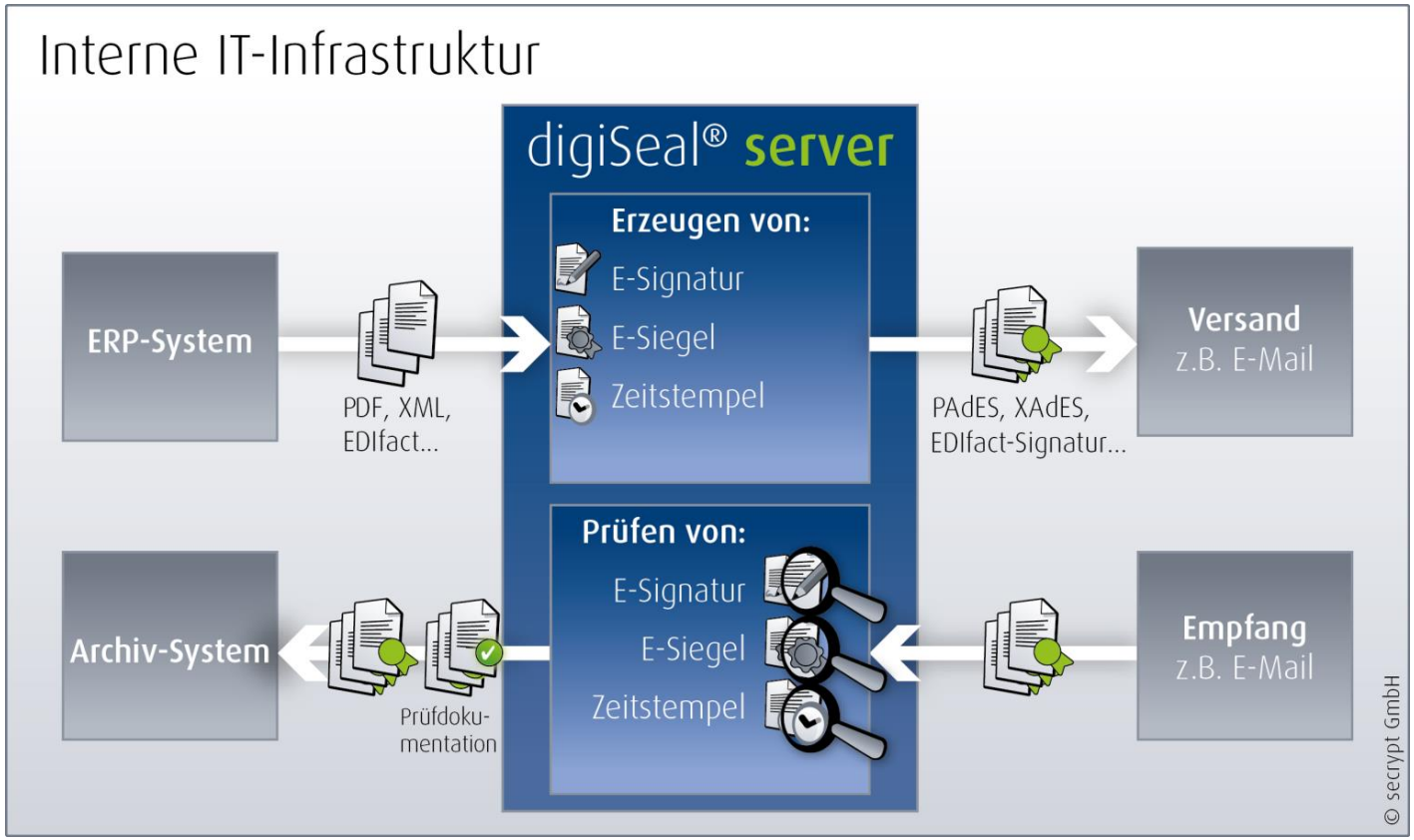
Lösungswelt

Zentrales E-Siegel dezentral am Client auslösen



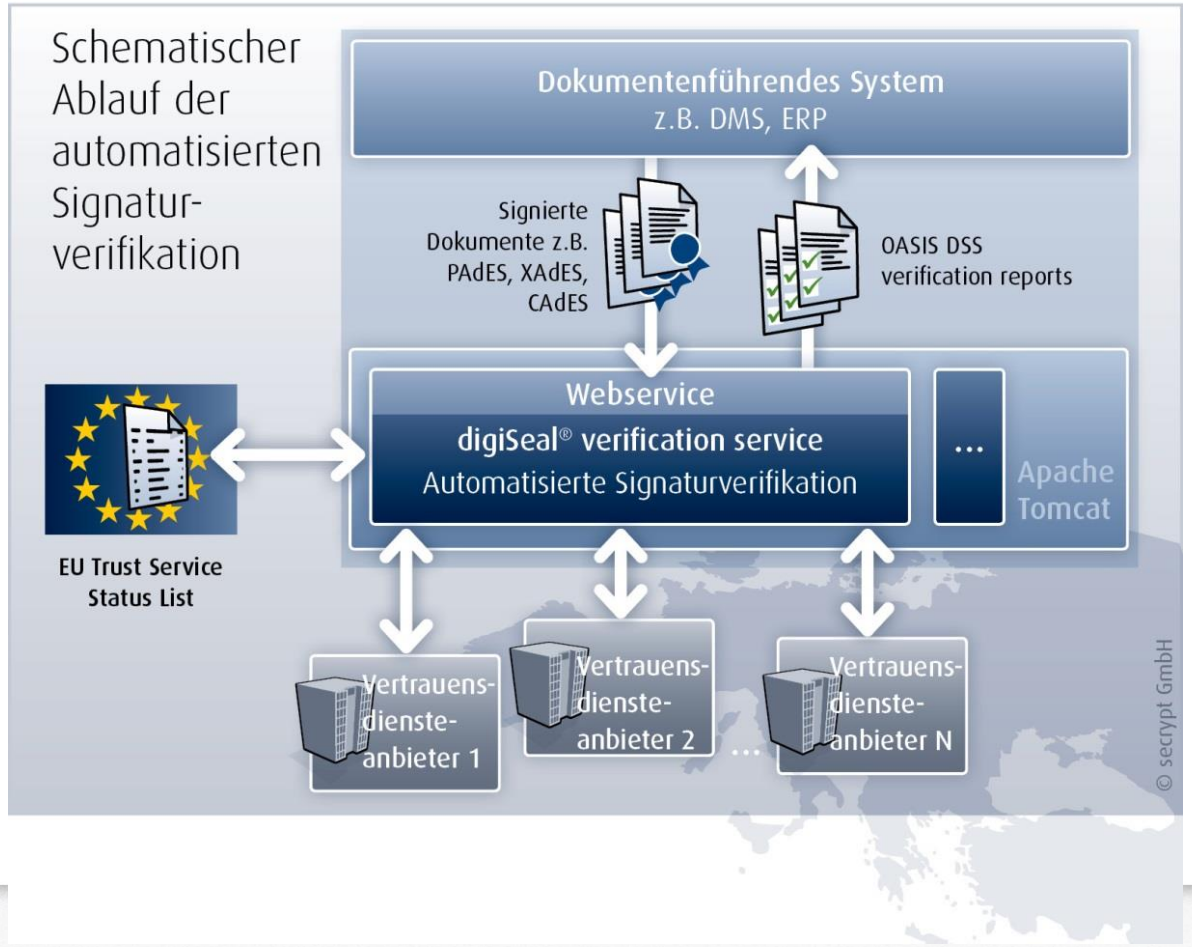
Lösungswelt

Automatisierte serverbasierte Nutzung



Lösungswelt

Nach dem Signieren kommt das Verifizieren



Randbemerkung:

EU-weit einheitlich geregelt, aber…

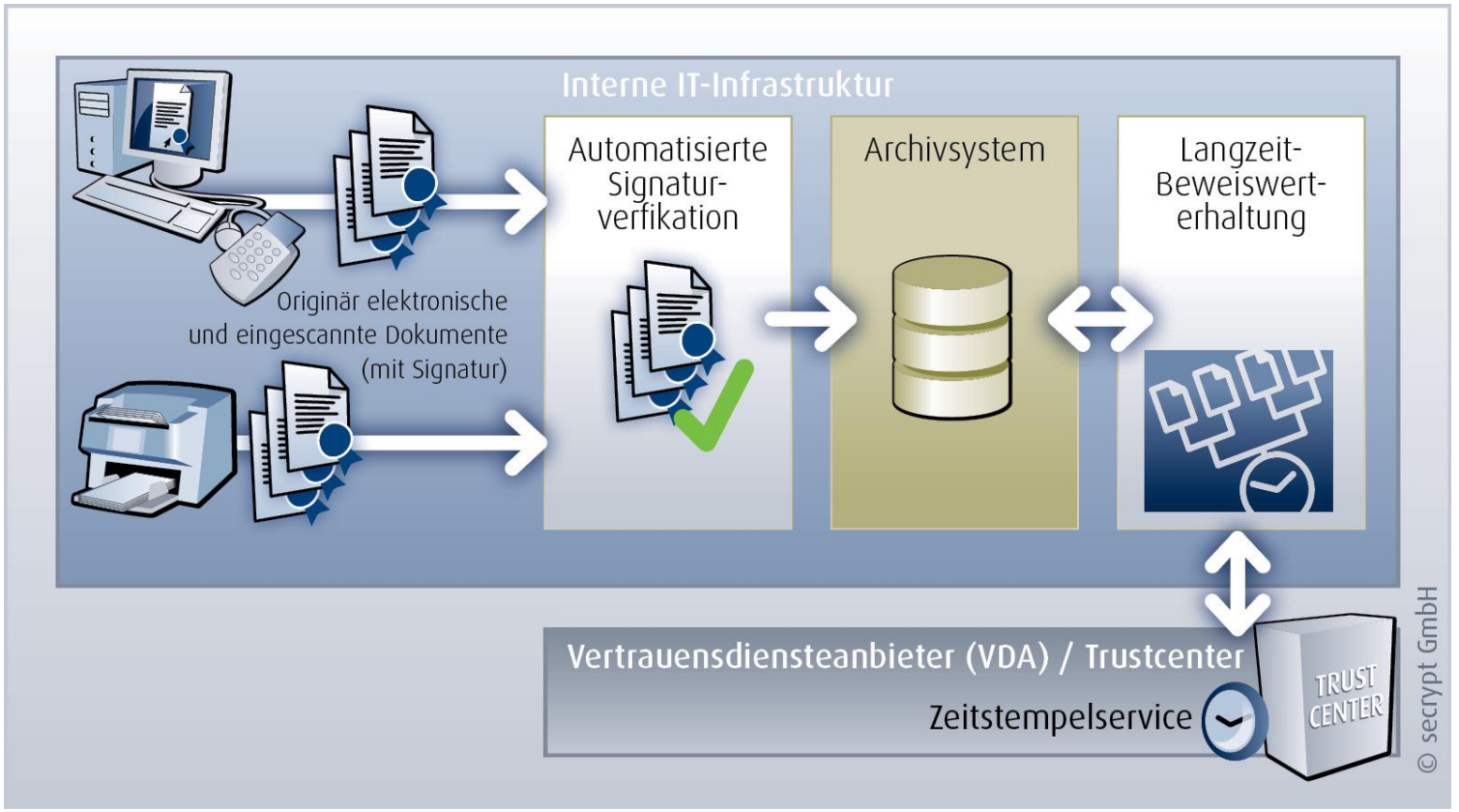
… kein einheitlicher und verbindlicher Algorithmenkatalog

… keine einheitliche Festlegung des Prüfmodells (Kette oder Schale)

→ Verifikationslösung muss dies berücksichtigen und entsprechend konfigurierbar sein

Lösungswelt

Nach dem Verifizieren kommt das Archivieren (Langzeit-Beweiswerterhaltung)



Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit.

Wir sind jederzeit gern für Sie da.

E-Mail: mail@secrypt.de
Tel.: +49 (30) 756 59 78-0
Fax: +49 (30) 756 59 78-18
Internet: www.secrypt.de