Elektronische Fernsignatur mittels Smartphone gemäß neuer EU-Verordnung eIDAS

conhIT-Satellitenveranstaltung 2016
von GMDS und BVMI

18.04.2016, 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

Status Quo

Die „qualifizierte“ elektronische Signatur ersetzt die handschriftliche Unterschrift
(§ 126a BGB Elektronische Form)

- Sie gewährleistet Integrität und Authentizität der signierten Dokumente
- Sie ist ausschließlich dem Signaturschlüsselinhaber zugeordnet
- Sie ermöglicht die Identifizierung des Signaturschlüsselinhabers
- Sie muss mit einer sicheren Signaturerstellungseinheit (Signaturkarte) erzeugt werden
- Sie wird von einem Trustcenter ausgegeben,
  z.B. D-TRUST (Tochter der Bundesdruckerei)
- Grundlage: Signaturgesetz (SigG) und Signaturverordnung (SigV)
  ab 2016: eIDAS (EU-Verordnung) ersetzt SigG

eIDAS-VO bietet neue Wege

eIDAS-VO: „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“

- Sie schafft ab 01.07.2016 europaweit standardisierte rechtliche und technische Rahmenbedingungen
- Ein in der EU qualifiziert elektronisch signiertes Dokument muss dann in jedem Mitgliedsstaat anerkannt werden
- Es werden neue Signaturverfahren definiert (Fernsignatur, elektronisches Siegel)
- Motivation für Fernsignatur: Realisierung vielfältiger wirtschaftlicher Vorteile (siehe Erwägungsgrund Nr. 52 eIDAS-VO)

Neuer Ansatz zum Schutz des Signaturschlüssels

Wo wird der Signaturschlüssel bei der Fernsignatur gespeichert?

- eIDAS-VO ändert Anforderungen in Bezug auf die Speicherung des privaten Signaturschlüssels
- Schlüssel nicht mehr im unmittelbaren Besitz des Signierenden (bisher: Signaturkarte mit Kryptochip)
- Fernsignatur: Zentrale Speicherung bei Vertrauensdiensteanbieter (VDA; Trustcenter) in einer sicheren Signaturerstellungseinheit (HSM: Hardware Security Module)
- VDA muss hohe Auflagen erfüllen (Zertifizierung, regelmäßige Auditierung, Überwachung durch Aufsichtsbehörde)
- Steigerung des Komforts durch Verzicht auf Signaturkarte und Lesegerät

Möglichkeiten der Fernsignatur

Entwicklung der Fernsignatur an einem Scheideweg

- Wird sie komfortabel nutzbar sein, aber dafür an Sicherheit einbüßen?
- Oder führt eine hochsichere Ausgestaltung zur „Nicht-Nutzbarkeit“ und zur Ablehnung durch den Anwender?
- Gratwanderung des für die Ausgestaltung verantwortlichen Europäische Komitees für Normung (CEN: Comité Européen de Normalisation):
  Ausreichender Komfort versus notwendiger Sicherheit

Sicherheit durch 2-Faktor-Authentifizierung

Normentwurf „Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen DIN CEN/TS 419241-1“

- Authentifizierung des Unterzeichners durch zwei Faktoren unterschiedlicher Kategorie (z.B. Besitz, Wissen, Biometrie)
- Übertragung der beiden Faktoren muss über zwei unterschiedliche Interfaces und Kanäle erfolgen
- Erst nach der Authentifizierung kann der Signaturschlüsselinhaber auf seinen privaten Schlüssel zugreifen
- Datentransport zwischen Anwender und Vertrauensdiensteanbieter (VDA):
  - Sicherer Kommunikationskanal (SAP: Signaturaktivierungsprotokoll)
  - Daten zum Schutz der Transaktion (SAD: Signaturaktivierungsdaten)

Biometrie als PIN-Ersatz

Beispiel

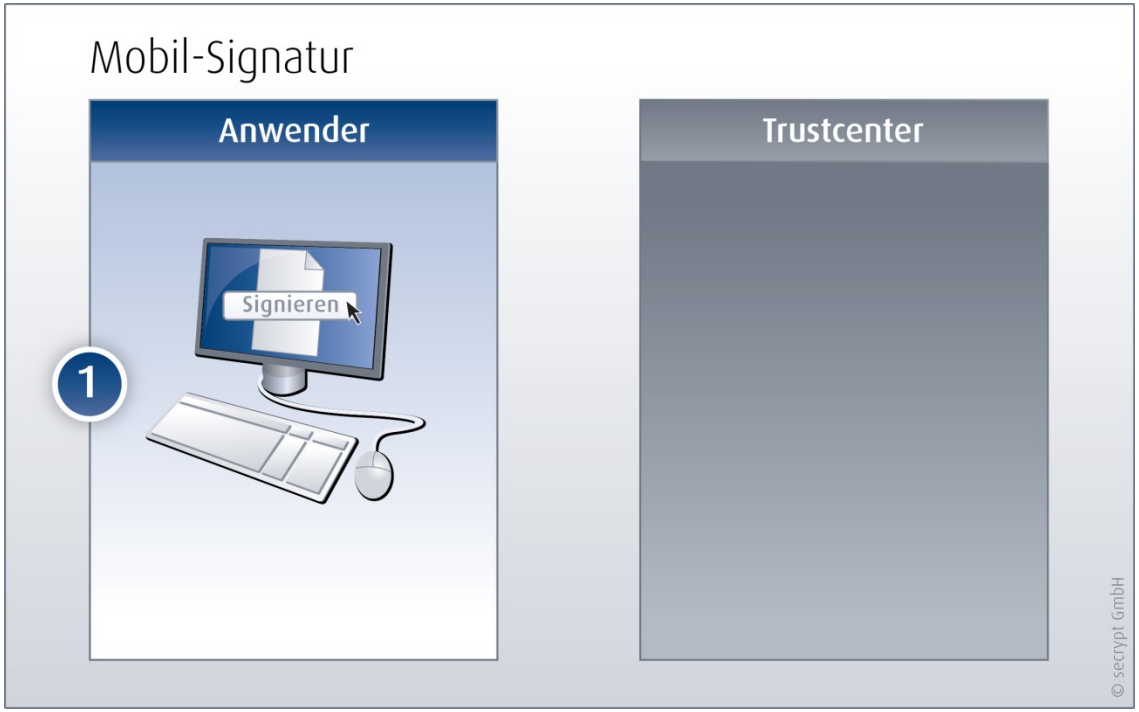
- Faktor 1: Anmeldung per Benutzername und Passwort über Kanal 1 (z.B. Workstation)
- Faktor 2: Kryptographische Authentisierung über Kanal 2 (z.B. Fingerabdruck, mTAN oder PIN-Eingabe via Smartphone)
- Sorgfaltspflicht des Signierenden gewinnt an Bedeutung (z.B. bei mTAN)

Unterschrift mit Smartphone

Schritt 1:

Anwender meldet sich (Faktor 1) an seiner Workstation an (Kanal 1)

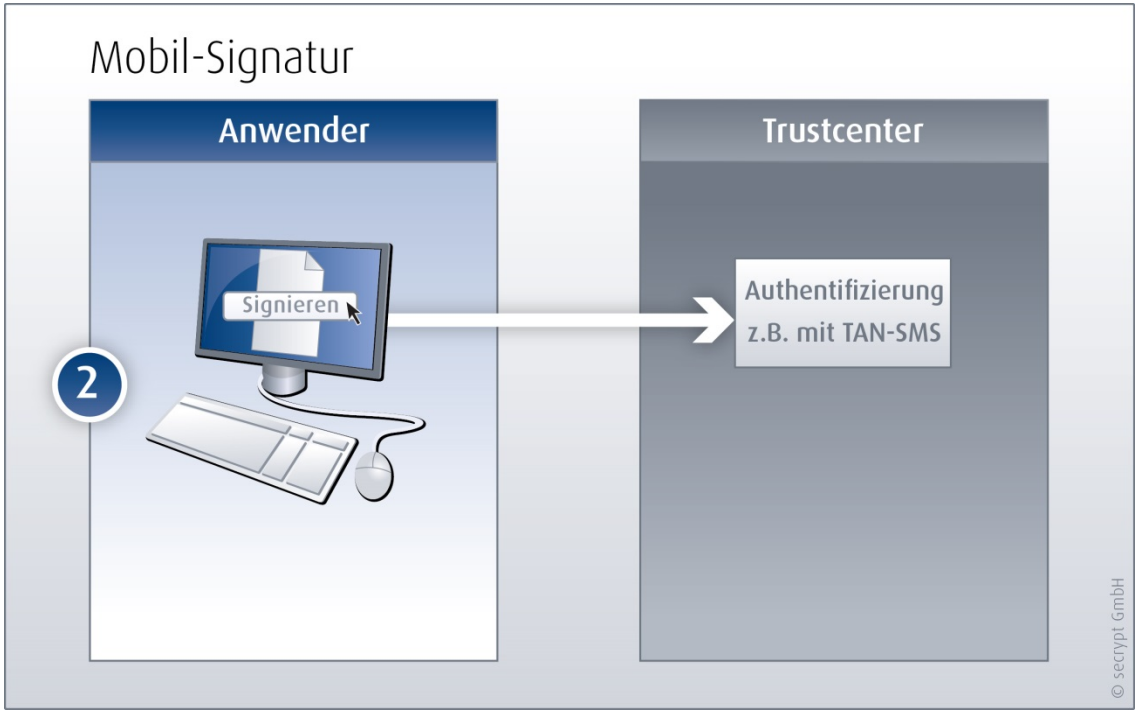
Er öffnet Dokument, z.B. im DMS, und betätigt „Signieren“-Button



Unterschrift mit Smartphone

Schritt 2:

Signaturanfrage beim Trustcenter und Start der Authentifizierung, z.B. mit mTAN-SMS (Faktor 2)

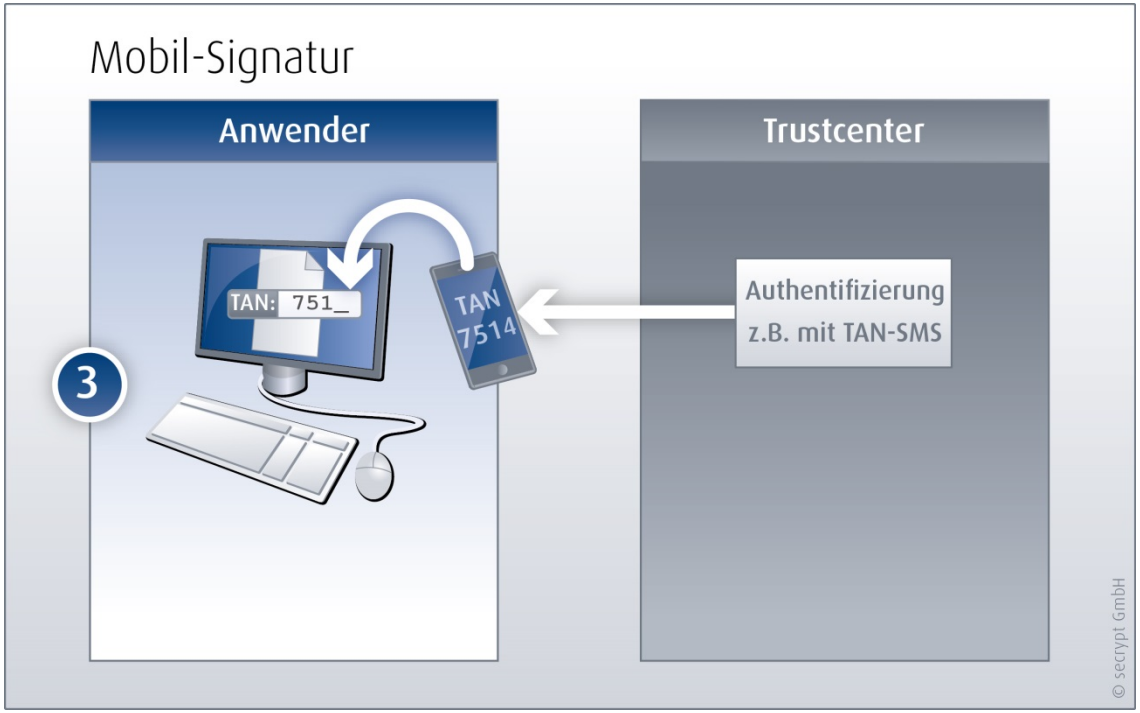


Unterschrift mit Smartphone

Schritt 3:

Trustcenter schickt Anfrage zur Authentifizierung an Mobilnummer (Kanal 2)

Anwender gibt mTAN zur Signaturfreigabe am Arbeitsbildschirm ein

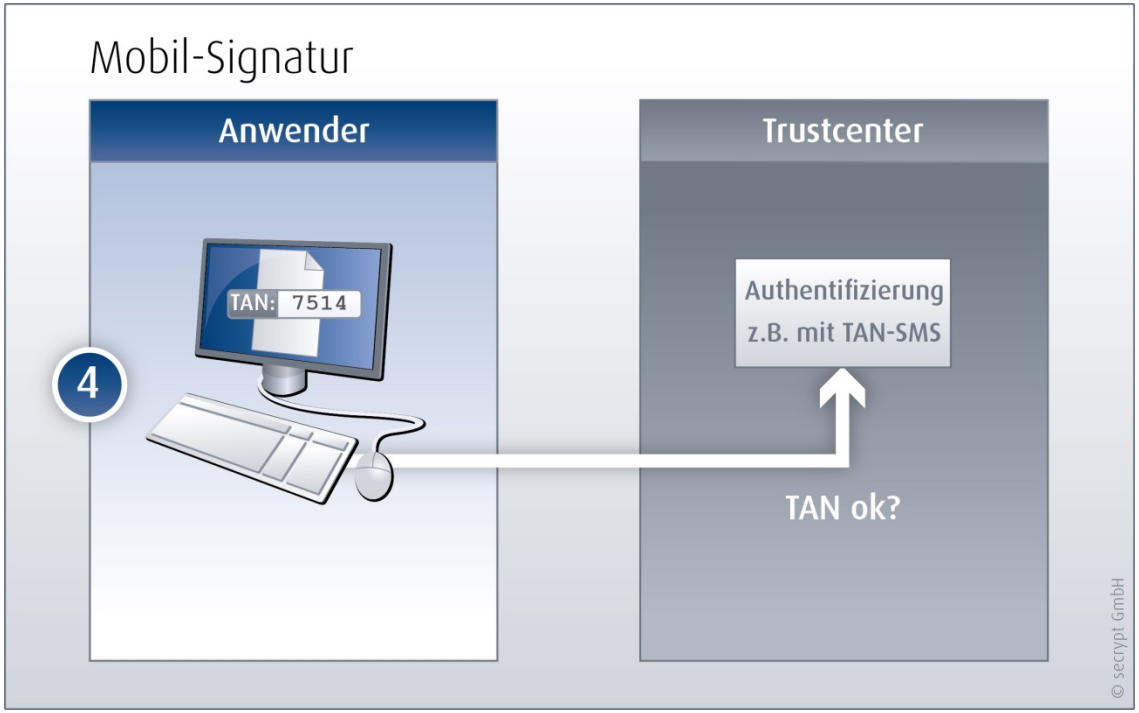


Unterschrift mit Smartphone

Schritt 4:

Trustcenter prüft Eingabe

Ist die mTAN korrekt?

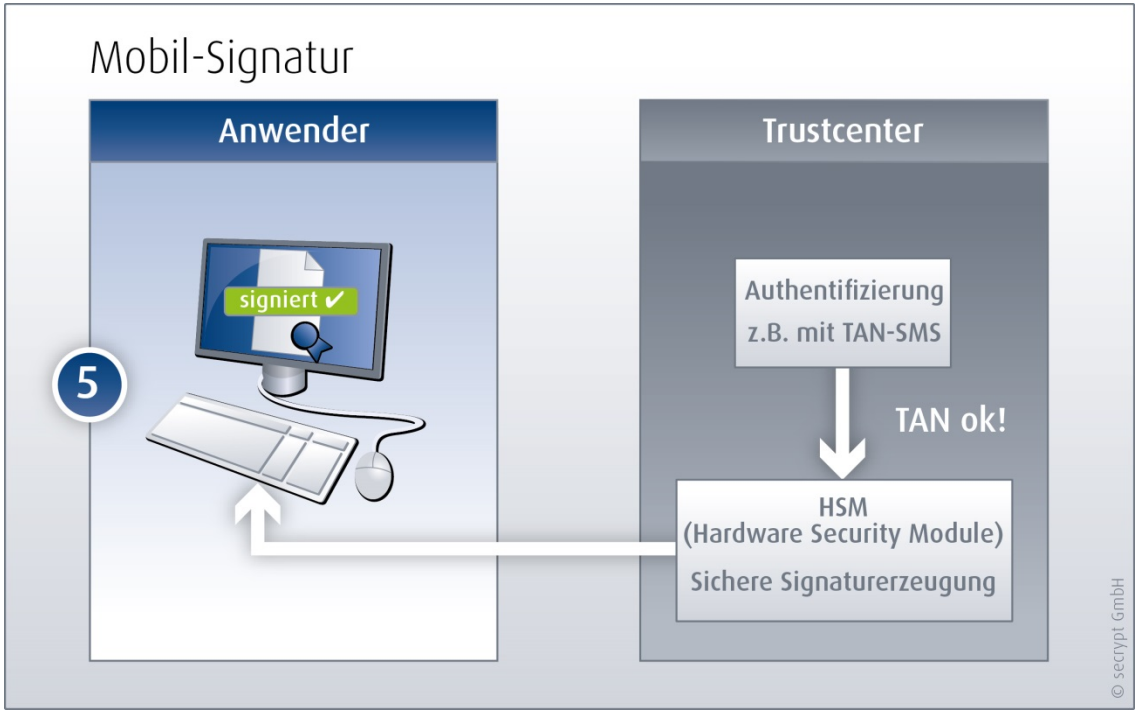


Unterschrift mit Smartphone

Schritt 5:

Trustcenter erzeugt die Signatur und übermittelt sie an den Anwender

Das Dokument ist signiert



Keine zusätzliche Hardware am Arbeitsplatz erforderlich

Vielen Dank für Ihre Aufmerksamkeit!

Wir sind jederzeit gern für Sie da.

conhIT
19.–21. April 2016
Connecting Healthcare IT

Halle 1.2, Stand D-106 (bei synedra)

Themen: Elektronische Siegel, Handy-Signatur, Arztbriefsignatur, Patientenaufnahme mit Unterschrift-Tablet, Signatur im KIS und Archiv…

Aktuelles White Paper

„Elektronische Signaturen im Gesundheitswesen“