
Die elektronische Signatur und ihre Verwendung beim elektronischen Abfallbegleitschein

Elektronische Signatur

1. Definition und Funktion: Integrität und Authentizität
2. Arten von Signaturen und Attributzertifikate
3. Rechtliche Bedeutung und Rahmenbedingungen
4. Elektronisch signieren in der Praxis und Sicherheitsvorkehrungen
5. Einsatz der elektronischen Signatur beim eANV
6. Bezug
7. Weitere Anwendungsmöglichkeiten

Elektronische Signatur:

- eine Art digitales Siegel
- Ersatz einer persönlichen Unterschrift
- statt Papier und Stift: mathematisches Verfahren
- ist einer elektronischen Datei beigefügt oder logisch mit ihr verknüpft
- schwer zu fälschen
- keine Verschlüsselung der signierten Datei!!!



Funktion der elektronischen Signatur:

1. Echtheit des Inhalts

Die Nachricht kommt so beim Empfänger an, wie der Absender sie unterschrieben hat. Ein verschlüsselter Hashcode (digitaler Fingerabdruck) weist nach, dass die Datei nach Signierung nicht mehr verändert wurde.

2. Echtheit des Absenders

Der Absender der Nachricht ist eindeutig und rechtsverbindlich nachvollziehbar. Ein Zertifikat belegt, dass die Identität der unterzeichnenden Person geprüft wurde.

3. Verifizierung

Empfänger kann überprüfen:

Unversehrtheit der Datei (1.)

=> **Integrität**

Identität des Absenders (2.)

=> **Authentizität**

PKI = Public-Key-Infrastructure

Jedem User wird ein individuelles Schlüsselpaar zugeordnet:

öffentlicher Schlüssel
(Public Key)

Der öffentliche Schlüssel
darf bekannt gegeben
werden.

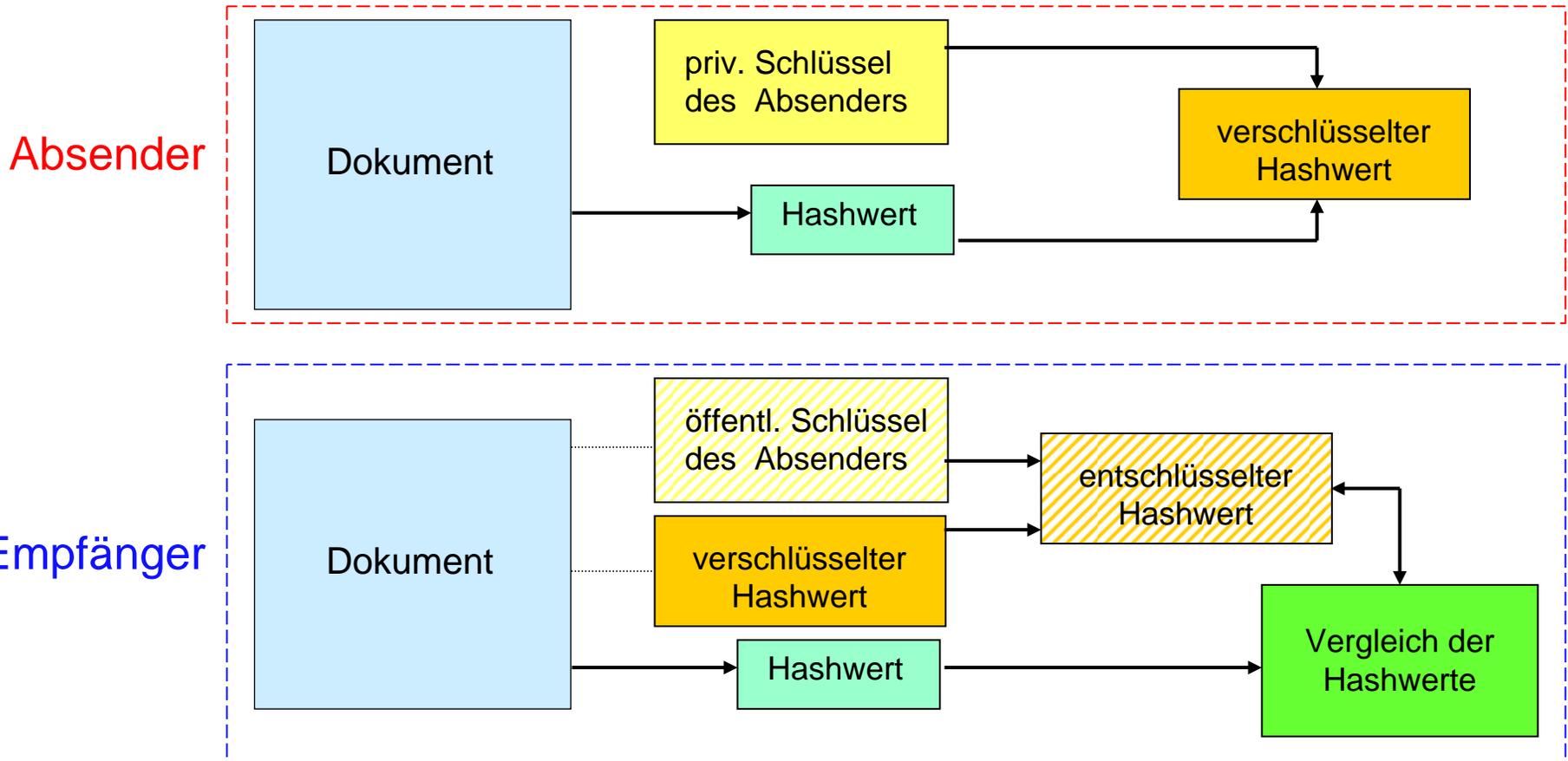
privater Schlüssel
(Private Key)

Der private Schlüssel
bleibt geheim.

Asymmetrische Verschlüsselung:

Die zwei Schlüssel des Schlüsselpaares sind mathematisch so miteinander verknüpft, dass nur sie wechselseitig zum Einsatz kommen können.

Integrität - Prüfung der Unverfälschtheit der Daten



1. Elektronische Signatur: Funktion - Authentizität (Personen-) Zertifikat

Zertifikat enthält Angaben

1. zur Identität des
Schlüsselhabers.
2. zur Gültigkeitsdauer.
3. zum Aussteller des
Zertifikats.
4. den öffentlichen Schlüssel
des Inhabers.



ZERTIFIKAT

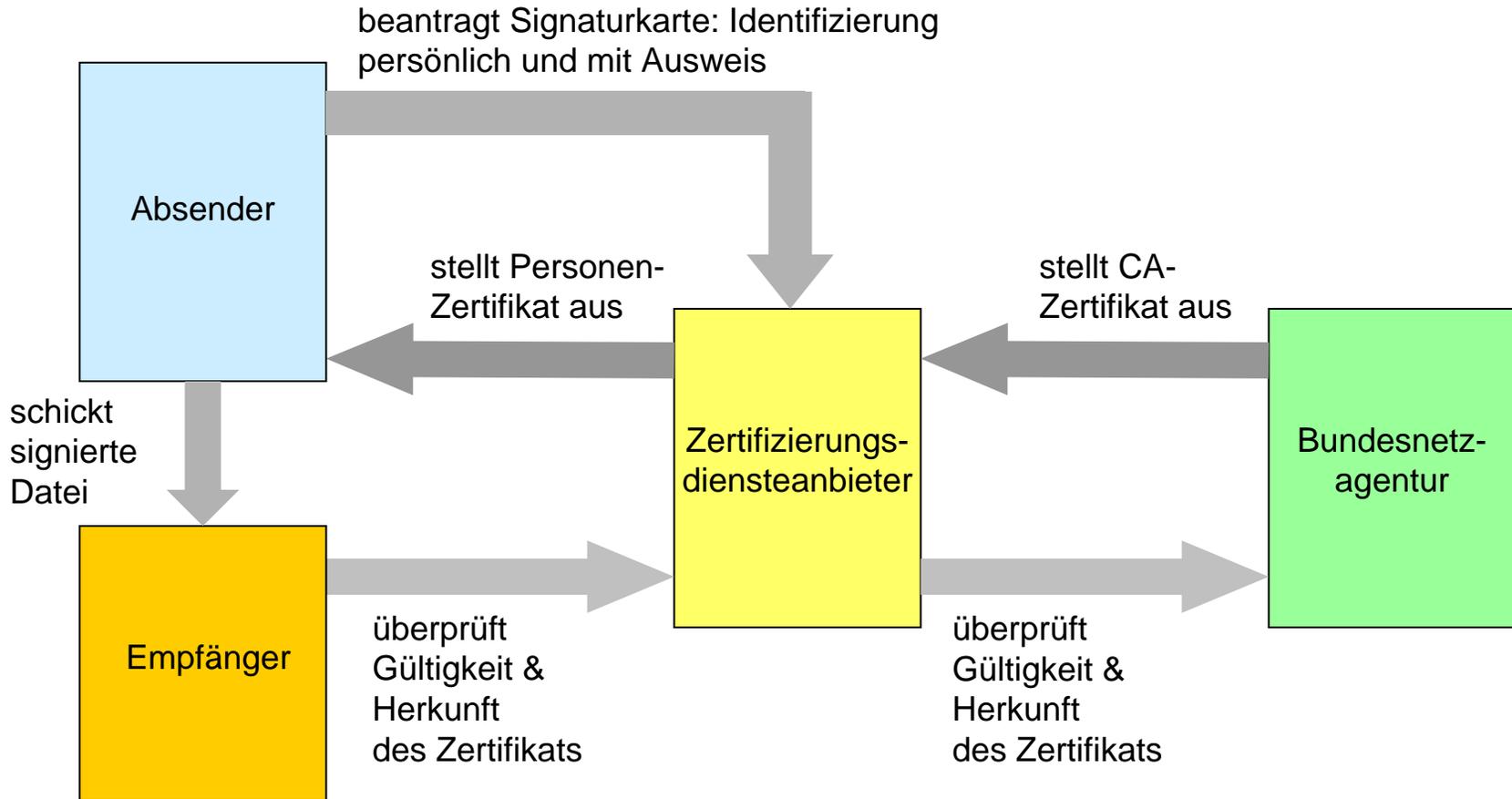
Name, Vorname, ggf.
Pseudonym

gültig von:
gültig bis:

Ausgestellt vom
Zertifizierungsdienste-
anbieter

Öffentlicher Schlüssel
(Signaturprüfchlüssel)

Authentifizierung - Prüfung der Identität des Absenders:



Attributzertifikate

- zur Selbstbeschränkung:
zur Beschränkung der Nutzung des Signaturschlüssels, wie z.B. "Maximal 1.000,- € pro Rechtsgeschäft."
- zur Vertretungsmacht für einen Dritten:
zum Nachweis, dass Sie ermächtigt sind, einen Dritten (Arbeitgeber, ...) zu vertreten.
- zu berufsbezogenen oder sonstigen Angaben:
Zum Nachweis, dass Sie einer bestimmten Berufsgruppe (Rechtsanwalt, Arzt, ...) zugehören und in dieser Eigenschaft über entsprechende Berechtigungen und / oder Qualifikationen verfügen.

(einfache) elektronische Signatur

fortgeschrittene elektr. Signatur

qualifizierte elektr. Signatur

qualifizierte elektr.
Signatur mit
Anbieterakkreditierung

Inhaber ist natürliche Person

(einfache) elektronische Signatur

Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

- ⇒ Signaturschlüsselinhaber muss keine natürliche Person sein
- ⇒ Sicherheitsniveau: gering

Beispiel:

- eingescanntes Bild der eigenen Unterschrift
- Organisationssiegel

fortgeschrittene elektronische Signatur

Wie die einfache elektronische Signatur, aber:

- ⇒ Signatur ist ausschließlich dem Signaturschlüssel-Inhaber zuzuordnen (natürliche Person)
- ⇒ die Identifizierung des Signaturschlüssel-Inhabers muss ermöglicht sein
- ⇒ die Mittel zur Erzeugung muss der Signaturschlüssel-Inhaber unter seiner Kontrolle halten
- ⇒ eine nachträgliche Veränderung der Daten muss erkannt werden können
- ⇒ Sicherheitsniveau: mittel

Beispiele: Softwarezertifikat, Stick, Chipkarte

qualifizierte elektronische Signatur

Wie die fortgeschrittene elektronische Signatur, aber:

- ⇒ die Signatur beruht auf einem zum Zeitpunkt der Signaturerzeugung gültigen qualifizierten Zertifikat
- ⇒ wird mit einer sicheren Signaturerstellungseinheit erzeugt: Chipkarte
- ⇒ mit **Zertifikat vom Zertifizierungsdiensteanbieter:**

mit Betriebsanzeige	mit Anbieterakkreditierung
haben ihren Betrieb lediglich bei der Bundesnetzagentur angezeigt	hat ein Akkreditierungsverfahren gem. SigG erfolgreich durchlaufen: Gütesiegel
Sicherheitsniveau: hoch	Sicherheitsniveau: sehr hoch

Rechtswirkung der qualifizierten elektronischen Signatur

- entspricht im Rechtsverkehr der handschriftlichen Unterschrift:
die elektronische Form entspricht der Vorschrift „gesetzliche Schriftform“ (§§126ff BGB):
⇔ Ausnahmen dieser Gleichstellung gibt es nur, wenn gesetzlich etwas anderes bestimmt ist (Kündigung von Arbeitsverhältnissen (§623 BGB), Bürgschaftserklärungen (§766 BGB), ...) .
- Durch die Nutzung Ihres Signaturschlüssels wird Ihnen die qualifizierte elektronische Signatur zugerechnet.
- Ermöglicht die rechtskräftige Nachprüfung der Integrität des Dokuments.

Europa:

EG-Richtlinie 1999/93/EG definiert die Vorgaben für die Regelungen elektronischer Signaturen in den Mitgliedsstaaten.

Deutschland:

- **Signaturgesetz (SigG)**
Rahmenbedingungen für elektronische Signaturen
- **Signaturverordnung (SigV)**
ergänzt SigG durch Einzelregelungen für Zertifizierungsdiensteanbieter sowie Produkte und Verfahren für Zertifikat- und Signaturerstellung
- **Bürgerliches Gesetzbuch (BGB)**, vor allem §§ 125 ff. (Form von Rechtsgeschäften)
- **Verwaltungsverfahrensgesetz (VwVfG) ...**

eANV: Verordnung zur Vereinfachung der abfallrechtlichen Überwachung, Abschnitt 4, § 19: Signatur, Übermittlung

„Die zur Nachweisführung Verpflichteten sowie die zuständigen Behörden haben die zu übermittelnden elektronischen Dokumente mit einer qualifizierten elektronischen Signatur ... zu versehen.“

Betrifft insbesondere die den

- Nachweiserklärungen und
- Begleitscheinen

entsprechenden elektronischen Dokumente

(sowie Erklärungen, Erstattung von Anzeigen, Fertigung von Vermerken, Erteilung von Bestätigungen und Entscheidungen, Übergabe oder Übersendung von Ausfertigungen oder Ablichtungen, Stellung von Anträgen, Erteilung von Freistellungen)

Was benötigt der Signaturanwender?

- Signaturchipkarte
- Kartenlesegerät
=> für eine „sichere PIN-Eingabe“
mit Zifferntastatur
- eine Signaturanwendung,
=> um eine Verknüpfung zwischen den
elektronischen Daten und der
Signaturkarte herzustellen



Signieren: Kartenverwendung

Innerhalb einer bestehenden Anwendungssoftware klickt der User auf den Befehl „Signieren“.

Er wird dann aufgefordert, seine Karte in das Lesegerät einzustecken und diese durch Eingabe des persönlichen PIN-Codes zu aktivieren.



Signieren: PIN-Eingabe

Erst durch Eingabe des geheimen PIN-Codes wird die Karte angesteuert und eine Signatur erzeugt.

Durch die Sicherheitskriterien
- „Besitz“ (der Signaturkarte) und
- „Wissen“ (des PIN-Codes)
ist die elektronische Unterschrift besonders geschützt.



Sicherheitsvorkehrungen durch den Nutzer:

- Signaturkarte sicher aufbewahren und bei Verlust sofort sperren
- PIN und zugehörige Passwörter zur Sperrung geheim halten
- PC immer auf dem neuesten Sicherheitsstandard halten
- Signieren Sie nur Informationen, die Sie vorher geprüft haben.

Sicherheitsvorkehrungen durch begrenzte Gültigkeit:

- **Verschlüsselungsverfahren:** Die verwendeten Codes werden regelmäßig durch das BSI darauf überprüft, ob sie mindestens 6 Jahre als sicher gelten. Ggf. werden die Anforderungen erhöht.
- **Zertifikate:** Nach dem Signaturgesetz dürfen qualifizierte Zertifikate nur eine begrenzte Gültigkeit besitzen => Folgekarten

Einsatz der digitalen Signatur beim Abfallnachweisverfahren

Abfallerzeuger, -beförderer und –entsorger benötigen für ihre Mitarbeiter jeweils eine qualifizierte elektronische Signatur:

- Mitarbeiter müssen jeweils zu gegebener Zeit die Nachweiserklärung bzw. den Begleitschein elektronisch signieren.
- Erzeuger, Beförderer und Entsorger müssen nacheinander signieren.
- Persönliche Signaturkarte ist nicht übertragbar: Jeder Mitarbeiter, der elektronisch signiert, benötigt eine individuelle Signaturkarte.

Übergangsfristen und Stichtage

- seit 2007: Praktizierung des elektronischen Abfallnachweisverfahrens bei Erlaubnis der zuständigen Behörde möglich
- 1. Quart. 2009: Zentrale Abfallnachweis-Plattform der öffentlichen Verwaltung geht mit vollem Funktionsumfang in Echtbetrieb
- bis 31.03.2010: freiwillige elektronische Nachweisführung mit Zustimmung der zuständigen Behörde
- ab 01.04.2010: Elektronische Nachweisführung obligatorisch
- ab 01.04.2010: Entsorger / Behörden müssen elektronisch signieren
- ab 01.02.2011: Erzeuger / Beförderer müssen elektronisch signieren

ZKS-Abfall: Zentrale Koordinierungsstelle der Länder

<http://www.zks-abfall.de>

- Informationen über das elektronische Abfallnachweisverfahren allgemein
- Registrierung, Stammdatenpflege, Beantragung einer behördlichen Nummer etc.
- Virtuelle Poststelle: Elektronische Postfächer für die Beteiligten
- Länder-eANV: Einfache Lösung zur Formularbearbeitung und
- Signatur (kostengünstige Lösung, sinnvoll bei geringen Aufkommen)

Private Anbieter von eANV-Produkten

... bieten Schnittstellen zur ZKS-Abfall, haben Signaturfunktion integriert und ermöglichen komfortable Bearbeitung:

„Modawi“ <http://www.modawi.de>

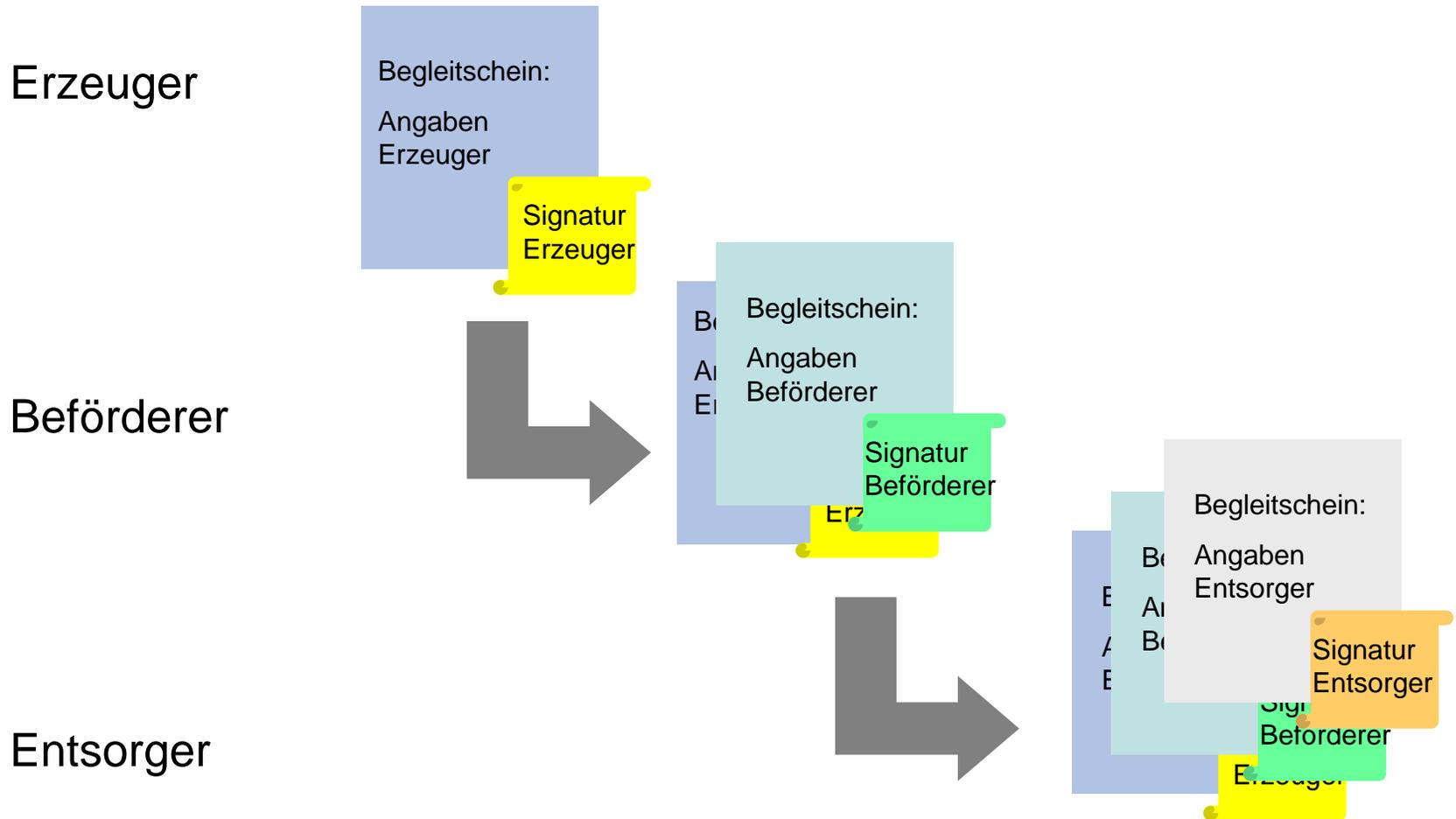
„Zedal“ <http://www.zedal.de>

„Nsuite“ <http://www.nsuite.de>

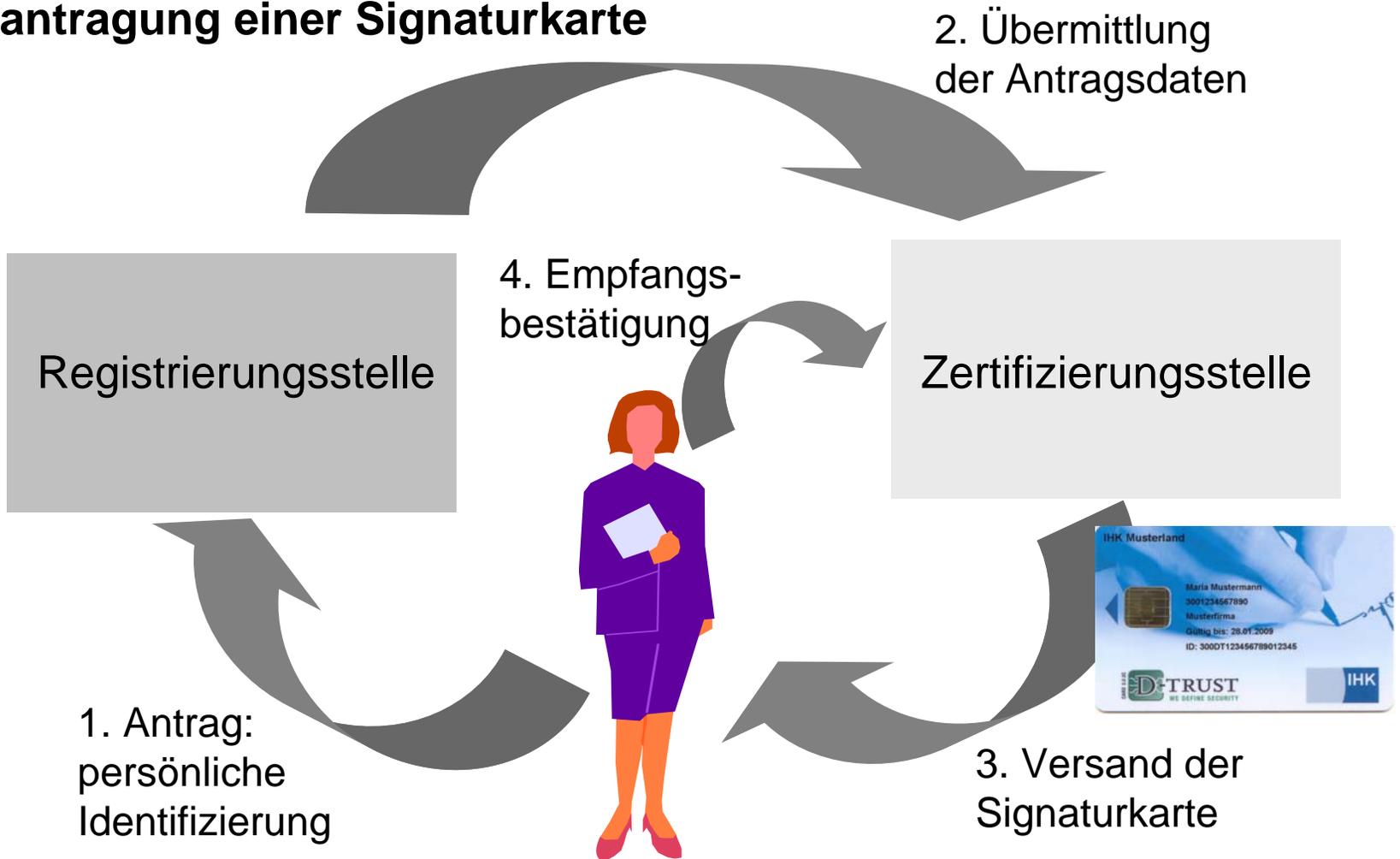
„eANV Portal“ <http://www.fum.de> ...

(alle kostenpflichtig)

Layerdarstellung



Beantragung einer Signaturkarte



qualifizierte elektronische Signaturkarten erhältlich bei diversen Zertifizierungsdiensteanbietern:

- TeleSec
- Signtrust
- DATEV
- Bundesnotarkammer
- TC TrustCenter
- D-Trust => DE-CODA / Chambersign ...



Kartenleser:

- Cherry
- Kobil
- Orga
- Reiner-SCT
- SCM Microsystems ...



Die „Chambercard“ der IHK

- Chipkarte
- zur Erstellung von qualifizierten elektronischen Signaturen
- Zertifizierungsdiensteanbieter: D-Trust
- Kartenlesegerät und zugehörige Software (Komplettpaket)
- Für gewünschte Attributzertifikate zur Firmenzugehörigkeit werden erforderliche Handelsregister- oder Firmenspiegel-Auszüge direkt durch die IHK zur Verfügung gestellt.
- Ausführliche Vorab-Informationen erleichtern die Entscheidung, welche Signaturkomponenten der Nutzer braucht und ermöglichen eine effiziente Registrierung bei der IHK.



- E-Vergabe
- gesicherte elektronische Kommunikation
- Elektronische Rechnungsstellung (Vorsteuerabzug)
- Rechtsverkehr (Elektronisches Gerichts- und Verwaltungspostfach, Online-Mahnbescheid)
- Elektronische Verträge
- Archivierung
- Anträge und Bescheide (bspw. ELSTER)
- Emissionshandel
- Ursprungszeugnisse
- Elektronischer Entgeltnachweis
- Verpackungsverordnung ...



Mehr Infos zur IHK-Signaturausstattung

Registrierungsstelle: IHK

IHK für München und Oberbayern
Informations- und Servicezentrum (ISZ)
Max-Joseph-Straße 2
80333 München
Telefon: 089 / 5116 - 150
ihkmail@muenchen.ihk.de
<http://www.muenchen.ihk.de>

Zertifizierungsdiensteanbieter:

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin
Telefon: 030 / 259391 - 0
info@d-trust.net
<https://www.d-trust.net>

Kooperationspartner:

DE-CODA GmbH
Brückenstr. 5 A
10179 Berlin
Tel.: 030 / 21 91 59 00
info@de-coda.de
<http://www.decoda.de>

Vielen Dank für Ihre Aufmerksamkeit.

Industrie- und Handelskammer für München und Oberbayern

Franziska Neuberger
Referentin E-Government
Max-Joseph-Straße 2
80333 München
Tel.: 089-5116-249
Fax: 089-5119-8249
Neuberger[a]muenchen.ihk.de