Bundesamt
für Sicherheit in der
Informationstechnik

# Die eIDAS-Verordnung und ihre (technische) Umsetzung

Jens Bender

Bundesamt für Sicherheit in der Informationstechnik

EDV-Gerichtstag / 30.06.2015

# eIDAS-Verordnung

- Allgemeine Bestimmungen
- Elektronische Identifizierung
- Vertrauensdienste
  - Allgemeine Bestimmungen
  - (Q|F) Signatur
  - (Q|F) Siegel
  - (Q|F) Zeitstempel
  - (Q|nQ) Zustelldienst
  - Q Webseitenzertifikate
- Elektronische Dokumente
- Schlussbestimmungen
- Anhänge

# Heute:

# (qualifizierte) Signaturen
# Komponenten und Anforderungen

**Signaturerstellungseinheiten**

**Signaturanwendungskomponenten**

**Signaturerstellung**

# Regelungshierachie

- Vertrag von Lissabon
- eIDAS-Verordnung
  - Unmittelbar geltendes Recht in allen MSen
- Enthält Ermächtigungen für
  - 1 Delegierter Rechtsakt (Anforderungen Zertifizierungsstellen)
  - 28 Implementierungsrechtsakte
    - Nur 4 verpflichtend zur erlassen, die anderen optional
      - **Bisher noch nicht klar, welche optionalen IAs kommen werden**
      - **„Bedarf des Marktes“ als Hauptkriterium**
    - Erstellung wird von „Expert Group“ unterstützt
    - Komitologie-Gruppe gibt „Meinung“ zu den Entwürfen der KOM ab
    - Erlass durch KOM
- Dritte Ebene: Standardisierung

# Obligatorische IA

- Trust Mark: EUSAFE
  - Logo für qualfizierte TSPs
- Trust List (ETSI TS 119 612 draft)
  - (Nationale) XML-Liste der (q)TSPs
- Signatur- und Siegelformate (ETSI)
  - Die gelisteten Formate müssen vom öffentlichen Sektor akzeptiert werden
  - Ausgenommen: Formate für Langzeitarchivierung
    - ETSI hierbei nicht kompatibel zu TR-ESOR
  - Weitere Formate möglich, dann muss Aussteller „Link zu einem Validierungsservice“ mitliefern
- Zu diesen IA hat Komitologie positive „Meinung“ abgegeben
  - Zur Zeit Übersetzung, …

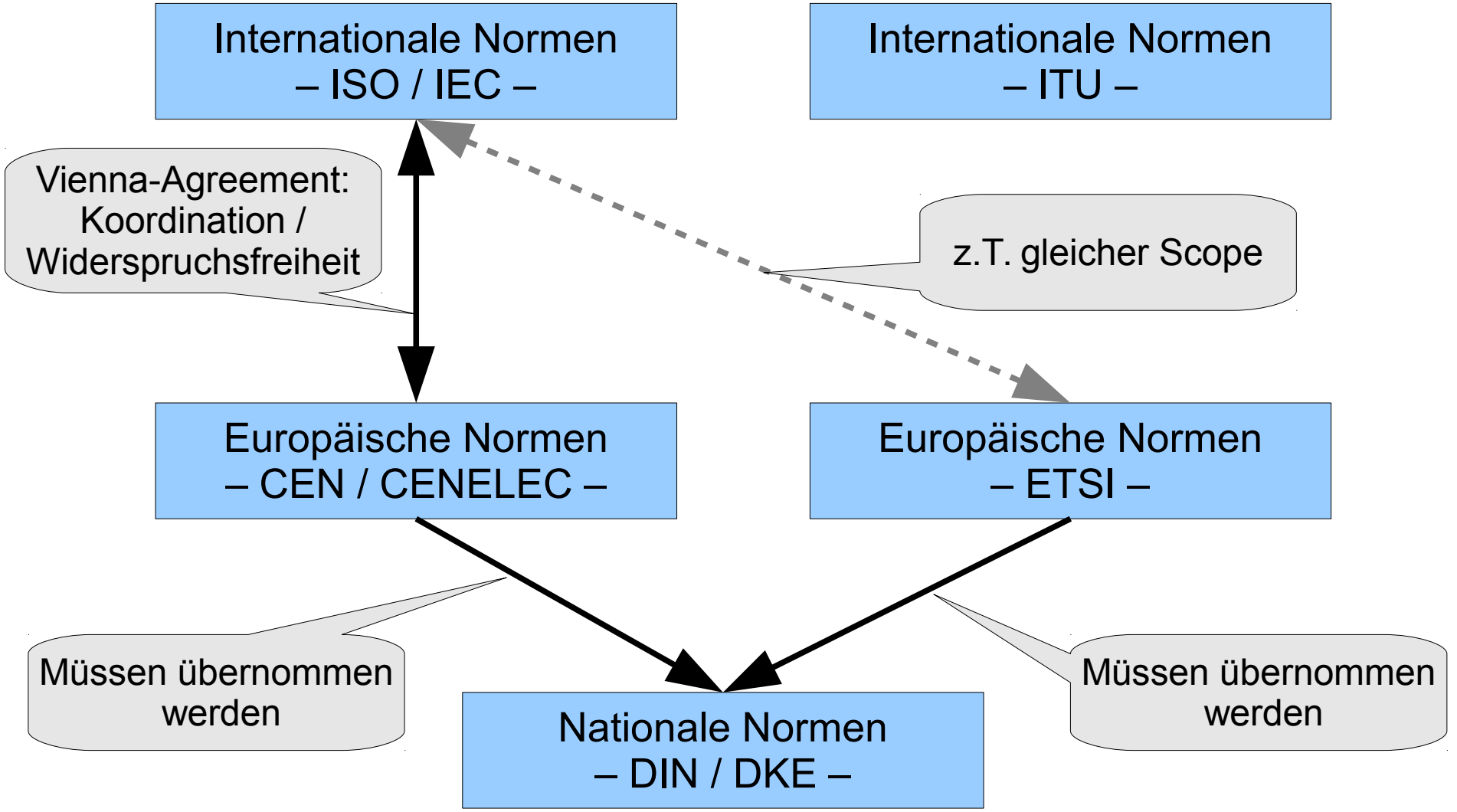
# Exkurs:
# Normen und Standards

# Normen

- Viele Durchführungsrechtsakte erlauben nur „Kennnummern von Normen“ als Inhalt
  - Sehr starke Stellung der (Industrie-)Normung als „tertiäres Recht“

- Normen erstellt durch internationale / Europäische / nationale Standardisierungsgremien
  - ISO / IEC, CEN / CENELEC, ETSI, DIN, …
  - Technische Richtlinien des BSI oder der BNetzA können nicht unter diesen Rechtsakten referenziert werden

# Viele Normungsgremien...



# … und ihre Wirkung

- Verweis auf Normen
  - Größere Präzision der technischen Umsetzung
  - Europäische Normen haben Vorrang vor DE-Normen
    - Kein Vorrang internationaler Normen, abhängig von Referenzierung
- Bei Erfüllung der Norm wird „davon ausgegangen, dass die Anforderungen [der VO] erfüllt sind“
  - Weniger Ermessen der Aufsichtsbehörde
  - Aber keine Verpflichtung, Norm einzuhalten!
    - Norm = Stand der Technik
  - Ein (q)TSP kann die VO auch „anders“ einhalten
    - → muss dies ggfs. gegenüber Aufsichtsbehörde nachweisen
- Viele Durchführungsrechtsakte optional
  - KOM: nur, falls Bedarf des Marktes / Stakeholder

# Heute:

# (qualifizierte) Signaturen
# Komponenten und Anforderungen

**Signaturerstellungseinheiten**

**Signaturanwendungskomponenten**

**Signaturerstellung**

# Signaturerstellungseinheiten

| SigG | eIDAS-VO |
| --- | --- |
| (bestätigte) Sichere Signaturerstellungseinheiten | (zertifizierte) Qualifizierte Signaturerstellungseinheiten |

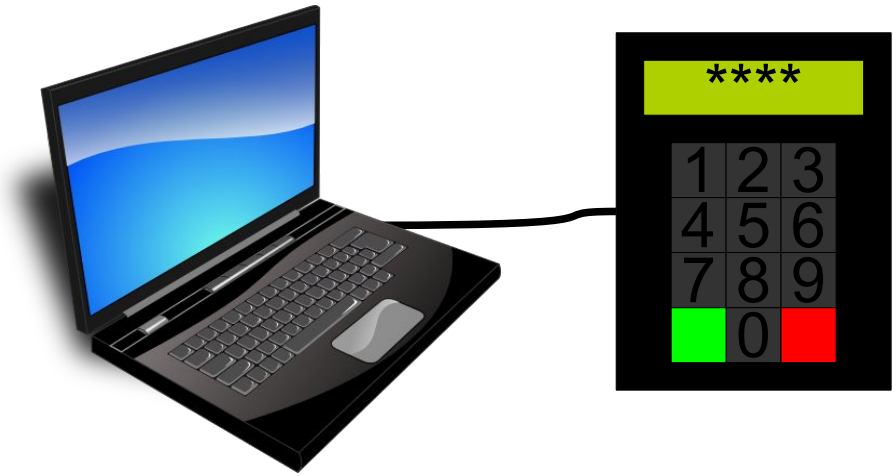
Anforderungen zwischen SigRL und eIDAS i.W. unverändert

Erweiterungen um Anforderungen für Server-Signaturen

Offen: Was genau ist die Signaturerstellungseinheit?

# Signaturanwendungskomponenten

- Aufgaben
  - Anzeige der zu signierenden Daten
  - PIN-Eingabe (oder andere Authentisierung des Anwenders)
  - Signaturprüfung
- Üblicherweise in DE
  - Kartenleser mit PIN-Eingabemöglichkeit
  - Lokale Software



# Signaturanwendungskomponenten – SigG vs. eIDAS –

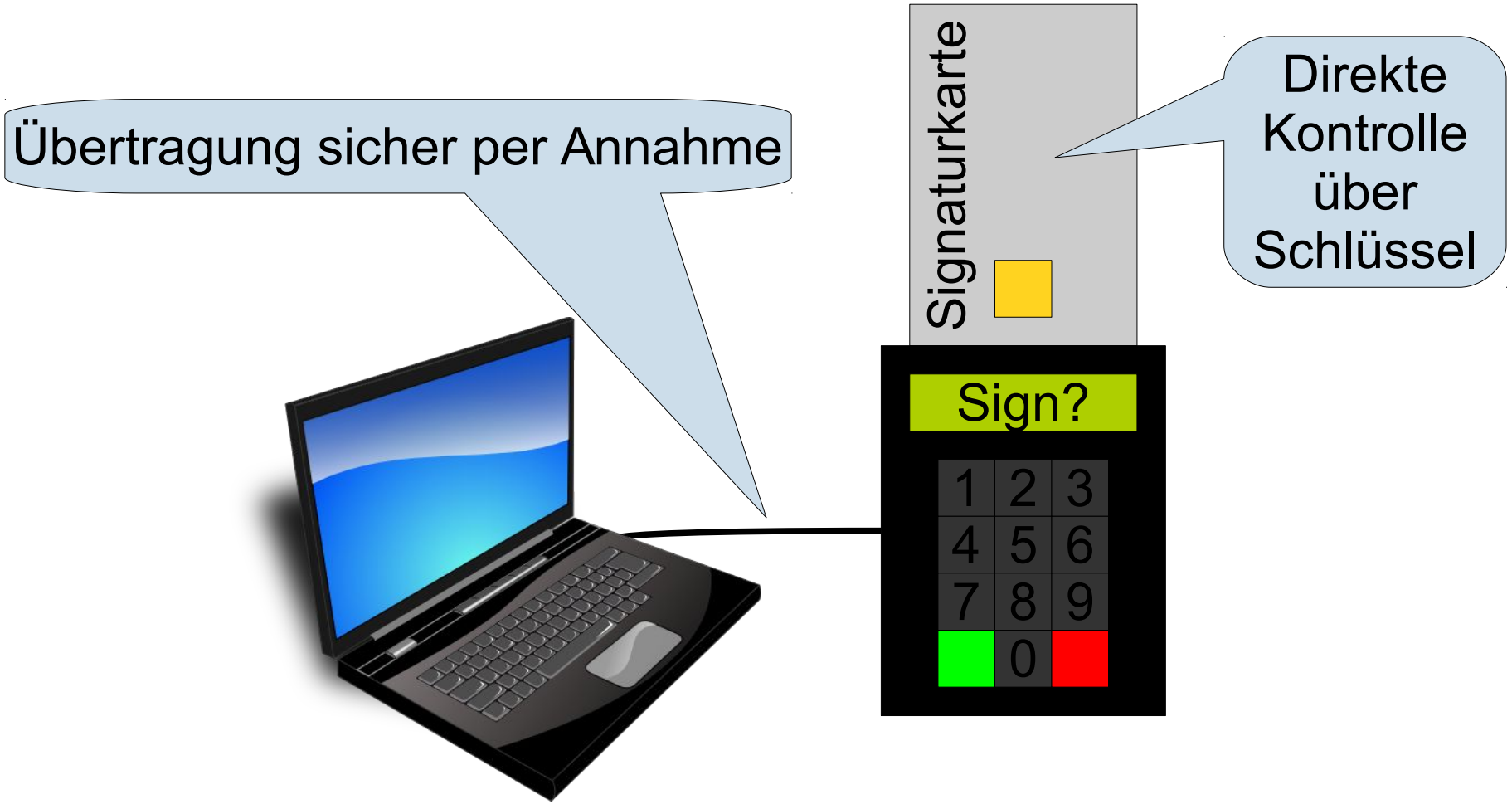
- SigG
  - § 15(7) [Akkreditierte ZDAs]
    - Bei Produkten für qualifizierte elektronische Signaturen **muss** die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 [...] **bestätigt** worden sein;
  - § 17(2) [Produkte für QES]
    - Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich […] Die Signaturschlüssel-Inhaber **sollen** solche Signaturanwendungskomponenten **einsetzen** oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.
- eIDAS-Verordnung Erwägungsgrund (56)
  - [...] der Anwendungsbereich der **Zertifizierungspflicht** [soll] **Signaturerstellungsanwendungen ausschließen**.

# Signaturanwendungskomponenten

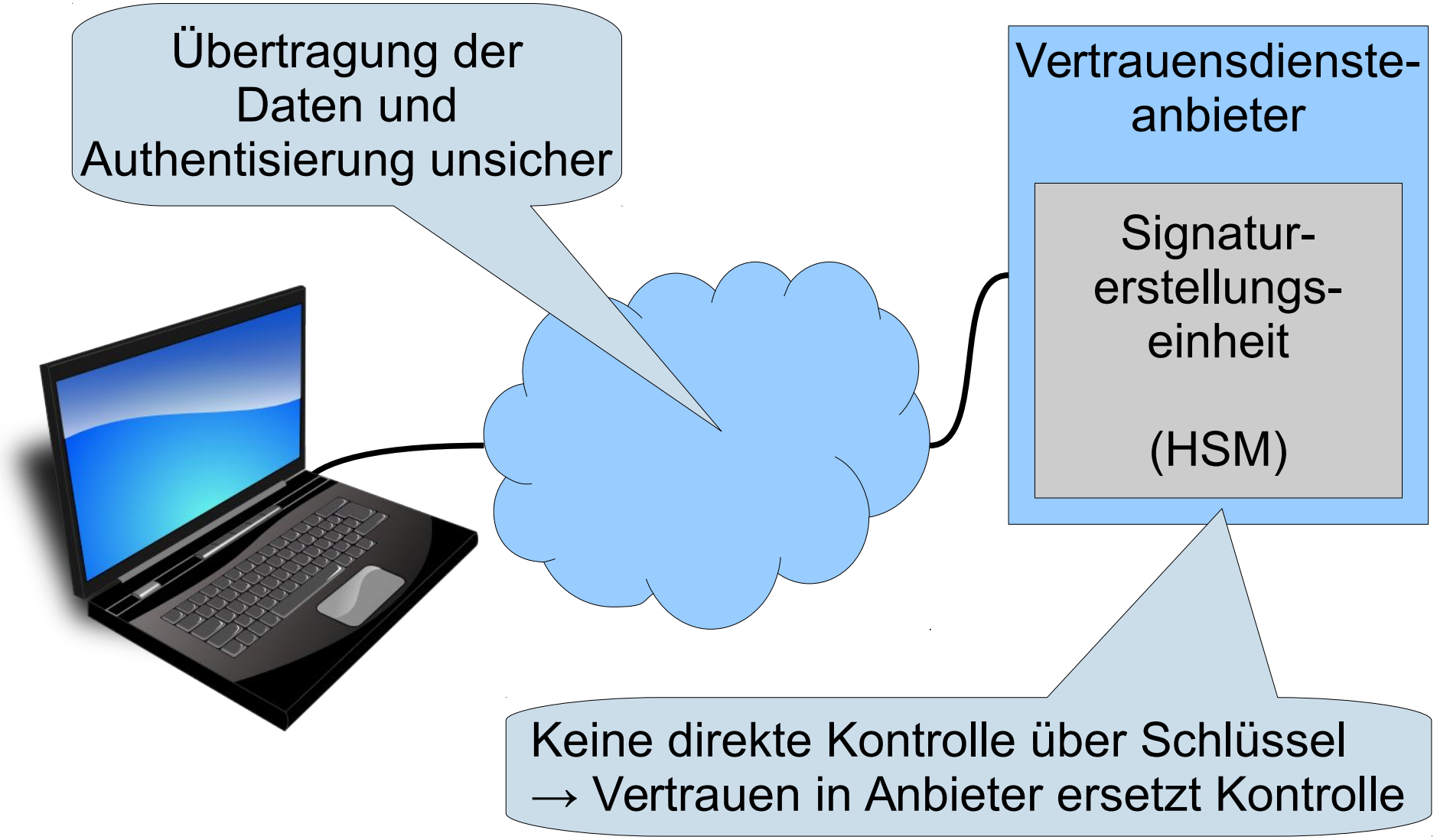
- Keine Anforderungen an SAKs
- Keine Zertifizierung / Bestätigung für SAKs
- Keine Anwendungsempfehlung „guter“ SAKs
  - Immerhin [eIDAS & SigRL]:
    Qualifizierte elektronische Signaturerstellungseinheiten dürfen [...] **nicht verhindern**, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.

- Es ist dem Anwender überlassen wie (und ob!) er sich zu signierende Daten anzeigen lässt
  - Was bedeutet das für die „Willenserklärung“?

# Signaturerstellung
# – Lokal –

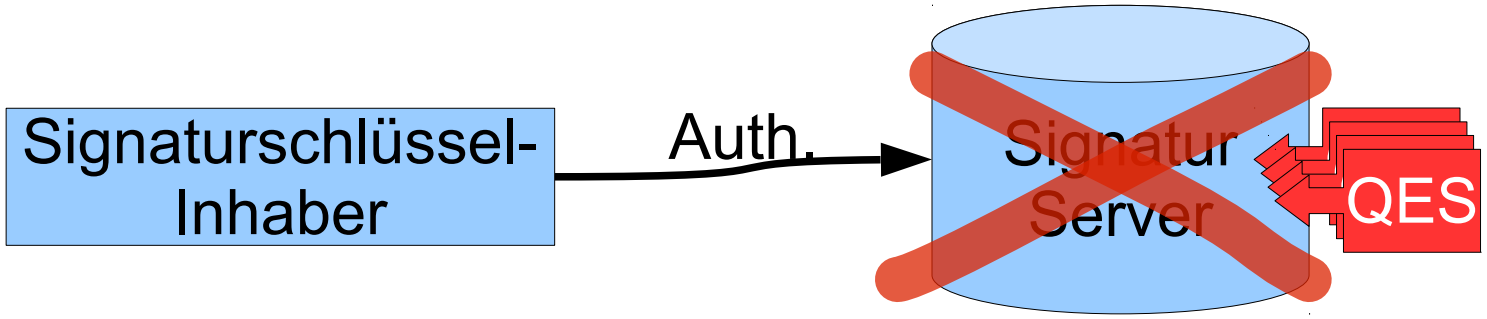


# Signaturerstellung
# – Entfernt –



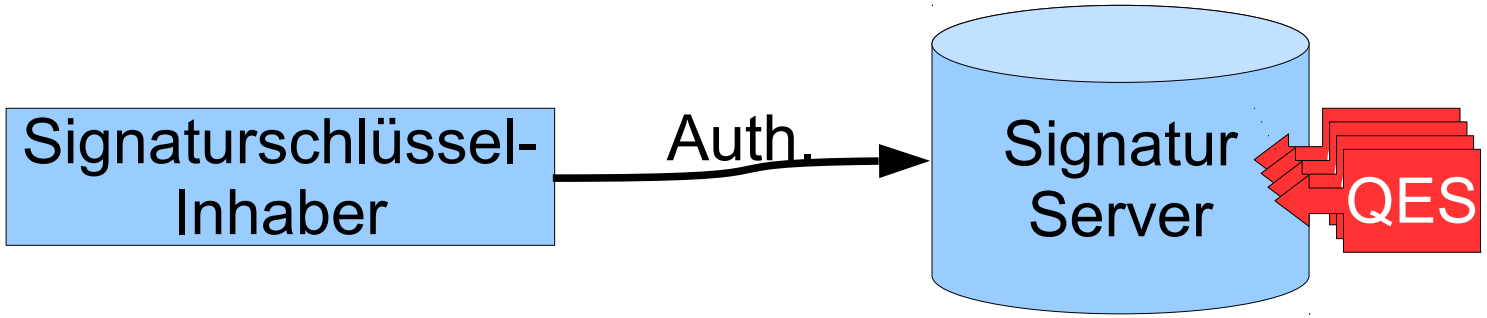
# Anforderungen nach SigG

- **SigRL Artikel 2(2):**
  - ✗ „fortgeschrittene elektronische Signatur“: eine elektronische Signatur, die folgende Anforderungen erfüllt:[...]
    - c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen **Kontrolle** halten kann;
- **Der Zertifizierungsdiensteanbieter hat [§5 SigG]**
  - ✗ Sich [...] zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit **besitzt**.
- ➔ **Keine entfernte Signatur**



# Anforderungen nach eIDAS-VO

- **Anforderungen an …**
  - qualifizierte elektronische Signaturerstellungseinheiten
    - „Kontrolle“ → „mit einem hohen Maß an Vertrauen unter […] Kontrolle“
  - qualifizierte Vertrauensdiensteanbieter
    - Speicherung und Verwaltung privater Signaturschlüssel durch Vertrauensdiensteanbieter explizit möglich
- Kein Besitznachweis notwendig
- Keine Anforderungen an Signaturanwendungskomponenten
  - Keine Anforderungen an Anzeige (Browser statt SAK)



# Signaturerstellung

- Übertragung der Daten
  - Weder SigG noch eIDAS-VO machen hierzu Vorgaben
- Authentisierung
  - SigG:
    - Besitz SSEE + PIN/Biometrie, Bestandteil der Bestätigung
  - eIDAS:
    - Anhang II (1) d [Anforderungen an QSEEs]
    - [QSEEs müssen gewährleisten, dass der Schlüssel] vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.
      - → **Gehört die Authentisierung zur QSEE?**

Preisfrage: Signiere ich das, was ich glaube zu signieren?

# (Technisches) Fazit

## Viele verschiedene Verfahren auf sehr unterschiedlichem Sicherheitsniveau

- Harmonischer als SigRL, aber bunter als SigG
  - SigRL: Artikel 3 (7) „ Die Mitgliedstaaten können den Einsatz elektronischer Signaturen im öffentlichen Bereich möglichen **zusätzlichen Anforderungen** unterwerfen.“
  - eIDAS: Artikel 27 (3) „Die Mitgliedstaaten verlangen [...] **keine** elektronische Signatur **mit einem höheren Sicherheitsniveau** als dem der qualifizierten elektronischen Signatur.“
- Rechtliche Folgerungen?

# Weitere Fragen...

- Neue Dienste:
  - (q) Siegel („Signatur für juristische Personen“)
  - (q) Elektronische Einschreiben (z.B. De-Mail)
  - qZertifikate für Webseitenauthentisierung (=SSL-Zertifikate)
- Organisatorische Fragen, z.B.
  - Aufsicht für nicht-q Vertrauensdienste
- Technische Fragen, z.B.
  - Ketten- oder Schalenmodell oder beides?
    - DE bisher Kettenmodell, die meisten anderen Länder (und die meisten anderen PKIen) Schalenmodell
  - Gibt es weiter eine zentrale Root in DE?
    - Alle qTSPs müssen (direkt) in einer Trusted List eingetragen werden

# Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185-189
53175 Bonn

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de