Instrumente des BSI für vertrauenswürdige Infrastrukturen

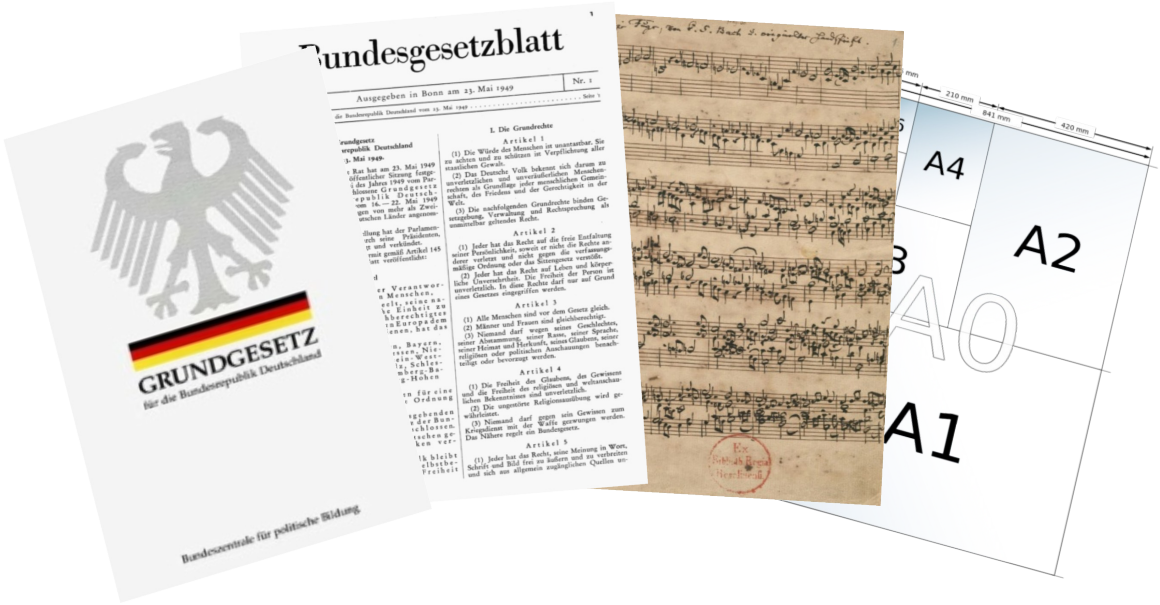
ULD-Sommerakademie:
„Vertrauenswürdige IT-Infrastruktur –
Ein (un) erreichbares Datenschutzziel“

31. August 2015 Kiel

Agenda

- Vertrauenswürdigkeit
- IT-Sicherheitsstandards & Normung
- Digitale Agenda, EGovG und DigV 2020
- Aktuelle Handlungsfelder des BSI
  - Vertrauensdienste und elektronische Identitäten
  - Aktuelle Regulierungen
- Ausblick

Gesellschaftliche Normen und technische Standards



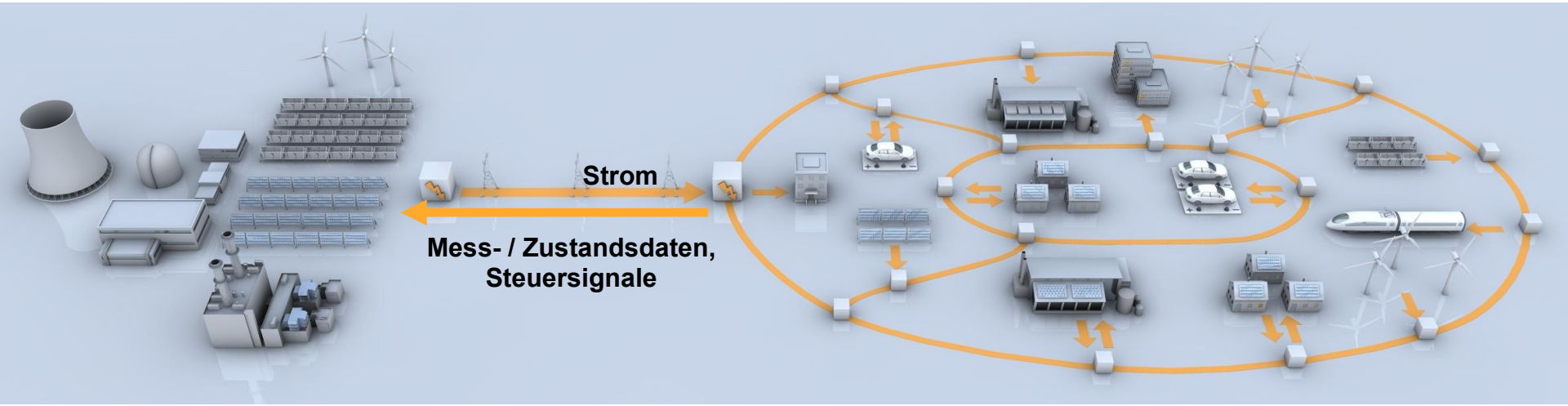
Normen gesellschaftlichen Zusammenlebens

- Sprache, Kommunikation, Infrastruktur
- Gesellschaftliche Werte / Grundrechte, wie Unversehrtheit, Freiheit, Lebensqualität, informationelle Selbstbestimmung (Art. 1 u. 2 GG), Fernmeldegeheimnis (Art. 10 GG)
- Spezialgesetze mit Bezug zu technischen Standards

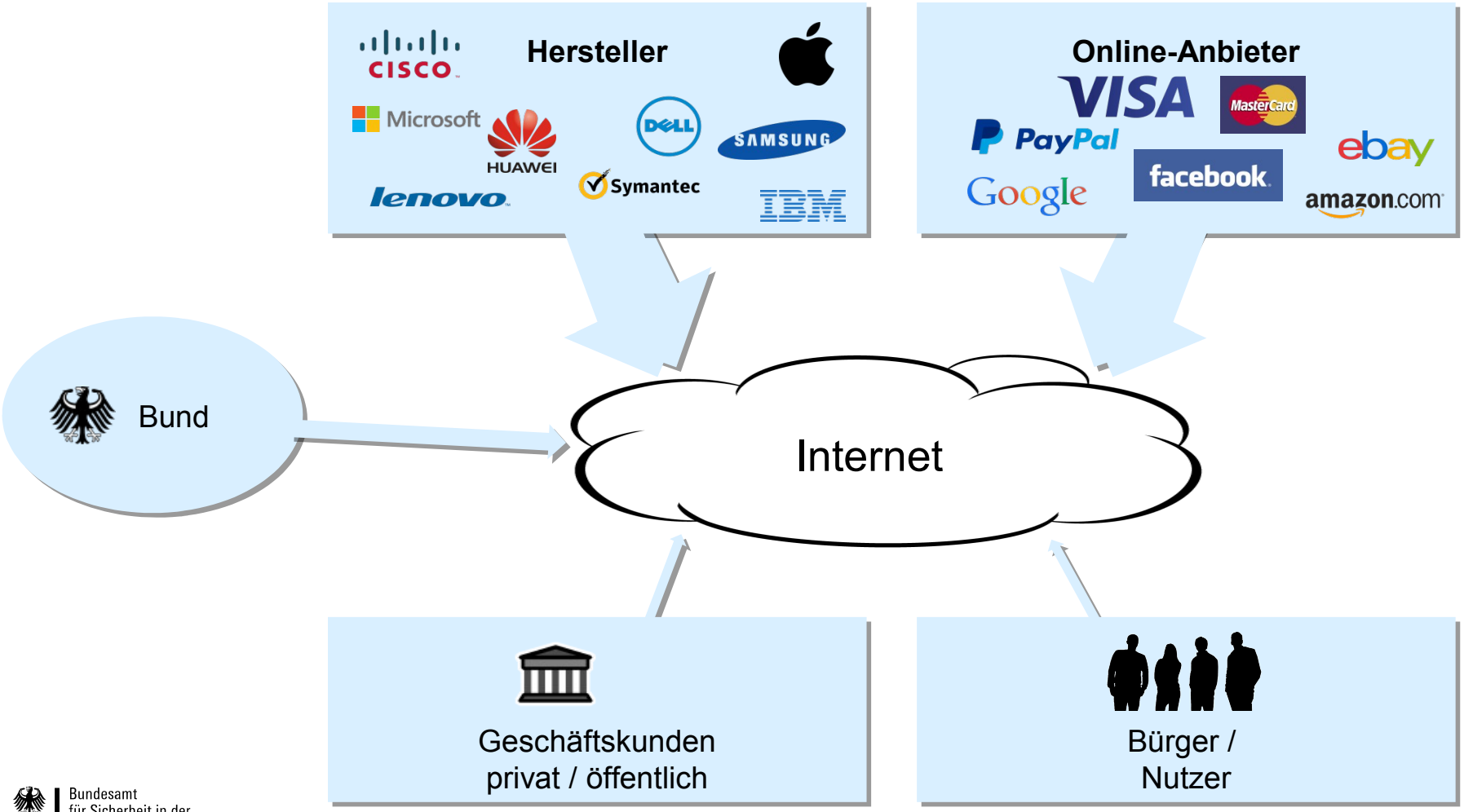
Bedeutung von IT-Sicherheitsstandards (1)

- Wirtschaft und Gesellschaft hängen von der Verfügbarkeit und Integrität von IT-Systemen ab
- Mangel an **Datenschutz** und **Vertrauenswürdigkeit** von gängigen Produkten
- **Öffentliche** und **Nationale Sicherheit** sind betroffen
- **Regierungen** sind gefordert Richtlinien für **angemessene Sicherheitsstandards** und unabhängige Produktprüfungen resp. Zertifizierungen zu setzen

Beispiel: Versorgungssicherheit in einem intelligenten Energienetz



Bedeutung von IT-Sicherheitsstandards (2)



Bedeutung von IT-Sicherheitsstandards (3)

Entwicklung Technischer Standards unterstützen

- Technische Richtlinien (TR)
- Schutzprofile (PP)
- Nationale und internationale Normung

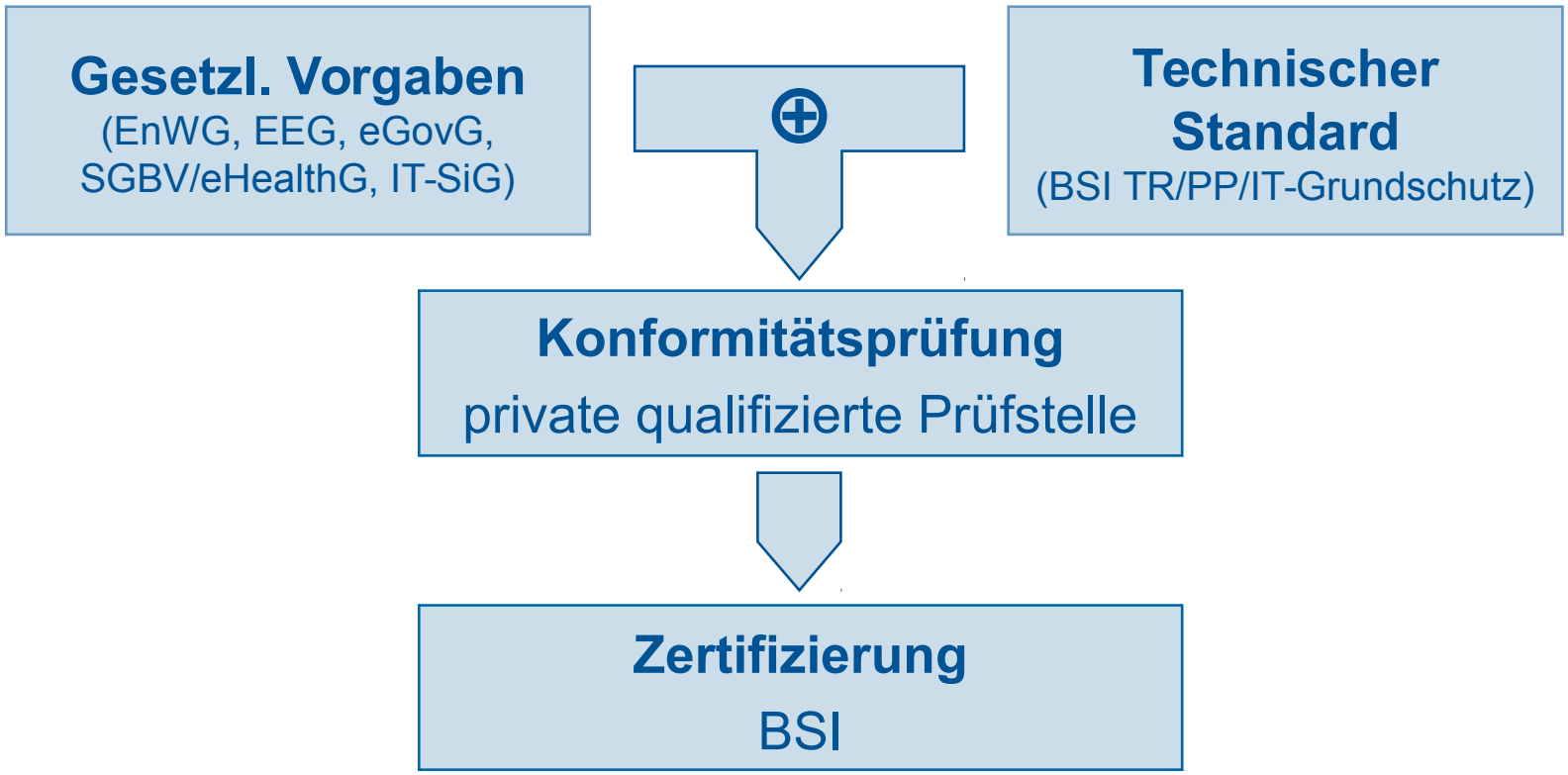
Zertifizierung

- Komponenten
- Produkte
- Dienstleistungen
- Dienstleister

Unterstützung von Gesetzgeber und Politik

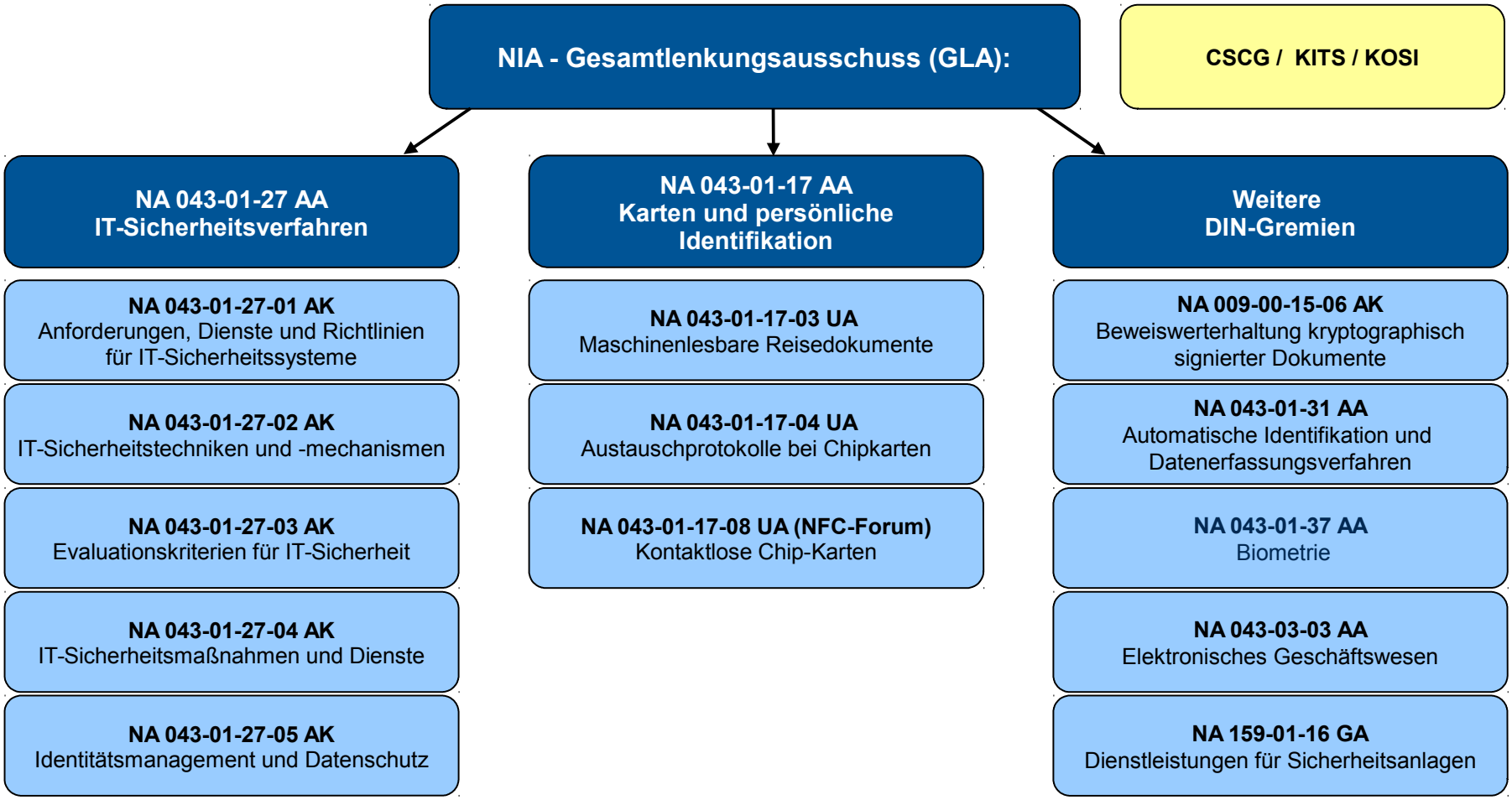
- Intelligente Messsysteme (EnWG/EEG)
- Gesundheitstelematik (SGB V § 291 / eHealth-Gesetz)
- eID-Verfahren (EU-KOM/eIDAS-VO)

BSI-Zertifizierung



Die Zertifizierung weist nach, dass ein Produkt/Verfahren die in den Rechtsvorschriften geforderten technischen Eigenschaften (TR, PP) erfüllt.

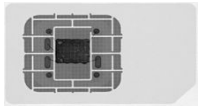
Bedeutung von IT-Sicherheitsstandards (4)



Normungsbedarf IT-Sicherheit - Beispiele

Moderne Sicherheitstechnologien

- **2-Faktor**-Authentisierung statt Passwort
- **End-to-End**-Sicherheitsfunktionen
- **Sicherheitselemente SE**, Token-basiert
  - Einsatz von SE in und an mobilen Endgeräten: NFC, FIDO
  - Trusted Computing (TPM)



Vertrauensdienste

- Account- und **Token-Management**
- **PKI**
- **eID-/Auth-Dienste**, z.B. Servicekonten

Technische Standards

- **Mitgestaltung** durch alle Stakeholder
- **Datenschutz**- und **GG**-Anforderungen berücksichtigen
- Transparenz, **diskriminierungsfreie Nutzung**

Digitale Agenda

Die Bundesregierung

Bundesministerium für Wirtschaft und Energie

Bundesministerium des Innern

Bundesministerium für Verkehr und digitale Infrastruktur

Bundesamt für Sicherheit in der Informationstechnik

Digitale Agenda für Deutschland

Grundsätze unserer Digitalpolitik	**Digitale Infrastrukturen**	**Digitale Wirtschaft und digitales Arbeiten**	**Innovativer Staat**
Handlungsfelder			
Digitale Lebenswelten in der Gesellschaft gestalten	**Bildung, Forschung, Wissenschaft, Kultur und Medien**	**Sicherheit Schutz und Vertrauen für Gesellschaft und Wirtschaft**	**Europäische und digitale Dimension der digitalen Agenda**

Bundesministerium für Wirtschaft und Energie

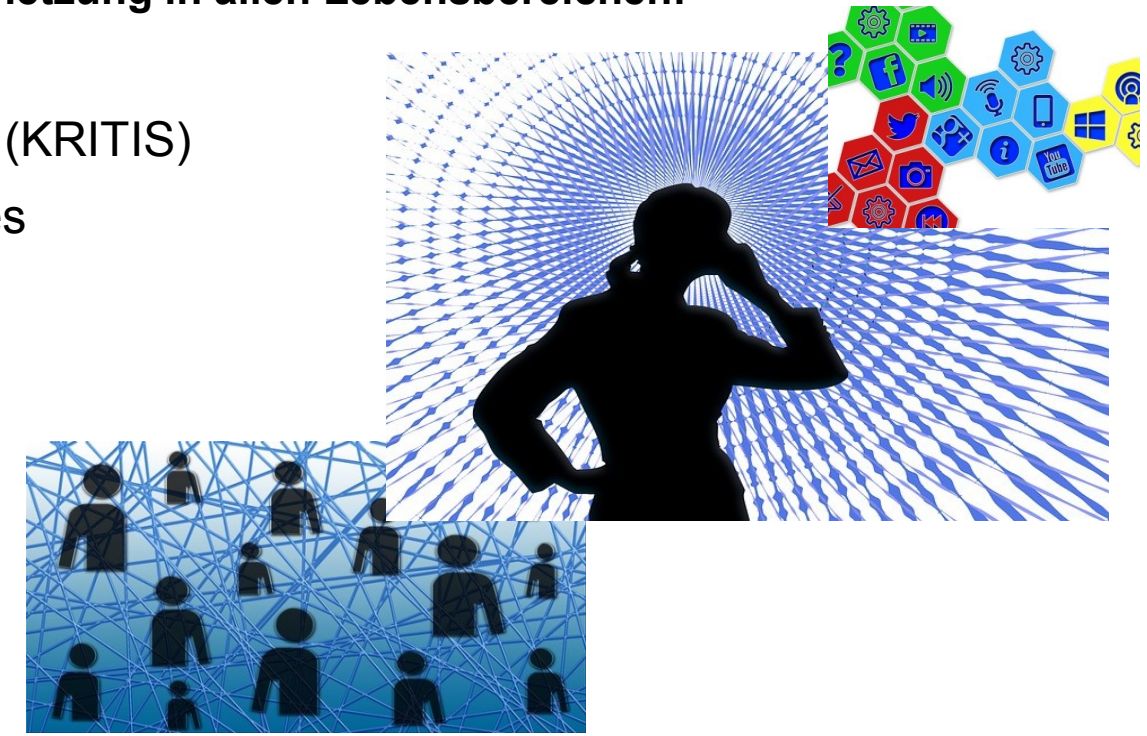
Bundesministerium des Innern

Bundesministerium für Verkehr und digitale Infrastruktur

Standardisierungsauftrag der Digitalen Agenda

Digitalisierung, Automation, Vernetzung in allen Lebensbereichen:

- Smart Grid, Smart Metering (KRITIS)
- Smart Home, Smart Services
- Industrie 4.0 / Fernwartung
- eMobility / car2car / car2x
- eHealth/**eGovernment**
- Cloud Computing
- **eID / ePayment**
- eCommerce
- Big Data



Vertrauenswürdigkeit, Verfügbarkeit, Transparenz

EGovernment-Gesetz und Digitale Verwaltung

- **EGovG**: Gesetz zur Förderung der elektronischen Verwaltung
  seit 1.8.2013 in Kraft

  - **Verbesserung digitaler Dienste**
  - Ermöglichung von Interoperabilität
    - insbesondere durch Prozessoptimierung sowie Datenschutz bei gemeinsamen Verfahren und Georeferenzierung
  - Schaffung von Transparenz

- **“Digitale Verwaltung 2020”**: eAkte, IT-PLR

Digitale Verwaltung 2020

EGovG - Digitale Dienste

- Erreichbarkeit durch mindestens einen **elektronischen Zugang**
  - Einrichtung qeS-fähige E-Mail-Adresse und innerbehördliche Organisation
- Bundesbehörden zusätzlich: **Erreichbarkeit** per De-Mail und eID-Funktion des PA
- Anschluss an das Gateway des Bundes, Aufbau der Infrastruktur für PA
- Technische **Ersetzung der Unterschrift**
  - § 3a VwVfG: Webformulare i.V.m. elektronischer Identifizierung per PA
- **Elektronische Aktenführung** (Bund) §§ 6 – 8 EGovG:
  Nur für Bundesbehörden verpflichtend, auch für andere sinnvoll

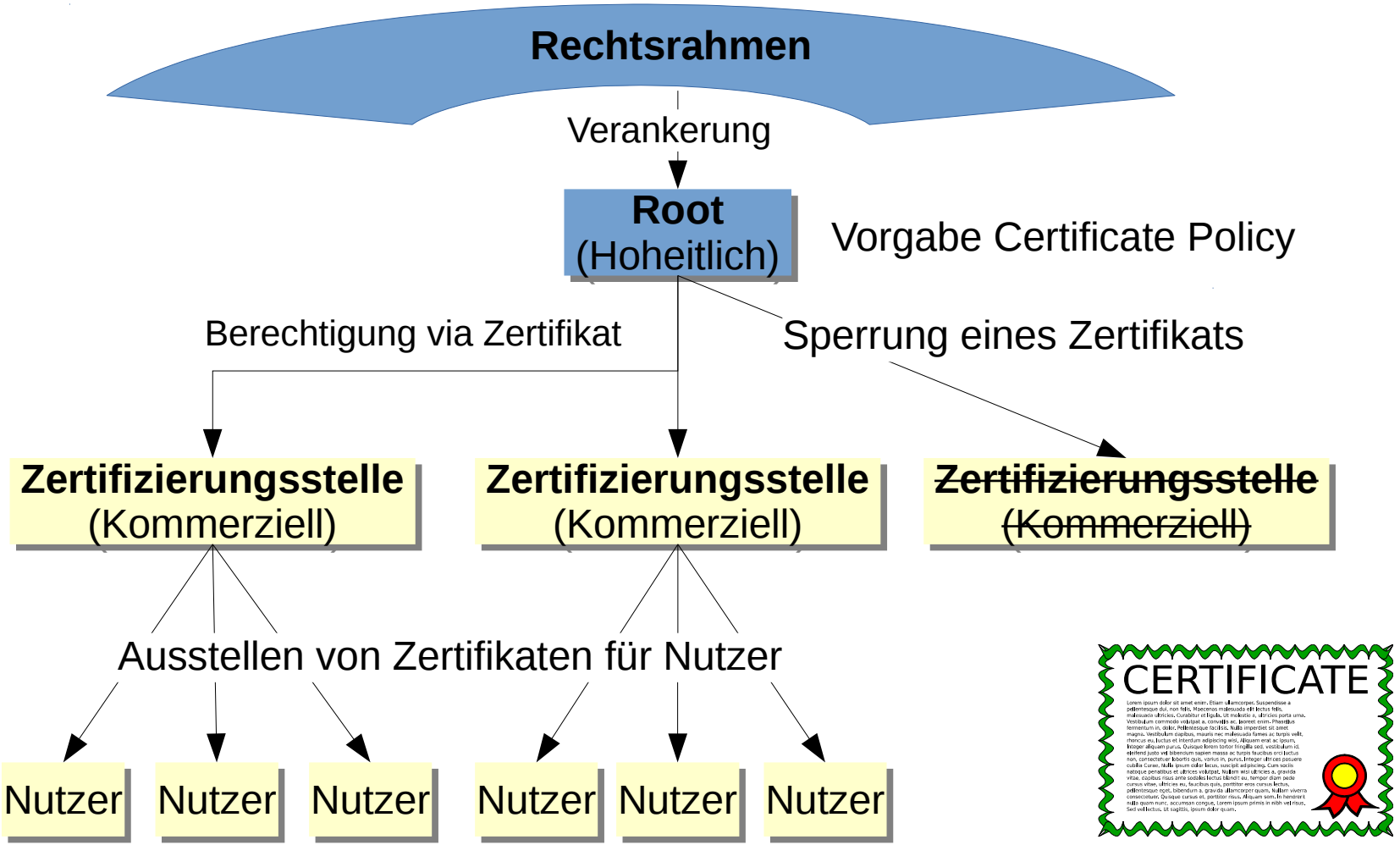
Beiträge des BSI

- Technische Richtlinien, verpflichtend und/oder empfehlend

- Orientierungshilfen und Handlungsleitfäden zur technisch-organisatorischen Umsetzung der gesetzlichen Anforderungen, Stand der Technik

- Einige **Handlungsfelder im Umfeld EGovernment**:
  - Der neue Personalausweis mit Online-Ausweisfunktion und De-Mail
  - Weitere Vertrauensdienste und elektronische Identitäten
  - Bausteine für die eAktenführung

Hoheitliche Durchsetzung der Vertrauenswürdigkeit mit PKI



Online-Ausweisfunktion

Schutz vor **Identitäts-diebstahl**

Sichere und **nutzer-freundliche** Identifizierung von zu Hause

eBusiness und **eGovernment**

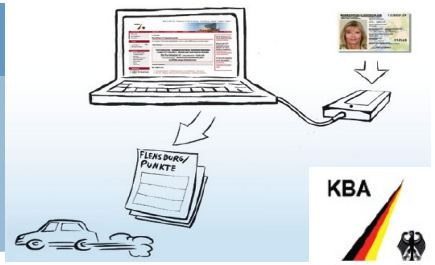
Online-Ausweisfunktion

- **Beidseitige Authentisierung**
  - Diensteanbieter mit Berechtigungszertifikat
  - Inhaber mit gültigem Ausweisdokument
- 2-Faktor Authentisierung des Inhabers durch
  - **Besitz** (Zertifikat im nPA) und
  - **Wissen** (PIN)
- Obligatorische Nutzung bei De-Mail
  - Sichere Kommunikationsinfrastruktur
- Schaffung neuer Anwendungen
  - E-Government-Initiative
  - Nutzung als Schriftformersatz
  - etc.

eGovernment

Kraftfahrtbundesamt

Punkteauskunft aus dem Verkehrszentralregister



Deutsche Rentenversicherung

Rentenauskunft online abrufen

Persönliche Daten ändern

Deutsche Rentenversicherung

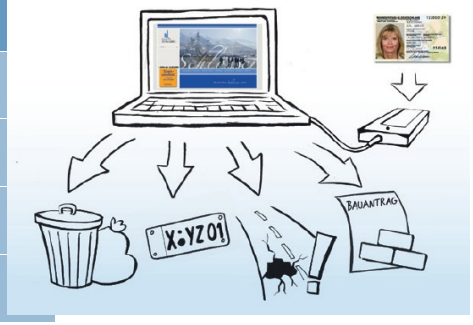
Verschiedene Bürgerservices bei kommunalen Verwaltungen

Baugenehmigung

Kfz An-/Abmeldung

Führungszeugnis online beantragen

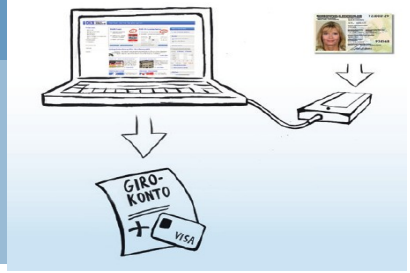
Wahlschein beantragen



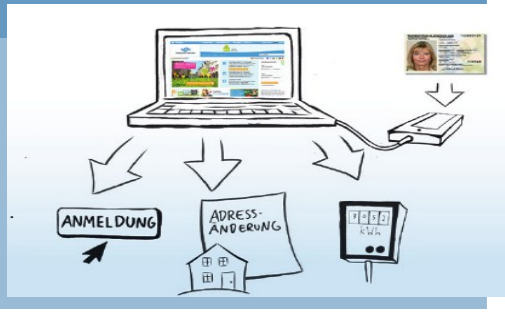
eBusiness

Versicherungen
Persönliche Daten ändern
Vertrag abschließen oder ändern
Login Webseite

Finanzen
Konto eröffnen
Persönliche Daten ändern
Login Website



Stadtwerke Münster – Dienstleister für Energie und Wasserversorgung
Zählerstandsangabe
Produktwechsel
Persönliche Daten ändern
Login Website



Sichere Identitäten (1)

Primäridentität

Authentische Daten + Kennzeichen (Geheimnis) = **abgeleitete Identität**

Übertragung Datengruppen

Registrierung Authentisierungsmittel (generiere Geheimnis)

Technologien abgeleiteter Identitäten

Authentisierungssysteme

SSL

SSL

OpenID

OAUTH 2

fido alliance

Authentisierungsmittel

Secure

Mobile Connect

Yubikey

VDV-Kernapp

Schwerpunkte: Nutzung an mobilen Endgeräten, NFC, FIDO

Technische Realisierung mobiler Identitäten oder „Warum wir Near Field Communication brauchen“

NFC ist über den „Umweg“ kontaktloser Chipkarten bereits im Alltag angekommen

- *Öffentlicher Personenverkehr:*

  Mehrere Millionen kontaktloser Buchungsvorgänge täglich

- *Payment:*

  Ausgabe kontaktloser Kredit- und Debit-Karten fast flächendeckend

- *EGovernment:*

  37 Mio. Personalausweise mit Online-Ausweisfunktion

Synergieeffekte vorhandener Infrastrukturen nutzen

- Die Interoperabilität mit kontaktlosen Infrastrukturen und Medien nach ISO/IEC14443 soll zur Standardeigenschaft marktüblicher NFC-Mobilgeräte werden
- NFC-Mobilgeräte werden zu mobilen Terminals für bestehende und zukünftige eID-Anwendungen
- Integration abgeleiteter Identitäten wie FIDO als zur eID-Funktion komplementären Identifizierungsfunktion
- **NFC Initiative für Interoperabilität**

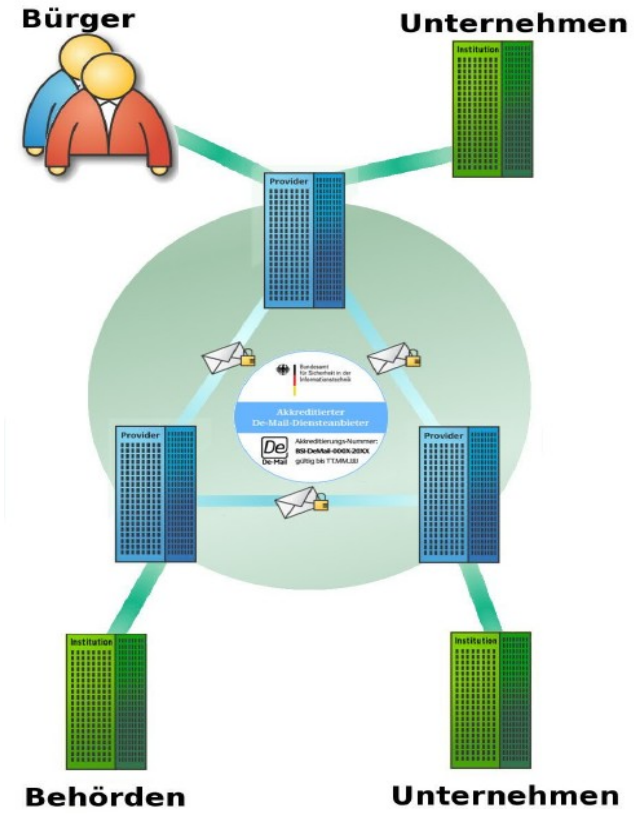
Bundesamt für Sicherheit in der Informationstechnik

Personalausweis mit Online-Funktion wird interoperable elektronische „Primäridentität“

De-Mail

De-Mails sind *sichere E-Mails*:

einfache E-Mail + Sicherheit + Datenschutz



Ziele sind u.a.

→ **Sicherheit,Vertraulichkeit und Nachweisbarkeit der Kommunikation**

→ **Identität der Kommunikationspartner ist sichergestellt**

→ **dennoch einfache Bedienbarkeit**

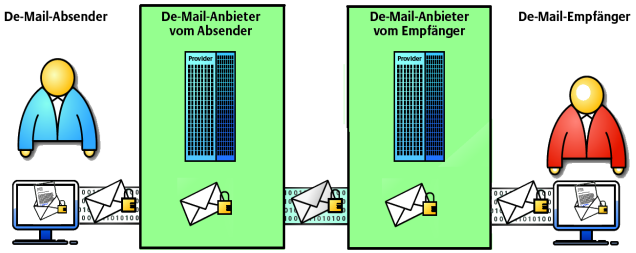
De-Mail ist ein geschlossenes System:

- Nachgewiesene Sicherheit & Vertrauenswürdigkeit durch definierte Anforderungen (De-Mail-Gesetz, Technische Richtlinie 01201des BSI)
- Unabhängige & sorgfältige Vorab-Prüfungen der angebotenen Dienste

Ende-zu-Ende-Verschlüsselung

De-Mail unterstützt zusätzliche Ende-zu-Ende-Verschlüsselung

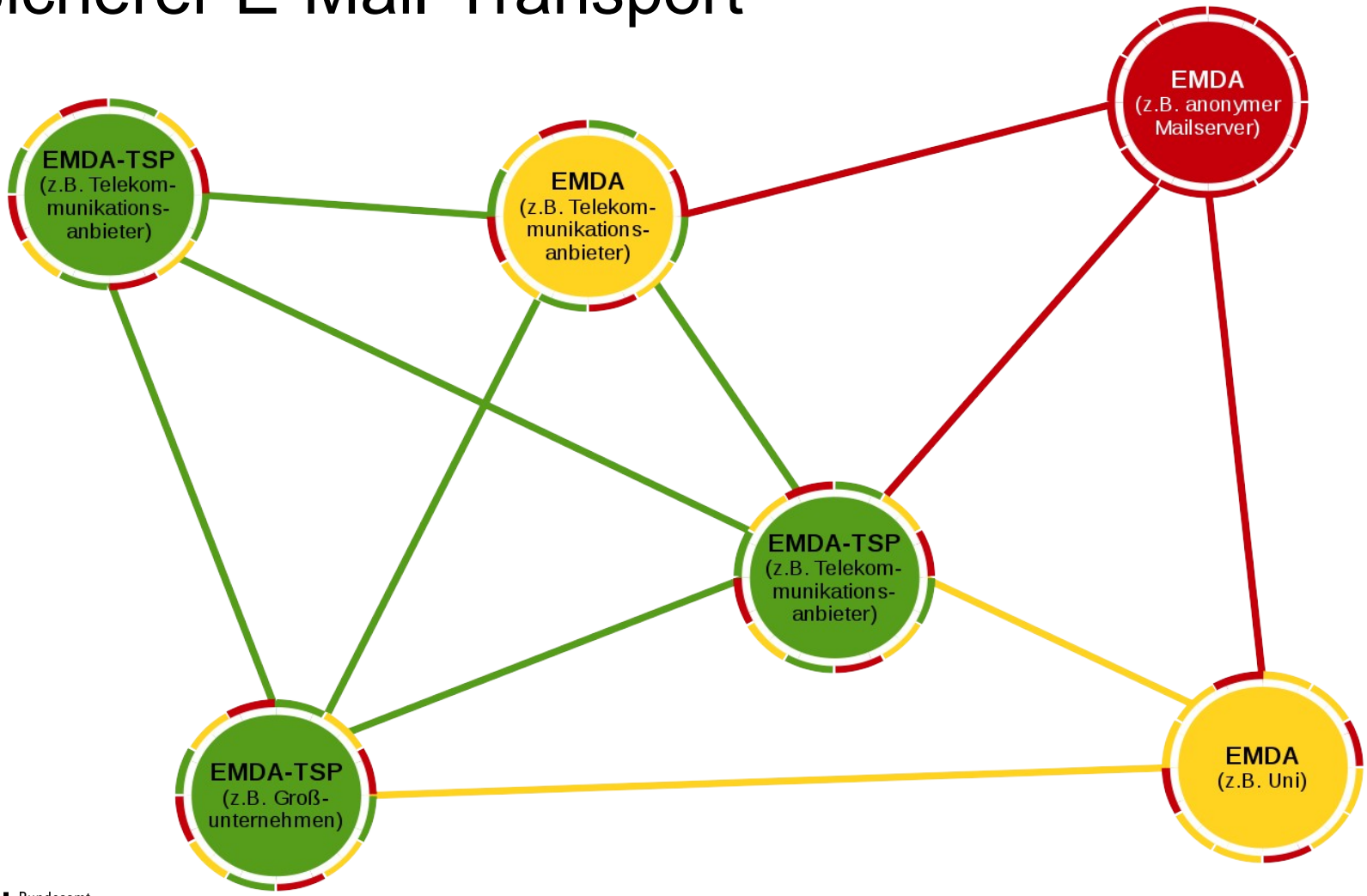
- Gatewayanbindung
  - Nutzung gängiger Plugins für E-Mail-Client
  - Hinterlegung des öffentlichen Schlüssels im öffentlichen Verzeichnisdienst möglich



- Login via Weboberfläche
  - NEU seit Frühjahr 2015: Browser-Erweiterung
  - Basis OpenSource-Programm „Mailvelope“
  - Leichte Bedienbarkeit, u.a. durch Vorschlag geeigneter Einstellungen bei Installation und gestützte Schlüsselverteilung

- Vor- und Nachteil dieser Verschlüsselung
  - Nur der Anwender hat Zugriff auf den eigenen privaten Schlüssel zur Entschlüsselung von so verschlüsselten und an ihn adressierten De-Mails.
  - Bei Schlüsselverlust/-löschung oder Vergessen des Passwortes durch diesen Eigentümer ist keine Entschlüsselung der De-Mails mehr möglich.

Technische Richtlinie
Sicherer E-Mail-Transport



Vertrauensniveaus & Mechanismen: TR 03107-1

- Maßnahme 10 der eID-Strategie des IT-PLR: Technische Richtlinie für Vertrauensdienste

  „Das BSI wird […] den Entwurf einer Technischen Richtlinie vorlegen, in der Vertrauensniveaus und entsprechende Kriterien für Vertrauensdienste definiert werden.“ (eID-Strategie)

- Betrachtung der Grundlagen und Mechanismen (z.B. eID, De-Mail, OSCI, TAN) für Vertrauensdienste (Identifizierung, Abgabe einer Willenserklärung, Dokumentenübermittlung und Übermittlung von Identitätsdaten)

- Mechanismen werden bestimmten Vertrauensniveaus zugeordnet (Hoch+, Hoch, Normal)

Übersicht über Vertrauensdienste und -niveaus

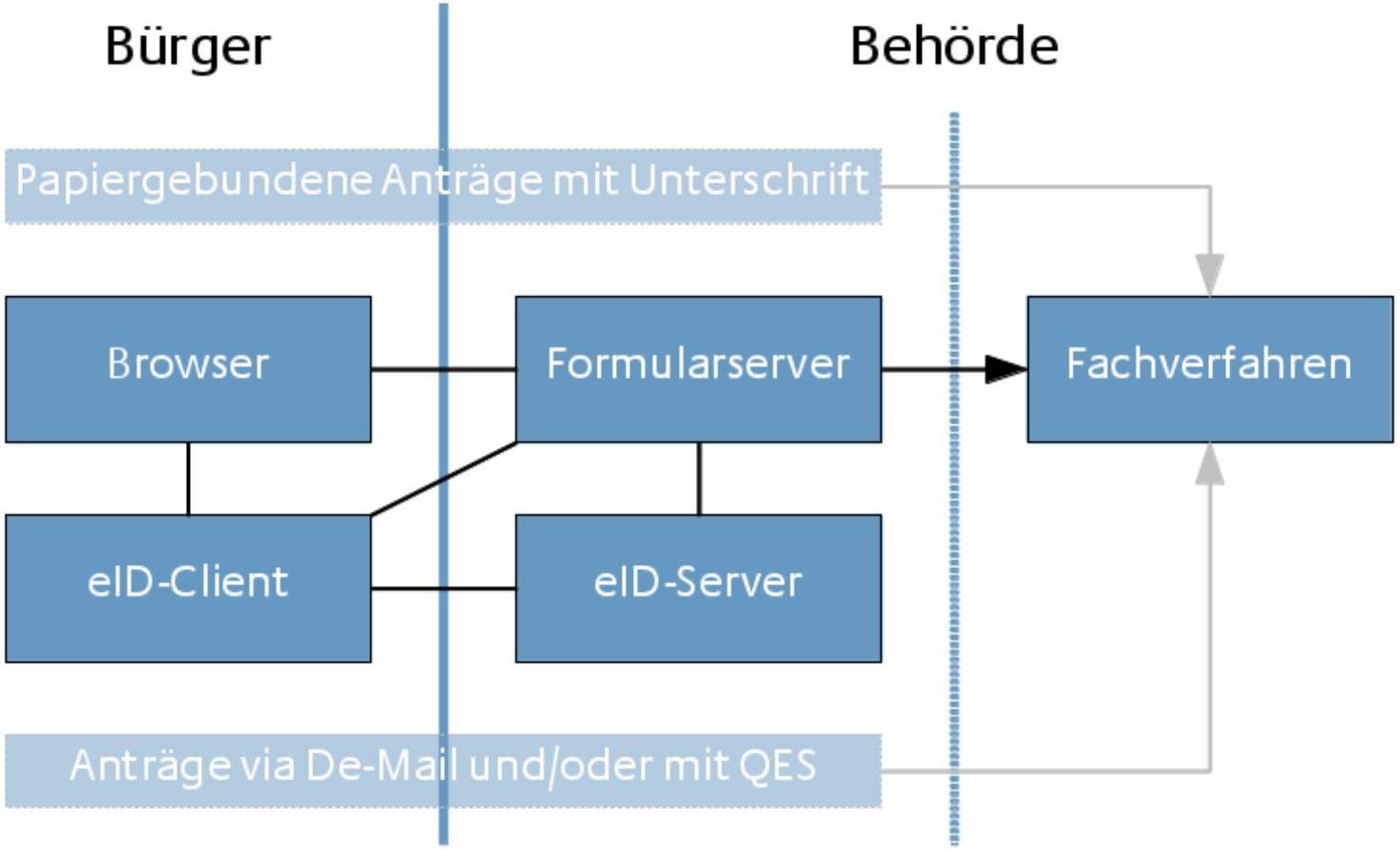
		Vertrauensniveaus normal	hoch	hoch+
Identifizierung	Personen: Registrierung/Erstidentifizierung	eID PA		
	Personen: Anmeldung / Login	UserID/Password Krypt. SW-Token Krypt. HW-Token eID PA		
	Dienste	SSL-Zertifikat Berechtigungs-Zertifikat		
Willenserklärung	Elektronische Signaturen	FES (SW-Token) FES (HW-Token) QES		
	Nicht signaturbasiert	Nutzerinteraktion TAN-Verfahren Formular + eID PA Absenderbestätigte De-Mail		
Dokumenten-übermittlung	Versand	De-Mail E-Mail + S/MIME OSCI (Transport-verschl. + Signat.) OSCI (E2E-Verschlüsselung +Signatur) Absenderbestätigte De-Mail		
	Web-Upload	SSL-Zertifikat eID PA		

Elektronischer Schriftformersatz mit elektronischem Identitätsnachweis

- Verwaltungsverfahrensgesetz § 3a
  - Die Schriftform kann ersetzt werden durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird.
  - In den Fällen [des Satzes 4 Nummer 1] muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 Personalausweisgesetz oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

- Technische Richtlinie TR 03107-2 regelt:
  - Erfüllung der verschiedenen Funktionen der Schriftform
  - Technische Anforderungen zur Umsetzung

Elektronischer Schriftformersatz mit elektronischem Identitätsnachweis



Sichere Identitäten (2)

Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-VO)

- Elektronische Identifizierung von Personen und Unternehmen in allen EU-Ländern
  - Assurance Level nach STORK oder ISO 29115 kompatibel mit BSI TR-03107
- Grenzüberschreitende elektronische Vertrauensdienste zur Ablösung von papiergebundenen Verfahren
  - Signaturen
  - Siegel
  - Zeitstempel
  - Zustelldienste
  - Webseitenzertifikate

Durchsetzung Technischer Standards für sichere Identitäten und Vertrauensdienste

Sichere Identitäten (3)

Die EU-Richtlinie 2007/64/EG wird u.a. überarbeitet, weil

- eine ausreichende Standardisierung und Interoperabilität unterschiedlicher Zahlungsdienste bei Kartenzahlungen sowie e- und mPayments nicht gegeben ist.

Zentraler Punkt der PSD 2 aus Sicht der Informationssicherheit:

- Notwendigkeit der „Strong Customer Authentication“ für das Abrufen von Kontoinformationen und das Durchführen von Transaktionen wird gefordert.
- Definition von Strong Customer Authentication mittels **Kombination von zwei der drei möglichen Faktoren**

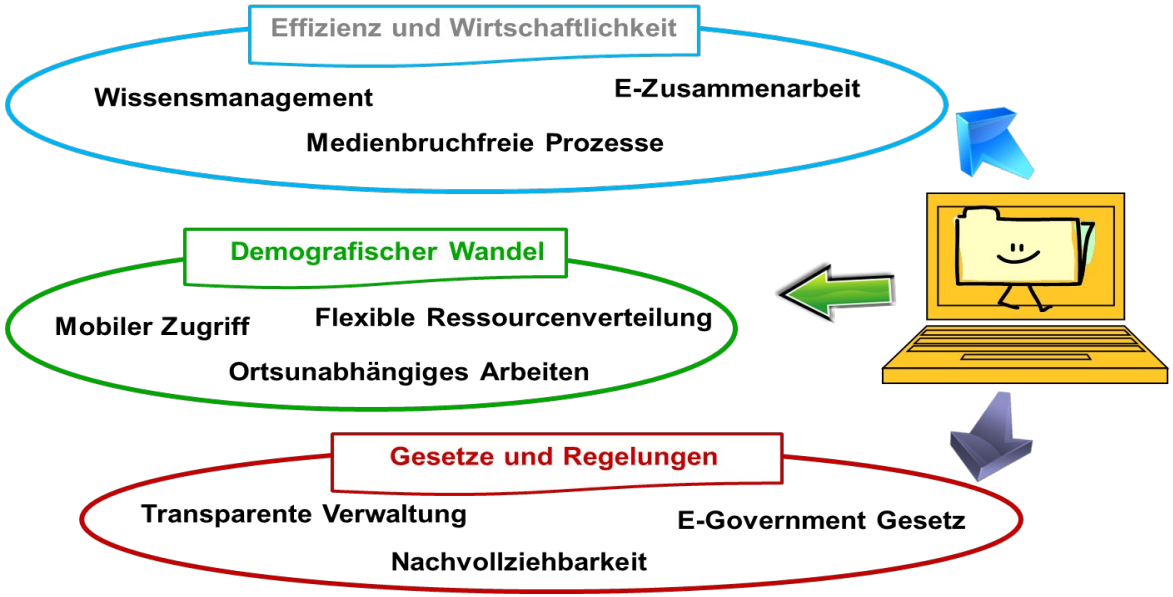
Chance für die Informationssicherheit:

- Gestalten einer sicheren, **datenschutzgerechten und anwendbaren Authentisierungslösung** durch die EZB, die European Banking Authority und das SecurePay-Forum

Durchsetzung Technischer Standards zur sicheren Identifizierung

Elektronische Aktenführung/Digitalisierung

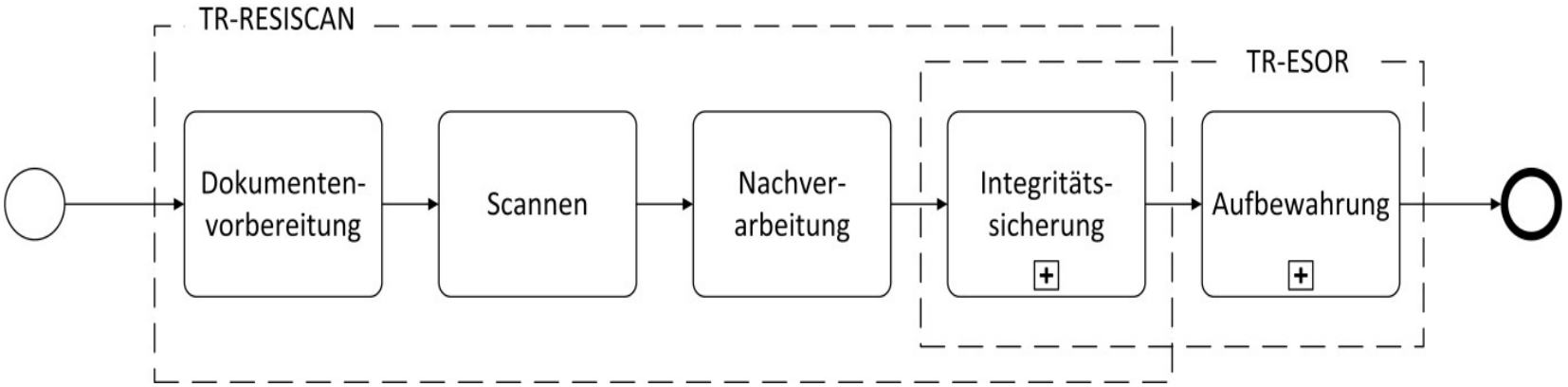
- §§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen und Langzeitaufbewahrung nach dem „Stand der Technik“
- Beweisregelungen zugunsten nach Stand der Technik eingescannter Dokumente, z.B. §§ 371 b, 298a ZPO
- Orientierungshilfen des BSI durch Technische Richtlinien



Beweiskraft-erhaltende Erstellung & Aufbewahrung elektronisch signierter Daten

→ Lösungsansätze für den **Beweiswerterhalt**: BSI TR-03125 ESOR

→ Lösungsansätze für das **ordnungsgemäße ersetzende Scannen**: BSI TR-03138 RESISCAN



Das IT-Sicherheitsgesetz - Regelungskomplexe

- Verbesserung der IT-Sicherheit bei Unternehmen
- Verbesserung der IT-Sicherheit des Bundes
- Stärkung des BSI
- Schutz der Bürger in einem sicheren Netz

Verbesserung der IT-Sicherheit bei Unternehmen

- WER wird reguliert
  - Betreiber kritischer Infrastrukturen
  - Ausnahme: Kleinstunternehmen
  - Vorrang von spezialgesetzlichen Regelungen
- WAS wird reguliert
  - Einhaltung von Mindeststandards (inkl. Nachweispflicht)
  - Meldepflicht für Sicherheitsvorfälle
- WIE wird reguliert - Kooperativer Ansatz – aber mit Sanktionsmöglichkeit (OWi), bei Kooperationsverweigerung

Ausblick

Vielfältige Vertrauensanker der Informationssicherheit

- Leistungsfähige Technologien sind vorhanden
- Usability ist wesentlicher Erfolgsfaktor
- security-by-design muss sich weiter durchsetzen
- Kooperativer Ansatz und Regulierung ergänzen sich
- IT-Sicherheitsstandards „Made in Germany“

Anforderungen für Nachfragemärkte

- **Technische Standards** entwickeln
- Unabhängiger **Nachweis** über deren Einhaltung ermöglichen (z.B. Zertifikat)
- **Verbindlichkeit** von Standards schaffen

Marktführer zur Wiederherstellung des Vertrauens motivieren

- Im öffentlichen Diskurs

Erhalt gesellschaftlicher Werte und der Grundrechte der Bürger

- Art. 1 / Art. 2 GG, Art. 10 GG

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Astrid Schumacher
Leiterin des Referats S 11 Sicherheit in eID-Anwendungen
Godesberger Allee 185-189
D-53175 Bonn

Telefon: 022899-9582-5371
Fax: 022899-10-9582-5371

astrid.schumacher@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de
www.buerger-cert.de