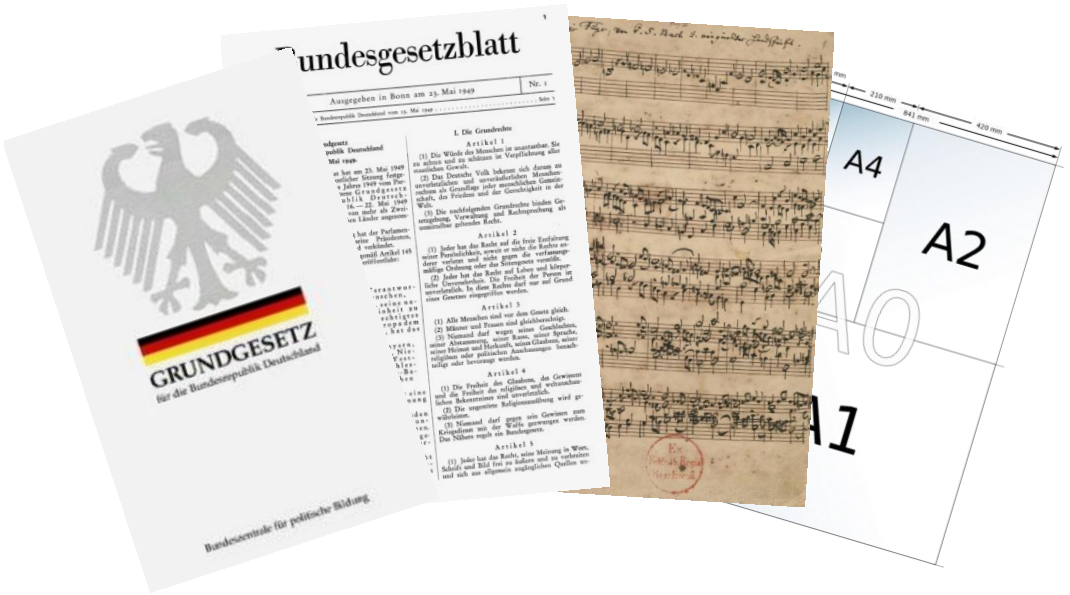
Normen und Standards für die IT-Sicherheit

- Gesellschaftliche Normen und technische Standards
- Bedeutung von IT-Sicherheitsstandards
- Standardisierungsauftrag der Digitalen Agenda
- Normungsbedarf IT-Sicherheit
- Voraussetzungen und Rahmenbedingungen
- Beitrag des BSI
- Beispiel eines spezialgesetzlichen Normungsprojekts
- Fazit

Bernd Kowalski
Bundesamt für Sicherheit der Informationstechnik
Workshop Normung und Standardisierung in Digitaler Agenda
Donnerstag, 30. Oktober 2014, BMWi, Berlin

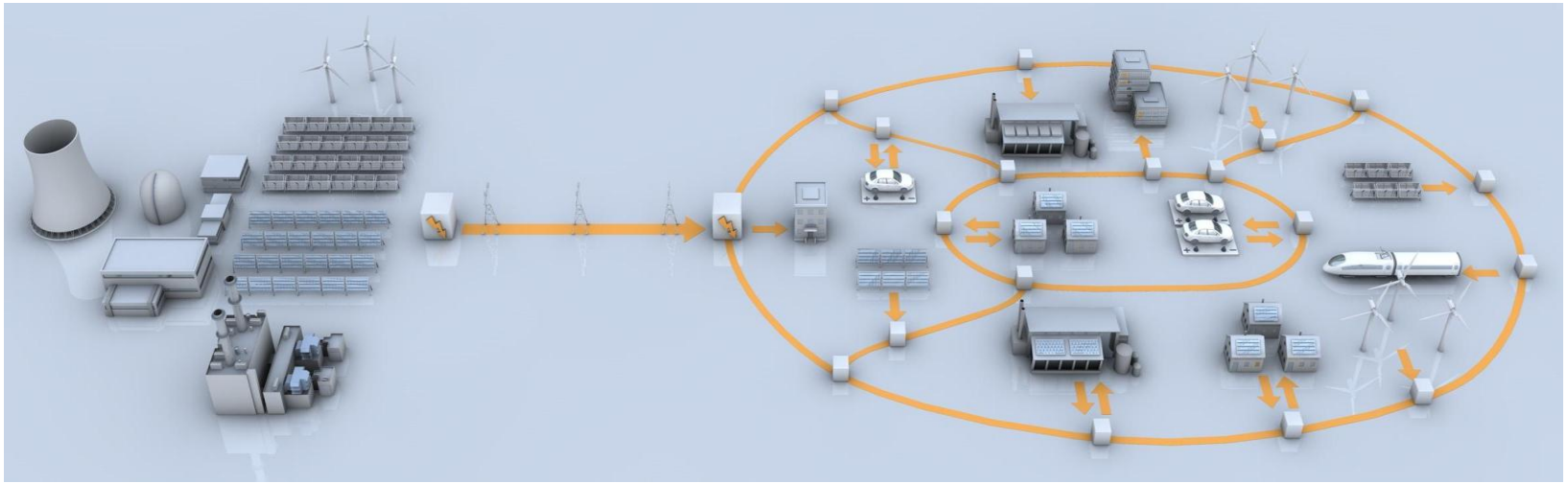
Gesellschaftliche Normen und technische Standards



Normen gesellschaftlichen Zusammenlebens:

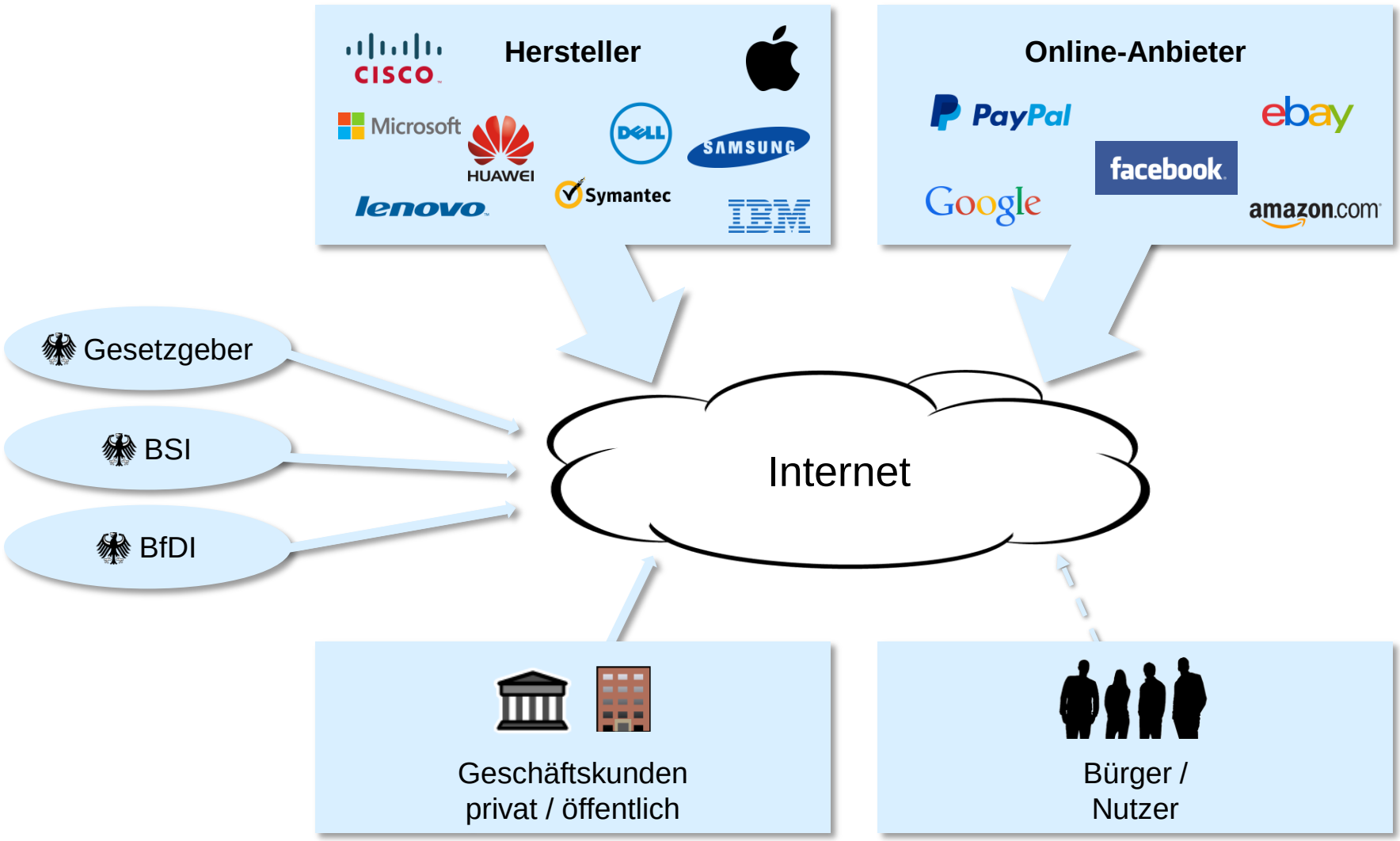
- Sprache, **Kommunikation**, Infrastruktur
- Gesellschaftliche **Werte / Grundrechte**, wie Unversehrtheit, Freiheit, Lebensqualität, informationelle Selbstbestimmung (Art. 1 u. 2 GG), Fernmeldegeheimnis (Art. 10 GG)
- **Spezialgesetze** mit Bezug zu **technischen Standards**

Bedeutung von IT-Sicherheitsstandards
…in Zeiten technologischen Wandels



- Wirtschaft und Gesellschaft hängen von **Verfügbarkeit** und **Integrität** der IKT ab
- **Datenschutz-** und **Vertrauensdefizite** in vielen Produkten & Dienstleistungen
- Wahrung der öffenlichen **Sicherheit**
- **Entwicklung** und **Durchsetzung** angemessener technischer Standards
- Schaffung von **Märkten** für technische Standards “Made in Germany”

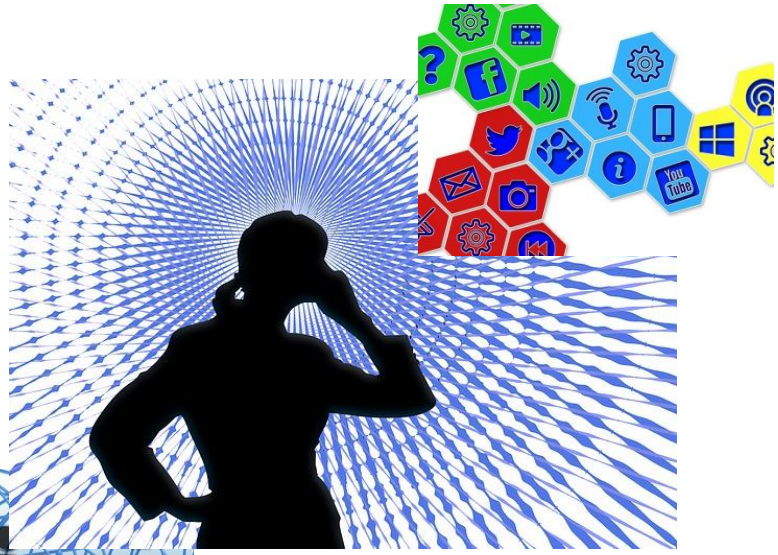
Wer setzt die Standards?



Standardisierungsauftrag der Digitalen Agenda

Digitalisierung, Automation, Vernetzung in allen Lebensbereichen:

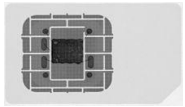
- Smart Grid, Smart Metering (KRITIS)
- Smart Home, Smart Services
- Industrie 4.0 / Fernwartung
- eMobility / car2car / car2x
- eHealth/eGovernment
- Cloud Computing
- eID / ePayment
- eCommerce
- Big Data



Verfügbarkeit, Vertrauenswürdigkeit, Transparenz

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. Bürgerkonten

Technische Standards

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

Voraussetzungen und Rahmenbedingungen

IT-Innovationen in Kernbereichen der deutschen Wirtschaft

- **Fertigungs-** / Automatisierungstechnik, Fe**r**nwartung
- **Verkehrstelematik**: Car-to-Car, Car-to-X, Assistenzsysteme

→ IT-Sicherheitsstandards „Made in Germany“

Anforderungen für Nachfragemärkte

- **Technische Standards** entwickeln
- **Nachweis** über deren Einhaltung ermöglichen (z.B. Zertifikat)
- **Verbindlichkeit** von Standards schaffen durch:
  - **Herstellererklärungen**, Branchenverpflichtungen
  - Verwaltungsvorschriften, LM in **Ausschreibungen**, EU- / D-**Recht**

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
- **TTIP**: Verteidigung deutscher / europäischer Sicherheitsstandards

Beitrag des BSI (1)

Entwicklung Technischer Standards unterstützen

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

Zertifizierung

- Komponenten
- Produkte
- Dienstleistungen
- Dienstleister

Unterstützen von Gesetzgeber und Politik

- Intelligente Messsysteme (EnWG/EEG)
- Gesundheitstelematik (SGB V § 291)
- eID-Verfahren (EU-KOM/eIDAS)
- TTIP (EU-KOM, BR)

Beitrag des BSI (2)
DIN-Normungsgremien

NIA - Gesamtlenkungsausschuss (GLA):

CSCG / KITS / KOSI

NA 043-01-27 AA
IT-Sicherheitsverfahren

- **NA 043-01-27-01 AK**
  Anforderungen, Dienste und Richtlinien für IT-Sicherheitssysteme
- **NA 043-01-27-02 AK**
  IT-Sicherheitstechniken u. -mechanismen
- **NA 043-01-27-03 AK**
  Evaluationskriterien für IT-Sicherheit
- **NA 043-01-27-04 AK**
  IT-Sicherheitsmaßnahmen und Dienste
- **NA 043-01-27-05 AK**
  Identitätsmanagement und Datenschutz

NA 043-01-17 AA
Karten und persönliche Identifikation

- **NA 043-01-17-03 UA**
  Maschinenlesbare Reisedokumente
- **NA 043-01-17-04 UA**
  Austauschprotokolle bei Chipkarten
- **NA 043-01-17-08 UA (NFC-Forum)**
  Kontaktlose Chip-Karten

Weitere DIN-Gremien

- **NA 009-00-15-06 AK**
  Beweiswerterhaltung kryptographisch signierter Dokumente
- **NA 043-01-31 AA**
  Automatische Identifikation und Datenerfassungsverfahren
- **NA 043-01-37 AA**
  Biometrie
- **NA 043-03-03 AA**
  Elektronisches Geschäftswesen
- **NA 159-01-16 GA**
  Dienstleistungen für Sicherheitsanlagen

Beitrag des BSI (3)
DKE-Normungsgremien

PG „Umsetzung EnWG“ / Kompetenzzentrum Normung eEnergy & Smart Grids

- DKE STD 1911 Lenkungsausschuss d. Kompetenzzentrums
- DKE/UK STD_1911.4 Koordinierung Smart Metering
- DKE/AK STD_1911.0.1 AK Preis-/Tarifmodelle
- DKE/AK STD_1911.0.2 Use Cases
- DKE STD-1911.3 Verteilnetzautomatisierung
- DKE STD -1911.11 Smart Grid Informationssicherheit (-> Smart Grid Coord. Group)
- DKE 461.0.14 Gateway und Datenübertragung
- DKE 461.0.142 COSEM(Datenstrukturen)-Modellierung für SMGW
- DKE 461.0.143 Webservices für SMGW
- DKE UK 931.1 IT-Sicherheit in der Automatisierungstechnik
- DKE AK 952.0.15 Sicherheit in der Elektrizitätsversorgung
- DKE 716.0.1 Normative Beschreibung eines Sicherheitskonzeptes für Energiemanagement im Gebäude
- …

Andere Gremien im DKE:

- DKE UK 713.1,2, 5, 12, 13, 14 Gefahrenmelde- und Überwachungsanlagen, Zutrittskontrollanlagen
- Überwachungsanlagen, Alarmanlagen
- DKE 967.1 Leittechnik für kerntechnische Anlagen
- DKE 351.3.7 Security Anforderungen an signaltechnischen Einrichtungen d. Bahn
- …

Beispiel eines spezialgesetzlichen Normungsprojekts: Intelligente Messsysteme für Strom und Gas (1)

EU-Richtlinien:

- Vorgaben für **Smart Metering**, **Strom** (2009/72/EG) und **Gas** (2009/73/EG): Einführung bei 80 % der Verbraucher bis 2020 o. Kosten-Nutzen-Analyse
- **Energieeffizienzrichtlinie** 2012/27/EU (Nationale Umsetzung bis 5.6.2014): Art. 9: Sichere Datenkommunikation, Datenschutz, Verbrauchsvisualisierung

Energiewirtschaftsgesetz (EnWG):

- Anforderungen und Pflichteinbaufälle **intelligenter Messsysteme** (§ 21 ff)
- **Sichere Anbindung** von Messeinrichtungen in ein Messsystem (§ 21c Abs.5)
- Verweis auf **Schutzprofile**, **Technische Richtlinie** (§ 21i Abs.1 Nr. 12)

Erneuerbare-Energien-Gesetz (EEG):

- Ferngesteuerte **Reduzierung der Einspeiseleistung** und Abruf der Ist-Einspeisung bei Netzüberlastung (§ 9) und Direktvermarktung (§ 34)

Rechtsverordnungen:

- Stromnetzzugang [umgesetzt] (§ 40 Abs. 5 EnWG: Bilanzierung / Variable Tarife)
- **Messsystem** [**notifiziert** am 23.09.2013] (Technische Mindestanforderungen:
- **BSI Schutzprofile / Technische Richtlinien**; Umsetzung Energieeffizienzrichtlinie)
- **Datenschutz** (§ 21g EnWG: Nutzung personenbezogener Daten)
- **Rollout** (Umsetzung der KNA, weitere Einbauverpflichtungen, Finanzierung)
- **Lastmanagement** (§ 14a EnWG: Nachtspeicher, Wärmepumpen, Elektromobile)

Beispiel eines spezialgesetzlichen Normungsprojekts: Intelligente Messsysteme für Strom und Gas (2)

Stakeholder

Staat

- Bundesministerium für Wirtschaft und Technologie
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesnetzagentur
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- PTB Physikalisch Technische Bundesanstalt, Braunschweig und Berlin

Verbände (u.a.)

- bdew Bundesverband der Energie- und Wasserwirtschaft e.V.
- VKU
- BITKOM
- DKE, FNN, VDE, DIN
- ZVEI
- Firmen im Gas- und Wasserfach figawa
- BEE Bundesverband Erneuerbare Energie e.V.
- OMS
- DVGW
- verbraucherzentrale Bundesverband
- bne Bundesverband Neuer Energieanbieter
- GdW
- vatm Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V.
- TeleTrusT Pioneers in IT security.

Hersteller (u.a.)

- Dr. Neuhaus
- Landis+Gyr
- PPC Power Plus Communications
- theben
- EMH metering
- devolo
- hager
- Itron
- GÖRLITZ
- elster
- DIEHL Metering

Beispiel eines spezialgesetzlichen Normungsprojekts: Intelligente Messsysteme für Strom und Gas (3)

Technische Standards, Prüfen und Zertifizieren

Schutzprofile (Protection Profile, PP)

Mindestsicherheits-anforderungen

- Gateway (Zertifiziertes PP-0073) V 1.3
- Sicherheitsmodul (Zertifiziertes PP-0077) V 1.02

Technische Richtlinie (TR 03109)

Mindestfunktionalität / Interoperabilität

- -1. Gateway (1.0)
- -2. Sicherheitsmodul (1.01)
- -3. Kryptographische Vorgaben (1.1 – 2014)
- -4. PKI (1.0)
- -5. Kommunikationsadapter
- -6. SMGW-Administrator (ersetzt -1. Anlage V)

Bauartzulassung

Eichrecht

- Gateway ist eichrechtlich relevant (PTB-A 50.8)
- Keine Sicherheits-anforderungen an Zähler möglich (Messgeräte-Richtlinie MID 2004/22/EG)

Fazit

- Die **Digitalisierung kommt**, so oder so!
- Um Einfluss zu erlangen, müssen Staat und Wirtschaft eine **gestalterische Rolle** einnehmen

Gestaltungsinstrumente:

- **Innovationskraft** aus den **Kernbereichen** der deutschen Wirtschaft
- Technische **Standards**
- **Unabhängige Prüf**- und **Zertifizierungsverfahren**
- **Verbindlichkeit** durch Rechtsnormen, Branchenabstimmung, Herstellerverpflichtungen
- Nationale **Referenzmärkte** („sell what you use“)

Ziele im Sinne der Digitalen Agenda:

- **Erhalt gesellschaftlicher Werte** und **technologischer Handlungsfähigkeit**
- **Teilhabe** an der **Wertschöpfung** und **Gestaltung neuer IKT auf In- und Auslandsmärkten**
- Aufwertung des „**Made in Germany**“ durch **vertrauenswürdige IT-Sicherheitsmerkmale**

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bernd Kowalski
Abteilung S
Godesberger Allee 185-189
53175 Bonn

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de