Bundesamt
für Sicherheit in der
Informationstechnik

Die eIDAS-Verordnung und ihre Umsetzung

Dr. Astrid Schumacher

Bundesamt für Sicherheit in der Informationstechnik

24. Deutscher EDV-Gerichtstag

Saarbrücken 24.09.2015

eIDAS-Verordnung

Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

- Elektronische Identifizierung
  - Personen und Unternehmen sollen mit ihren eigenen eIDs Dienste in anderen EU-Ländern nutzen können
- Vertrauensdienste
  - Sollen grenzüberschreitend in ganz Europa funktionieren
  - Sollen gleichen Rechtsstatus haben wie Papierverfahren

Stand der Dinge

- 18.09.2014: Verordnung tritt in Kraft: unmittelbare Rechtswirkung in allen MS-Staaten
  - Aufhebung der SigRL (1999/93/EG)
- 18.09.2015: Freiwillige Anerkennung von eIDs
  - Durchführungsrechtsakte für eID müssen erlassen sein
  - verpflichtende Durchführungsrechtsakte für Trust Services müssen erlassen sein*
- 01.07.2016: Regelungen zu Vertrauensdiensten wirksam
  - Durchführungsrechtsakte für TSP ~~müssen~~ sollten erlassen sein
- 18.09.2018: Verpflichtende Anerkennung von eIDs

Sinn und Zweck

- Art. 25-34 VO und allg. Vorschriften für Vertrauensdienste in Art. 13-24 VO: Novellierung bzw. Ersatz der europäischen Signaturregelungen nach der Signaturrichtlinie von 1999 (RL 1999/93/EG, Abl. 1999 L13, 12):

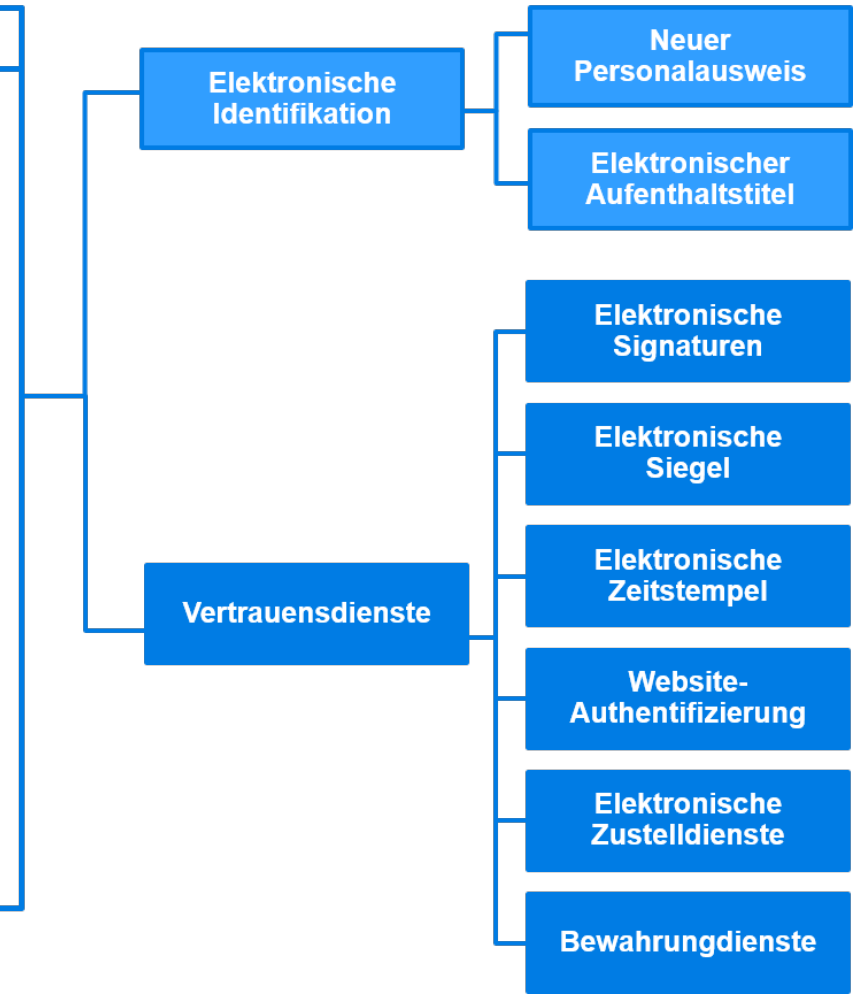
  „**Stärkung und Erweiterung der Vorschriften der SigRL**“

  durch die eIDAS-VO sowie Ergänzung um einen einheitlichen Rechtsrahmen für alle elektronischen Sicherheitsdienste (Erwägungsgrund 3)
- Sicherstellung des ordnungsgemäßen Funktionierens des Binnenmarktes – Integrationsfunktion des Unionsrechts
- Marktstrategie!

Regelungsinhalte

Regelungsinhalte

- Einheitliche Maßgaben für sichere elektronische Geschäftsprozesse in Europa
- Vorgaben zur rechtlichen Bedeutung und technischen Umsetzung
- QES und Siegel = Ersatz der Unterschrift
- QES und Siegel = höchster Beweiswert
- Einheitliche Vorgaben zur Sicherheit von eID und Vertrauensdiensten
- Notifizierung und EU-weite Anerkennung von eID
- Notifizierung qualifizierter Vertrauensdienste (VDA) durch einheitliche Zertifizierungsstellen je EU-Land
- Einheitliche Sicherheitsvorgaben und periodische Prüfungen
- Eintragung der VDA in Vertrauensliste (TSL)
- Behörden müssen alle notifizierten eID-Verfahren und Produkte qualif. VDA annehmen und prüfen können
- Technische Vorgaben in Ausführungsbestim-mungen und verbindlichen europäischen Normen



Verpflichtende Durchführungsrechtsakte (IAs)

- eID
  - Sicherheitsniveaus („niedrig“, „substantiell“, „hoch“) gemäß Art. 8 Abs. 3
  - Organisatorische Zusammenarbeit gemäß Art. 12 Abs. 7
  - Interoperabilitätsrahmen (Technische Zusammenarbeit) gemäß Art. 12 Abs. 8
- Qualifizierte Vertrauensdienste allgemein
  - Vertrauenslisten gemäß Art. 22 Abs. 5
  - Vertrauenssiegel (Logo) gemäß Art. 23 Abs. 3
- Elektronische Signaturen und elektronische Siegel
  - Fortgeschrittene Signatur- und Siegel-Formate gemäß Art. 27 Abs. 5 bzw. Art. 37 Abs. 5 (gemeinsamer IA)
  - Qualfizierte elektronische Signaturerstellungseinheiten gemäß Nachsatz von Art. 30 Abs. 3 (einziger verpflichtender IA, der noch fehlt)

Signaturerstellungseinheiten

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

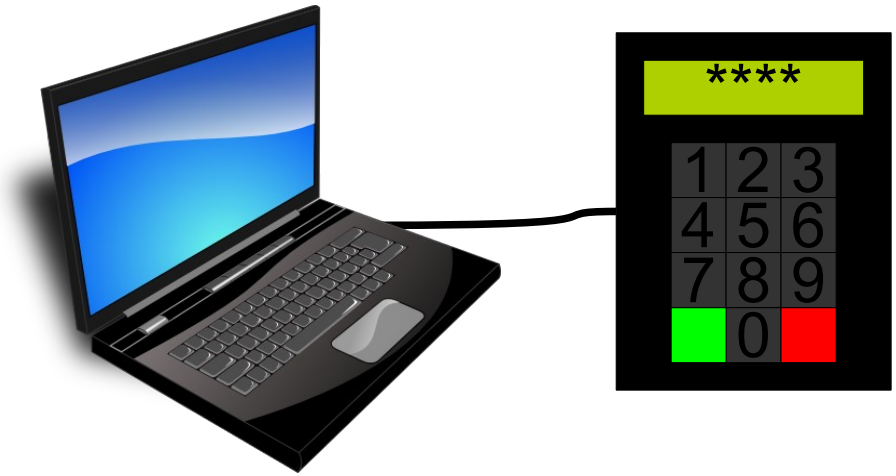
Anforderungen zwischen SigRL und eIDAS i.W. unverändert

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-VO –

- 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-VO Erwägungsgrund (56)
  - [...] der Anwendungsbereich der **Zertifizierungspflicht** [soll] **Signaturerstellungsanwendungen ausschließen**.

Signaturanwendungskomponenten

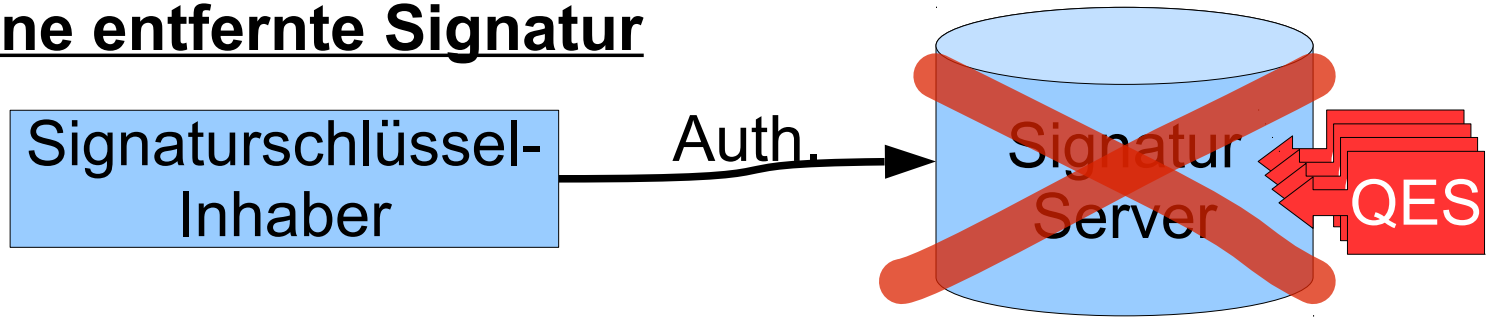
- Keine Anforderungen an SAKs
- Keine Zertifizierung / Bestätigung für SAKs
- Keine Anwendungsempfehlung „guter“ SAKs
  - Immerhin [eIDAS-VO & SigRL]:
    Qualifizierte elektronische Signaturerstellungseinheiten dürfen [...] **nicht verhindern**, dass dem Unterzeichner diese Daten vor dem Unterzeichnen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

- Es ist dem Anwender überlassen wie (und ob!) er sich zu signierende Daten anzeigen lässt
  - Willenserklärung?

Anforderungen nach SigG

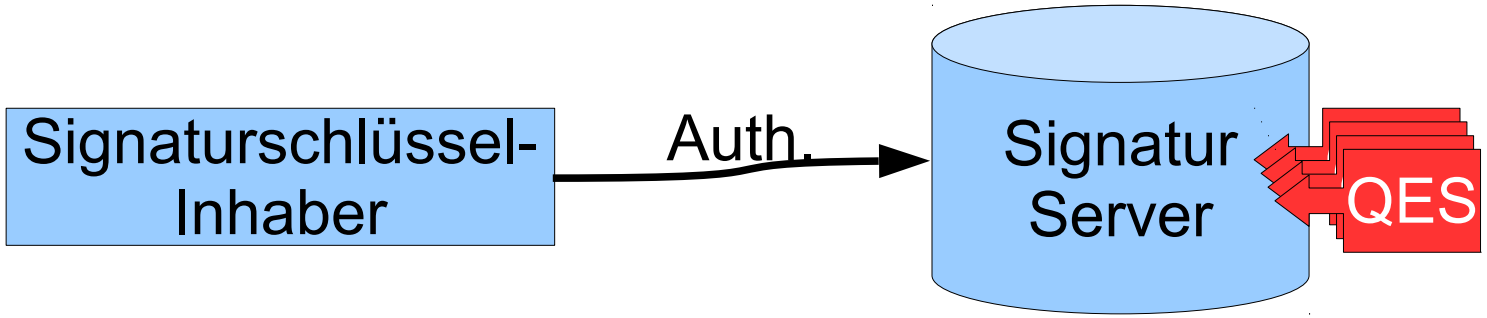
- **SigRL Artikel 2(2):**
  - ✗ „fortgeschrittene elektronische Signatur“: eine elektronische Signatur, die folgende Anforderungen erfüllt:[...]
    - c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen **Kontrolle** halten kann;
- **Der Zertifizierungsdiensteanbieter hat [§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)



Zwischen-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-VO: Artikel 27 (3) „Die Mitgliedstaaten verlangen [...] **keine** elektronische Signatur **mit einem höheren Sicherheitsniveau** als dem der qualifizierten elektronischen Signatur.“
- Rechtliche Folgerungen?
  - Novellierung der dt. Sig.regelungen
  - Übernahme relevanter eIDAS-VO-Teile
  - Nicht mehr anwendbare Teile des dt. SigRecht sind zu streichen
  - Weitergeltende Regelungen sind anzupassen

Anwendungsvorrang

- eIDAS-VO setzt dt. Regelungen nicht ausser Kraft: getrennte Rechtsordnungen Union/Mitgliedsstaaten; kein Geltungsvorrang
- Jedoch: Nationale Regelungen dürfen der eIDAS-VO nicht widersprechen bzw. Eingrenzung auf nationale Anwendung.
- Rechtlicher Handlungsbedarf in DEU

Anwendungsbereich

- Art 1: Vertrauensdienste = el. Sig., el. Siegel, el. Zeitstempel, el. Zustelldienste; Art. 2 I: EU-Vertrauensdiensteanbieter, nicht: geschlossene Systeme

- Die eIDAS-VO berührt nicht das nationale Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrens-mäßige Formvorschriften (Erwägungsgrund 21, Art. 2 III).

- Trennung von materiell-rechtlichen und verfahrensrechtlichen Formerfordernissen (Schriftform ist jeweils Ausnahme); sowie: beweisrechtliche Fragen

Langzeitsicherung

- Bisher regelt § 17 SigV, wie der Beweiswert von Signaturen für Zeiträume über den Ablauf der Gültigkeit von Algorithmen hinaus gesichert werden kann (Übersignatur vor Ablauf der Sicherheitseignung)

- Nach eIDAS-VO können für den Erhalt der Vertrauenswürdigkeit ein Bewahrungsdienst (für qual. Sig. und qual. Siegel) genutzt werden, Art. 24 VO

- Neuer Dienst „Preservation“ muss noch ausgestaltet werden: Standardisierung! u.a. BSI-TR-ESOR 03125

Elektronisches Siegel

- Art. 2 Nr. 24-32, Art. 35-38 eIDAS-VO: Siegel ist einer juristischen Person zugeordnet (eindeutige Identifizierung)
- Rechtliche Vermutung des Ursprungs und der Unversehrtheit der damit verbundenen Daten, Art. 35 II VO
- Siegel sind nicht zur Abgabe von WE bestimmt, hierfür weiterhin el. Sig. notwendig + ggfs. Attribute /-zertifikate (z.B. Behördeneigenschaft)
  - lediglich Sicherung der Integrität und Kennzeichnung der Herkunft der el. Daten vom „Siegelersteller“, „technische Sig.“, keine Gleichwertigkeit zur handschriftlichen Unterschrift; vgl. auch Erwägungsgrund 65
  - Keine Absicherung der Authentizität
  - keine Prüfbarkeit der Berechtigung: erhöhtes Risiko der Verwendung durch Nichtberechtigte?

Elektronisches Einschreiben

- Zustellung durch qualifizierten Dienst
  - Konformitätsprüfung
  - Verleihung des Qualifikationsstatus durch Aufsichtsstelle
- Katalog zulässiger Identifizierungsmethoden Art. 24 I eIDAS-VO
- Öffentlich zugängliche Vertrauenslisten

→ Hohe Sicherheit durch neutrale Dienste und technisch-organisatorische Anforderungen

(Qualifizierte) Dienste für die Zustellung elektronischer Einschreiben

- Definition
  - **Nachweis** der Absendung und des Empfangs der Daten
  - **Schutz** vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung
- Voraussetzungen für **qualifizierte** Dienste
  - **Identifizierung** des Absenders mit einem hohen Maß an Vertrauenswürdigkeit
  - Identifizierung des Empfängers vor der Zustellung der Daten
  - Absenden und Empfangen der Daten ist durch eine **fortgeschrittene elektronische Signatur/Siegel** gesichert
  - Jede **Veränderung** der Daten wird dem Absender und dem Empfänger deutlich angezeigt
  - Datum und Zeit des Absendens, Empfangens oder einer Änderung der Daten werden durch einen **qualifizierten elektronischen Zeitstempel** angezeigt

Auswirkungen auf De-Mail

- Rechtswirkung De-Mail
  - Schriftformersatz (§ 3a II VerwVerfG / § 36a II SGB I)
  - Beweiswert: Anscheinsbeweis (§ 371a II ZPO)
  - → bleibt erhalten, auch weiterhin explizit für De-Mail

- Zusätzlich nach eIDAS-VO, sofern
  - entsprechende Versandoptionen (Versand-, Eingangs-bestätigung, absenderbestätigt, persönlich) gesetzt und
  - Anbieter besitzt Qualifikationsstatus nach VO
  - → Vermutung der Integrität, Authentizität und Zeitpunkte (Art. 43 II)

Rechtswirkungen elektronischer Signaturen

- Art. 2 III eIDAS-VO: VO berührt nicht das nationale Recht oder das Unionsrecht in Bezug auf den Abschluss und die Gültigkeit von Verträgen oder andere rechtliche oder verfahrensmäßige Formvorschriften (s.a. Erwägungsgrund 21)

- Art. 25 II eIDAS-VO: eine qeISig hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift, (s. auch Erwägungsgrund 49 Satz 2: Rechtswirkungen werden durch nationales Recht festgelegt)

Auswirkungen auf nationale Formvorschriften

- § 126 I BGB: gesetzliche Schriftform
- § 126 III BGB: Ersatz durch el. Form
- § 126a BGB: el. Form = qelSig nach SigG
- Nationaler Gesetzgeber kann weiterhin die elektronische Form ausschließen, wenn er nur die Schriftform (eigenhändige Unterschrift) zulassen will
  - §§ 126 III, 126a BGB, 3a II VwVfG, 87a III AO, 36a II SGBI, 130a I und 130b ZPO, 12 HGB, 39a BeurkG
  - Ersetzung der Schriftform durch el. Form – Ersetzung des Merkmals „Unterschrift“ durch die qelSig
  - Schriftform ~~gleich~~ qelSig
  - Vertrauensinfrastruktur dt. Sig.Recht = eIDAS-VO?

Haftungsfragen

- Art. 11 VO: der notifizierende MS und der Systembetreiber haftet für Schäden, die vorsätzlich oder fahrlässig zugefügt werden und auf eine Verletzung der sie betr. Pflichten bei einer grenzüberschreitenden Transaktion zurückzuführen sind
- Nationale Regelungen zum Begriff des Schadens, Klageverfahren und Beweislastverteilung sind davon unberührt (Erwägungsgrund 18)
- §§ 5 III 1-3 SigV, 11 IV SigG: Haftung für Verrichtungsgehilfen
- Keine spezielle Haftungsregelung für Siegel

Beweisvorschriften

- Systematik nach dt. Recht:
  - Eignung als Beweis
  - Qualifizierung des Beweismittels
  - Beweiswert

- Abstufungen:

  → Freie Beweiswürdigung

  → Anscheinsbeweis (Erschütterung möglich)

  → rechtliche Vermutung (Gegenbeweis notwendig)

Beweisvorschriften (ab dem 1.7.2016)

- Elektronische Dokumente (ohne und mit Sig.) müssen als Beweismittel zugelassen sein, Art. 46 VO, jedoch: keine Beweisregelung

- Anerkennung von el. Sig. und Siegeln in Gerichtsverfahren nach Art. 25 I, 35 I VO

- Anscheinsbeweis für qualif. sig. priv. Dokumente (§ 371a ZPO)

- Vermutungen für:
  - Authentizität und Integrität (qualif. Siegel)
  - Integrität und Zeitpunkt (el. Daten mit qualif. Zeitstempel)
  - Integrität, Authentizität und Zeitpunkte (el. Einschreiben)

Beweisvorschriften

- Beweiswirkung qualif. Siegel, Art. 35 II VO
  - Ggfs. Anpassung des § 371 a III ZPO, aber weiterhin Unterscheidung zwischen behördlich gesiegelt und signiert
- Beweiswirkung qualif. Zeitstempel, Art. 41 II VO
  - Neue Rechtslage, da bisher nicht geregelt
- Beweiswirkung qualif. el. Einschreiben, Art. 43 II VO
  - Neue Rechtslage, da bisher nicht geregelt

Konkretisierungsbedarf

- Anforderungen an SAKs?
- Keine beweisrechtliche Lösungen für
  - Präsentationsproblem
  - Fremdsignatur

- Anscheinsbeweis des § 371 a ZPO auch für qSiegel?
- Validierung der qualifizierten Elemente ist keine Voraussetzung für Beweiskraftregelung!
- Durchführungsrechtsakte: Durchsetzen von Standards?
- Identifizierung (Art. 24 I) und Attribute (Art. 28 II)
- Aufsicht über qualifizierte TSPs

Referenzen / Weiterführend

- Rossnagel, Alexander: Neue Regeln für sichere elektronische Transaktionen, NJW 2014, 3686 ff., sowie Der Anwendungsvorrang der eIDAS-VO, MMR 2015, 359
- Jandt, Silke: Beweissicherheit im elektronischen Rechtsverkehr – Folgen der europäischen Harmonisierung, NJW 2015, 1205
- Sosna, Sabine: EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten – eIDAS-Verordnung, CReport 12/2014, 825 ff.

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Astrid Schumacher
Leiterin des Referats S 11:
Sicherheit in eID-Anwendungen

Godesberger Allee 185-189
53175 Bonn

astrid.schumacher@bsi.bund.de

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