Bundesamt
für Sicherheit in der
Informationstechnik

Sicherer E-Mail-Transport (BSI TR-03108)

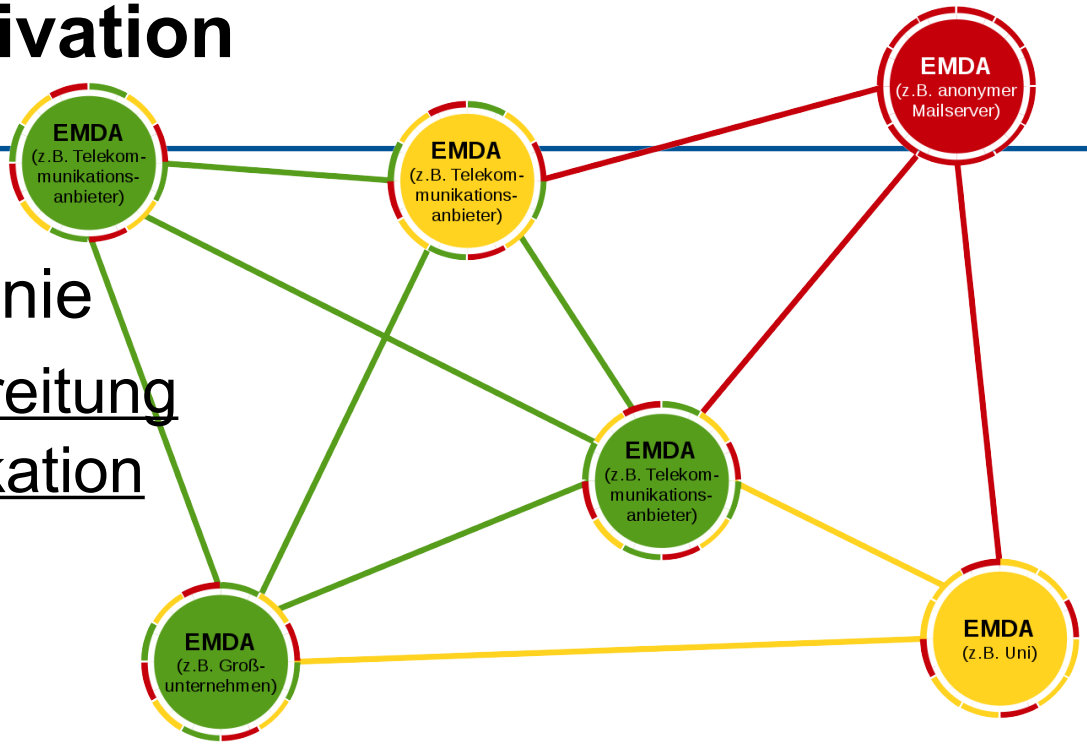
Florian Bierhoff und Thomas Gilles

RTR-GmbH Workshop / 05.11.2015

Agenda

- Motivation
- Entwurfsentscheidungen
- Medienecho zum Entwurf
- Konzeptionelle Übersicht
- Sichere Transportverbindungen
  - DANE/TLSA und DNSSEC
- Authentische Zertifikate
  - BSI TR-03145 Secure Certificate Authority operation
- Nächste Schritte

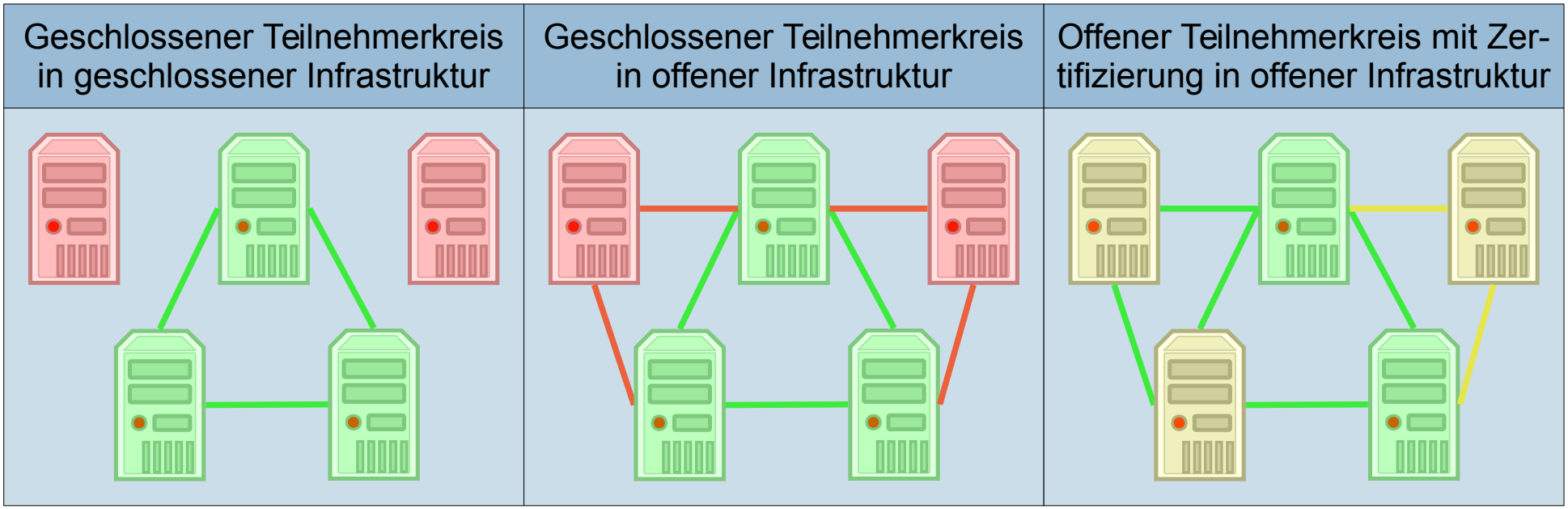
Motivation



- Ziel der Technischen Richtlinie
  - Vergleichbarkeit und Verbreitung sicherer E-Mail-Kommunikation
- Punkt-zu-Punkt Sicherheit
  - Serverseitige Umsetzung
    - Kein Aufwand für NutzerInnen
  - Verwendung hochwertiger Algorithmen (TLS)
- Im Vergleich zu De-Mail
  - Keine geschlossene Infrastruktur
    - Keine Verbindlichkeiten oder hohes Vertrauensniveau
- Im Vergleich zu Ende-zu-Ende
  - Nachrichten liegen auf „Punkten“ unverschlüsselt vor

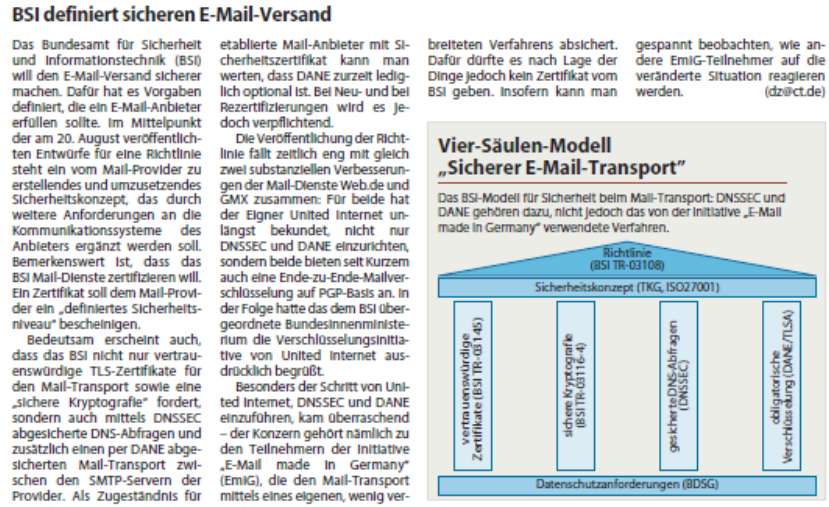
Entwurfsentscheidungen

- Anforderungen an Komponenten und Schnittstellen
  - Komponente: ein EMDA
  - Schnittstellen: zu anderen EMDA und NutzerInnen
- Betrachtung der gesamten offenen E-Mail-Infrastruktur



Medienecho zum Entwurf

- Umfangreiche positive Berichterstattung vom Heise Verlag (iX, c't, Heise Online)
- Berichterstattung auf Blogs, wie Netzpolitik.org und FinnChristiansen.de
- Pressemitteilung wurde vom Behörden Spiegel, ComputerBild.de und Winfuture.de aufgegriffen



BSI definiert sicheren E-Mail-Versand

Das Bundesamt für Sicherheit und Informationstechnik (BSI) will den E-Mail-Versand sicherer machen. Dafür hat es Vorgaben definiert, die ein E-Mail-Anbieter erfüllen sollte. Im Mittelpunkt der am 20. August veröffentlichten Entwürfe für eine Richtlinie steht ein vom Mail-Provider zu erstellendes und umzusetzendes Sicherheitskonzept, das durch weitere Anforderungen an die Kommunikationssysteme des Anbieters ergänzt werden soll. Bemerkenswert ist, dass das BSI Mail-Dienste zertifizieren will. Ein Zertifikat soll dem Mail-Provider ein „definiertes Sicherheitsniveau" bescheinigen.

Bedeutsam erscheint auch, dass das BSI nicht nur vertrauenswürdige TLS-Zertifikate für den Mail-Transport sowie eine „sichere Kryptografie" fordert, sondern auch mittels DNSSEC abgesicherte DNS-Abfragen und zusätzlich einen per DANE abgesicherten Mail-Transport zwischen den SMTP-Servern der Provider. Als Zugeständnis für etablierte Mail-Anbieter mit Sicherheitszertifikat kann man werten, dass DANE zurzeit lediglich optional ist. Bei Neu- und bei Rezertifizierungen wird es jedoch verpflichtend.

Die Veröffentlichung der Richtlinie fällt zeitlich eng mit gleich zwei substanziellen Verbesserungen der Mail-Dienste Web.de und GMX zusammen: Für beide hat der Eigner United Internet unlängst bekundet, nicht nur DNSSEC und DANE einzurichten, sondern beide bieten seit Kurzem auch eine Ende-zu-Ende-Mailverschlüsselung auf PGP-Basis an. In der Folge hatte das dem BSI übergeordnete Bundesinnenministerium die Verschlüsselungsinitiative von United Internet ausdrücklich begrüßt.

Besonders der Schritt von United Internet, DNSSEC und DANE einzuführen, kam überraschend – der Konzern gehört nämlich zu den Teilnehmern der Initiative „E-Mail made in Germany" (EmIG), die den Mail-Transport mittels eines eigenen, wenig verbreiteten Verfahrens absichert. Dafür dürfte es nach Lage der Dinge jedoch kein Zertifikat vom BSI geben. Insofern kann man gespannt beobachten, wie andere EmIG-Teilnehmer auf die veränderte Situation reagieren werden. (dz@ct.de)

Vier-Säulen-Modell „Sicherer E-Mail-Transport"

Das BSI-Modell für Sicherheit beim Mail-Transport: DNSSEC und DANE gehören dazu, nicht jedoch das von der Initiative „E-Mail made in Germany" verwendete Verfahren.

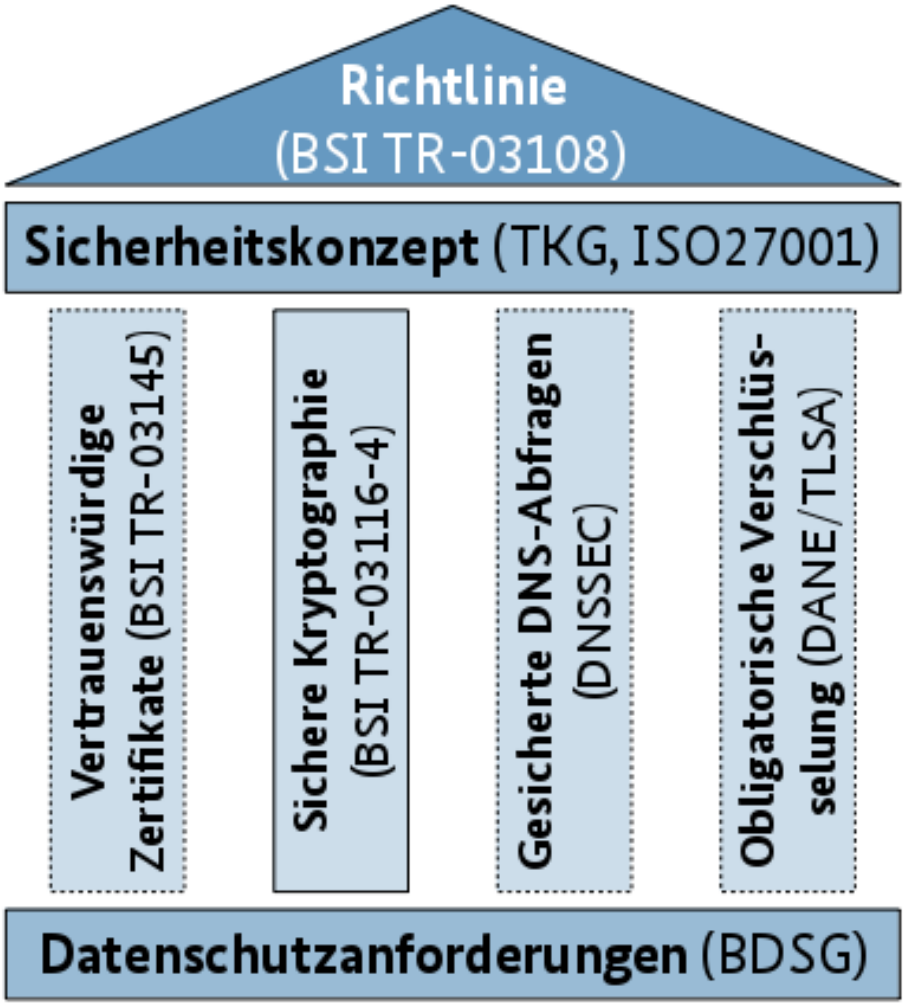
Quelle: c't (20/2015)

NETZPOLITIK.ORG

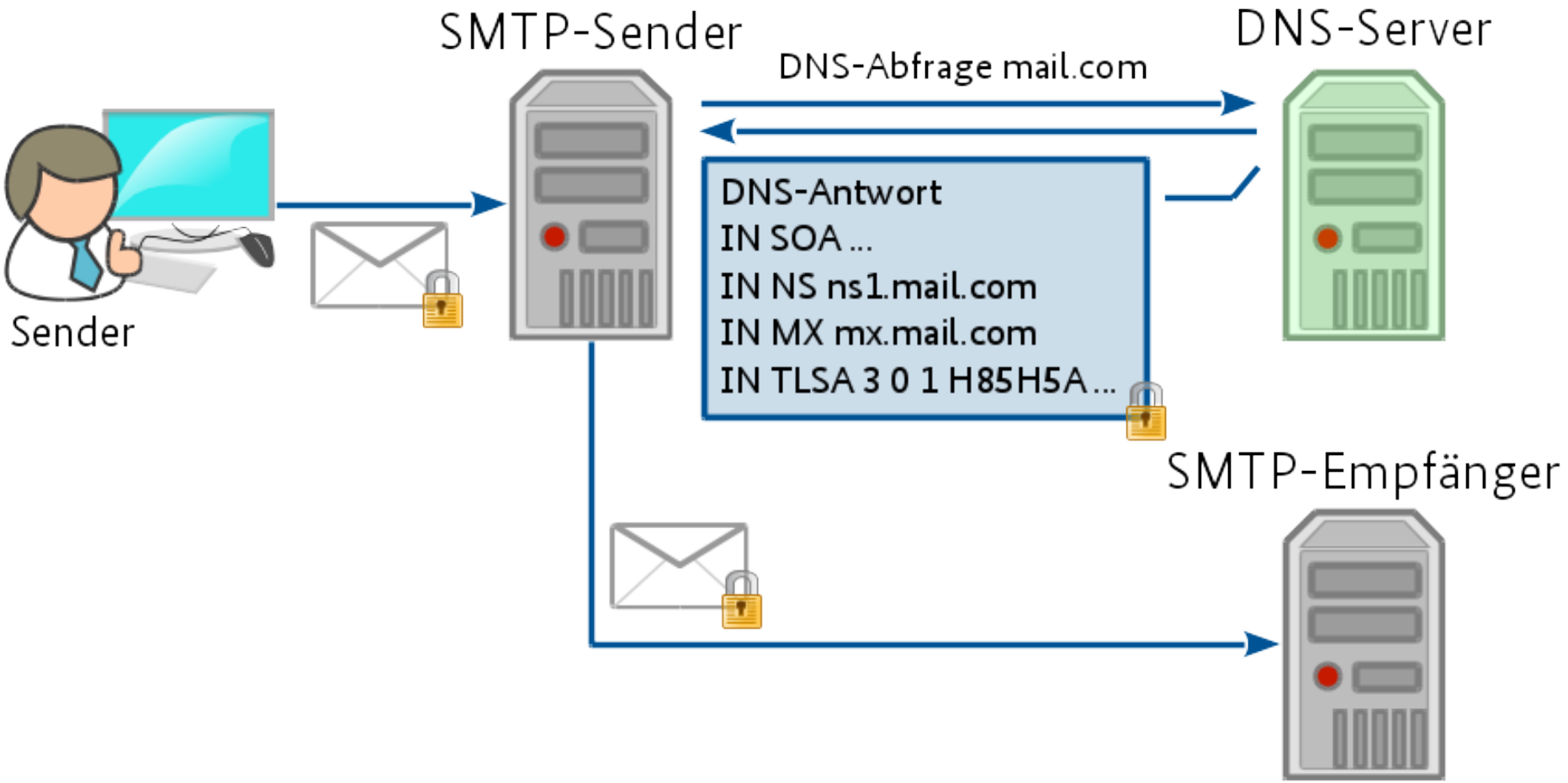
Computer Bild .de

Konzeptionelle Übersicht

- ISO/IEC 27001 (od. Sicherheitskonzept nach TKG)
  - IT-Sicherheitsmanagment
- BSI TR-03145
  - Anforderungen an CA
- BSI TR-03116-4
  - Kryptographie-Anforderungen
- DNSSEC
  - Signierte DNS-Server-Aw.
- DANE/TLSA
  - Verbindung zum Mail-Server
- Datenschutz
  - Serverstandort: Deutschland



Sichere Transportverbindungen DANE/TLSA und DNSSEC

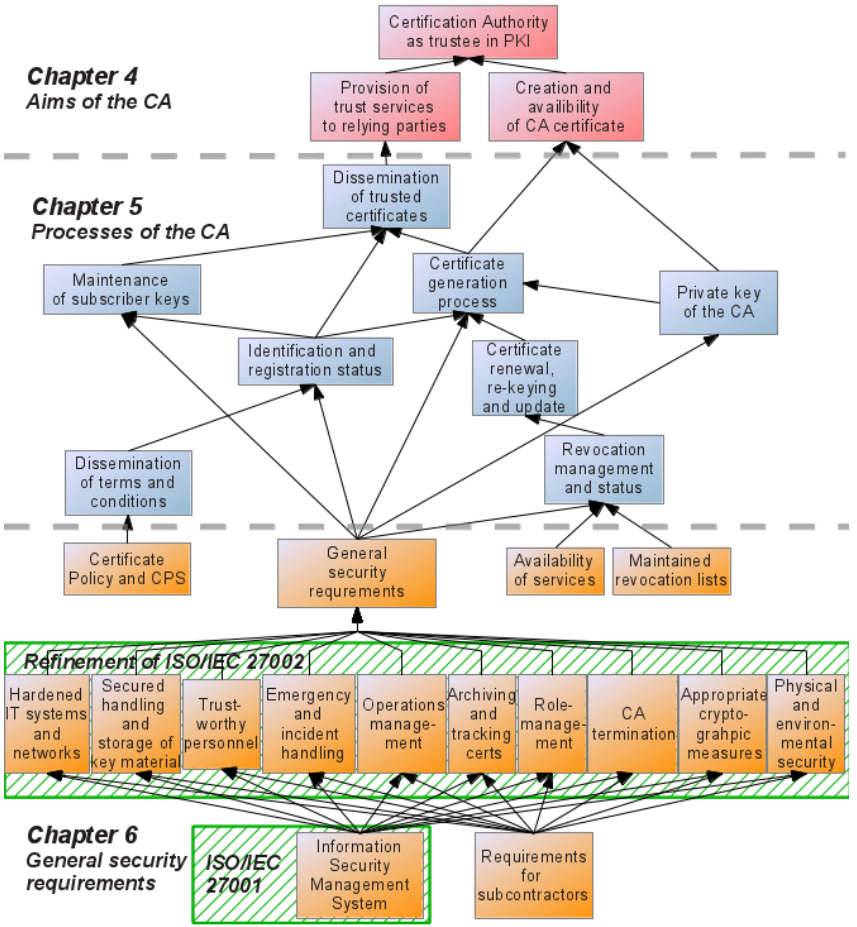


Authentische Zertifikate

- Ist das Zertifikat meines Kommunikationspartners vertrauenswürdig?
  - Prüfung über Certificate Authority (CA)
    - Zusätzliches Vertrauen durch Dritten
      - Prüfung der Zertifikatskette bis zum Vertrauensanker (Cert-Path)
      - Prüfung gegen die Sperrliste der CA (CRL)
  - Prüfung via DANE (DNS-based Authenticaton of Named Entities)
    - DNSSEC sichert die Vertrauenswürdigkeit
      - Zusätzliches Vertrauen durch Dritten → DNS-Server
    - Insbesondere für die Client-Kommunikation geeignet
      - Unabhängigkeit von Zertifikatsspeicher des Browsers
- Ist die CA vertrauenswürdig?
  - Sicherheitsnachweis und Vergleichbarkeit über TR-03145

BSI TR-03145
Secure Certification Authority operation

- Anforderungen an den sicheren Betrieb einer CA
- Basiert auf ISO/IEC 27001
- Zielt auf Sicherheitsniveau „high“
- Basis für ISO/IEC 14516-2 (3rd WD)
- Vergleichbarkeit der Sicherheit von CAs
- Verpflichtend für CAs im Bereich „Smart Metering“



Nächste Schritte

- Fortentwicklung der Technischen Richtlinie
  - Einarbeitung der Kommentare zum Entwurf
  - Gründung einer fachlichen Arbeitsgruppe
    - Finalisierung zur Version 1.0
    - Ständige Fortentwicklung

- Etablierung Zertifizierungsverfahren
  - Erstellung einer Prüfspezifikation
  - Fachprüfung von Auditoren
  - Annahme von Zertifizierungsanträgen

- Öffentlichkeitsarbeit, denn nur wenn viele EMDA die Anforderungen umsetzen, profitieren viele E-Mail-NutzerInnen!

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Referat S11 „Sicherheit in eID-Anwendungen“
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-0
Fax: +49 (0)22899-10-9582-0

e-mail-trsp@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de