



**Themen-Panel “IT-Sicherheit”
beim
IT-Forum Darmstadt - Rhein-Main-Neckar
am 16. Mai 2008**

**Martin Schallbruch
IT-Direktor
im Bundesministerium des Innern**



Bedrohungslage



Bedrohungslage der Informationstechnik (1)

■ Steigende **Quantität**

- Zunahme der Anzahl von Schadprogrammen
- Kontinuierliche Zunahme der Anzahl erkannter Schwachstellen in IT-Produkten

■ Steigende **Qualität**

- Trend zu unauffälligen Spionageprogrammen (z.B. Trojanische Pferde)
- „Schnell“, hochentwickelt, zielgerichtet, kaum feststellbar





Bedrohungslage der Informationstechnik (2)

■ **Veränderte Täterstrukturen**

- Trend zur arbeitsteiliger Kriminalität
- Opfer als Mittäter (z.B. Bot-Netze)

■ **Veränderte Motive**

- 2007 als Ende der Ära nicht kommerzieller Schadprogramme
- Gezielte Angriffe auf IT wichtiger Infrastrukturen möglich und praktiziert (z.B. Estland)
- Gezielte Wirtschaftsspionage über das Internet





Bundesministerium
des Innern

Strategie der Bundesregierung



Nationaler Plan als Dachstrategie der Bundesregierung zur IT-Sicherheit

■ Strategie der Bundesregierung:

Das Bundeskabinett hat am 13. Juli 2005 eine umfassende IT-Sicherheitsstrategie verabschiedet, den „*Nationalen Plan zum Schutz der Informationsinfrastrukturen*“

Nationaler Plan
zum Schutz der
Informationsinfrastrukturen 

■ Koalitionsvertrag 2005:

Der Koalitionsvertrag erteilt dem Bundesinnenministerium den ausdrücklichen Auftrag, den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ umzusetzen.



Ziele des Nationalen Plans

Der „Nationale Plan“ verfolgt 3 strategische Ziele:

- **Prävention:** Informationsinfrastrukturen angemessen schützen
- **Reaktion:** Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
- **Nachhaltigkeit:** Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

Adressaten sind

Verwaltung, kritische Infrastrukturen, Unternehmen, Öffentlichkeit



Strategisches Ziel 1: Prävention

Sicherheitsrisiken beim Einsatz von Informationstechnik werden reduziert, indem

- **Wissen** über Bedrohungen und Schutzmöglichkeiten vermittelt,
- Sicherheitsverantwortlichkeiten geregelt, **Sicherheitsmanagement** etabliert und Sicherheitsmaßnahmen umgesetzt sowie
- **vertrauenswürdige Produkte** und Verfahren eingesetzt werden.





Strategisches Ziel 2: Reaktion

Auf Störungen in Informationsinfrastrukturen muss schnell reagiert werden.

- Dazu gehören das **Sammeln und Analysieren** von Informationen,
- die **Warnung und Alarmierung** von Betroffenen sowie
- das Ergreifen von **Maßnahmen zur Schadensminimierung**.





Strategisches Ziel 3: Nachhaltigkeit

Um die nationalen Informationsinfrastrukturen auch langfristig zu schützen, benötigt Deutschland langfristig:

- **Fachkompetenz** in Behörden und Unternehmen,
- Nationales **IT-Sicherheits-Know-How** (FuE) sowie
- **vertrauenswürdige IT-Sicherheitsprodukte** und IT-Dienstleistungen sowie entsprechende Unternehmen.





Deutsche IT-Sicherheitswirtschaft



Deutsche IT-Sicherheitswirtschaft - Bestandsaufnahme

Vielfältige, mittelständisch geprägte Landschaft:

- Kryptounternehmen und IT-Sicherheitsspezialisten (z.B. Secunet, SIT, Utimaco, Flexsecure, Genua)
- Chipproduzenten (NXP, Infineon)
- Dokumenthersteller (Bundesdruckerei, G & D)
- Integratoren (z.B. T-Systems, SIS, Software AG, ..)



Deutsche IT-Sicherheitswirtschaft - Chancen

- Gute FuE-Kapazitäten in Deutschland
- Kooperationen Forschung – Unternehmen (ausbaufähig)
- „Beschaffungsleitfaden“ des Bundes
- „Made in Germany“ hat bei Sicherheitsprodukten guten Klang
- Referenzprojekte in D
- Kooperation mit Systemhäusern und anderen Partnern

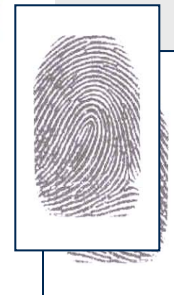


Der elektronische Reisepass: Ein Hochsicherheitsprodukt



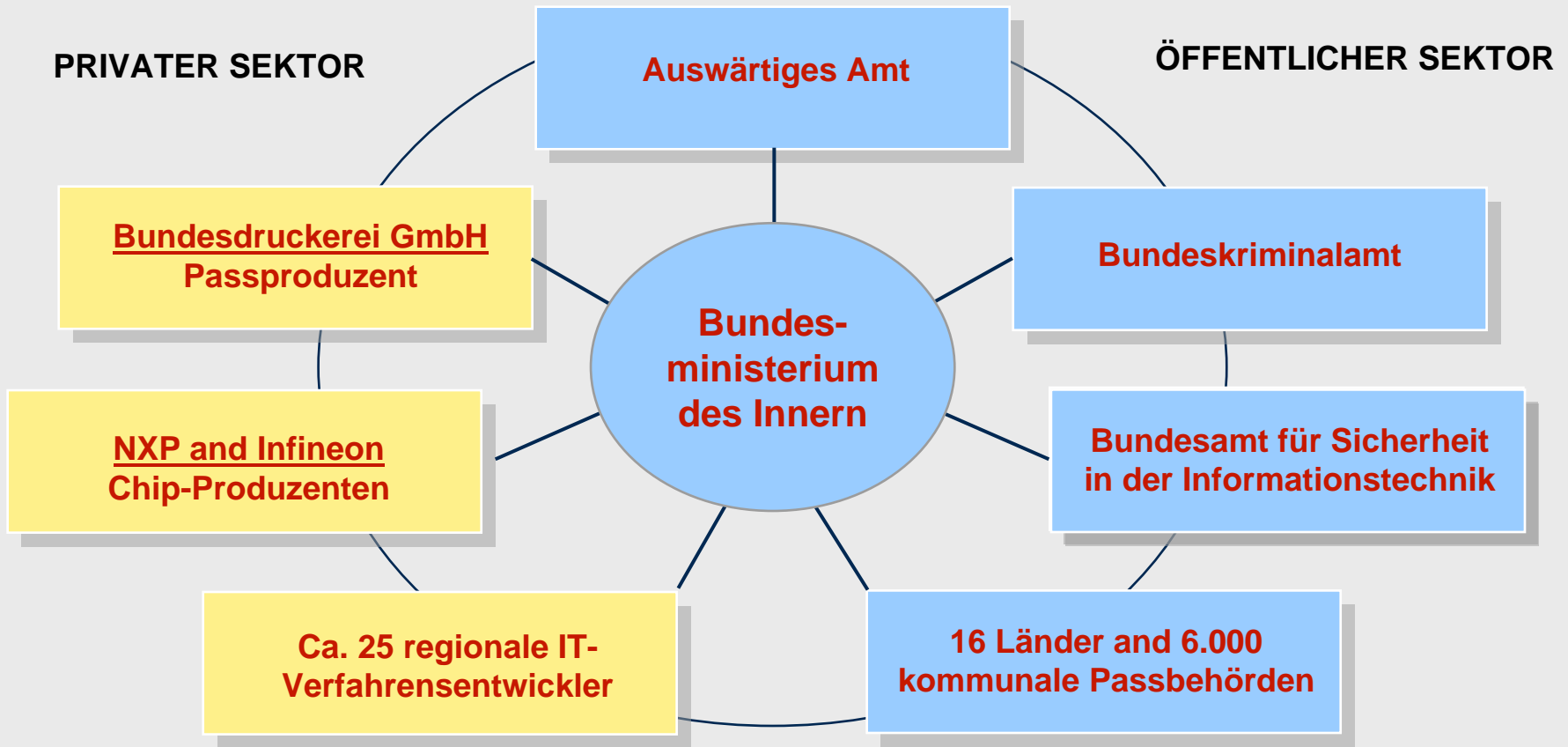
1. Nov. 2005 bis 31. Okt. 2007
4,7 Mio. ePässe der ersten
Generation mit Foto im Chip
ausgegeben

Seit 1. Nov. 2007
als erster EU-Mitgliedstaat
zusätzliche Speicherung der
Fingerabdrücke im ePass
bislang rund 1,5 Mio. ePässe
der zweiten Generation
ausgegeben



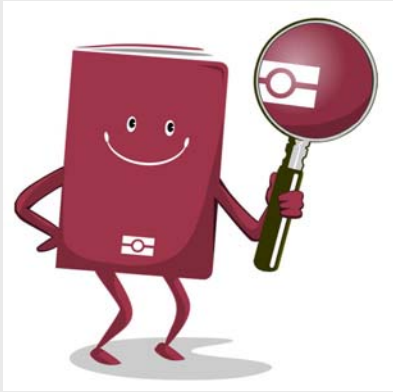


ePass: Kooperation von öffentlichem und privatem Sektor





ePass: Meilensteine „made in Germany“

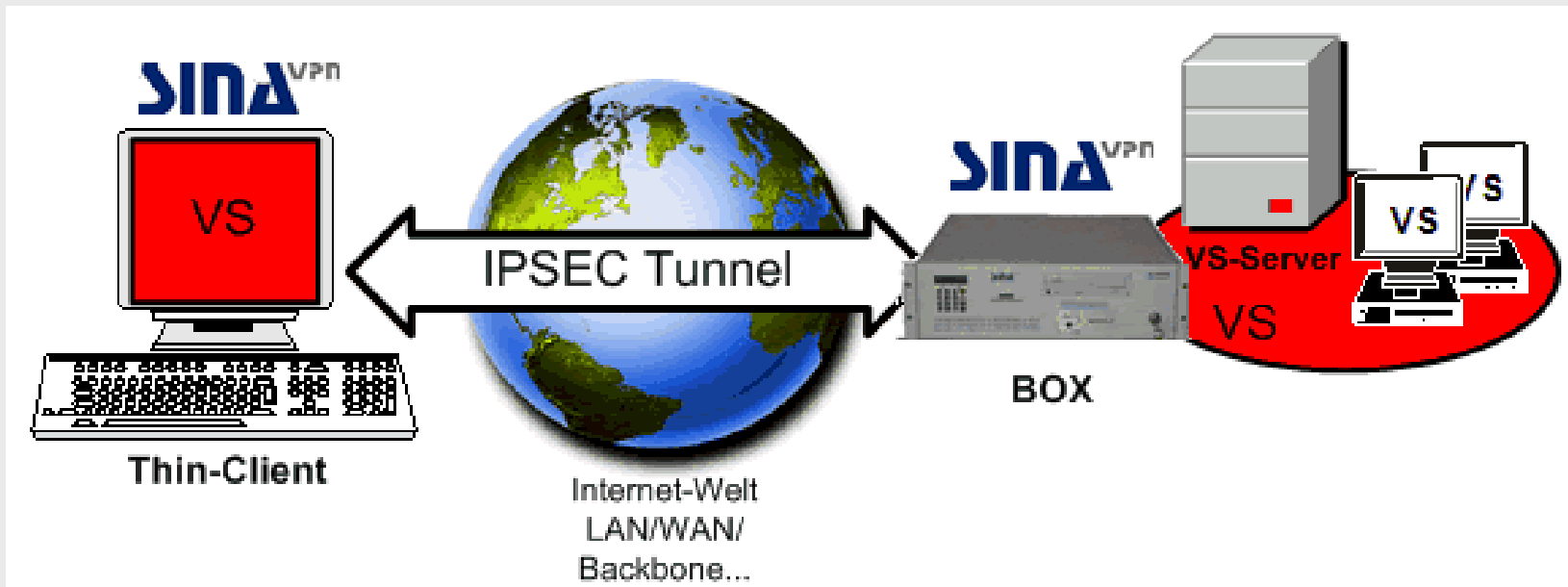


- Entwicklung der Extended Access Control (Zurgriffschutz für die Fingerabdrücke im ePass) durch BSI
→ von der EU-Kommission zum EU-weiten Standard erklärt
- Entwicklung eines Zertifizierungsprozesses für 1-Finger-Scanner auf Grundlage der FBI-Standards für 4-Finger-Scanner
→ Zusammenarbeit von BSI mit Fraunhofer als Prüfstelle
- Entwicklung von Technischen Richtlinien zur Passdatenerfassung und -übermittlung
→ als Passverordnungen verbindlich für alle deutschen Passbehörden
- Aufbau eines effektiven EAC-Zertifikatsmanagements, um ePass-Lesegeräte in den Passbehörden EAC-fähig zu machen
→ bislang EU-weit einmalig



Beispiel 2

SINA („Sichere Inter-Netzwerk-Architektur“)





Herzlichen Dank für Ihre Aufmerksamkeit.

Martin Schallbruch
IT-Direktor im Bundesministeriums des Innern
ITD@bmi.bund.de