

# ■ Erfolgskriterien von Public-Key- Infrastrukturen

**A. Beyer – TU Ilmenau**

**S. Hellmann – TeleTrust e.V.**

**M. Hesse – Fachhochschule Gelsenkirchen**

**F. Holl – Fachhochschule Brandenburg**

**P. Morcinek – Fachhochschule Brandenburg**

**S. Paulus – SAP AG**

**H. Reimer – TeleTrust e.V.**



- ▶ **Hintergrund der Studie**
- ▶ **Vorgehensweise der Studie**
- ▶ **Ergebnisse:**
  - ▶ **Technische Perspektiven**
  - ▶ **Betriebswirtschaftliche Aspekte**
  - ▶ **Nutzungsbedingungen**
- ▶ **Empfehlungen:**
  - ▶ **Technische Perspektiven**
  - ▶ **Betriebswirtschaftliche Aspekte**
  - ▶ **Nutzungsbedingungen**
- ▶ **Ausblick**

- ▶ **Gemeinsame Studie der Fachhochschule Brandenburg und dem TeleTrust e.V.**
- ▶ **Auftraggeber:**
  - ▶ **Bundesministerium für Bildung und Forschung (BMBF) der BRD**
- ▶ **Ziel:**
  - ▶ **ermitteln von Erfolgs- und Hemmnisfaktoren von PKI-Projekte**

- ▶ **Bearbeitung strukturiert in drei Teil-Aspekte:**
  - ▶ **Technische Perspektiven**
  - ▶ **Betriebswirtschaftliche Aspekte**
  - ▶ **Nutzungs- oder soziologische Aspekte**
- ▶ **Herangehensweise:**
  - ▶ **Literaturstudie**
  - ▶ **Expertenbefragungen**
  - ▶ **High-Level-Expertenworkshop**

- ▶ **Austauschbarkeit von Algorithmen ist bei staatlichen Anwendungen sinnvoll**
  - ▶ **weniger beim Unternehmenseinsatz**
- ▶ **Interoperabilität und Anwendungsintegration sind marktgetrieben**
- ▶ **Chipkarten werden durch andere Token ergänzt**
  - ▶ **Formfaktor spielt keine wesentliche Rolle**
  - ▶ **Biometrie wird zunehmend eingesetzt**
- ▶ **Isolierte Betrachtung von Mensch und Technik macht keinen Sinn**

- ▶ **PKI ohne Anwendung ist eine Infrastruktur ohne Wert**
  - ▶ **Wert kommt von den unterstützten, neu möglichen oder verschlankten Prozessen**
- ▶ **PKI ist in erster Linie ein „Business Enabler“**
  - ▶ **nur nachrangig eine Sicherheitstechnologie**
  - ▶ **PKI hat in einer RoSI-Berechnung „nichts zu suchen“**
- ▶ **PKI muss beweisen: ohne PKI sind Prozesse teurer als mit**
- ▶ **Bei einer etablierten PKI folgen wegen der Vorteile bald weitere Geschäftsprozesse**

- ▶ **Einfache und nachvollziehbare Vertrauensentscheidungen für Benutzer**
- ▶ **Unternehmenspolitische Konflikte vor PKI-Implementierung lösen**
  - ▶ **Technische „Kniffe“ scheitern an menschlichen / soziologischen Problemen**
- ▶ **Qualifizierte Zertifikate „sind die Mühe nicht wert“**
  - ▶ **Kosten-Nutzen-Verhältnis für Unternehmen nicht akzeptabel**

- ▶ **Interoperabilität ist an verschiedenen Punkten problematisch**
  - ▶ **Integration der PKI in Geschäftsprozesse**
  - ▶ **Verwaltung von Schlüsseln**
- ▶ **Organisationsübergreifende Vertrauensbeziehungen**
  - ▶ **Vertrauen ist prozessbezogen**
- ▶ **Sicherheit ergibt sich aus Vertrauen und Kontrolle**
  - ▶ **Kontrollverlust kompensieren durch Vertrauensbildung**

- ▶ **Token und ihre Personalisierung bilden einen erheblichen Kostenfaktor jeder PKI-Implementierung**
  - ▶ **höhere Flexibilität der in Hardware implementierten Algorithmen und Parameter**
  - ▶ **Untersuchung alternativer Formen zur SmartCard**
- ▶ **Schlüsselmanagement als wesentliche PKI-Grundfunktionalität anwendungsübergreifend realisieren**
  - ▶ **„virtueller Schlüsselbund“ zur Förderung der Interoperabilität von Schlüsselmanagement**

- ▶ **Einbeziehen neuer IT-Infrastrukturtrends**
  - ▶ **Beispielsweise modellieren von Vertrauensbildung bei Service Orientierte Architekturen**
  - ▶ **Entwickeln von Frameworks für die Anwendungsintegration**

- ▶ **Marketing gegen das negative Image von PKI**
  - ▶ **veröffentlichen von Best Practice Beispielen**
- ▶ **Kaffeersatzleserei bei Kalkulationen für IT-Sicherheit**
  - ▶ **ROSI praktikabler, handhabbarer machen**
  - ▶ **Kennzahlensysteme für Sicherheitseigenschaften von Geschäftsprozessen erweitern**
- ▶ **Haftungsregelungen und ihre Konsequenzen für PKI-Anwendungen im B2B und B2C Umfeld untersuchen**
- ▶ **Gütesiegel für Vertrauensbildung im elektronischen Geschäftsverkehr**

- ▶ **Spannungsfeld von Technik, Wirtschaft und soziologischen Aspekten im PKI-Umfeld untersuchen**
  - ▶ **Vertrauensbildung im elektronischen Geschäftsverkehr verbessern**
- ▶ **Umgang mit zweckmäßigen qualifizierten Zertifikaten auf europäischer Ebene fördern**
- ▶ **Einfache Formen organisationsübergreifender Vertrauensmodelle untersuchen („instant workgroups“)**
- ▶ **Forderung und Förderung „Globaler“ Digitaler Identitäten mit öffentlicher Akzeptanz**
- ▶ **Sicherheitsbewusstes Verhalten durch lukrative Maßnahmen (Steuervorteile) fördern**

- ▶ **PKI im Spannungsfeld von Technik, Betriebswirtschaft und Sozialwissenschaft**
  - ▶ **Nachweis: Enabling-Technologie für Geschäftsprozesse**
- ▶ **Vergleichende Untersuchung in Industrien, die eine hohe technologische und Prozess-Standardisierung erreicht haben**
  - ▶ **Warum gibt es dort wirksamere Standards?**
- ▶ **Entwicklung von Simulations- bzw. Szenariotechniken für unterschiedliche Geschäftsfälle**
- ▶ **Themenhorizont erweitern:**
  - ▶ **Was für PKI im Speziellen gilt, gilt weitgehend auch für die allgemeine IT-Sicherheit**
  - ▶ **Fragestellungen für die breitere Sicherheits-Diskussion wichtig**

- Erfolgskriterien von Public-Key-Infrastrukturen

**Vielen Dank für Ihre Aufmerksamkeit!**

**Fragen ?**



hesse {at} internet-sicherheit {dot} de