Bundesamt
für Sicherheit in der
Informationstechnik

Erfahrungen bei der Anwendung von
Risikoabschätzungsverfahren in RFID-Anwendungen

# Security Assessments und Security-by-Design

PIA Experten-Symposium am 25.11.2011

Bernd Kowalski

# Rolle des BSI bei RFID-Anwendungen

- Das BSI fokussiert auf Themen der *Informations- und Funktionssicherheit*
- Kontaktlose Technologie wird seit Jahren in *sicherheitsrelevanten Anwendungen* und auch in *kritischen Infrastrukturen* eingesetzt (z.B. ÖPV, Zutrittskontrolle, Mitarbeiterausweise, Fälschungsschutz).
- Weitere Anwendungen mit Schutzbedarf stehen vor der Einführung (Contactless payment, NFC, Nutzung von RFID zur Sicherung der logistischen Warenkette)

Kontrollterminal bei VRS und VRR für kontaktloses Ticketing
Bildquelle: Haas-IT traffic solutions

Player beim Contactless Payment
Einzelbildquellen: MasterCard, VisaCard, NFC-Forum

# IT-Security Assessments bei RFID-Anwendungen

- Das BSI hat im Jahr 2006 begonnen, IT-Sicherheitsbetrachtungen in den Einsatzgebieten Öffentlicher Personenverkehr, Zutrittskontrolle, NFC und Handelslogistik durchzuführen.
- Für alle 3 Bereiche der IT-Sicherheit (Informations-, Funktionssicherheit und Datenschutz) wurden Schutzbedarf und potentielle Gefährdungen ermittelt.
- Um den ermittelten Handlungsbedarf zu adressieren, wurden die Aktivitäten zu den Technischen Richtlinien "Sicherer RFID-Einsatz" (TR-03126) durch das BSI implementiert.


Einsatzgebiete der TR RFID
Einzelbildquellen: Deutsche Bahn, VRR, BMI, FIFA

Funktionssicherheit, Informationssicherheit, Datenschutz

Schutzbedarf | Gefährdungen | Maßnahmen

**Technische Richtlinie für den sicheren RFID-Einsatz**

Grundlegende Inhalte der TR RFID

# Ziele der Technischen Richtlinien „Sicherer RFID-Einsatz“

- Unterstützung der sicheren, praxisnahen Implementierung von RFID-Anwendungen
- Definition des State-of-the-Art bei Informations- und Funktionssicherheit
- Unterstützung der Anwendungsbetreiber und Service Provider mit spezifischem Know-how zur sicheren Implementierung von RFID-Anwendungen
- Schaffung von Akzeptanz durch Transparenz und Berücksichtigung der Interessen der Beteiligten.
- Unterstützung von Konformitätsprüfungen und Zertifizierungen


Mögliches Zertifikat auf Basis der Richtlinienreihe TR 03126 (TR RFID, Technische Richtlinie für den sicheren RFID-Einsatz)

# Struktur der TR RFID

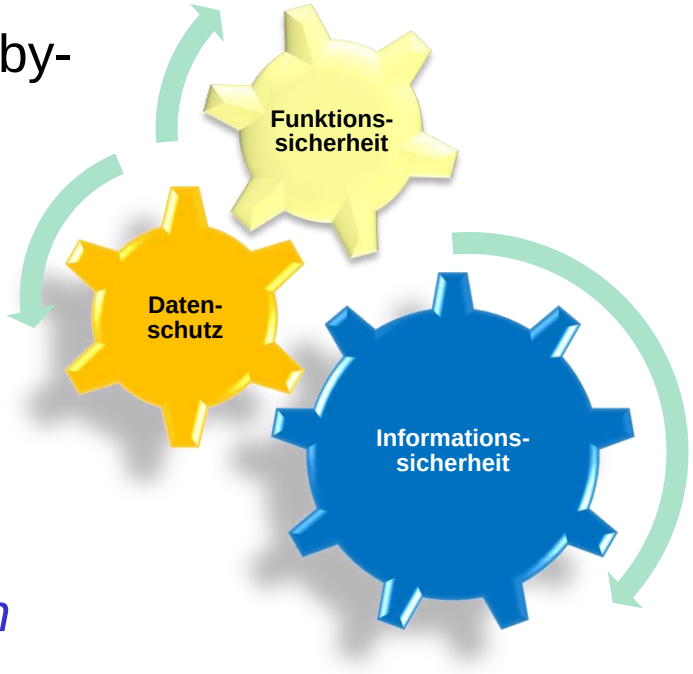
# “Lessons learned” der Security Assessments zu den TR RFID

- Interessen von Anwendungsbetreibern, Nutzern, IT-Sicherheits- und Datenschutz-beauftragten können synchronisiert und bedient werden
- Know-how zu Security-by-Design, Privacy-by-Design bei RFID-Betreibern, Lieferanten nur in Ausnahmefällen vorhanden

➲ *Technische Richtlinien sind unbedingt nötig*

- Anforderungen zu Security-by-Design und Privacy-by-Design müssen synchronisiert werden und in Lastenheft, Spezifikationen einfließen.
- Separate Umsetzung von IT-Sicherheit und Datenschutz nicht praxisgerecht und ineffizient

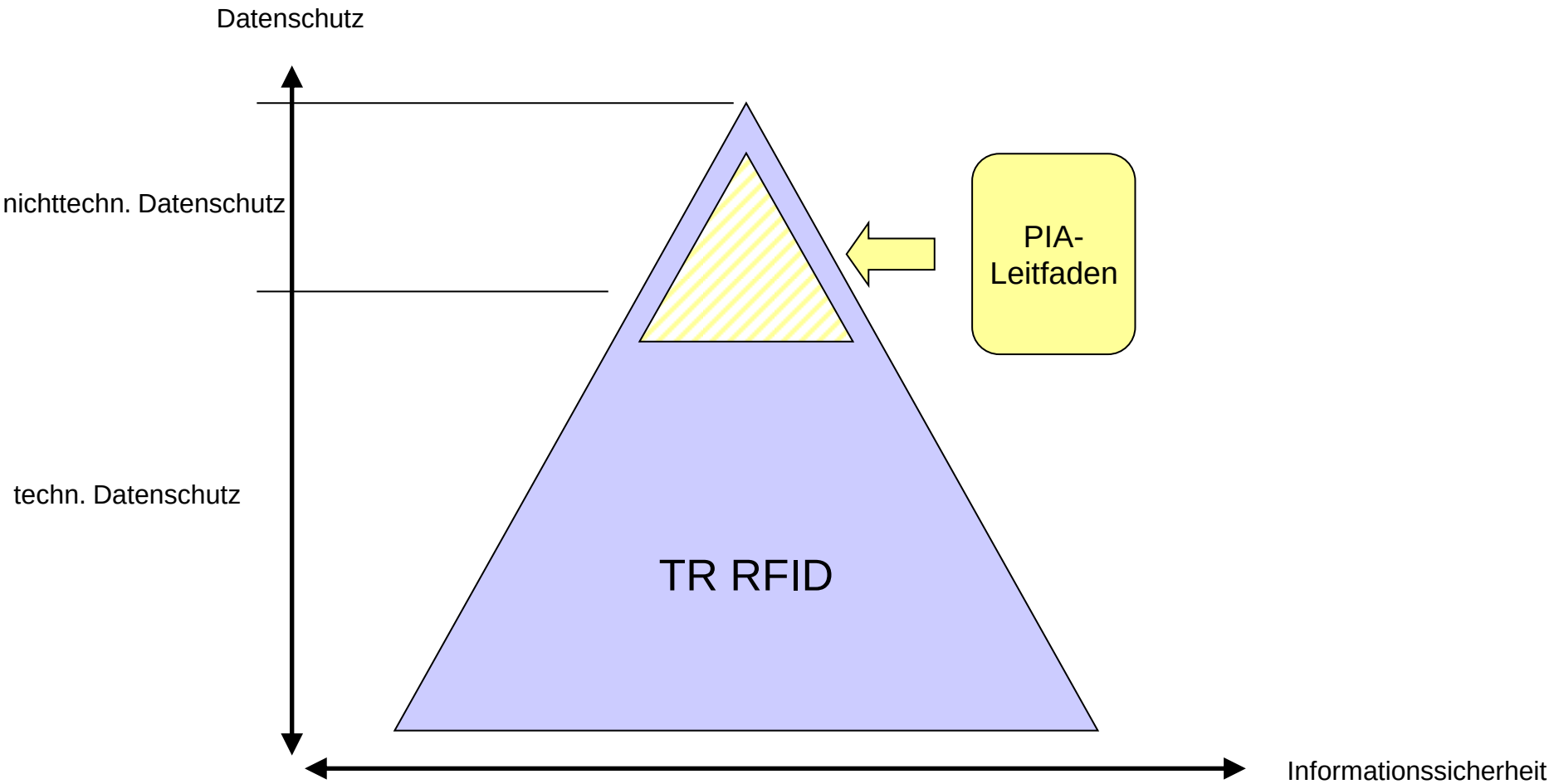
➲ *Die gemeinsame Betrachtung von Funktions-, Informationssicherheit und Datenschutz sind elementar für die erfolgreiche Implementierung von sicheren RFID-Anwendungen.*



# Zusammenwirken von PIA und TR RFID

- Die Initiative der EC zum *PIA Framework und* die Aktivitäten zur *TR RFID verfolgen die gleichen Ziele!*
- Beide Aktivitäten unterstützen sich optimal:
  - BSI TR RFID (Nr. 6 der EU-Empfehlung zu RFID):
    Fokus auf Informations- und Funktionssicherheit, Datenschutz und Schutz der Privatsphäre bisher nur sehr generell betrachtet worden.
  - EC PIA-Framework (Nr. 5 der EU-Empfehlung zu RFID):
    Fokus auf Datenschutz und Schutz der Privatsphäre
  - Beide Verfahren basieren auf der Vorgehensweise nach ISO/IEC 27005
- Die TR RFID eignen sich ideal als Templates zur Umsetzung des PIA-Frameworks

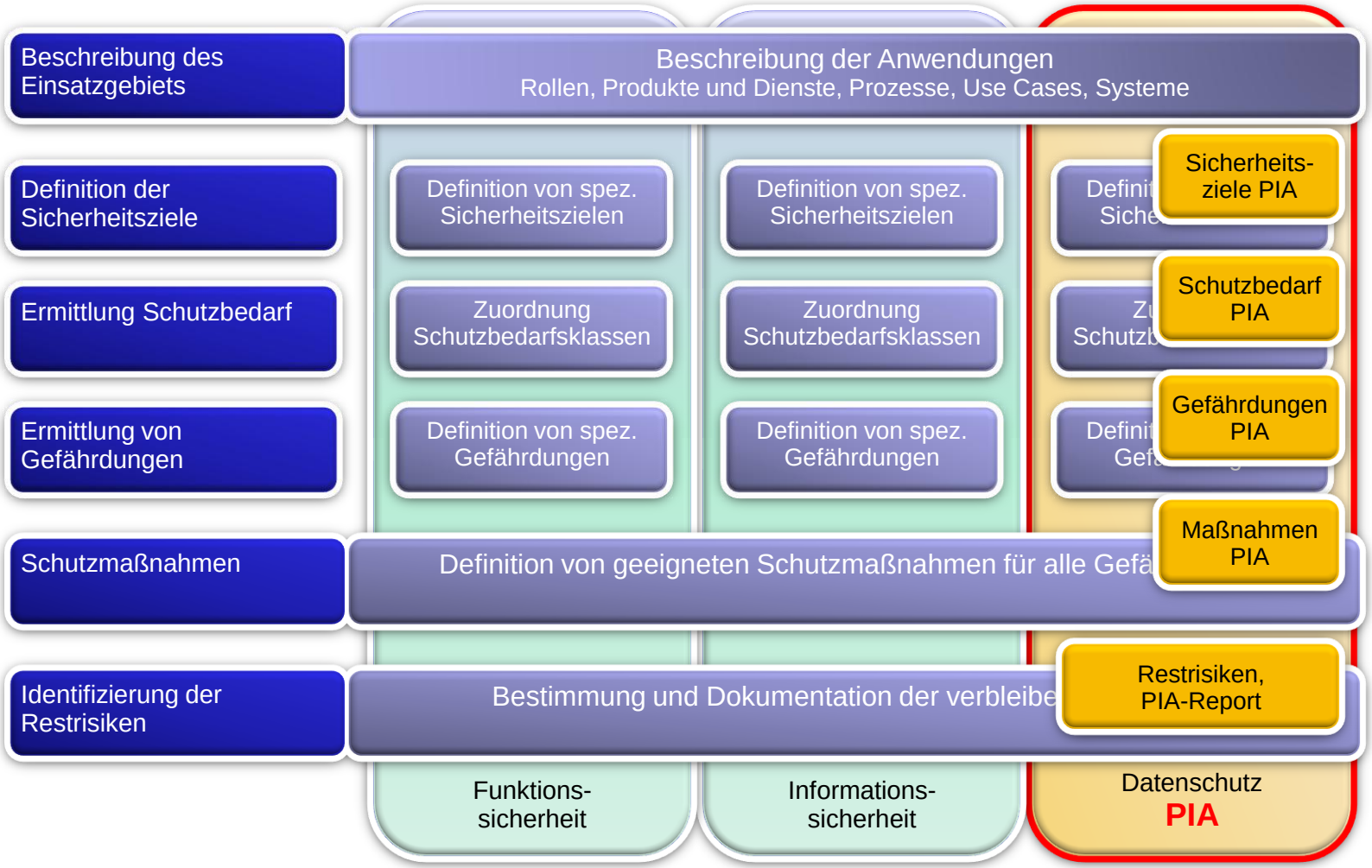
# Zusammenwirken von PIA und TR RFID




Die Technische Richtlinie für den sicheren RFID-Einsatz als
Basis für die BSI-Aktivitäten zum Privacy Impact Assessment

# Erweiterung der TR RFID zum Template für den PIA-Prozess

Handlungsstrang "Datenschutz" der TR RFID wird zur Umsetzung des PIA–Prozesses erweitert:



# Kombinierte Konformitätstests und ggf. Zertifizierungen

- Bei Nutzung der TR RFID als PIA-Template lassen sich Konformitätstests und Zertifizierungen zu den Sicherheitszielen des Datenschutzes (PIA) und der Funktions- und Informationssicherheit (TR RFID) kombiniert durchführen.
- Ein PIA und ein PIA-Report können auf Basis der TR RFID auch separat erstellt werden.

| | Funktions-sicherheit | Informations-sicherheit | techn. Datenschutz | nichttechn. Datenschutz |
|---|---|---|---|---|
| TR RFID (EUC-REC #6) | √ | √ | √ | **2012** |
| PIA-Leitfaden (EUC-REC #5) | - | - | - | √ |
| ToDo: Prüfkriterien | √ | √ | √ | √ |

**Σ: Umsetzung der Europäischen Empfehlung zu RFID in Deutschland!**

# Value Proposition der Umsetzung des PIA-Prozesses mit den TR RFID

- Die TR RFID werden akzeptiert und haben Praxistauglichkeit bewiesen. Referenzen sind z.B. die VDV Kernapplikation (mehrere Mio. Kartenbesitzer), FIFA WM2006, etc
- Die TR RFID ist ideal geeignet, den PIA-Prozess anwendungsgerecht, effizient und transparent umzusetzen.
- Zur Implementierung von Security-by-design und Privacy-by-design müssen Anforderungen der Informations-, Funktionssicherheit und des Datenschutzes berücksichtigt werden. Die TR RFID unterstützt dies. Konzepte, die sich nur auf Datenschutz oder nur auf IT-Sicherheit fokussieren, leisten dies nicht.
- Die TR RFID bietet wirksame Unterstützung für Betreiber und Service Provider bei der effizienten Implementierung von sicheren und PIA-konformen RFID-Systeme.

# Perspektiven

- Das BSI arbeitet zur Zeit an der Erweiterung der existierenden TR RFID zu PIA Templates
- Die TR RFID werden künftig neben den Zielen der Informations- und Informationssicherheit auch den PIA-Prozess unterstützen.
- Das BSI wird dabei auch weiterhin die Kooperation mit Verantwortlichen und Beteiligten – insbesondere den Datenschutzverantwortlichen – suchen.
- Das BSI wir eine Zertifizierung nach TR RFID anbieten.

Bundesamt
für Sicherheit in der
Informationstechnik

# Vielen Dank für Ihre Aufmerksamkeit!


Bernd Kowalski

Abteilungspräsident

Sichere elektronische Identitäten,

Zertifizierung und Standardisierung

Tel.: 0228-9582-5700

Mail: bernd.kowalski@bsi.bund.de