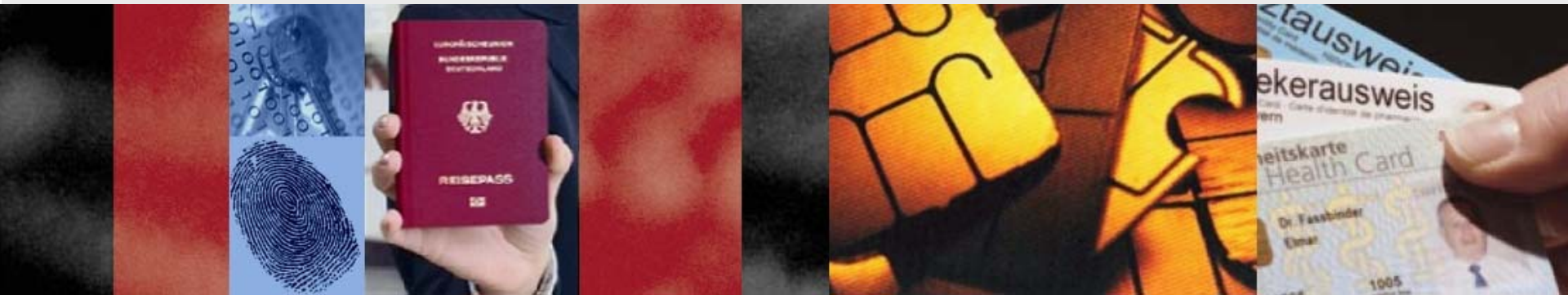




Sicherheit der Komponenten der Telematik-Infrastruktur



IT - Sicherheit im Gesundheitswesen Regelungen und Maßnahmen für eine sichere TI im Zuge der Einführung der eGK

Bernd Kowalski

Bundesamt für Sicherheit in der Informationstechnik (BSI)



... ist die Bundesbehörde für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Aufgaben (u.a.):

- Zertifizierung von Komponenten und Systemen
- Entwicklung von Prüfvorschriften wie Schutzprofile (PP) und Technische Richtlinien (TR)
- eGK, ePass, ePA
- eCard-Strategie des Bundes
- ...





Zulassung von Telematik-Komponenten

gematik Zulassungsstelle

Funktionsfähigkeit und Interoperabilität

Funktionstest
Konformitätstest
Integrationstest
Interoperabilitätstest
durch

gematik

Sicherheitstechnische Tests und Abnahme

IT Sicherheitszertifizierung und
ggf. Bestätigung (nach SigG)
durch

Zugelassene Zertifizierungs-
und Bestätigungsstelle

BSI

Materialprüfung

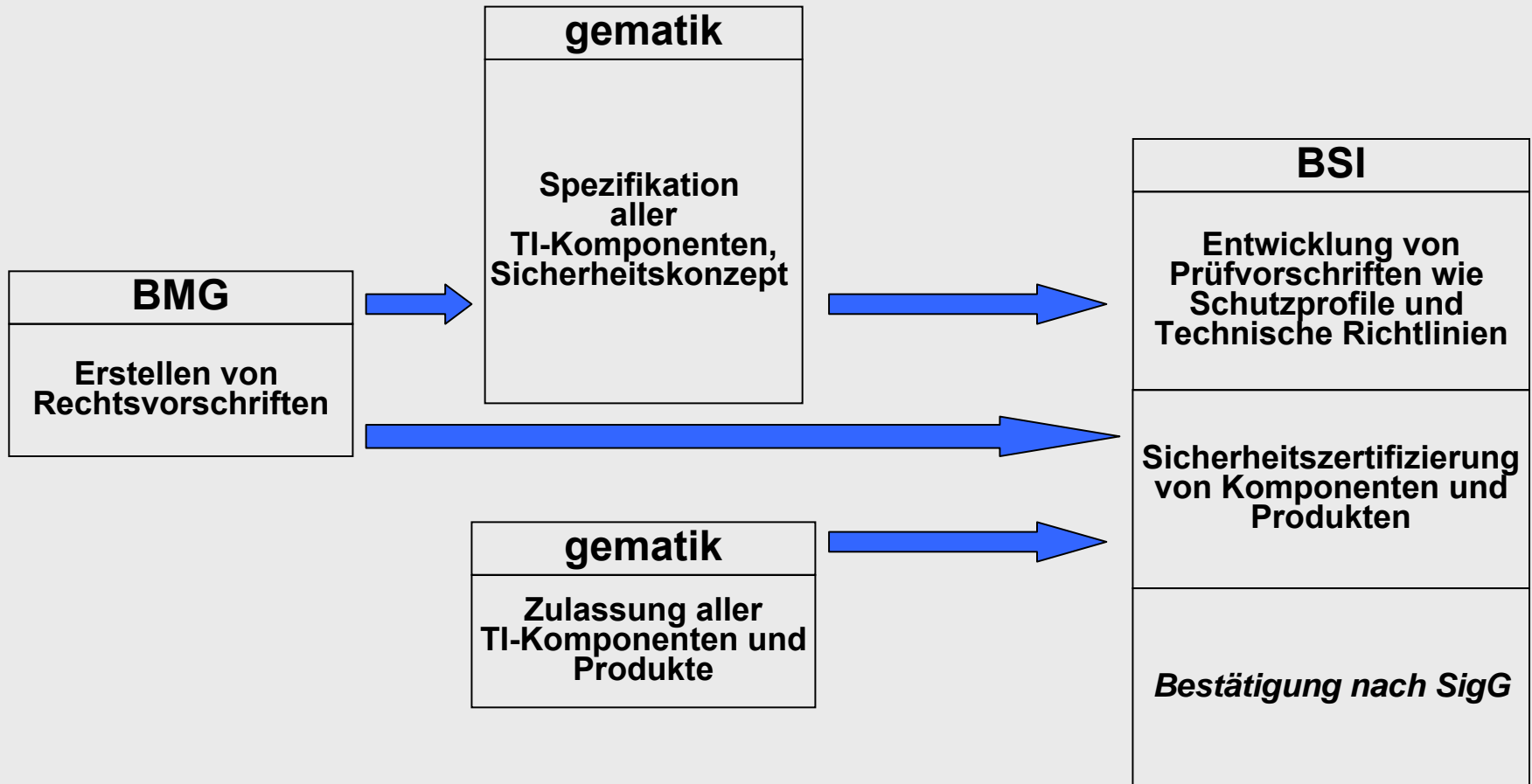
Durchführung
elektrischer, physikalischer,
mechanischer Tests

Prüfstellen

Zulassung / Prüfnachweise
Rechtsgrundlage: § 291b SGB V

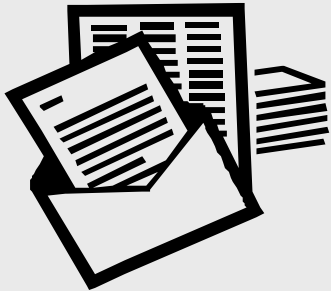


Zusammenspiel BMG – gematik- BSI





Anforderungen an die Sicherheit (Beispiel Datenschutz)



“Personenbezogene Daten des Versicherten müssen mit geeigneten Maßnahmen vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung geschützt sein“

Diese Anforderung muss durch Sicherheitseigenschaften der Telematikinfrastuktur und ihrer Komponenten umgesetzt werden.

Je besser die IT-Sicherheit, desto weniger sind zusätzliche Maßnahmen in der IT-Umgebung notwendig



eGK (Versicherten ausweis)

Die eGK-Spezifikation definiert:

- erforderliche Kommandos der eGK
- die von diesen verwendeten Kryptoalgorithmen gemäß BSI-TR 03116
- erforderliche Datenstrukturen in der eGK
- die Zugriffsrechte auf bestimmte Daten in Form der sogenannten Access-Rules

Genau diese Elemente sind Grundlage für die Sicherheitszertifizierung und müssen in den Prüfvorschriften erfasst werden (“Security Functional Requirements”).





HBA (Heilberufsausweis)

- Authentisierung des Karteninhabers (PIN)
- Authentisierung gegenüber eGK
- Authentisierung gegenüber z.B. SMC-B
- Authentisierung gegenüber Konnektor / Server
- Entschlüsseln von Dokumenten, z.B. für den späteren Arztbrief
- Qualifizierte elektronische Signatur z.B. für das spätere eRezept



Voraussetzung für eine Zertifizierung: Prüfvorschriften

Schutzprofile (Protection Profiles, PP):

- gemäß Common Criteria, internat. Anerkennung durch Sich.behörden
- Anforderungen an die IT-Sicherheits-Funktionalität (abstrakt)
- Anforderungen an die Vertrauenswürdigkeit (Prüfvorgang)

Technische Richtlinien (TR):

- nationale Prüfvorschriften mit Referenz auf internat. Standards
- Anforderungen an Funktionalität, an technische Prozesse, die Interoperabilität von IT-Sicherheitskomponenten; Def. von Testfällen
- Beispiele: TR für Komfort – und Stapelsignatur für HBA, SMC und KT oder: TR ePass zum Testen der BAC/EAC-Protokolle



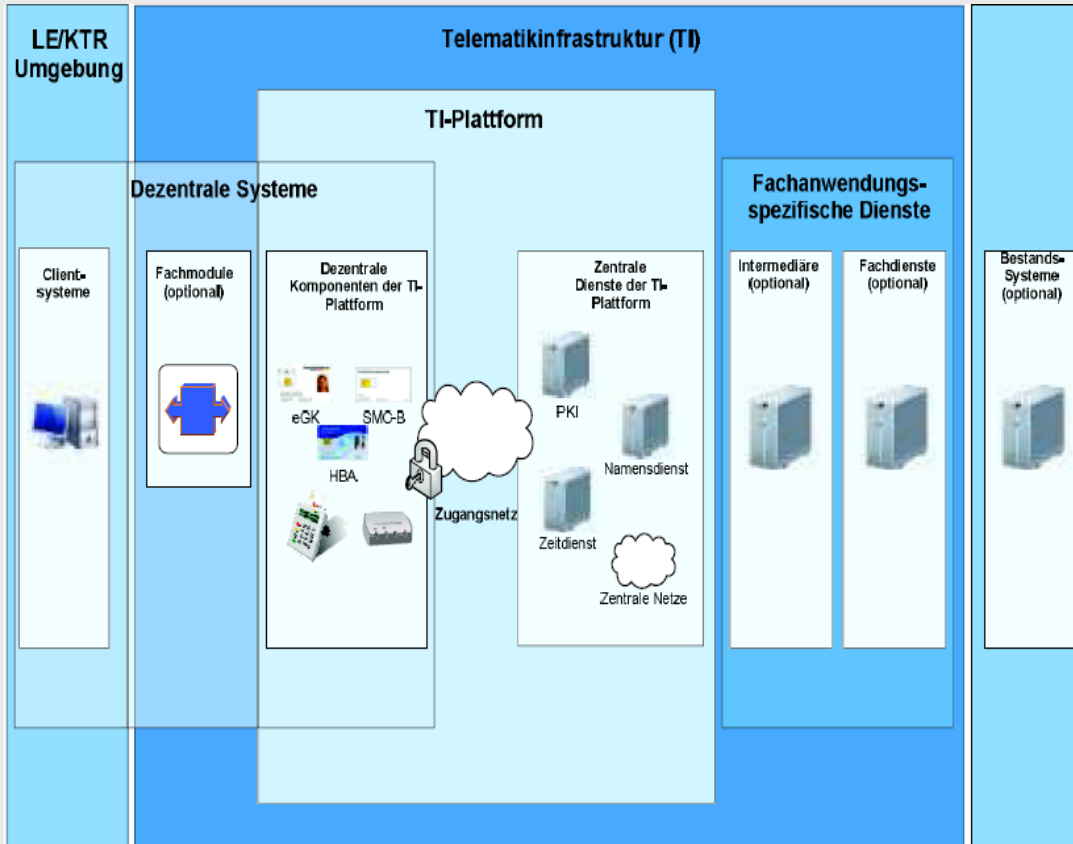
Prüfvorschriften des BSI im Kontext der Telematik - Infrastruktur

Schutzprofile (Protection Profiles, PP):

- PP zur eGK (Version 2,9)
- PP zum HBA (Version 1.10)
- PP zur SMC Typ A (Version 1.2)
- PP zur SMC Typ B (Version 1.2)
- PP zur SMC Typ K
- PP zum Netzkonkto
- PP zum Anwendungskonn.
- PP mobilen Kartenterminal (Version 0.9.8)
- PP station. Kartenterminal (V 1.73)
- PP SAK
- PP VPN-Konzentratof

Technische Richtlinien (TR):

- TR 03114 zur Stapelsignatur (V 2.0)
- TR 03115 zur Komfortsignatur (V 2.0)
- Betriebskonzept Terminal IDs (Anlage zur TR 03115)
- TR 03116 Sicherheitsvorgaben Krypto
- TR 03120 Kartenterminalidentität



(Quelle: Lastenheft Basis-TI, Version 1.0.0)



Fazit

- Alle sicherheitsrelevanten Komponenten der Telematikinfrastruktur (TI) werden nach entsprechenden IT-Sicherheits-Prüfvorschriften (PP, TR) des BSI geprüft und zertifiziert.
- Hohes Sicherheitsniveau der IT-Komponenten in der TI gewährleistet leistungsfähige und zukunftsfähige Prozesse und Fachdienste auf einem nachweisbar hohen Datenschutz- und Datensicherheitsniveau.

**Neben dem BfDI unterstützt das BSI die gematik
in zentralen Fragen des Datenschutzes bzw. der IT-Sicherheit**



Vielen Dank für Ihre Aufmerksamkeit !



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Bernd Kowalski
Godesberger Allee 185
53175 Bonn

Tel: 0228-9582-5700
Fax: 0228-10-9582-5700

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de