Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheitszertifizierung

von

Komponenten des Digitalen Tachographen für Nutzfahrzeuge

Dipl.-Math. Irmela Ruhrmann
Dipl.-Phys. Osman Kocar
Bundesamt für Sicherheit in der Informationstechnik

13. Oktober 2006

GRUNDLAGEN

Das Bundesamt für Sicherheit in der Informationstechnik wurde 1991 auf Gesetzesgrundlage errichtet.
§ 3 des BSI-Gesetzes vom 17.12.1990 (Bundesgesetzblatt I S. 2834) definiert die Aufgaben.

BSI heute:

- **etwa 480 Mitarbeiter**
- **weiter im Ausbau**

GRUNDLAGEN

Aufgaben nach § 3 des BSI-Gesetzes

1. Untersuchung von Sicherheitsrisiken ...
2. Entwicklung von Kriterien ...
3. Prüfung und Bewertung der Sicherheit
   von informationstechnischen Systemen
   oder Komponenten und Erteilung von
   Sicherheitszertifikaten
4. ...
5. ...

Rechtliche Vorgaben

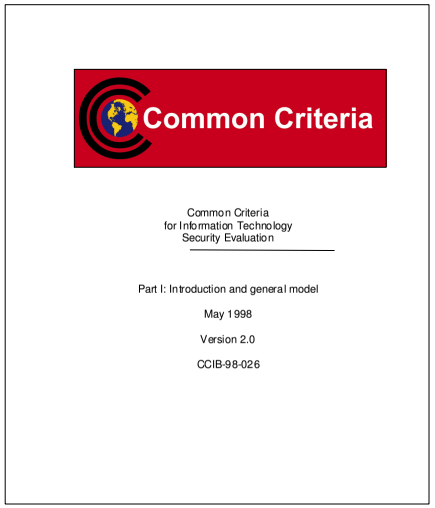
- BSI Gesetz (BSIG: Dezember 1990)
- BSI Zertifizierungsverordnung (BSI ZertV)
- Kostenverordnung (BSI-KostV)
- Erlasse des Innenministers
  (z.B. zur Bewertung von Kryptomechanismen,
  Einhaltung der DIN EN 45001/ISO 17025)
- Spezielle Beispiele:
  - EU-Direktive zum digitalen Tachographen
  - EU-Verordnung zur digitalen Signatur
  - deutsches Signatur Gesetz

Motivation für Hersteller

- Unabhängige Produktprüfung durch externe Organisation
- Qualitätsverbesserung des Produktes bezüglich der Sicherheitseigenschaften
- Dokumentiertes Design, dokumentierte Prüfung
- Kompetente kommerzielle Prüfstellen (akkreditiert und für CC lizenziert)
- Überwachung der Prüfung durch übergeordnete Zertifizierungsstelle
- staatliche Zertifizierungsstelle garantiert Neutralität und internationale Anerkennung des Zertifikates
- Marktvorteil durch anerkanntes Prüfsiegel

GRUNDLAGEN

Historie



IT-Sicherheitskriterien

1985: US-Orange Book

1989: Grünbuch des BSI

1991: Information Technology Security Evaluation Criteria (ITSEC)

ISO/IEC 15408

1999: Common Criteria (CC) V2.1

2005: Common Criteria (CC) V2.3

2006: CC V 3.1 Offizielle Version seit September 2006

EAL Stufen 1 - 7

EAL 1 stellt eine Prüfung und Bewertung des Produktes, wie es an Kunden ausgeliefert wird, bereit. Diese Prüfung beinhaltet unabhängiges Testen auf der Grundlage überprüfter Handbücher und einer Spezifikation der Sicherheitsfunktionen

EAL 2 beinhaltet zusätzlich eine Schwachstellenanalyse

EAL 3 erfordert eine vollständigere Testabdeckung der Sicherheitsfunktionen und zusätzlich Dokumentation und Anwendung bestimmter Verfahrensweisen zur Entwicklung

EAL 4 erfordert eine weitergehende und detailliertere Entwurfsbeschreibung, Teilbeschreibungen der Implementierung (Source-Code) und verbesserte Verfahren zur Entwicklung

ZERTIFIZIERUNGSVERFAHREN

Prüfstellen

- Atos Origin GmbH
- atsec information security
- CSC Ploentzke AG
- Datenschutz Nord GmbH
- DFKI (Deutsches Forschungsinstitut für Künstliche Intelligenz)
- Industrieanlagen-Betriebsgesellschaft (IABG) mbH
- media transfer AG
- secunet SwissIT AG
- SRC Security Research & Consulting GmbH
- Tele Consulting (TC) GmbH
- brightsight bv (ehemals TNO-ITSEF BV)
- T-Systems GEI GmbH
- TÜV Informationstechnik (TÜVIT) GmbH

Aktuelle Schutzprofilentwicklungen

- Protection Profile - Biometric Verification Mechanism
- Protection Profile - Heilberufeausweis (HBA), Version 1.0
- Protection Profile - elektronische Gesundheitskarte (eGK), Version 1.02
- Protection Profile - Sicherheitsmodul-Karte, Version 1.0
- Protection Profile - Machine Readable Travel Document with "ICAO Application" (e-Passport)
- Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use
- Low Assurance Protection Profile for an Office Based Photocopier Device
- Low Assurance Protection Profile for a VPN Gateway
- Low Assurance Protection Profile for a Voice over IP Infrastructure

Vorrausetzung für eine IT-Sicherheitszertifizierung

IT-Produkte mit Sicherheitsfunktionalität zur Wahrung der

- **Verfügbarkeit von Daten**
- **Vertraulichkeit von Informationen**
- **Unversehrtheit / Integrität von Daten**

ZERTIFIZIERUNGSVERFAHREN

Produktkategorien

Software Produkte

- **Betriebssysteme**
  - **Mainframe**
  - **Midsize**
  - **Smartcards**
- **PC Sicherheitsprodukte**
  - **Security Shells**
  - **Integrity Protection**
- **Data Communication Products**
- **Firewalls**
- **Biometrische Sicherheitsprodukte**
- **Smartcardanwendungen**
- **Signaturanwendungen**

Hardware Produkte

- **Chipcard Reader**
- **Smartcard Reader**
- **Smartcard Controller**
- **Tachograph Components**
  (Weg- und Geschwindigkeitsgeber, Fahrtenschreiber, Tachographkarten)

ZERTIFIZIERUNGSVERFAHREN

Rollenverteilung im Zertifizierungsprozess

Hersteller	➔	Produkt, Designdokumentation, dokumentierte Tests und Analysen, Konfigurationsmanagement, Sichere Entwicklungsumgebung
Zertifizierungsstelle	➔	Know-How über Kriterien und Prüfverfahren, Garant für Neutralität, wahrt Gleichwertigkeit der Prüfverfahren, begleitet die Prüfung, Abnahme der Prüfdokumentation, stellt Zertifikat aus
Prüfstelle	➔	Designprüfung, Tests und Analysen, Penetration Tests, Audit in Entwicklung und Produktion, Prüfdokumentation

ZERTIFIZIERUNGSVERFAHREN

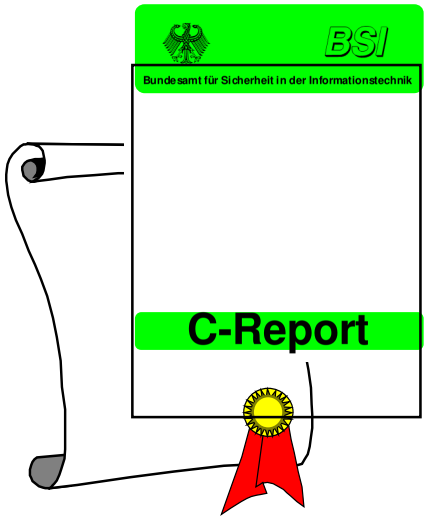
Phasen

Vorbereitung der Zertifizierung:

- Abbildung der Sicherheitsleistung auf Schutzprofil (z.B. eGK,...)
- Abstimmung des Meilensteinplans
- Evaluierungsvertrag mit Prüfstelle
- Antrag auf Zertifizierung beim BSI

Evaluation

- Evaluierung durch die Prüfstelle
- Prüfbegleitung durch die Zertifizierungsstelle
- Anpassung an Updates der Spezifikationen bzw. Schutzprofile
- Abschluss mit Evaluationsendbericht



Zertifizierung

- Erstellung des Zertifizierungsreports mit Auflagen für den operationellen Einsatz
- Erteilung des Zertifikats

Assurance Continuity

- Problematik in der Zertifizierung -
  ein Zertifikat nur gültig für eine bestimmte Version
- Auch bei geringfügigen Änderungen bisher eine Re-Evaluierung und die Beantragung / Erteilung eines neuen Zertifikates erforderlich
- Neues Zertifikat verbunden mit Zeit- und Kostenaufwand
- Bei geringfügigen Änderungen Aufwand nicht verhältnismäßig

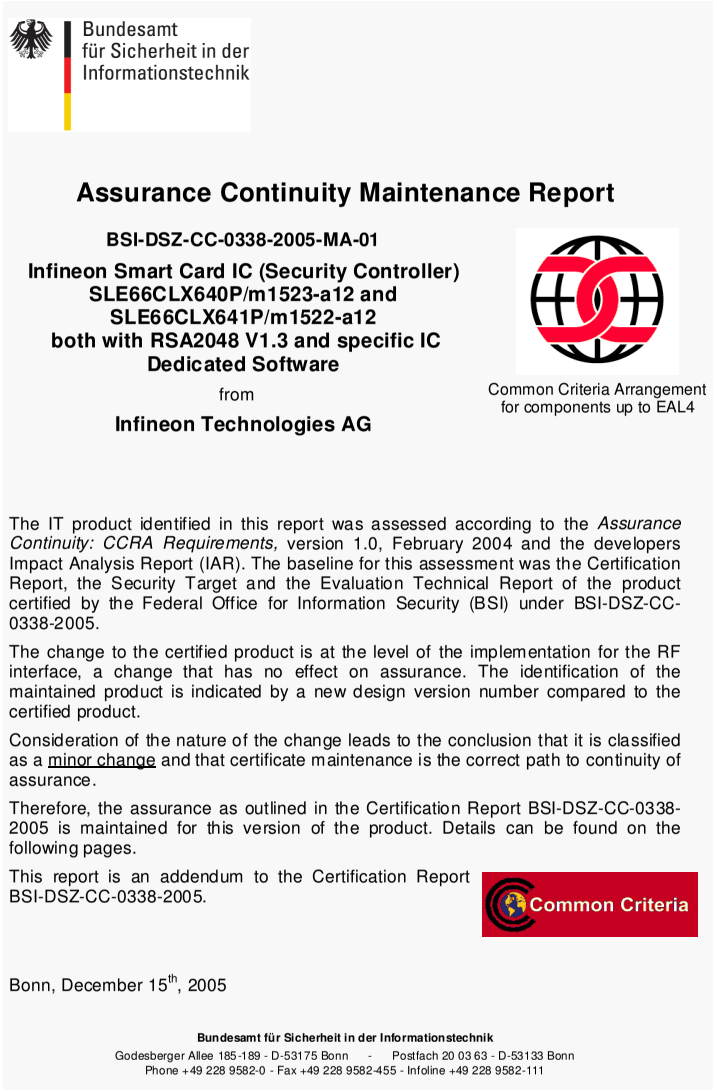
Aufrechterhaltung der Gültigkeit des Zertifikates bei Änderungen am Produkt

Assurance Continuity

- ‘major change’: Re-Evaluierung
- ‘minor change’: Maintenance
- International abgestimmte und anerkannte Verfahren
- bewährte Verfahren in der BSI-Zertifizierung
- Zertifizierungsstellen stimmen sich in bezug auf ‘major’ und ‘minor’ ab

Assurance Continuity - Beispiele

- **Digital Tachograph DTCO 1381, Release 1.2 from Siemens AG, Siemens VDO Automotive**
- **Digital Tachograph SE5000 Revision 6.0 with the product number 900208R6.0 and Software Version 800515R01 from Stoneridge AB**
- **Infineon Smart Card IC (Security Controller) SLE66CLX640P/m1523 -a12 and SLE66CLX641P/m1522-a12 both with RSA2048 V1.3 and specific IC Dedicated Software**
- **Philips P5CT072V0M und P5CC072V0M Secure Smart Card Controller with updated IC Dedicated Software**



Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0338-2005-MA-01

Infineon Smart Card IC (Security Controller) SLE66CLX640P/m1523-a12 and SLE66CLX641P/m1522-a12 both with RSA2048 V1.3 and specific IC Dedicated Software

from

Infineon Technologies AG

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements*, version 1.0, February 2004 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0338-2005.

The change to the certified product is at the level of the implementation for the RF interface, a change that has no effect on assurance. The identification of the maintained product is indicated by a new design version number compared to the certified product.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0338-2005 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0338-2005.

Common Criteria

Bonn, December 15th, 2005

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

INTERNATIONALE ANERKENNUNG

Vermeidung der Mehrfachzertifizierung

Durch Abkommen zur gegenseitigen Anerkennung von Zertifikaten:

- **Anerkennung von CC / ITSEC Zertifikaten**

Unter gewissen Bedingungen

Internationale Anerkennung von Zertifikaten

- **Internationale Vereinbarung (2000) / Common Criteria / bis zu EAL4 / 24 Nationen weltweit**

- **Europäische Vereinbarung (1998) / Common Criteria + ITSEC / alle Evaluationsstufen / 14 Europäische Nationen**

INTERNATIONALE ANERKENNUNG

Common Criteria - Zertifikate CC-RA

Vereinbarung Mai 2000

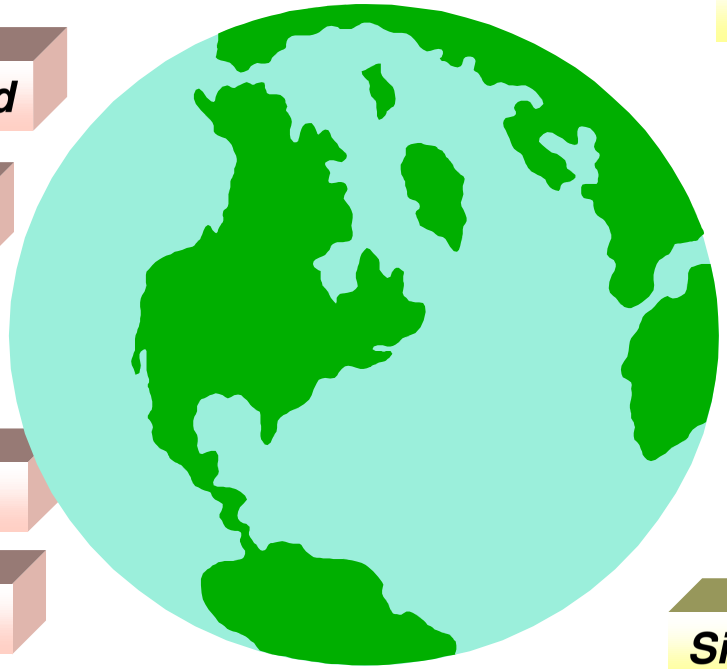
- Evaluierungsstufen bis einschließlich EAL4
- Mitglieder ‘Certificate Producing’ und ‘Certificate Consuming’
- Anerkennung von Zertifikaten für IT Produkte und Schutzprofile (Protection Profiles - PP)

www.commoncriteriaportal.org

INTERNATIONALE ANERKENNUNG

Anerkennende und zertifizierende Nationen

- Australien und Neuseeland
- Kanada
- Niederlande
- Großbritannien
- Deutschland
- USA
- Japan
- Frankreich
- Spanien
- Süd Korea
- Norwegen



Anerkennende Nationen

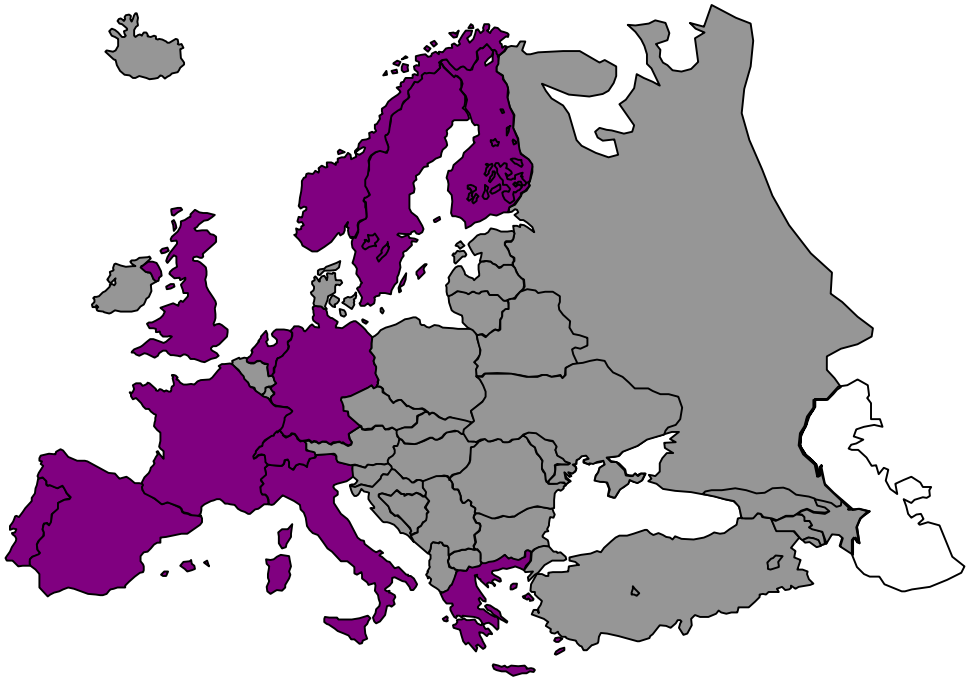
- Finnland
- Griechenland
- Israel
- Italien
- Indien
- Dänemark
- Turkei
- Schweden
- Ungarn
- Singapur
- Tschechien
- Österreich

INTERNATIONALE ANERKENNUNG

ITSEC/CC - Zertifikate SOGIS - MRA

IT Security Certified

Deutschland
Finnland
Frankreich
Griechenland
Grossbritannien
Italien
Niederlande
Norwegen
Portugal
Schweden
Schweiz
Spanien



INTERNATIONALE ANERKENNUNG

ITSEC/CC - Zertifikate SOGIS - MRA

Abkommen März 1998

- **Alle Evaluationsstufen**
- **Einseitige Anerkennung sofern keine nationale Zertifizierungsstelle vorhanden**
- **Abkommen modifiziert zur Erweiterung auf CC Zertifikate EAL 1 - EAL 7**

ZERTIFIZIERTE PRODUKTE

Aktuelle Tachograph-Zertifikate

Deutsches
IT-Sicherheitszertifikat
erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit
in der Informationstechnik

• Siemens AG, Siemens VDO Automotive	Tachograph (Digital Tachograph DTCO 1381)
• Giesecke & Devrient GmbH	Smartcard mit Tachograph Anwendungen
• T-Systems International GmbH, Service Line SI, T-Telesec	Tachograph Chipkarte
• ORGA Kartensysteme GmbH	Smartcard mit Tachograph Anwendungen

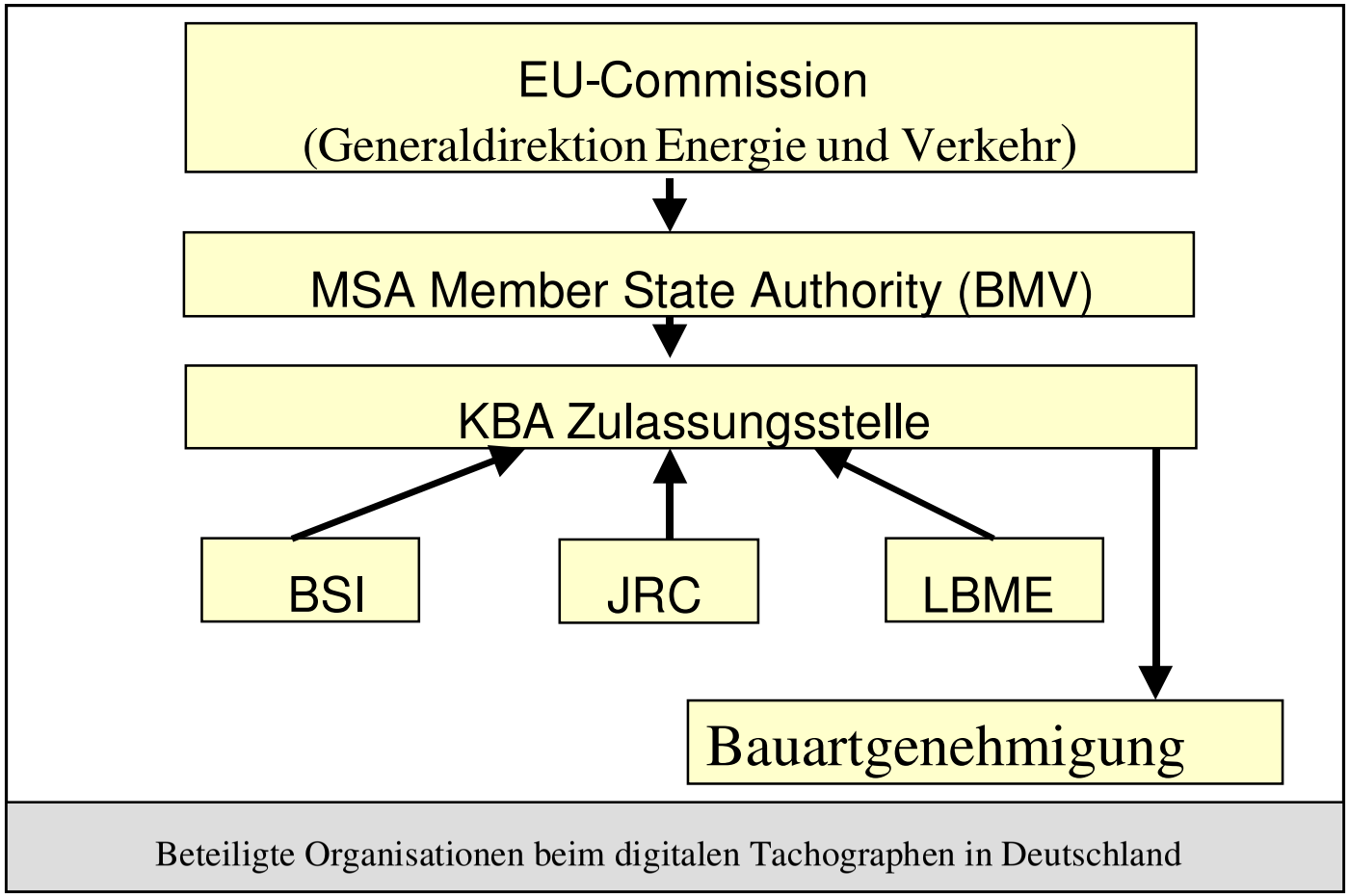
DIGITALE TACHOGRAPHEN

- Gesetzliche und Organisatorische Rahmenbedingungen
- Technisches Konzept
- Sicherheitsziele des Digitalen Tachographen
- Sicherheitsmaßnahmen gegen Informationsgewinn
- Schutz gegen Manipulation und die Bewertung der Sicherheitsmaßnahmen

GES. U. ORG. RAHMENBEDINGUNGEN

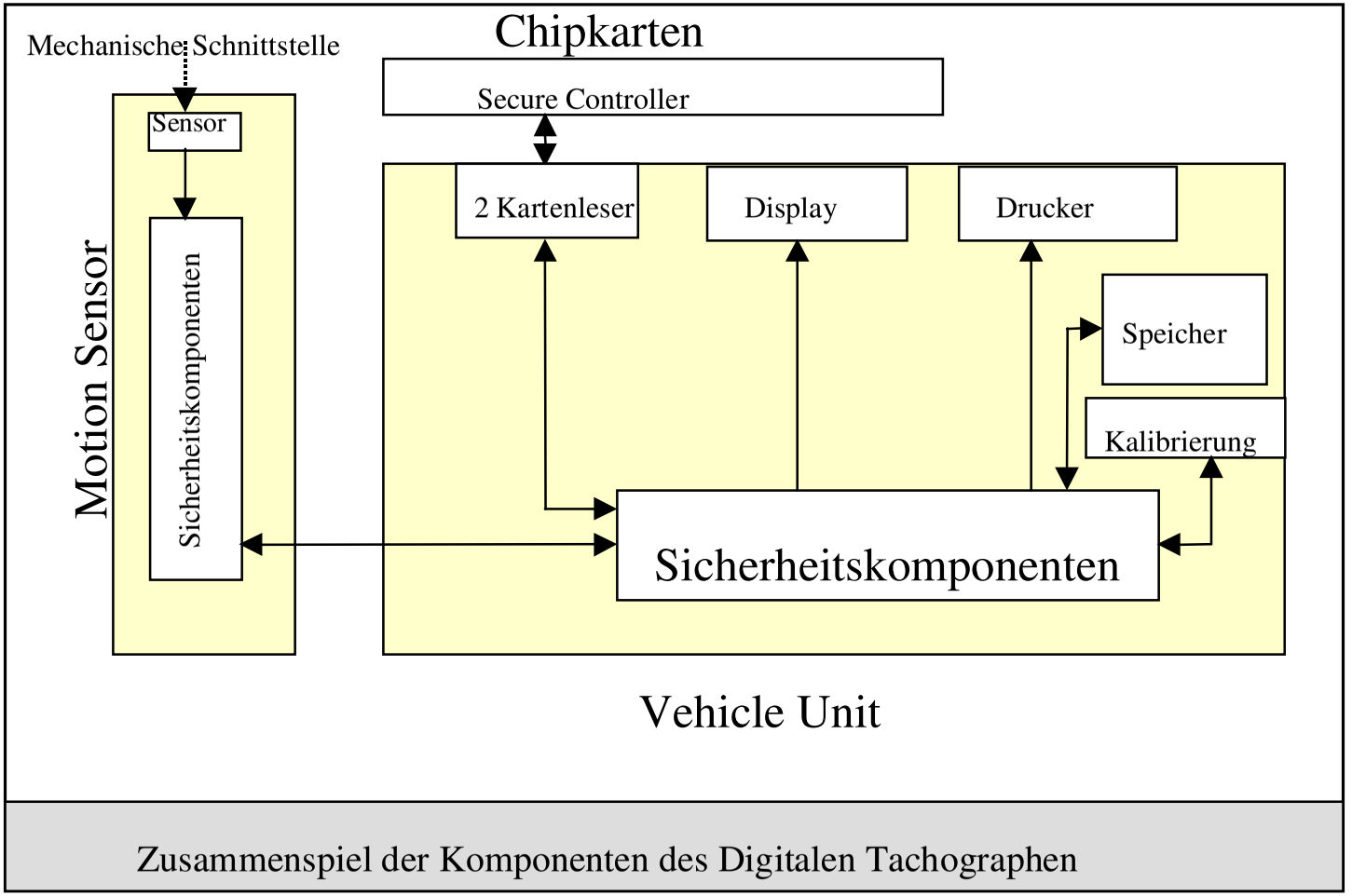
- Technische Spezifikation des digitalen Tachographen: Appendix 10 des Anhangs I (B) der Verordnung (EG) Nr. 1360/2002 zur Anpassung der Verordnung (EWG) Nr. 3821/85
- Einbaupflicht des Digitalen Tachographen ab 1.5.06 (neuzugelassene Nutzfahrzeuge ü. 3,5 T. oder Fahrzeuge mit mehr als 9 Personen.)
- Einbaupflicht wurde veröffentlicht im Amtsblatt der Europäischen Union am 11.04.06
- Organisatorische Maßnahmen zur Durchsetzung der Verordnung I(B) in den Mitgliedstaaten der EU

GES. U. ORG. RAHMENBEDINGUNGEN



Beteiligte Organisationen beim digitalen Tachographen in Deutschland

TECHNISCHES KONZEPT



Zusammenspiel der Komponenten des Digitalen Tachographen

SICHERHEITSZIELE DES TACHOGRAPHEN

- Die von den Kontrollbehörden zu prüfenden Daten müssen verfügbar sein und die Handlungen der kontrollierten Fahrer und Fahrzeuge hinsichtlich Lenk-, Arbeits-, Bereitschafts-, und Ruhezeiten sowie Fahrzeuggeschwindigkeit vollständig und genau widerspiegeln.

- Identifizierung und Authentisierung, Zugriffkontrolle, Zuordnungsmöglichkeit, Audit (Protokollierung), Genauigkeit, Zuverlässigkeit während des Betriebes, Datenaustausch und die Kryptographische Unterstützung.

MASSNAHMEN GEGEN INFORMATIONSGEWINN

- **Maßnahmen in der Entwicklungsumgebung**
  - Bauliche Maßnahmen (Zugang zur sensitiven Informationen, Dokumentation, usw.)
  - Technische Maßnahmen (Zugriff zur Software-Code, Hardwareteile und Sensitive Informationen
  - Organisatorische Maßnahmen (Vertreterregelungen für Zugriffe auf bestimmte Informationen
- **Maßnahmen im Kontext der Konstruktion**
  - Das Gehäuse des Tachographen kann geöffnet werden (--> Protokollierung)
  - Das Gehäuse des Tachographen kann nicht geöffnet werden

Im Kontext der Konstruktion dürfen die im Tachographen gespeicherten Informationen durch den Angreifer weder ausgelesen noch manupuliert werden

Direkte Angriffe auf die Sicherheitsfunktionen

- Test der Korrektheit der Sicherheitsfunktionen (Qualitätssicherung)
- Direkte Angriffe auf die Sicherheitsfunktionen (z.B.: I&A zwischen Motion Sensor und Vehicle Unit), z.B.: Replay Angriffe, Erraten der Geheimnisse durch Analyse Methoden oder durch Abhören der Leitung:

  Bewertung der Sicherheitsfunktion gegen ein hohes Angriffspotenzial im Kontext der Tachographen:

- **Zeit für die Identifizierung und Durchführung des Angriffs**
- **Wissenstand des Angreifers (Layman, Proficient oder Expert)**
- **Erforderliches Wissen über die Komponenten (none, public, sensitive)**
- **Anzahl der benötigten Komponenten zur Durchführung des Angriffs**
- **Art der erforderlichen Geräte (none, standard, specialised, bespoke)**

- **Punkte > 25 (hohes Angriffspotential)**

Suche nach Schwachstellen

Es handelt sich dabei um indirekte Angriffe: Deaktivierung, Umgehung, Veränderung oder Ausschaltung der Sicherheitsfunktionen

Die Suche nach Schwachstellen hängt von der Konstruktion der Komponenten und von der Implementierung der Sicherheitsfunktionen ab

Einige Beispiele für die Schwachstellen Analyse im Kontext der Tachographen:

- **SPA Analyse**
- **Störungstest**
- **Probing (Kontaktierung mit einem Nadel)**
- **DPA Analyse (Differential Power Analysis)**

- **Punkte > 25 (hohes Angriffspotential)**

KOMPONENTEN D. DIGITALEN TACHOGRAPHEN

Ausblick:

Die IT-Sicherheitskriterien wie CC oder ITSEC stellen eine geeignete Prüfgrundlage dar, um die Komponenten des Digitalen Tachographen gemäß spezifizierter Anforderungen zu prüfen und zu bewerten.

Bundesamt für Sicherheit in der Informationstechnik
Referat 322
Postfach 200 363
D-53133 Bonn
Infoline: (01888) 9582-5111
eMail: zerti@bsi.bund.de
http://www.bsi.bund.de