KI-FACHKONFERENZ

Artificial Intelligence Act

Dr. Peter Deussen
Dr. Christoph Peylo
Daniel Loevenich

Frankfurt, 22.11.2021

Vertrauenswürdigkeit von KI-Systemen erfordert die Beteiligung aller Stakeholder

Cybersicherheit zu gewährleisten ist schwierig…

… und bei KI-Systemen?

“**Unsecurable**”
Chris Inglis (2010), Former Deputy Director National Security Agency

“**Indefensible**”
Gen. Keith Alexander (2011), Former Director NSA und Commander of the United States Cyber Command

“**Hopeless**”
Ron Rivest (2012), Co-Inventor of RSA-Crypto Systems, Turing Award (2002)

KI-Systeme sind überaus complex und erfordern einen hohen Entwicklungsaufwand

Zusätzliche Herausforderungen durch KI

Zusätzliche Herausforderungen durch KI

R. Witherspoon with “Glasses”

Recognized as

Russell Crowe

Sticker

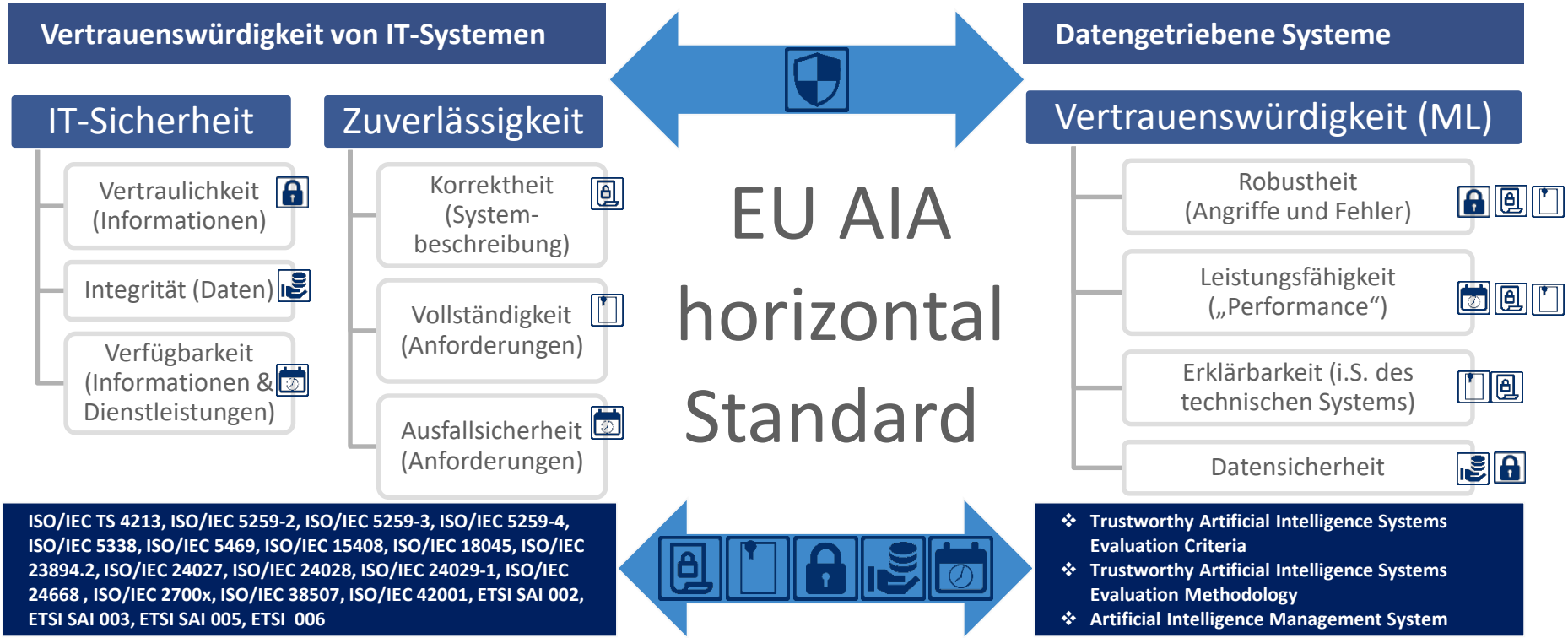
Recognized as

Speed Limit 45mph

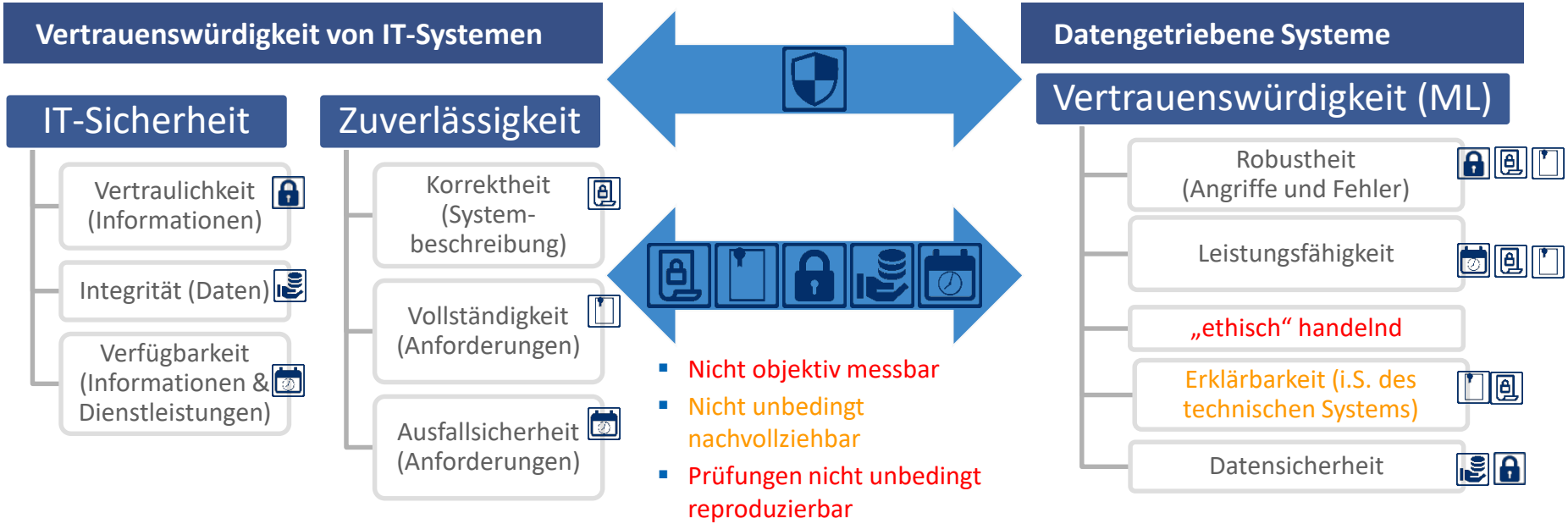
IT-Sicherheit und Datensicherheit als zentrale Eigenschaften vertrauenswürdiger KI-Anwendungen: 5 Leitfragen für den Workshop

1. Mein Produkt enthält KI-Methoden als Teil der verwendeten Informationstechnik. Welche spezifischen zusätzlichen Risiken ergeben sich durch den Einsatz von KI? Muss ich die KI-Sicherheit nach EU-Act getrennt von der IT-Sicherheit für mein Produkt verstehen und nachweisen?
2. Ich bette KI-Komponenten in mein Produkt ein, die für das Endprodukt sicherheitsrelevant sind. Wie kann mir ein horizontaler KI-Standard im Sinne des EU-AI-Acts helfen, meinen Rechtspflichten bzgl. der Gesamtsicherheit meines Produktes nachzukommen?
3. Welche Hilfestellung darf ich von horizontalen Standards bei der KI-Regulierung in meinem Marktsegment/meiner Branche/meinem Sektor erwarten? Wie lassen sich Widersprüche zwischen den horizontalen und den sektoralen Reglungen vermeiden?
4. Ich biete KI-Lösungen als (Dienst-)Komponenten im B2B-Markt an. Wie kann ich die Anforderungen meiner Kunden im Sinne der angestrebten KI-Regulierung mit horizontalen Standards abdecken? Wie kann ich die zur Wertschöpfungskette orthogonale Anforderungskette in meinem Geschäftsmodell abbilden und in meinem Unternehmen/meiner Organisation/meiner Supply Chain verankern? Lässt sich Artikel 40 dazu nutzen?
5. Was kann ich tun, um die KI-Sicherheit in meinem Unternehmen rechtzeitig und nachhaltig zu verankern?

Basis für horizontale KI-Sicherheitsstandards



Problem: Der EU Vorschlag nimmt das Konzept der HLEG von „Trustworthyness“ auf. D.h. trustworthy = legal + robust + ethical.



Struktur und Beziehungen zwischen den Standards müssen transparent sein.

Horizontaler Standard

Sektoraler Standard

- Einsatzorientiert
- Use Cases
- Beispiele:
  - Medizin
  - Verkehr
  - Landwirtschaft
- Stakeholder sind die Unternehmen und Verbände
- Mitwirkung ist unerlässlich

Artikel 40 und seine Anwendung

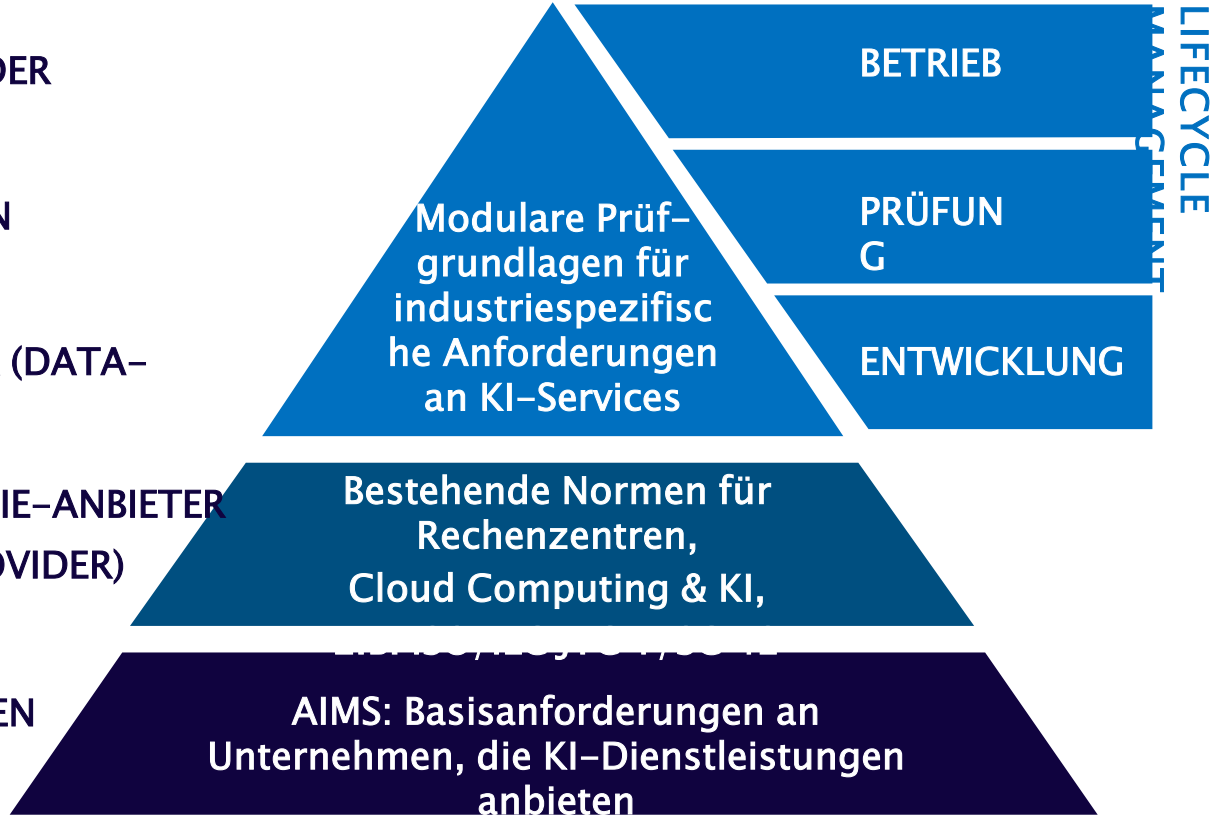
EU AIA Article 40

Chapter 2: Requirements for High Risk AI-systems

- Article 8: High Risk AI systems comlpy with the following requirements
- Article 9: Risk management system
- Article 10: Data and data governance
- Article 11: Technical documentation
- Article 12: Record keeping
- Article 13: Transparency and provision of information of users
- Article 14: Human oversight
- Article 15: Accuracy, Robustness and cybersecurity

Artificial Intelligence Management System (AIMS)

- Einhaltung von Mindest-standards für vertrauens-würdige KI
- Zertifizierungen nach AIMS sind möglich
- ISO-Standard



Artificial Intelligence Management System: Basisanforderungen an Anbieter und Nutzer von KI-Systemen

- ISO/IEC 42001 – Artificial Intelligence Management Systems (currently under development in ISO/IEC JTC 1/SC 42)

- Horizontaler Rahmen für das Management von KI-Systemen
- Risiko-basiert (Organisations-Risiken + Folgeabschätzung)
- Integrierbar mit anderen Management-Systemen (Qualität, Sicherheit, usw.)

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner:

Dr. Peter Deussen
Microsoft Deutschland GmbH

peter.deussen@microsoft.com

Ihr Ansprechpartner:

Dr. Christoph Peylo
Prj Digital Trust (CDO/PJ-DT)
Robert Bosch GmbH

Christoph.Peylo@de.bosch.com

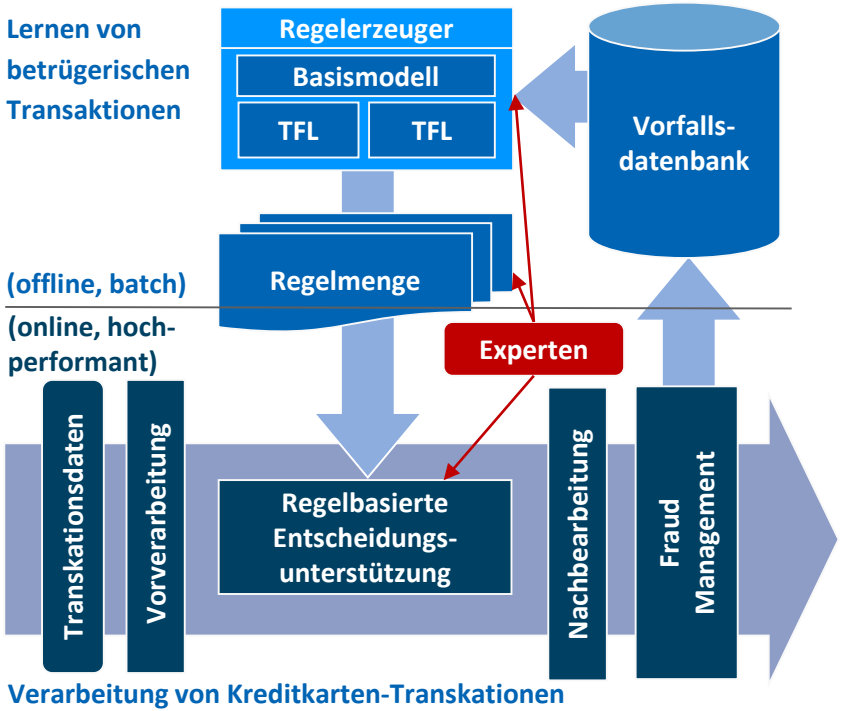
Ihr Ansprechpartner:

Daniel Loevenich
Bundesamt für Sicherheit in der Informationstechnik

daniel.loevenich@bsi.bund.de

Beispiel: Kreditkartenbetrug (Use Case-Vorschlag für ein Projekt der NRM KI)

Systemarchitektur nach Fh IAIS



Verarbeitung von Kreditkarten-Transkationen

Cloud-basierter KI-Service

- Cloud-Provider liefert
  - IAAS,PAAS
  - Development Support (KI-Framework)
  - „Prüf“-Werkzeuge
  - End Customer Life Cycle Support
- u.U. externer Dienstleister für die Daten
- Kreditkartenanbieter
  - Operation im Expertenmodus
  - „gesamt“-verantwortlich → AIMS

Konformitätsvermutung des Herstellers (Idee: Freiwillige Zertifizierung nach CSA nutzen, um Konformität zu demonstrieren)

Eingebettete Künstliche Intelligenz

Vorschlag der ICT-Focus-Group: NLF Rechtsakt wird durch CSA-Brücke gefüllt