



Bundesamt
für Sicherheit in der
Informationstechnik

Schutz vor Manipulationen an digitalen Grundaufzeichnungen

Fachgespräch im Bundesministerium der Finanzen

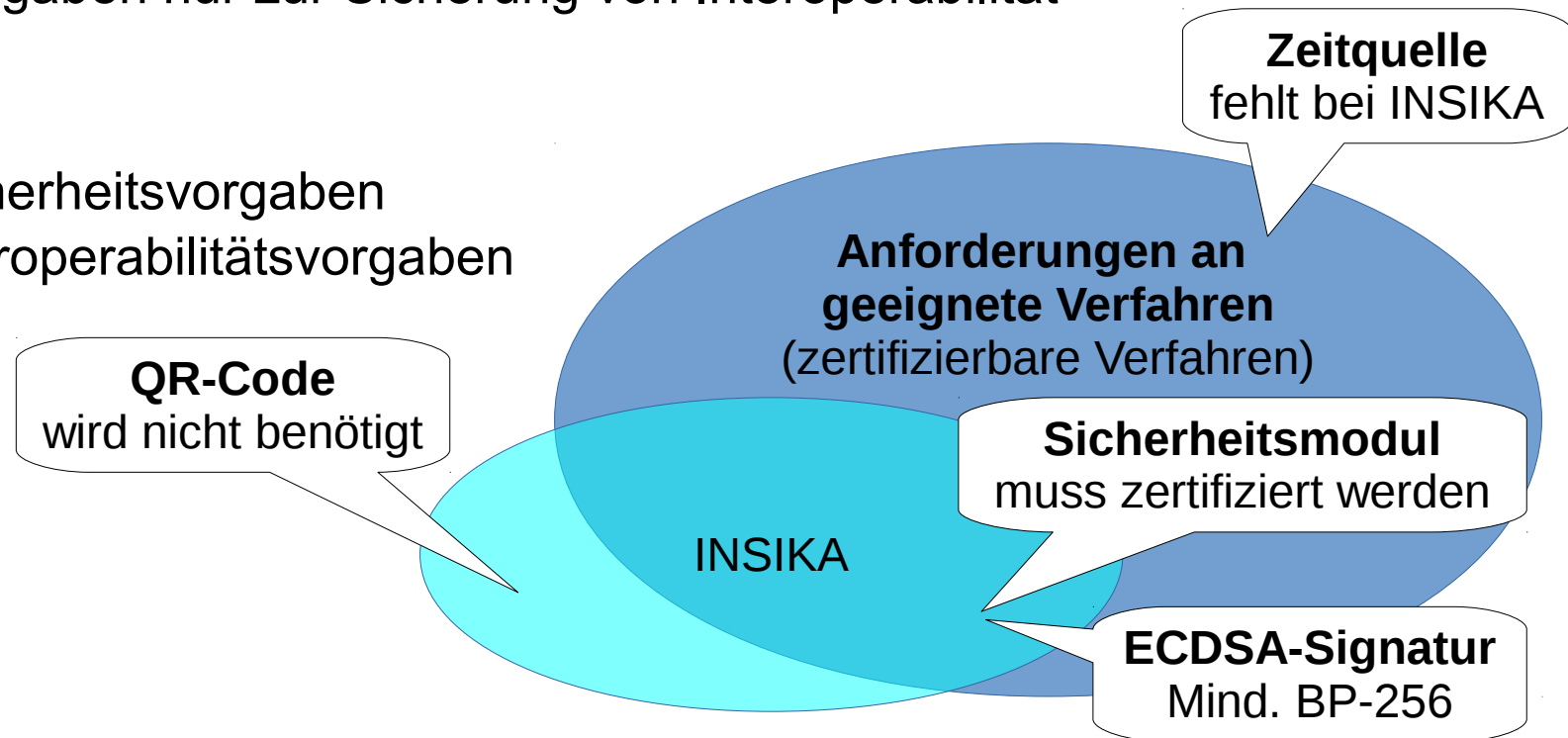
Grundkonzeption

Technologieoffenes Verfahren

- Förderung von Innovationen / Marktprinzip / Einsatzzweck
- Festlegung von (technikneutralen) Mindest-Sicherheitsanforderungen
- Festlegung von technischen Vorgaben nur zur Sicherung von Interoperabilität

Zertifizierungsverfahren

- Prüfung der Einhaltung von Sicherheitsvorgaben
- Prüfung der Einhaltung von Interoperabilitätsvorgaben



Manipulationssicherheit von Grundaufzeichnungen

Grundaufzeichnungen dürfen nicht (nachträglich) manipuliert werden

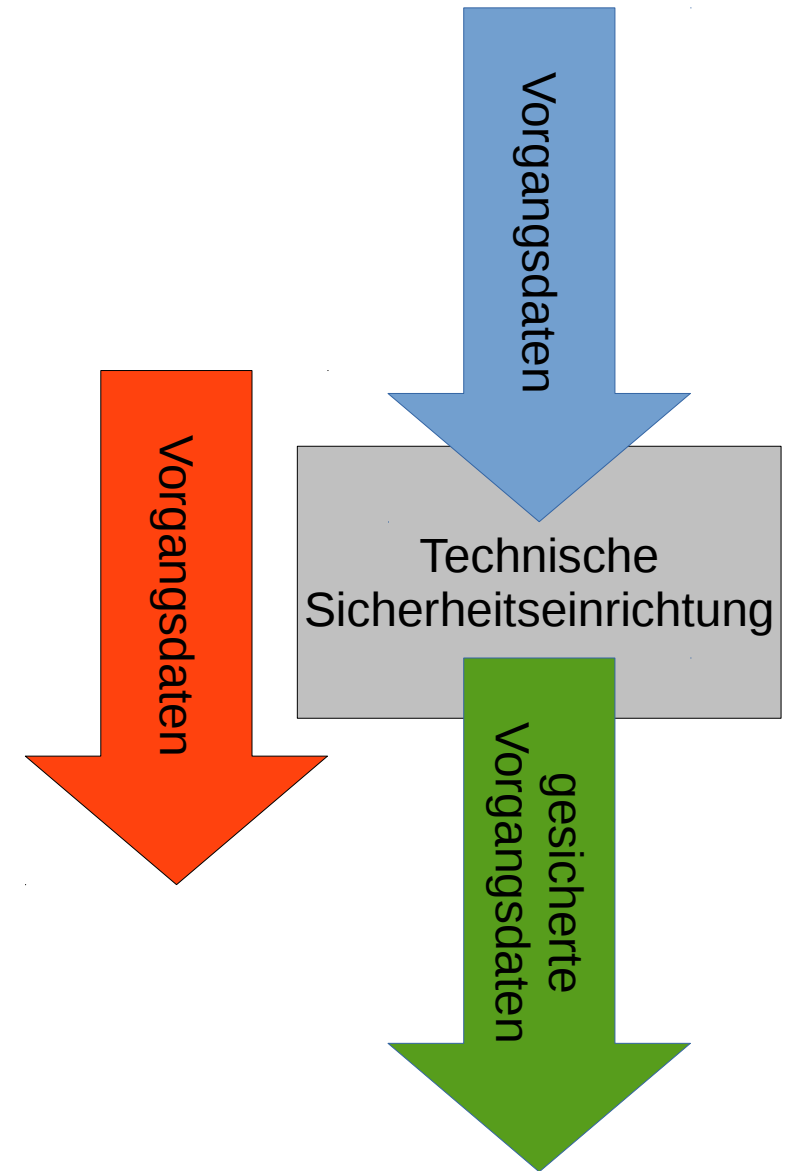
- Löschen von erfassten Vorgängen
- Hinzufügen von zusätzlichen Vorgängen
- Verändern von erfassten Vorgängen

Manipulation von Grundaufzeichnungen bei der Eingabe kann nicht verhindert werden

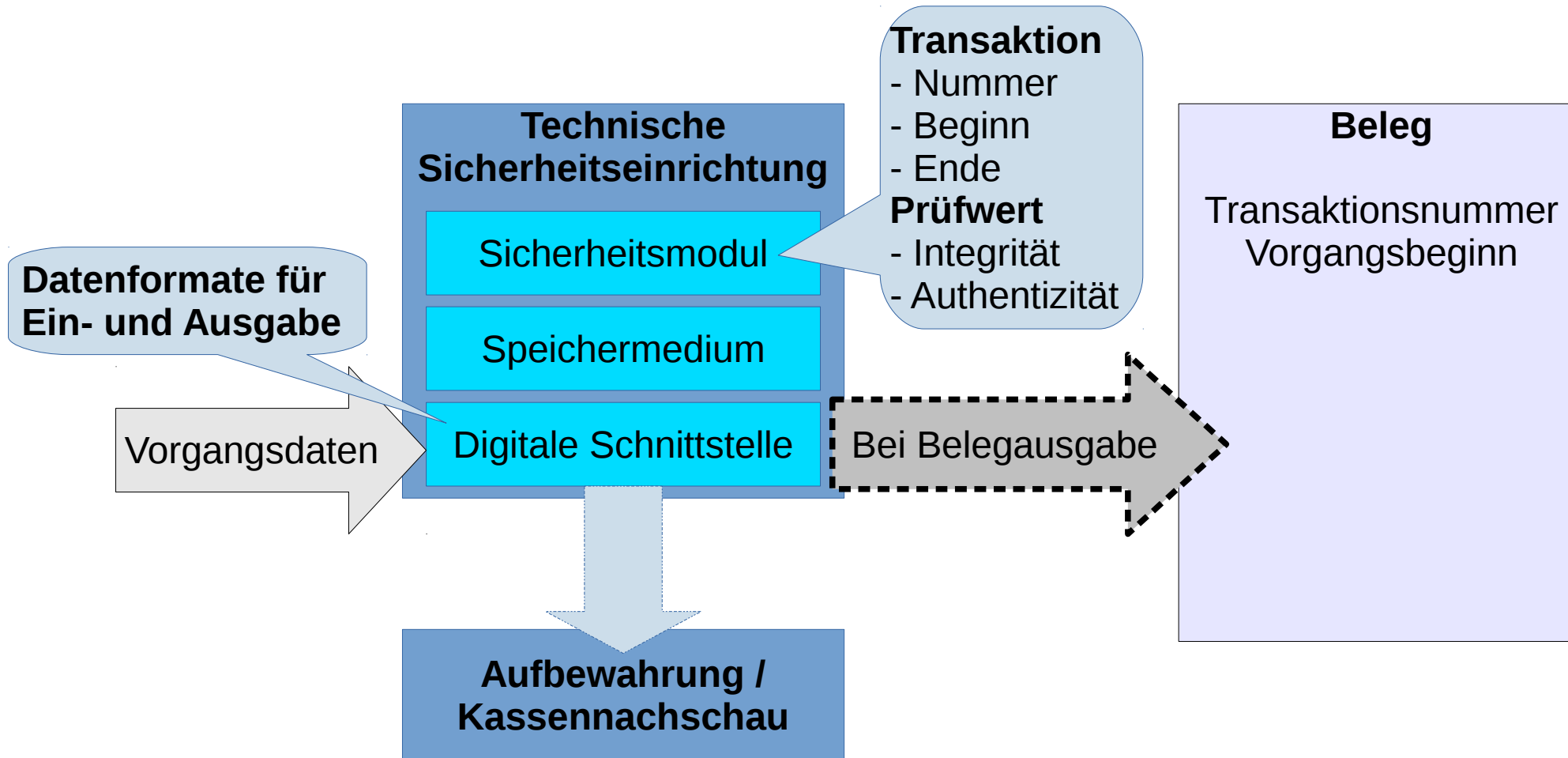
- Nicht-erfassen von Vorgängen
- Falsch-erfassen von Vorgängen

Nachträgliche Korrektur von Vorgängen bleibt möglich

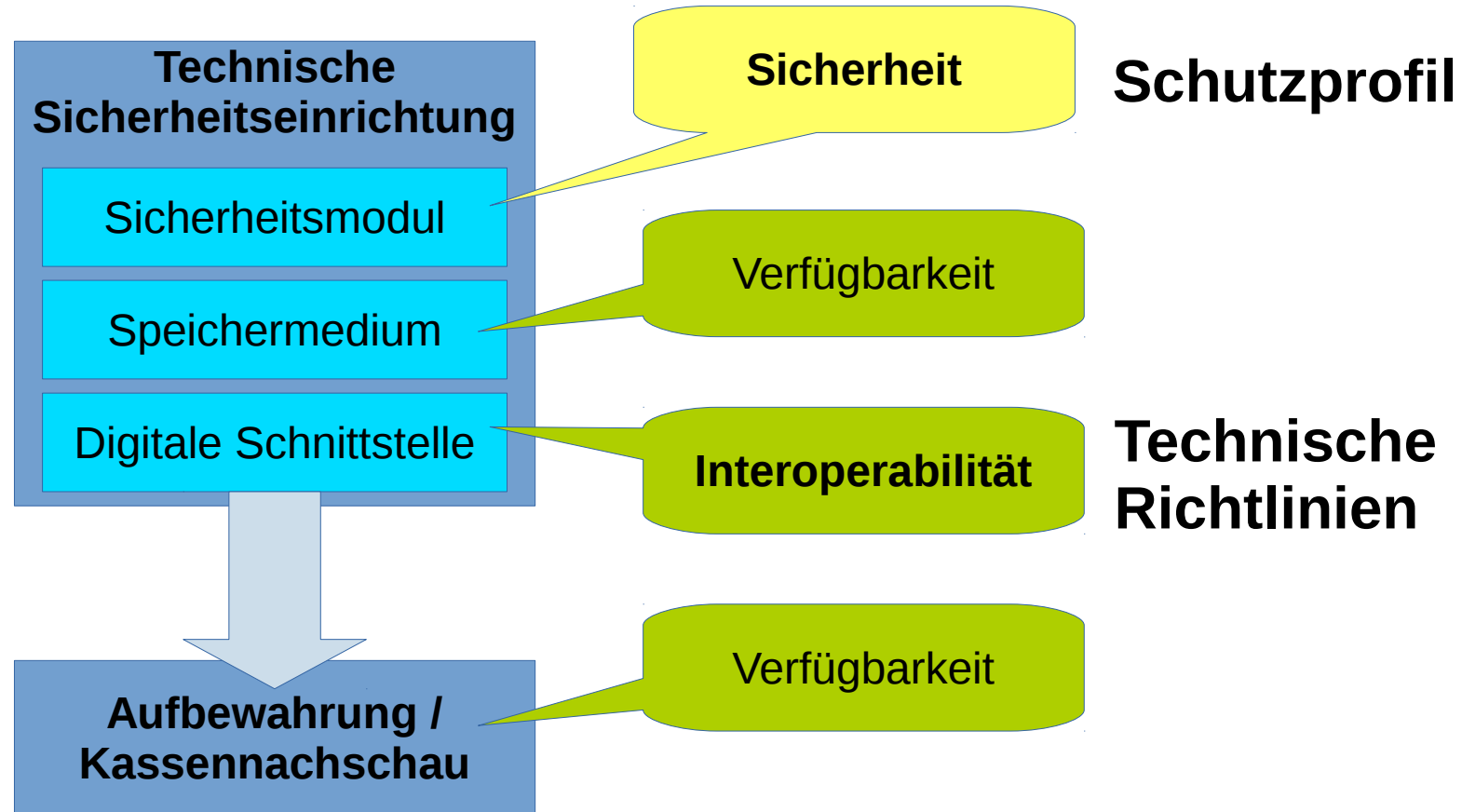
- Stornieren eines Vorgangs → zusätzlicher Vorgang
-



Sicherung von Grundaufzeichnungen



Zertifizierung der Sicherheitseinrichtung



Sicherheitszertifizierung

Schutzprofil Sicherheitsmodul (Protection Profile)

- EAL 4+ / AVA.VAN.5 → hohes Angriffspotential
- Beschreibt Sicherheitsziele und Anforderungen an Sicherheitsfunktionen
- Produktspezifische Konkretisierung durch Hersteller (Security Target)
- Nachweis der Einhaltung der Anforderungen
 - Evaluierung durch akkreditierte Prüfstelle
 - Zertifizierung durch BSI
- Zertifikate sind befristet

Betrachtung des Lebenszyklus eines Sicherheitsmoduls

- Fertigung
- Personalisierung
- Inbetriebnahme
- Nutzung
- Außerbetriebnahme
- Vernichtung

Hersteller des Sicherheitsmoduls

- erstellt ein Konzept
- zur Sicherung der Unversehrtheit des Moduls
- über den gesamten Lebenszyklus
- als Teil der Zertifizierung



Bestimmung von Beginn & Ende eines Vorgangs

Vorgänge sollen....

- zeitnah erfasst werden (keine „nachträgliche“ Erfassung)
- zeitlich aufgefunden werden können (z.B. bei Testkauf)
- in endlicher Zeit abgeschlossen werden (keine dauerhaft „offenen“ Vorgänge)

Optionen für Zeitquellen (technologieoffen)

- Interne Zeitquelle: Aufwändig...
- Externe Zeitquelle: „sichere“ entfernte Zeitquelle
 - Signed NTP
- Externe Zeitquelle: „unsichere“ lokale Zeitquelle
 - Zeitaktualisierung als (regelmäßige) Transaktion
 - Transaktionszeit ist streng monoton wachsend
- Mischformen
 - z.B. täglicher Abgleich mit externer Zeitquelle anschließend interne Zeitquelle

*Keine “besonders hohen”
Anforderungen an die Zeit*

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Dennis Kügler
Referatsleiter
Dennis.Kuegler@bsi.bund.de
Tel. +49 (0) 22899 9582 5183
Fax +49 (0) 22899 10 9582 5183

Bundesamt für Sicherheit in der Informationstechnik
Referat S15, Chip-Sicherheitsanalyse
Godesberger Allee 185-189
5175 Bonn
www.bsi.bund.de

