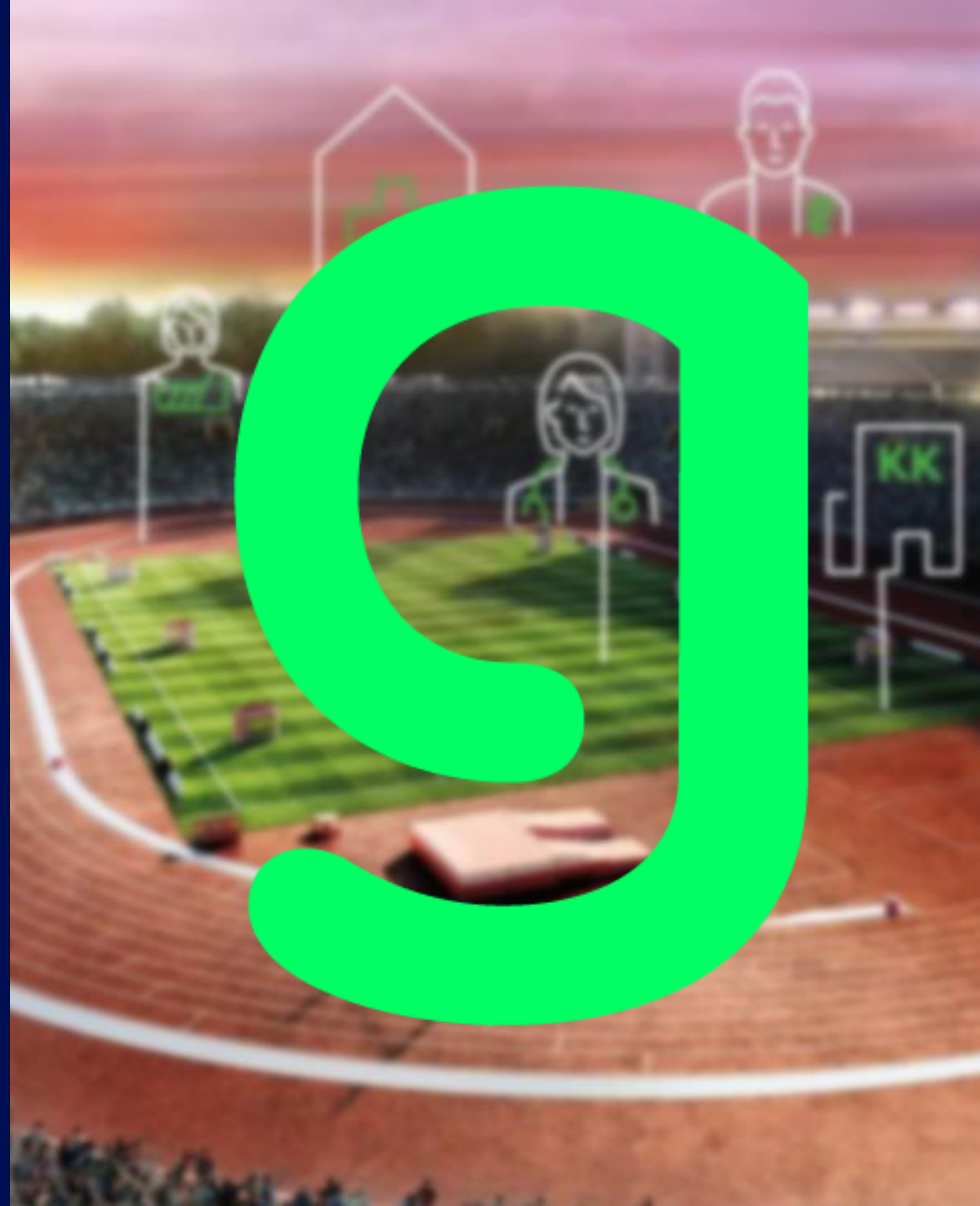
Willkommen zum Betriebsforum

Berlin, der 24. Juni 2025



gematik

Update TI-Lagebild, TI-Status und Service Map

Oliver Klein (gematik GmbH, Leiter Sevice Information Management)

Refresh: Service Map, TI-Lagebild, TI-Status

Service Map ⓘ

- Abbildung der Abhängigkeiten der TI-Produkte untereinander (A braucht B)
- Berücksichtigung aller betrieblichen Ausprägungen (Produktinstanzen)
- Modellierung von Anwendungsszenarien und ihren benötigten Abhängigkeitsketten

TI-Lagebild

- Zustandsanzeige der wesentlichen TI-Anwendungen, berechnet auf Basis des Probings und der Service Map
- Benennung ggf. gestörter Anwendungsszenarien bei Störungen
- Benennung von bekannten Störungsursachen

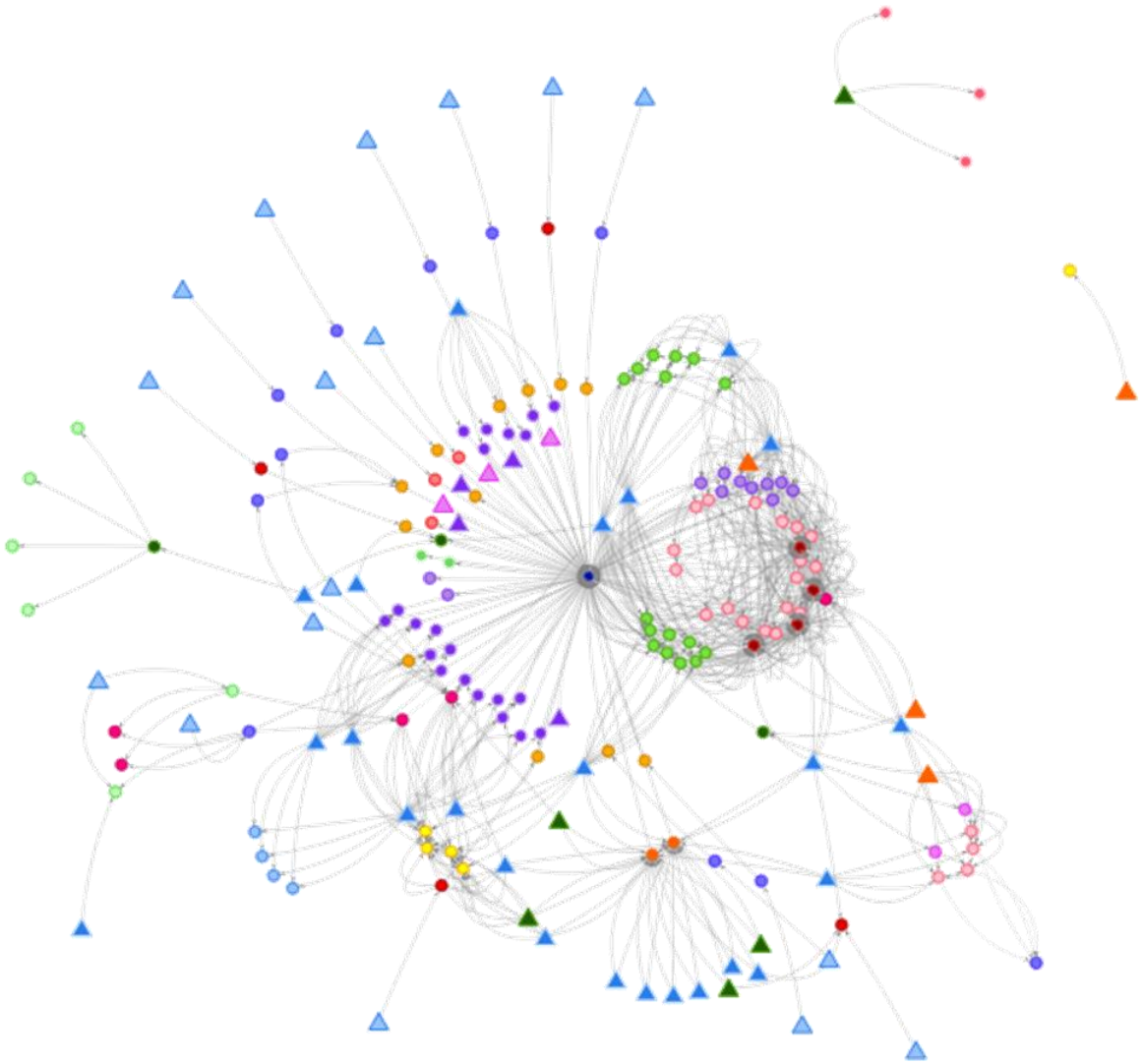
TI-Status

- Störungsinformationen der gematik
- Zusätzliche Links zum TI-Changeplaner, Wartungen und sonstigen Informationen

Neues zur Service Map

Service Map – Umsetzung

aktueller Stand

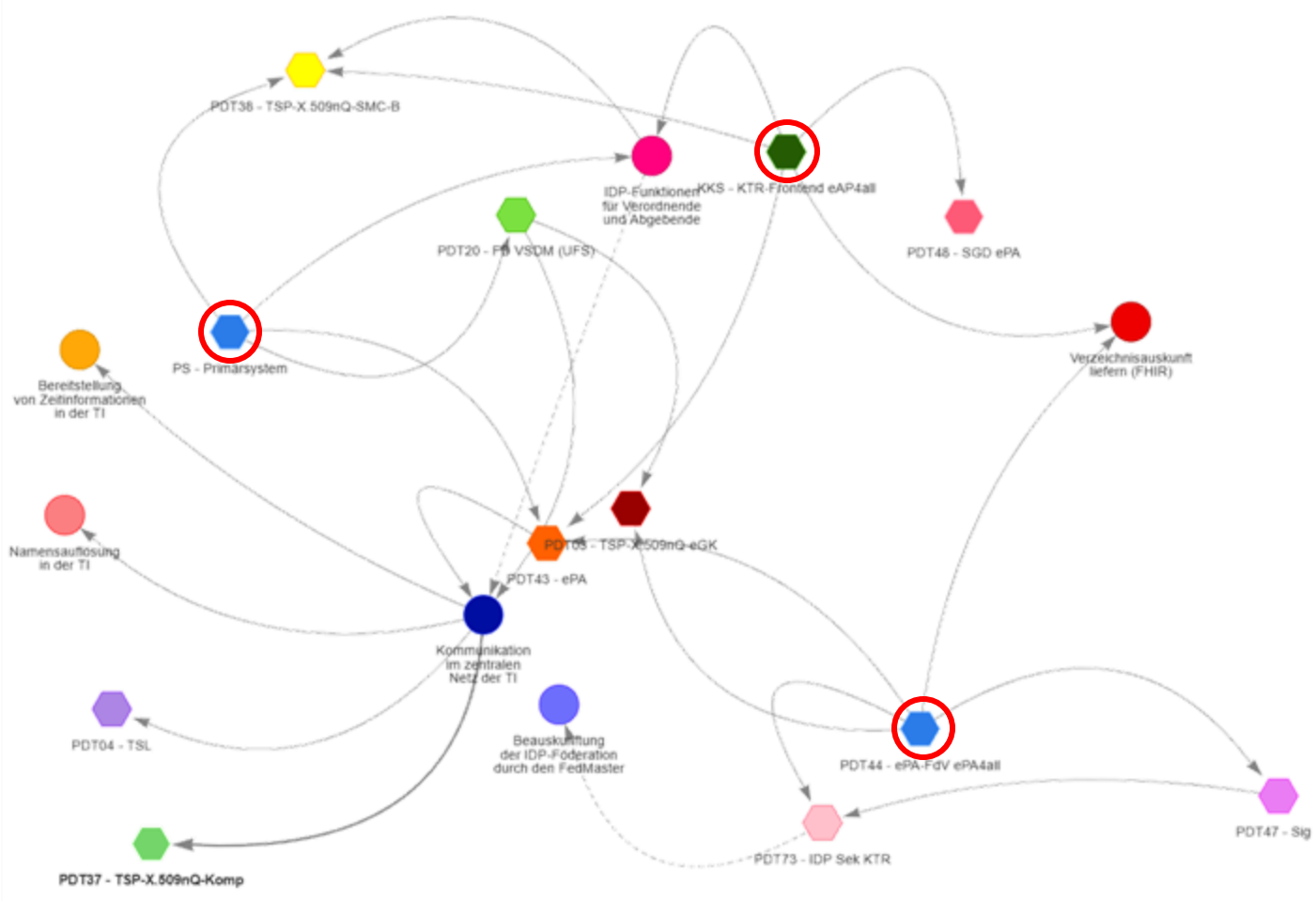


Alle relevanten Produkte der PU sind in der Service Map abgebildet, Stand April 2025:

- 147 technische Anwendungsszenarien
  - 60 außenrelevante Anwendungsszenarien
    - 7 TI-Anschluss
    - 8 E-Rezept
    - 20 ePA
    - 5 KIM
    - 3 VSDM
    - 3 DEMIS
    - 14 Sonstige WANDA
- 203 technische Produktkomponenten von 140 Produktinstanzen
- 803 Wirkbeziehungen (‚A braucht B‘)

Service Map am Beispiel der ePA

Schematische Darstellung ohne Instanziierung



Anwendungsszenarien der ePA

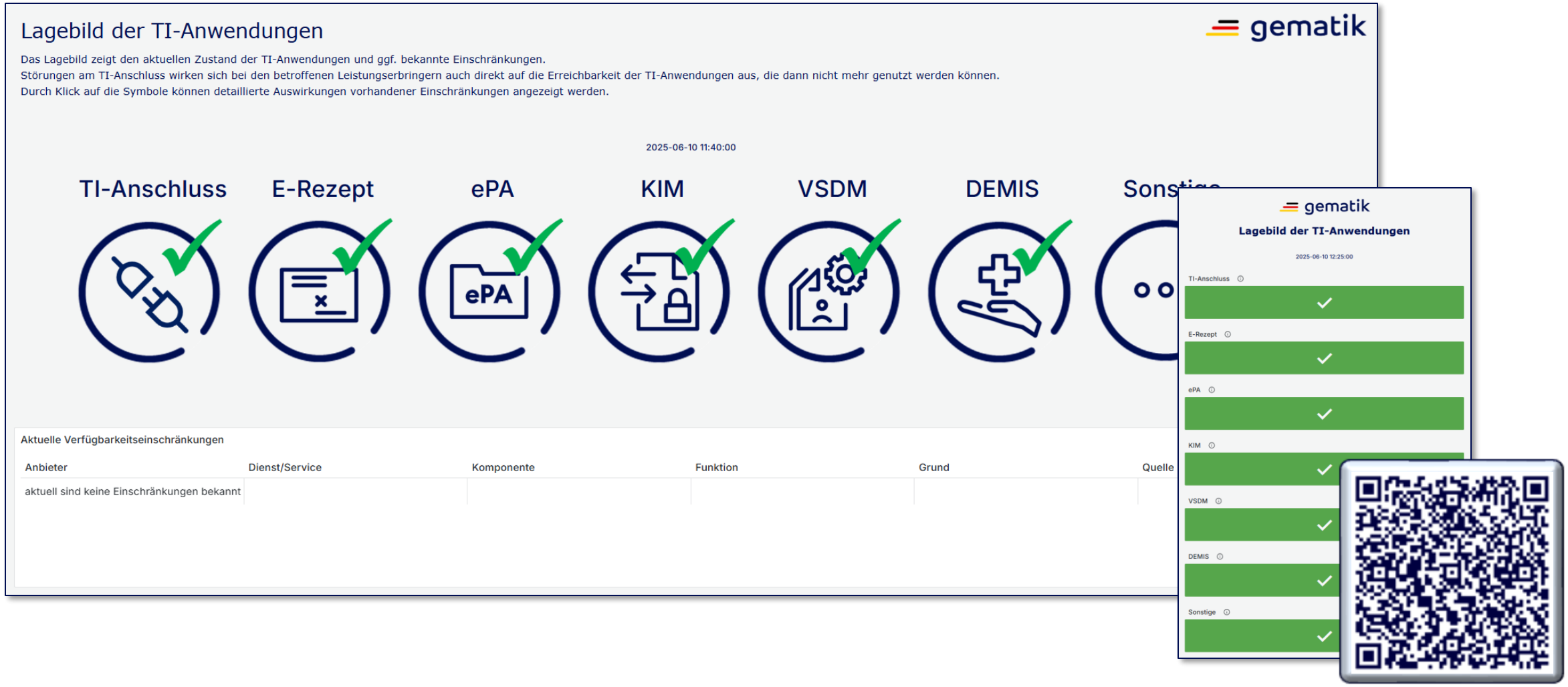
- Primärsystem (Leistungserbringer):
  - Befugnisse ablegen durch LE
  - Dokumentenoperationen durch den LE
  - Dokumentenoperationen durch den LE mit Signierung
  - Login der LE
  - Widersprüche abfragen durch LE
- ePA-FdV (Versicherte):
  - Befugnisse ablegen durch den Versicherten
  - Dokumente/Kategorien verbergen durch Versicherten
  - Dokumentenoperationen durch den Versicherten
  - Identifikation des Versicherten am Frontend (Ersteinrichtung)
  - LEI blockieren durch Versicherten
  - Login des Versicherten am Frontend
  - Login des Versicherten am Frontend bei abgelaufenem IDP-Caching
  - Widersprüche ablegen durch Versicherten
- KTR-Frontend (Kostenträger):
  - Akten anlegen durch KTR
  - Aktenumzug von Vorgängerversion
  - LEI blockieren durch OSt
  - Login der KTR /OSt
  - Widersprüche ablegen durch OSt

Service Map

neu: TI-Anschluss als eigene Kategorie

- Initiiert durch die Einführung der TI-Gateways und die zunehmenden Versicherten-Anwendungsszenarien wurde eine neue Kategorie in der Service Map eingeführt: der TI-Anschluss. (VPN-Zugangsdienste und TI-Gateways).
- Die Anwendungen der TI werden durch Störung einzelner Anschlusswege nicht mehr als beeinträchtigt dargestellt, da eine Störung am Anschluss ohnehin alle Anwendungen bei Leistungserbringern mit diesem Anschluss betrifft
- Die Kategorie TI-Anschluss umfasst die VPN-Zugangsdienste (traditioneller Anschluss an die TI mittels Konnektor in der Institution) und die TI-Gateways (neuer Anschluss an die TI über zentrale Highspeed-Konnektoren der TI-Gateway-Anbieter)

Das aktuelle Lagebild der TI



Feedbacks und Wünsche zum Lagebild und zur Störungskommunikation

Ich erwarte eine konsistente Störungskommunikation, bisher gab es oft Abweichungen zwischen Lagebild und den Informationen im TI-Status

Als Krankenhaus muss ich Störinformationen so schnell wie möglich haben, um nicht unnötig Zeit in die lokale Analyse zu stecken

In meinem Helpdesk wünsche ich mir Zugriff auf die Störungshistorie, um Anfragen auch rückwirkend einordnen zu können

Als Primärsystemhersteller möchte ich die Informationen aus den Lagebildern automatisiert abrufen und meinen Kunden direkt zur Verfügung stellen

Als Institution interessieren mich nur Störungen, die mich auch betreffen, ich kenne ja meine SMC-B, meinen HBA usw.

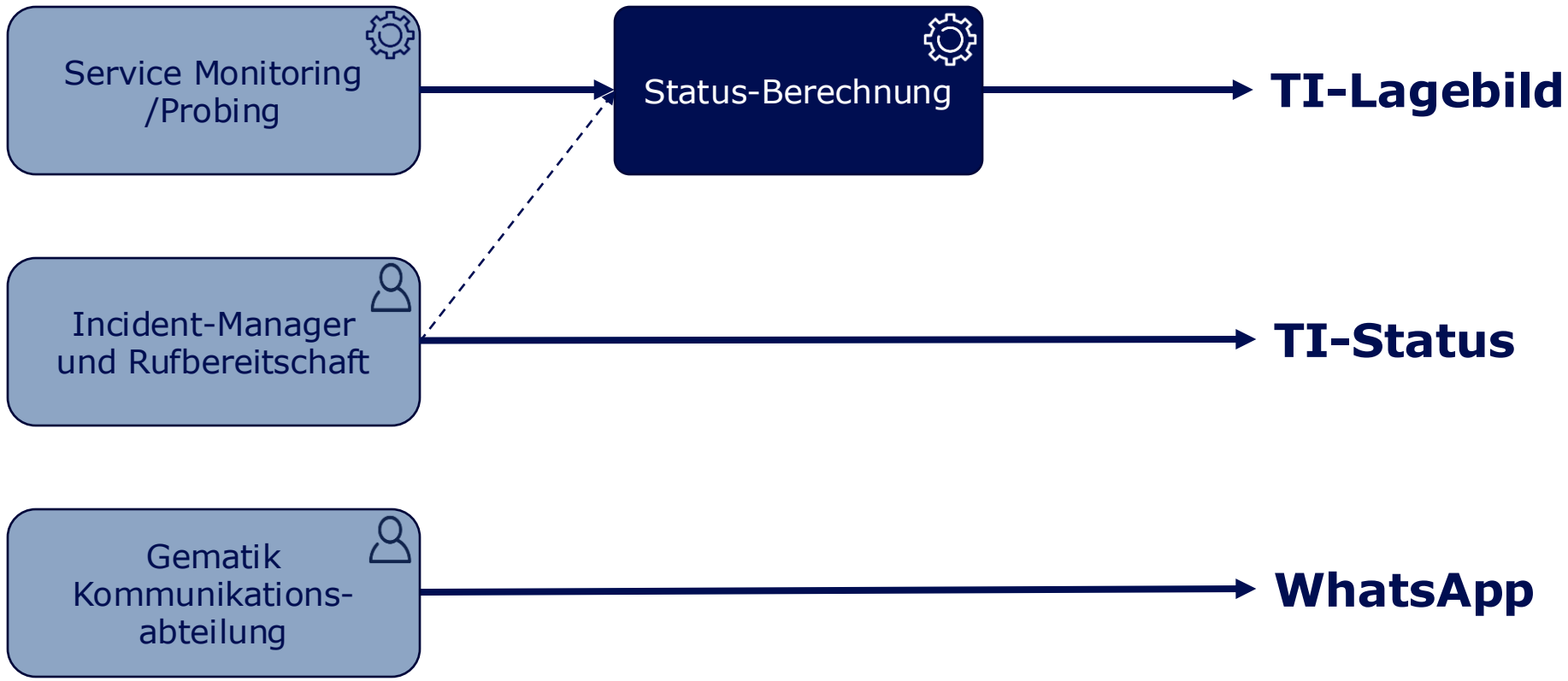
Neuerungen zum Lagebild und zur Störungskommunikation

- ✓ Redesign der TI-Status-Seite für konsistente Störungskommunikation
- ✓ API für TI-Status-Informationen
- ✓ Parametrisierbares Lagebild (API)

Redesign der TI-Status-Seite

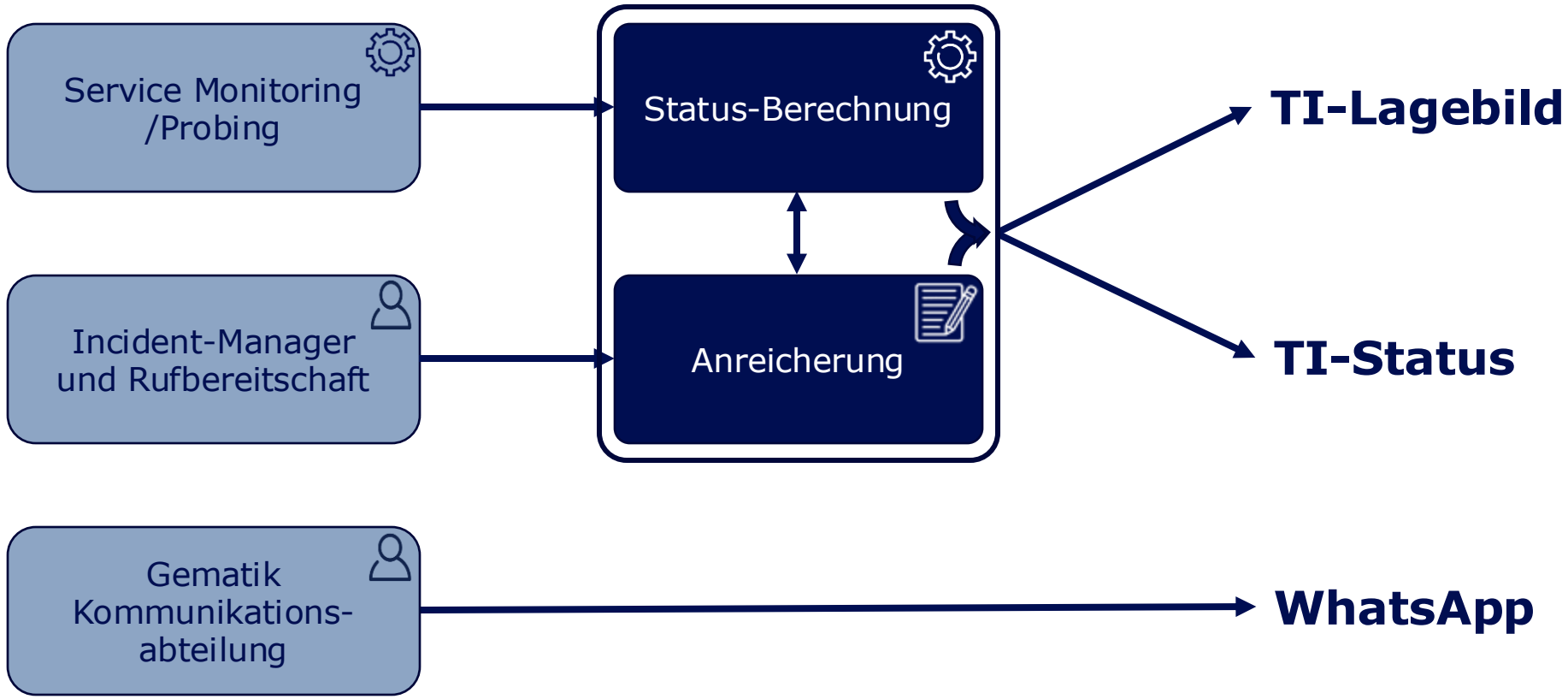
Störungsinformation vorher (bis Ende April 2025)

Probing/Service Map, Lagebild, TI-Status, WhatsApp



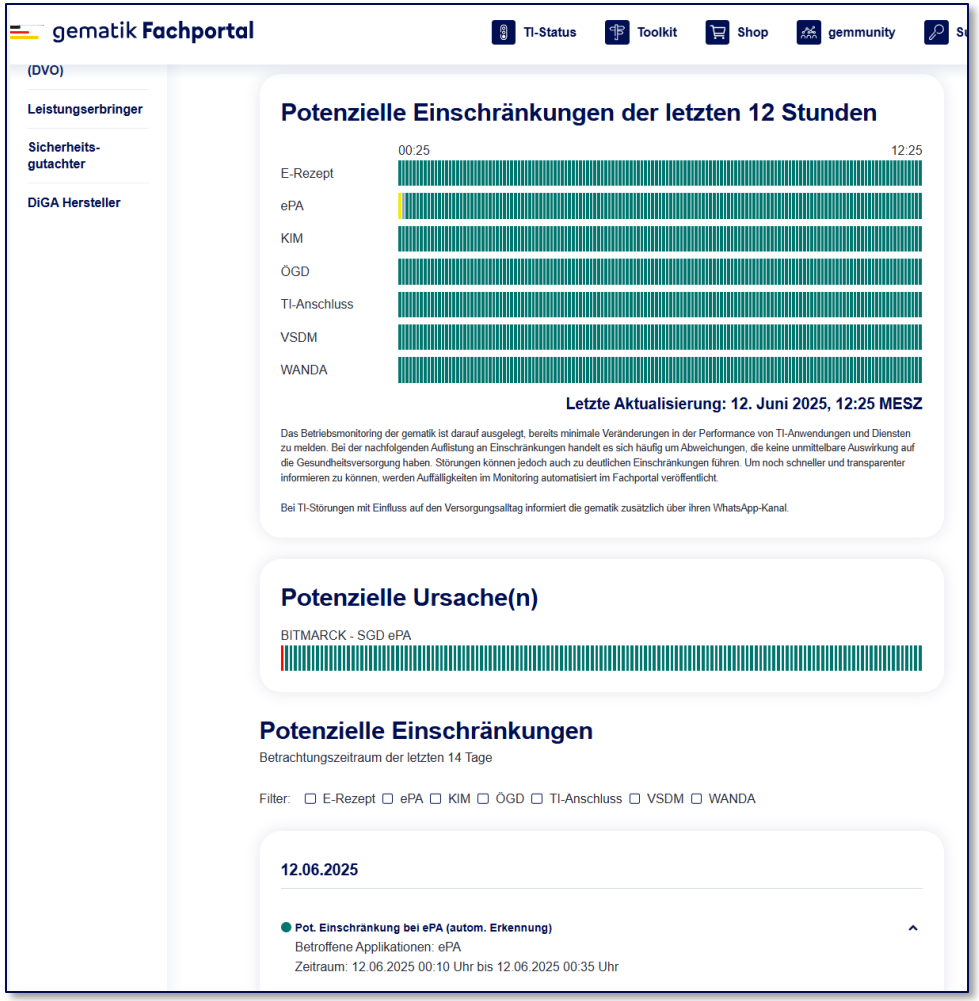
Störungsinformation nachher (ab Mai 2025)

Probing/Service Map, Lagebild, TI-Status, WhatsApp



TI-Status Neuauflage

TI-Status



- Auf TI-Status im Fachportal veröffentlich die gematik alle bekannten Störungen
- Seit Mai 2025 wird dafür die TI-Status-Seite dynamisch aufgebaut und enthält für die bekannten Störungen die Daten aus dem TI-Lagebild der Anwendungen auf Basis der Service Map
- Diese automatisch ausgespielten Meldungen zu Störungen werden bei Bedarf redaktionell ergänzt oder ggf. korrigiert

API für TI-Status-Informationen

TI-Status-Informationen auch via API

Alle Störungsinformationen aus der TI-Status-Seite sind auch via API abrufbar

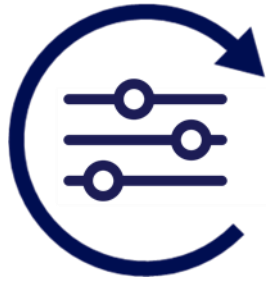
Die Dokumentation zur API ist via GitHub abrufbar

Parametrisierbares Lagebild

Parametrisierbares Lagebild

Über die API kann das Lagebild unter Angabe bekannter lokaler Gegebenheiten aufgerufen werden

Damit werden Störungen ignoriert, die für die lokale Konstellation nicht relevant sind



Mögliche Paramater:

- TI-Zugang (genutzter VPN-Zugangsdienst oder TI-Gateway)
- TSP-SMC-B (genutzter Anbieter zur Validierung der Institutionskarte)
- TSP-HBA (genutzter Anbieter zur Validierung des Heilberufsausweises)
- KIM (genutzter KIM-Dienst-Anbieter)

Nutzung der Rest-API für das parametrisierbare Lagebild

Abruf der möglichen Filterwerte

- Abruf der möglichen Parameter:
  https://ti-lage.prod.ccs.gematik.solutions/lageapi/v2/tilage/filter
- Aus jeder Filtergruppe kann ein CI gewählt werden, was der eigenen lokalen Konfiguration entspricht, z.B. habe ich meine SMC-B bei T-Systems wähle ich CI-0000137


```
[
  {
    "filterGroup": "TSP SMC-B",
    "pdt": "PDT38",
    "prodTypeName": "TSP-X.509nQ-SMC-B",
    "cis": [
      {
        "ci": "CI-0000019",
        "orgShortName": "D-Trust"
      },
      {
        "ci": "CI-0000137",
        "orgShortName": "T-Systems"
      },
      {
        "ci": "CI-0000186",
        "orgShortName": "medisign"
      },
      {
        "ci": "CI-0000192",
        "orgShortName": "Stolle & Heinz"
      }
    ]
  },
  {
    "filterGroup": "TI-Zugang
    ...
  },
  …
]
```

Nutzung der Rest-API für das parametrisierbare Lagebild

Abruf des parametrisierten Lagebilds

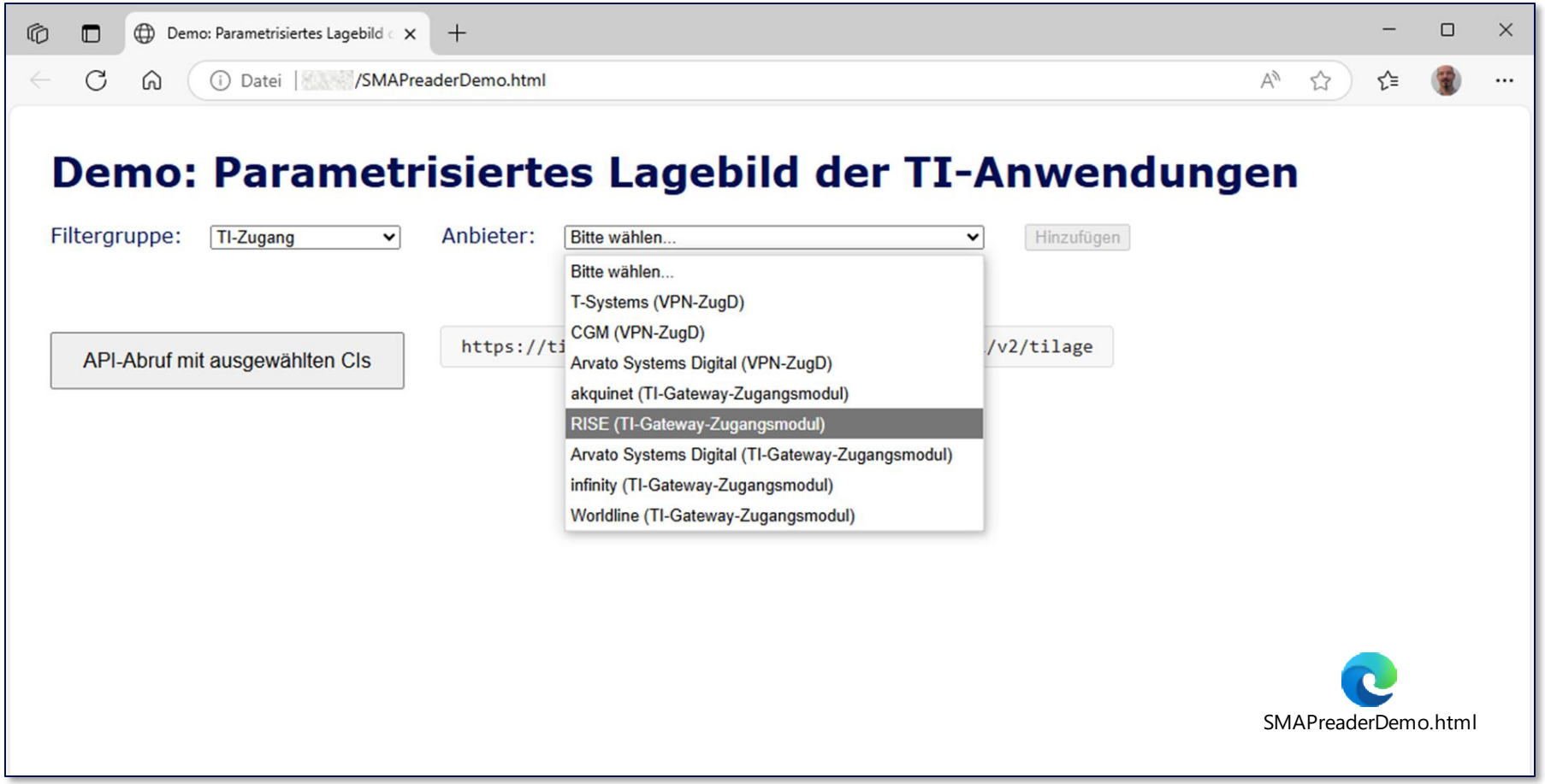
- Abruf des Lagebilds:
  https://ti-lage.prod.ccs.gematik.solutions/lageapi/v2/tilage
- Beim Aufruf können die gewünschten CIs mit folgenden Parametern angegeben werden:
  - ciTspSmcb=<CI-Nummer> für TSP-SMC-B
  - ciAccess=<CI-Nummer> für TI-Zugang
  - ciTspHba =<CI-Nummer> für TSP-HBA
  - ciKim =<CI-Nummer> für KIM

```
{
  "appStatus": {
    "erezept": {
      "outage": "none",
      "hasMaintenance": false,
      "hasSubComponentMaintenance": false,
      "affectedFunctions": []
    },
    ...
  },
  "cause": [
    {
      "ci": ">Betroffenes CI>",
      "component": "*",
      "service": "<betroffener Dienst>",
      "organization": "<Anbieter>",
      "function": "<Betroffene Funktion>"
    }
  ]
}
```

- Beispiel für den parametrisierten Aufruf:
  https://ti-lage.prod.ccs.gematik.solutions/lageapi/v2/tilage?ciTspSmcb=CI-0000137&ciAccess=CI-0000164&ciTspHba=CI-0000146&ciKim=CI-0000409

Lagebild-API für parametrisierten Aufruf

Einfaches Anwendungsbeispiel als Web-Seite mit HTML und JavaScript



We believe that transparency is needed to create trust, and it's also needed to create a dialogue.

(Julie Sweet, American Businesswomen)

Security Monitoring 2.0

Sebastian Labinski (gematik GmbH, Leiter Cyber Defense Center)

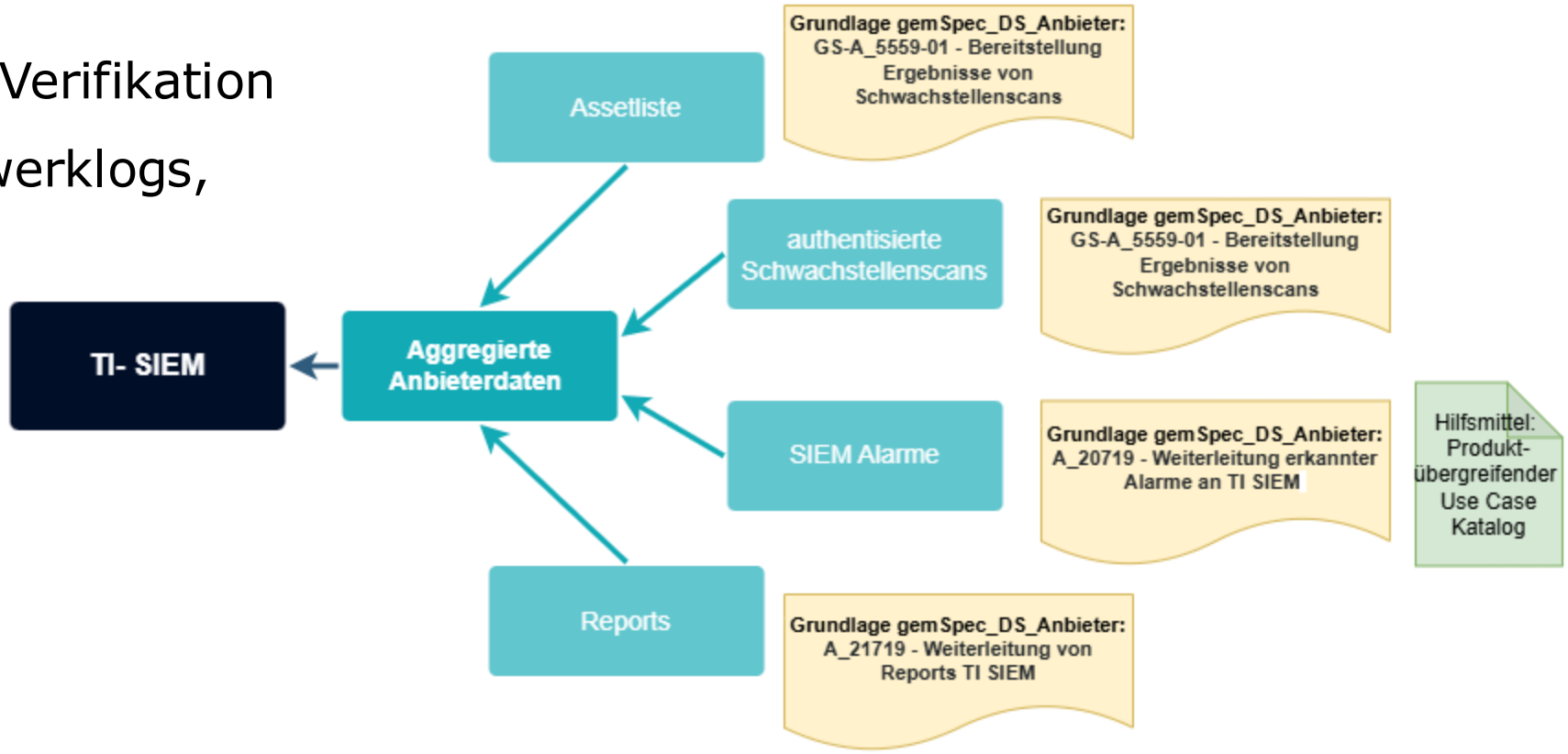
Agenda

- Security Monitoring 1.0
- Der Paradigmenwechsel
- Kurzfristige Maßnahmen
- Langfristige Strategie

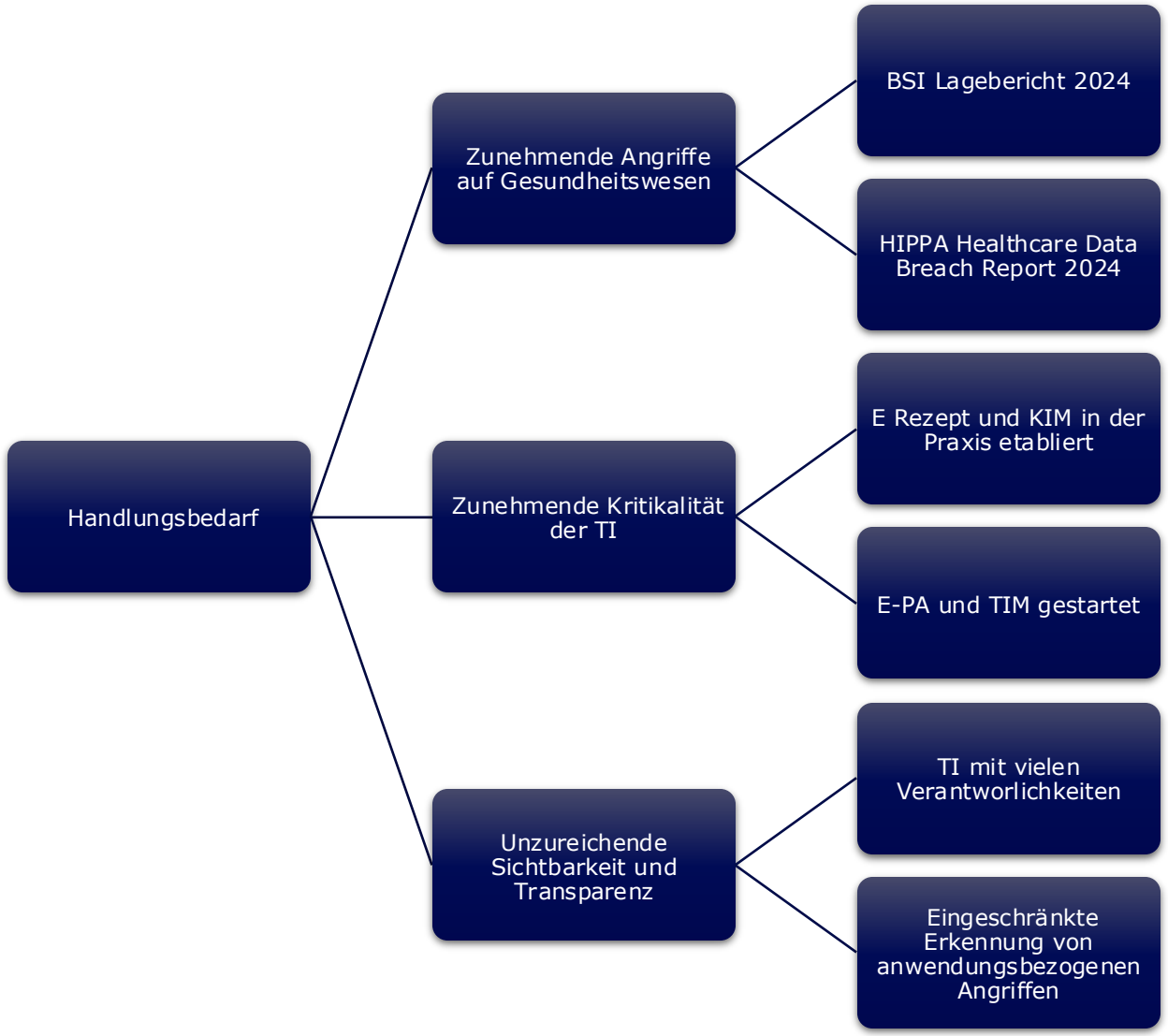
Security Monitoring 1.0

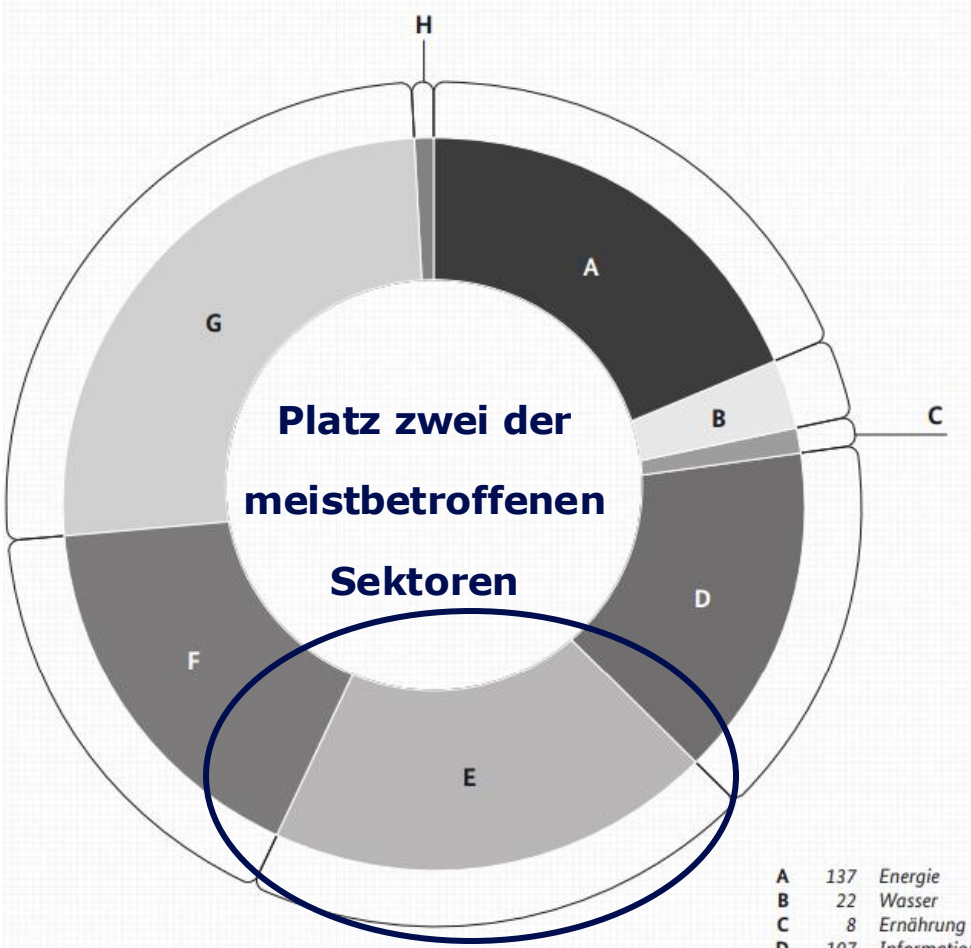
Fokus auf:

- Hoher Eigenverantwortung der Anbieter (Betrieb eigenes SIEM)
- Aggregierten Daten zur Verifikation
- Überwachung von Netzwerklogs, Betriebssystemlogs etc.
- Schwachstellenanalyse



Warum ist ein Paradigmenwechsel erforderlich?





A	137	Energie
B	22	Wasser
C	8	Ernährung
D	107	Informationstechnik und Telekommunikation
E	141	Gesundheit
F	120	Finanz- und Versicherungswesen
G	185	Transport und Verkehr
H	6	Siedlungsabfallentsorgung
	726	**Gesamt**

Abbildung 24: Meldungen nach KRITIS-Sektoren im Berichtszeitraum

Start der ePA für alle

Deutsches Ärzteblatt

Politik

Nach Kritik: Gematik will Sicherheit der elektronischen Patientenakte stärken

Montag, 30. Dezember 2024

30.12.2024

gematik schließt neue Sicherheitslücke der ePA

02.05.2025

Stellungnahme zum CCC-Vortrag zur ePA für alle

https://www.gematik.de/newsroom/news-detail/aktuelles-stellungnahme-zum-ccc-vortrag-zur-epa-fuer-alle

… vor dem bundesweiten Rollout werden weitere technische Lösungen umgesetzt und abgeschlossen sein. Die zusätzlichen Sicherungsmaßnahmen sind bereits in Erarbeitung und haben folgenden Fokus:
Verhinderung, dass Ausweise der Telematikinfrastruktur missbräuchlich verwendet werden können.
Schließung der Sicherheitslücke durch eine zusätzliche Verschlüsselung der Krankenversichertennummer.
Sensibilisierung der Nutzerinnen und Nutzer der Telematikinfrastruktur im Umgang und Schutz der technischen Infrastruktur, Ausweisen und Karten.
Ausweitung der Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung.

Was ist eigentlich eine Anomalie?

Untypisches Verhalten, das Indiz für einen **Angriff** (Abuse Case) einen **technischen Fehler** jedoch auch **unerwartetes Nutzungsverhalten** sein kann.

Detektierte Anomalien in der TI müssen analysiert und bewertet werden
- technischer Fehler
- Angriff
- False Positive / benign Positive

Anwendungsfall basierte Erkennung: Erkennung einer Anomalie im Kontext eines Anwendungsfalls (z.B. Lastverhalten, Antwortzeiten, Fehlerhäufungen) **--> etabliert BDE**

ID basierte Erkennung: Erkennung einer Anomalie im Kontext einer Identität (bzw. seiner Umgebung) **--> kaum etabliert, neuer Fokus**

Wie läuft die Zusammenarbeit?

- **Fokus Anbieter:**
  - hinreichende eigene Anomalieerkennung seiner Dienste
  - Analyse erkannter Anomalien und Einbindung der gematik
  - Unterstützung der Analyse von Anomalien die durch die gematik erkannt wurden
  - Unterstützung Identifikation und Reaktionsprozesse

- **Fokus gematik (Operations)**
  - Anomalieerkennung auf Betriebsdaten, um kritische Betriebszustände rechtzeitig zu erkennen (SIM, Produktteams)

- **Fokus gematik (Sicherheit)**
  - Anomalieerkennungen um sicherheitskritische Zustände zu erkennen (CDC, Produktteams)
  - Vortragsschwerpunkt --> Angriffserkennung

- **Enge Zusammenarbeit** zwischen Operations, Sicherheit und Anbietern bei Detektion, Analyse und Reaktion erforderlich

Was heißt das konkret?

Für die Erkennung von Anomalien, die auf Angriffe aber auch technische Fehlkonfigurationen hindeuten, erkennen zu können, ist es erforderlich Logdaten, die personenbeziehbare Daten wie IP Adressen oder **Nutzer IDs, (TID, Konnektor ID, SMC-B Seriennummern, ICCSN etc.**) enthalten auf Seiten der gematik zu analysieren.

Die Analyse ist auf diese Szenarien beschränkt.

Nutzer IDs werden durch den TI Anbieter vor der Übermittlung (idealerweise in einer VAU) pseudonymisiert und an die gematik übermittelt.

Die **Analyse** erfolgt ebenfalls **auf Grundlage der pseudonymisieren Logdaten**.
Eine De-Pseudonymisierung erfolgt ausschließlich bei erkannten Anomalien und gezielt auf diese Nutzer ID.

Die Umsetzung zum Security Monitoring 2.0 inkl. Verfahren zur Reaktion auf erkannte Anomalien werden in einem **Security Monitoring Konzept** detailliert beschrieben und mit Gesellschaftern, BSI, BfDI abgestimmt.

Auf welcher gesetzlichen Grundlage tut die gematik das?

§ 331 Maßnahmen zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur

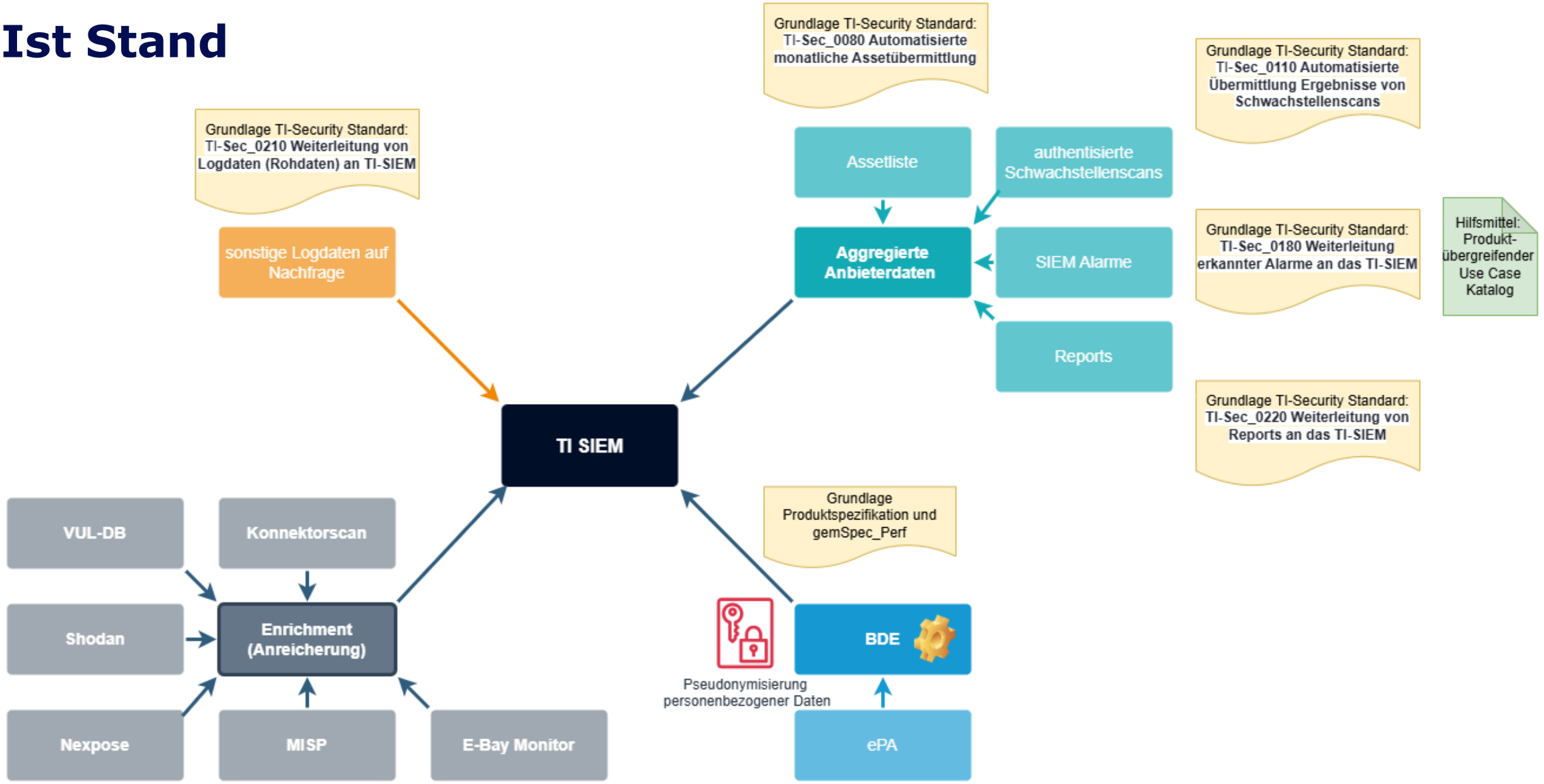
1) Die Gesellschaft für Telematik hat ab dem 1. Januar 2021 für Komponenten und Dienste der Telematikinfrastruktur sowie für Komponenten und Dienste, die die Telematikinfrastruktur nutzen, aber außerhalb der Telematikinfrastruktur betrieben werden, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik solche **Maßnahmen zur Überwachung des Betriebs** zu treffen, die erforderlich sind, um die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu gewährleisten. Die Gesellschaft für Telematik kann zur Erfüllung ihrer Aufgaben nach Satz 1 die entsprechenden Komponenten und Dienste untersuchen.

(2) Die Gesellschaft für Telematik legt fest, welche näheren Angaben ihr die Anbieter der Komponenten und Dienste offenzulegen haben, damit die Überwachung nach Absatz 1 durchgeführt werden kann.

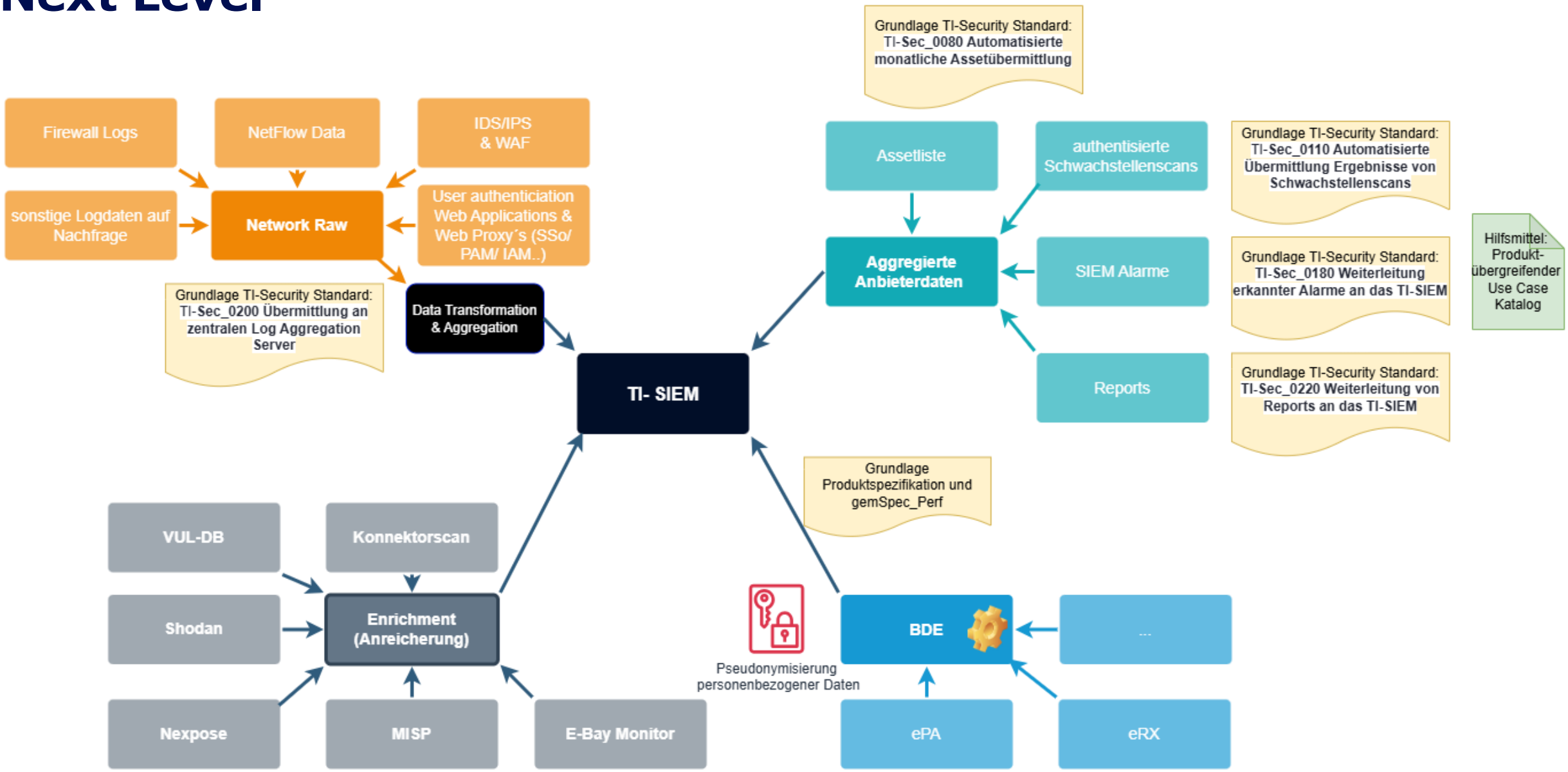
(3) Die Verpflichtung der Gesellschaft für Telematik nach § 330 Absatz 1 Satz 1, zur Vermeidung von Störungen angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst auch den **Einsatz von geeigneten Systemen zur Erkennung von Störungen und Angriffen**. Der Einsatz der Systeme erfolgt im Benehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik.

(4) Die Gesellschaft für Telematik darf die für den Einsatz der Systeme nach Absatz 3 erforderlichen Daten, **einschließlich personenbezogener Daten**, verarbeiten. Die im Rahmen des Einsatzes dieser Systeme verarbeiteten Daten sind unverzüglich zu löschen, wenn sie für die Vermeidung von Störungen nach § 330 Absatz 1 Satz 1 nicht mehr erforderlich sind, spätestens jedoch nach zehn Jahren.

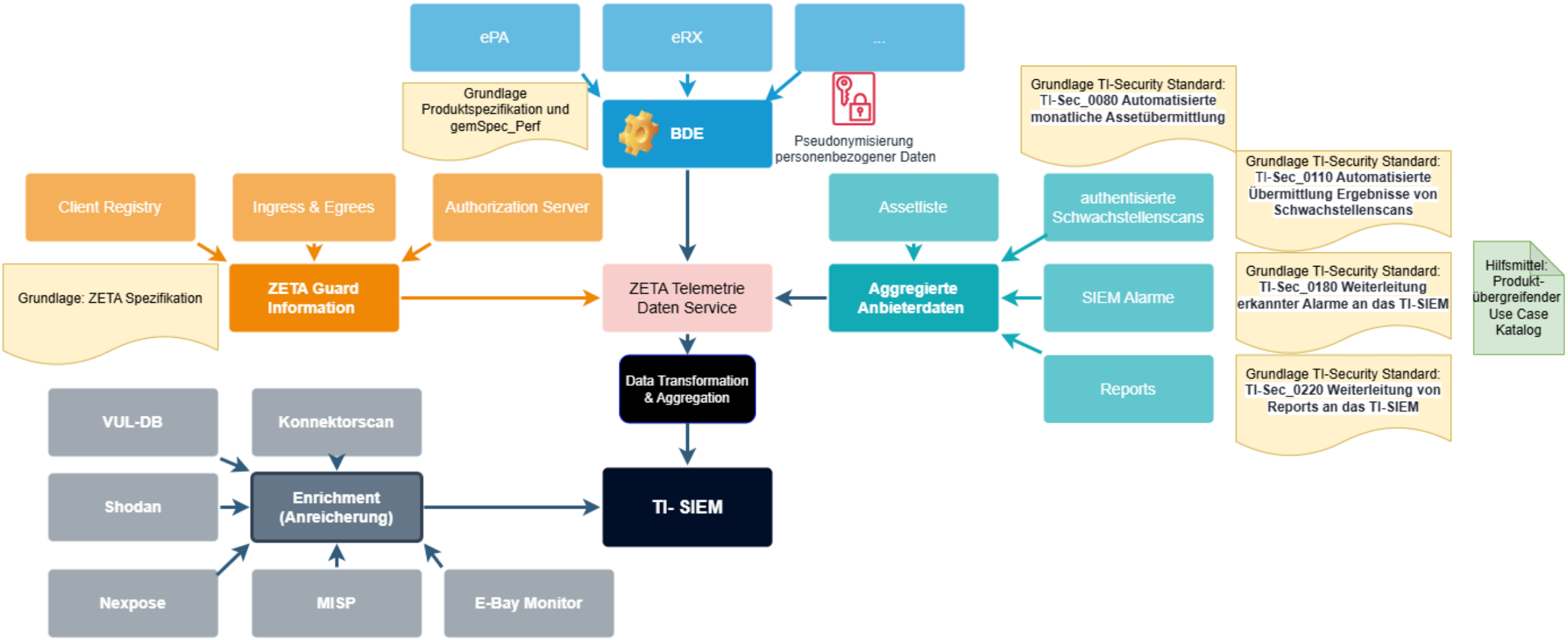
Ist Stand

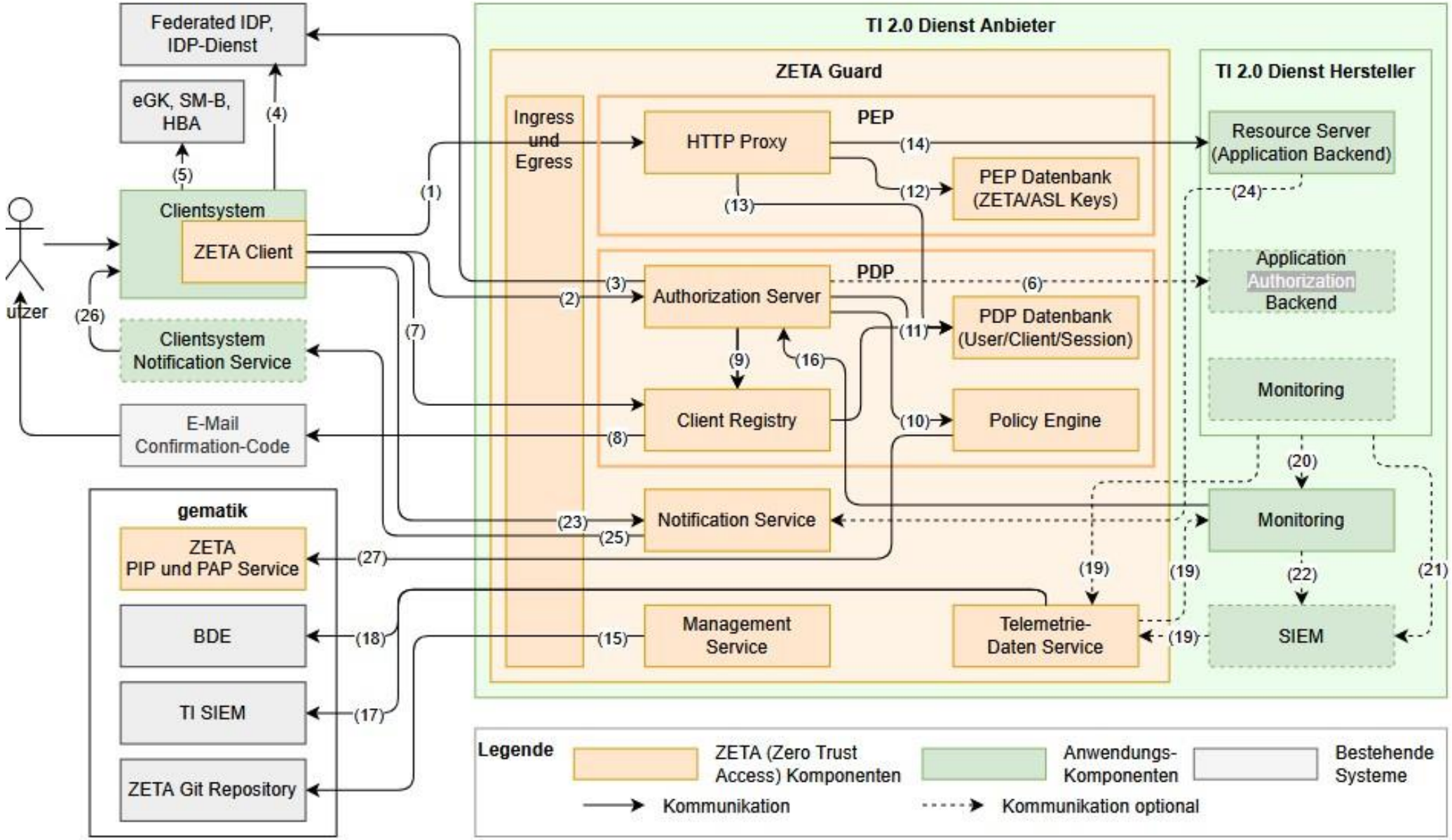

Grundlage TI-Security Standard: TI-Sec_0080 Automatisierte monatliche Assetübermittlung
Grundlage TI-Security Standard: TI-Sec_0110 Automatisierte Übermittlung Ergebnisse von Schwachstellenscans
Grundlage TI-Security Standard: TI-Sec_0210 Weiterleitung von Logdaten (Rohdaten) an TI-SIEM
Assetliste
authentisierte Schwachstellenscans
sonstige Logdaten auf Nachfrage
Aggregierte Anbieterdaten
SIEM Alarme
Grundlage TI-Security Standard: TI-Sec_0180 Weiterleitung erkannter Alarme an das TI-SIEM
Hilfsmittel: Produkt-übergreifender Use Case Katalog
Reports
Grundlage TI-Security Standard: TI-Sec_0220 Weiterleitung von Reports an das TI-SIEM
TI SIEM
Grundlage Produktspezifikation und gemSpec_Perf
VUL-DB
Konnektorscan
Shodan
Enrichment (Anreicherung)
BDE
Pseudonymisierung personenbezogener Daten
Nexpose
MISP
E-Bay Monitor
ePA

Next Level


Grundlage TI-Security Standard: TI-Sec_0080 Automatisierte monatliche Assetübermittlung
Firewall Logs
NetFlow Data
IDS/IPS & WAF
Assetliste
authentisierte Schwachstellenscans
Grundlage TI-Security Standard: TI-Sec_0110 Automatisierte Übermittlung Ergebnisse von Schwachstellenscans
sonstige Logdaten auf Nachfrage
Network Raw
User authenticiation Web Applications & Web Proxy´s (SSo/ PAM/ IAM..)
Aggregierte Anbieterdaten
SIEM Alarme
Grundlage TI-Security Standard: TI-Sec_0180 Weiterleitung erkannter Alarme an das TI-SIEM
Hilfsmittel: Produkt-übergreifender Use Case Katalog
Grundlage TI-Security Standard: TI-Sec_0200 Übermittlung an zentralen Log Aggregation Server
Data Transformation & Aggregation
TI- SIEM
Reports
Grundlage TI-Security Standard: TI-Sec_0220 Weiterleitung von Reports an das TI-SIEM
Grundlage Produktspezifikation und gemSpec_Perf
VUL-DB
Konnektorscan
Shodan
Enrichment (Anreicherung)
Pseudonymisierung personenbezogener Daten
BDE
...
Nexpose
MISP
E-Bay Monitor
ePA
eRX

Next Level mit ZETA





https://gemspec.gematik.de/downloads/gemSpec/gemSpec_Zero_Trust/gemSpec_Zero_Trust_V1.0.0_CC.html

Fazit

Anbieter bleiben weiterhin verpflichtet, den sicheren Betrieb ihrer Produkte zu gewährleisten

Um die Sicherheit aber auch Stabilität der Telematikinfrastruktur zu gewährleisten, ist eine anbieterübergreifende Anomalieerkennung erforderlich

- Qualitätssicherung
- 4 Augen Prinzip
- Anbieterübergreifende Korrelation

Details der Umsetzung werden in einem Security Monitoring Konzept beschrieben und mit den relevanten Stakeholdern abgestimmt

Gegenseitiges Vertrauen ist essentiell – Es geht nur gemeinsam!

Gemeinsam für einen stabilen und sicheren TI Betrieb

Sebastian Labinski – Leiter Cyber Defense Center