Total IT-Security

Methodik und Architektur zur Absicherung moderner IT-Infrastrukturen

Thomas J. Wilke, mailto@tjw.li

Gliederung

- Begriffe
- Ausgangssituation
- Ziele / Problemstellungen
- Strategien / Methodik
- Architektur
- Zusammenfassung / Ausblick

Begriffe

Sicherheit

Sicherheit ist ein Maß für die Schutzbedürftigkeit von Objekten oder Subjekten in einem definierten Umfeld.
Die Schutzbedürftigkeit korreliert mit der (wirtschaftlichen) Bedeutung, die dem Objekt oder Subjekt im jeweiligen Umfeld zugeschrieben wird.

- Total IT-Security

  Methodik und Architektur zur ganzheitlichen (totalen) technischen Durchsetzung von Regelwerken in Systemen, die eine hohe Heterogenität und Funktionsvernetzung aufweisen.

Begriffe

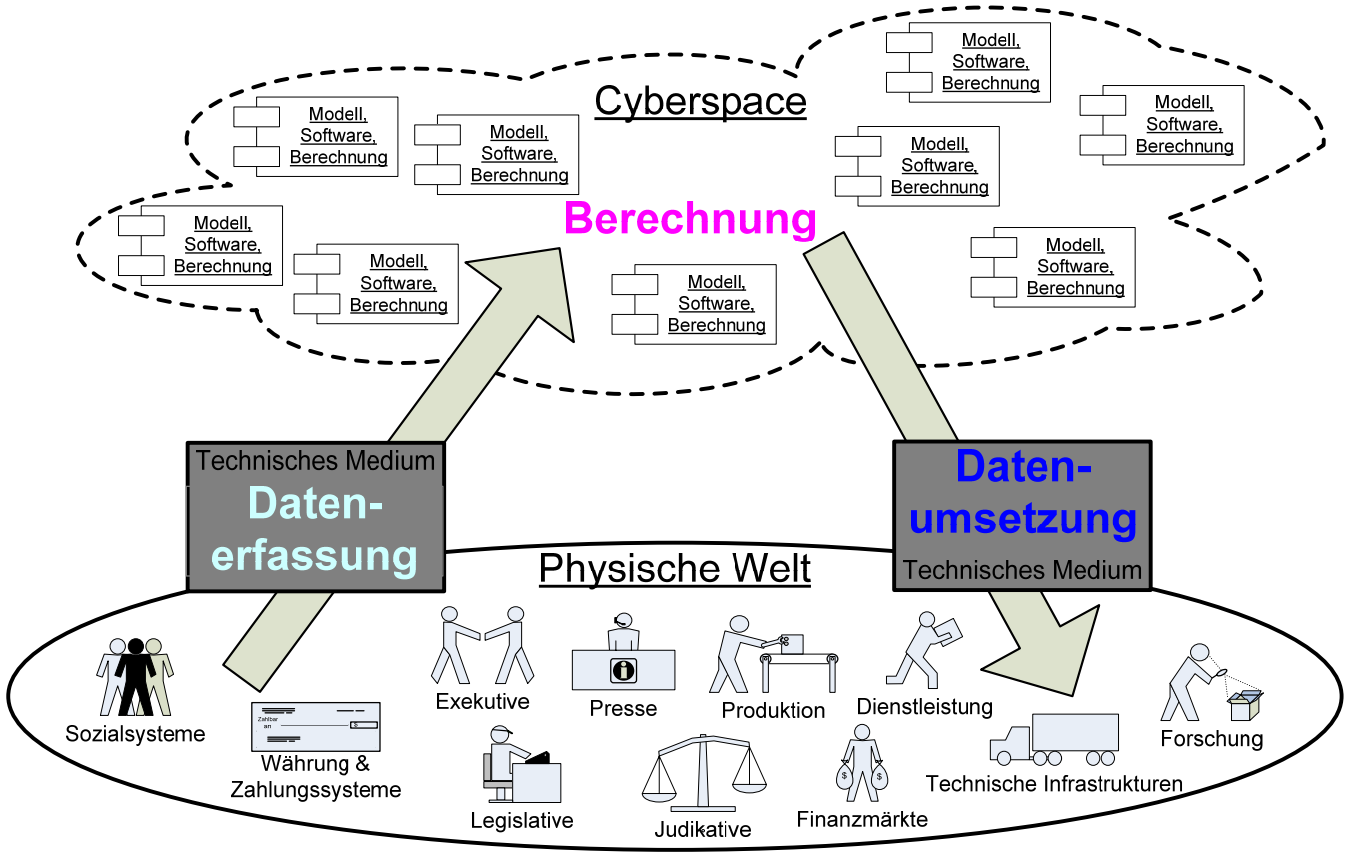
- Offene Systeme

  Systeme, deren Funktionalität im regulären Betrieb aufgrund ihrer Architektur prinzipiell verändert werden kann.

- IT-Infrastruktur

  Eine IT-Infrastruktur ist eine Menge von Subjekten und Objekten, die im Zusammenhang mit der technischen Darstellung und Verarbeitung von Daten steht und die der hoheitlichen Verantwortung einer (natürlichen oder juristischen) Person zugeordnet ist.

Ausgangssituation: Cyberspace & physische Welt



Ausgangssituation: technische Aspekte

- Etablierte und akzeptierte technische Systeme
- Hohe Heterogenität der technischen Strukturen
- Unterschiedliche Wirkebenen und hohe Funktionsvernetzung
- Offene Systeme zur Verarbeitung sicherheitsrelevanter Funktionalität
- Sicherungsmechanismen mit sehr begrenztem Sicherungsfokus, die isoliert voneinander wirken.

Ausgangssituation: organisatorische Aspekte

- Mangelnde Festlegung und Formalisierung von Organisations- und Kompetenzstrukturen
- Mangelnde Sicherheitsregelwerke und Risikovorsorge
- Zu erfüllende ökonomische und gesetzliche Vorgaben
- Outsourcing
- Geringe Transparenz der technischen Gegebenheiten

Ausgangssituation: Stand der Wissenschaft

- Hochentwickeltes Wissen in spezifischen Sicherungsdisziplinen für z.B. Kommunikationsabsicherung, Maleware, Kryptografie, Verfügbarkeit, Korrektheit von Software, DRM, …
- Dominanz präventiv wirkender Sicherungsverfahren
- Isoliert wirkende Sicherungsverfahren
- Primär technisches oder organisatorisch orientiertes Problemverständnis
- Geringes Wissen über Methodik zum Design und der technischen Durchsetzung von Regelwerken in funktionsvernetzten Systemen

Ausgangssituation: Angriffe

- Sehr breites Spektrum an Angriffsmotivation
- Unterschiedliches Technikverständnis der Systemhersteller, -betreiber, Nutzer und Angreifer
- Unzureichende Überdeckung von Schutzwirkung und Gefährdungslage
- Technisch komplexe Angriffe:
  Attackiertes Ziel ≠ Wirkungsziel der Attacke
- Kombinierte Angriffe: Social Engineering

Ziele

- Optimierung existierender und/oder Etablierung neuartiger Geschäftsprozesse zur Effizienzsteigerung und/oder Wertsteigerung des Betriebs
- Funktionale Flexibilität, um auf marktwirtschaftliche und gesetzliche Veränderungen angemessen reagieren zu können
- Kosten/Nutzen Maximierung des IT-Betriebs.
- Wahrung der Betriebssicherheit beim Einsatz von IT-Systemen

Anforderungen

- Schutz von Werten innerhalb der IT-Systeme
- Verankerung von Mechanismen in IT-Systemen zur Wahrung wirtschaftlicher & gesetzlicher Regeln
- „Skalierbare“ Sicherheit, mit der Schutzwirkung und Gefährdungslage in Übereinstimmung gebracht werden können
- Wirkungsverzahnte Sicherungsverfahren, die Prävention, Erkennung und Reaktion auf verschiedenen Wirkebenen realisieren

Problemstellungen

- Homogene Durchsetzung von Sicherheitsregelwerken innerhalb der IT-Systeme
- Verbindliche Nachvollziehbarkeit der Vorgänge innerhalb der IT-Systeme
- Direkte Durchsetzung der organisatorischen Kompetenzstrukturen innerhalb der IT-Systeme
- Fortgeschrittener Datenschutz
- Erkennung und Behandlung von unbekannten Bedrohungssituationen

Strategien

Komplexitätsreduzierung

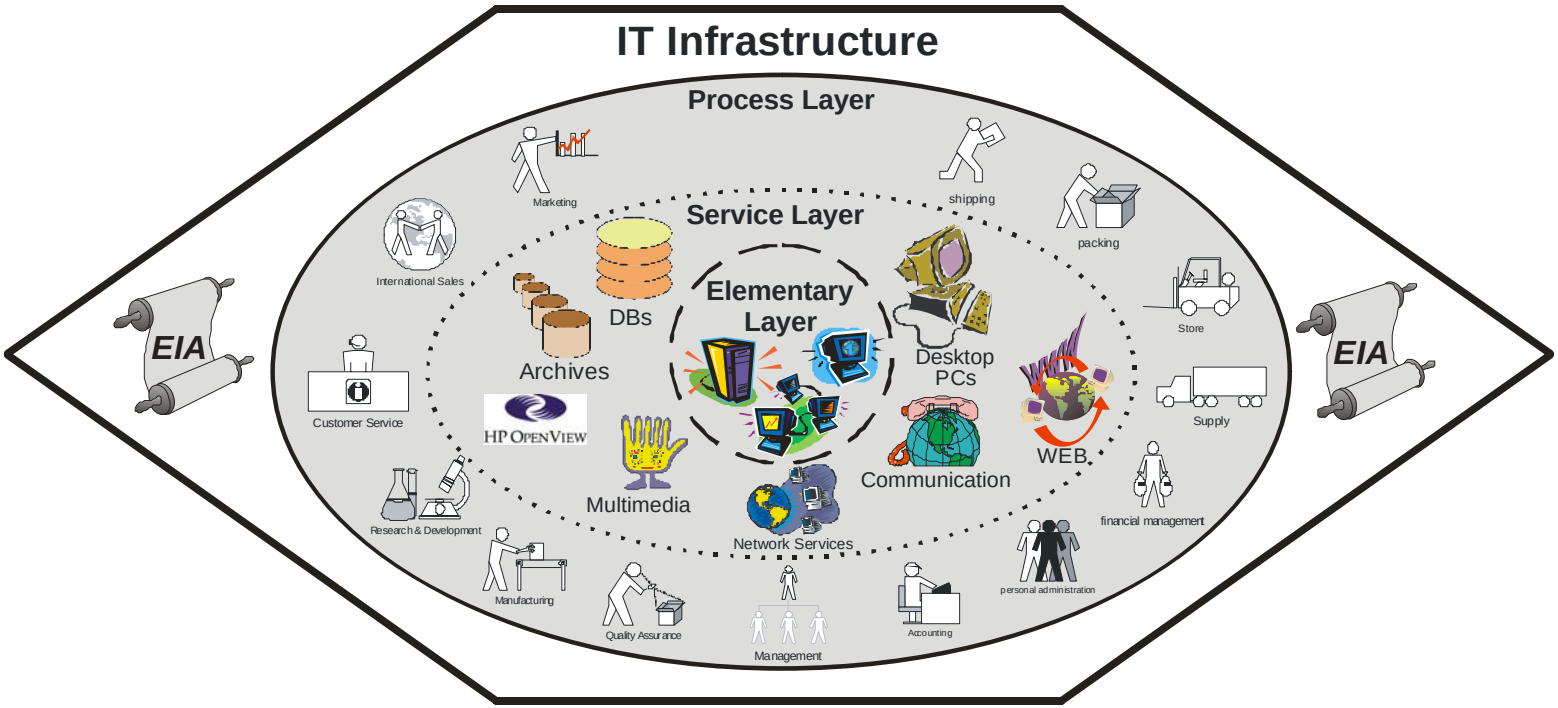
- Identifizierbarkeit der Elemente einer IT-Infrastruktur
- Funktionale Isolierbarkeit der Elemente einer IT-Infrastruktur
- Strategische Informationsverteilung

Methodik: Wirkebenenmodell

Process Layer
Process description with workflows and roles

Service Layer
Desription of Services: Dektop Pcs, DB, DNS, Mail, WEB, HP OV...

Elementary Layer
Description of Hardware Elements



Methodik: Komplexitätsreduzierung

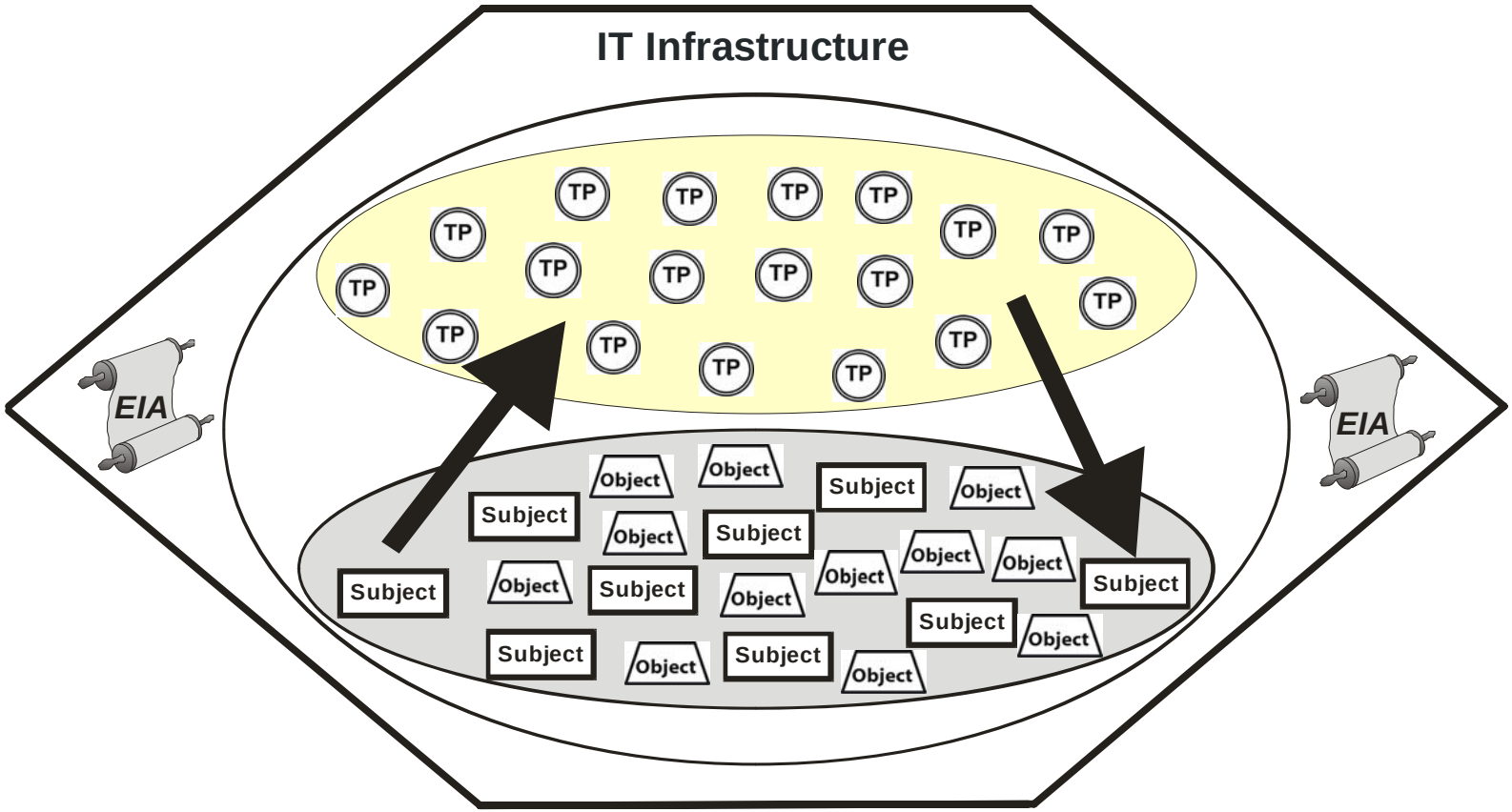
- Wirkverbindliche Elemente mit beschränkter Funktionskomplexität
- Beschränkung der möglichen auf die benötigten Interaktionen und Funktionen von Elementen
- Einheitliche Terminologie der Sicherheitsklassifikation, Rechte und Elementidentifikation (Common Terms)

Methodik: Elementidentifizierbarkeit

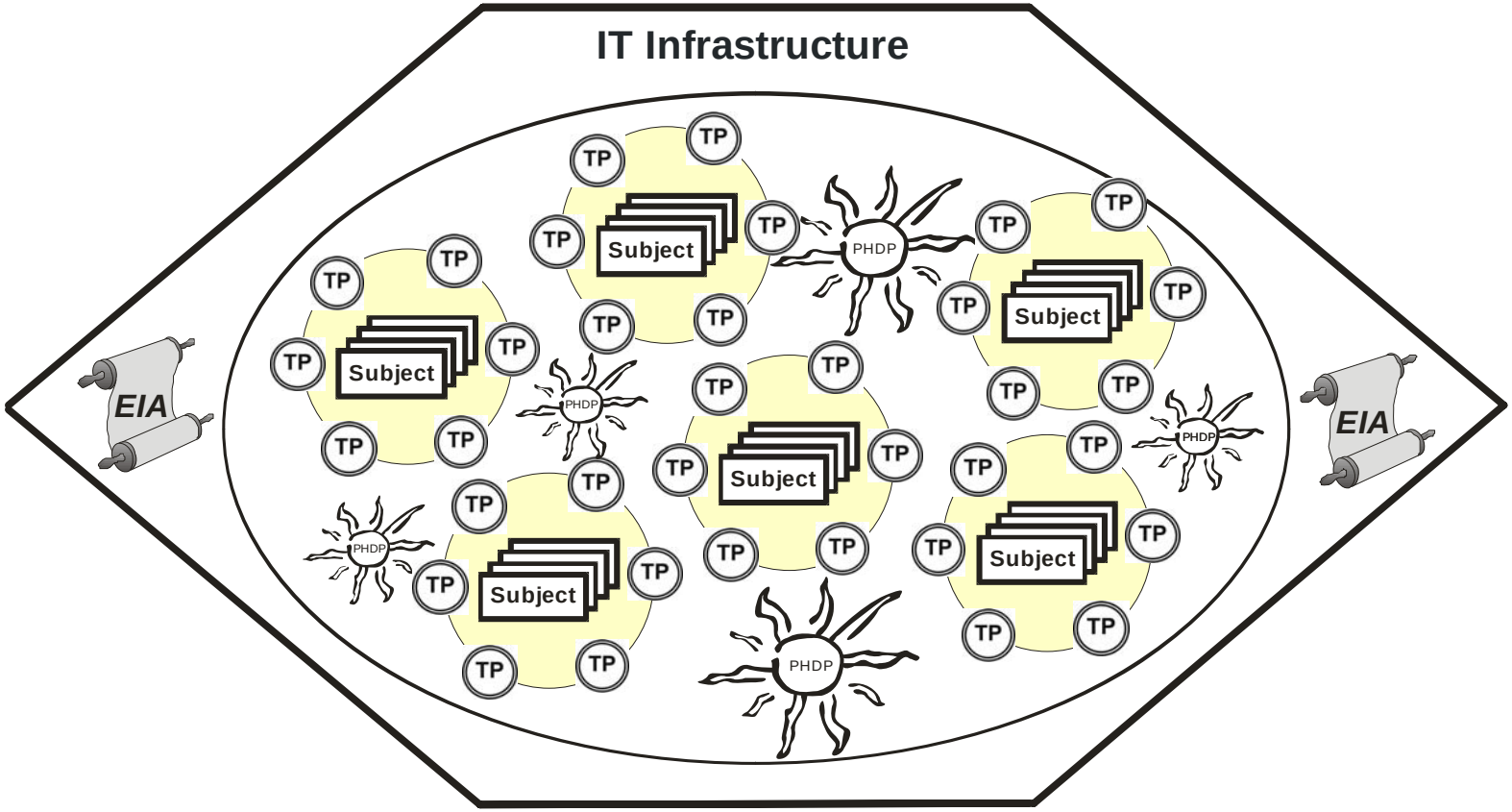
- Zentral organisierte Registrierung und Kennzeichnung
  aller Subjekte und
  technisch wirkungsrelevanter Objekte

- Dezentrale Objektkennzeichnung und Vorgangsregistrierung

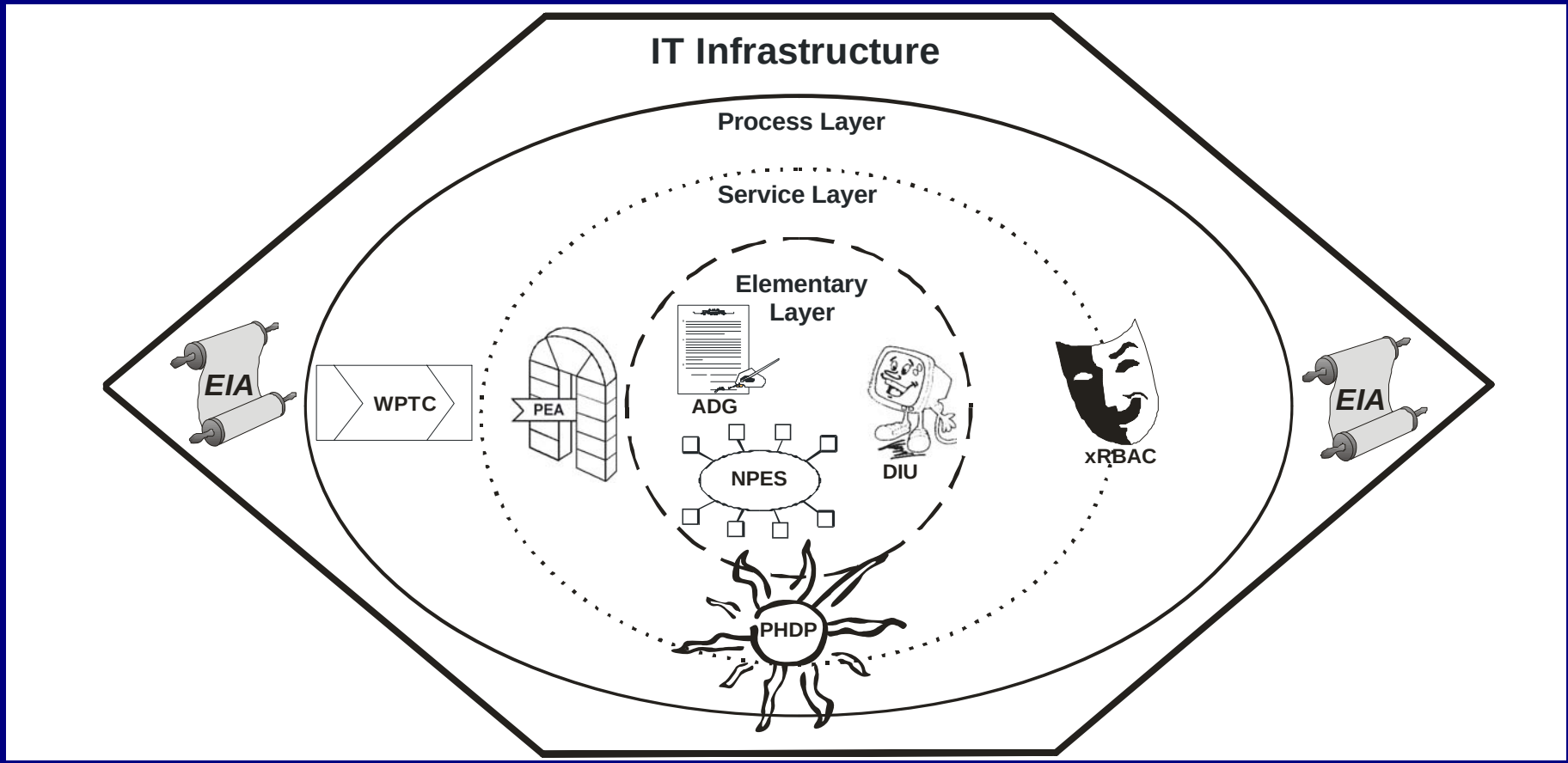
Architektur: Wirkungsprinzip



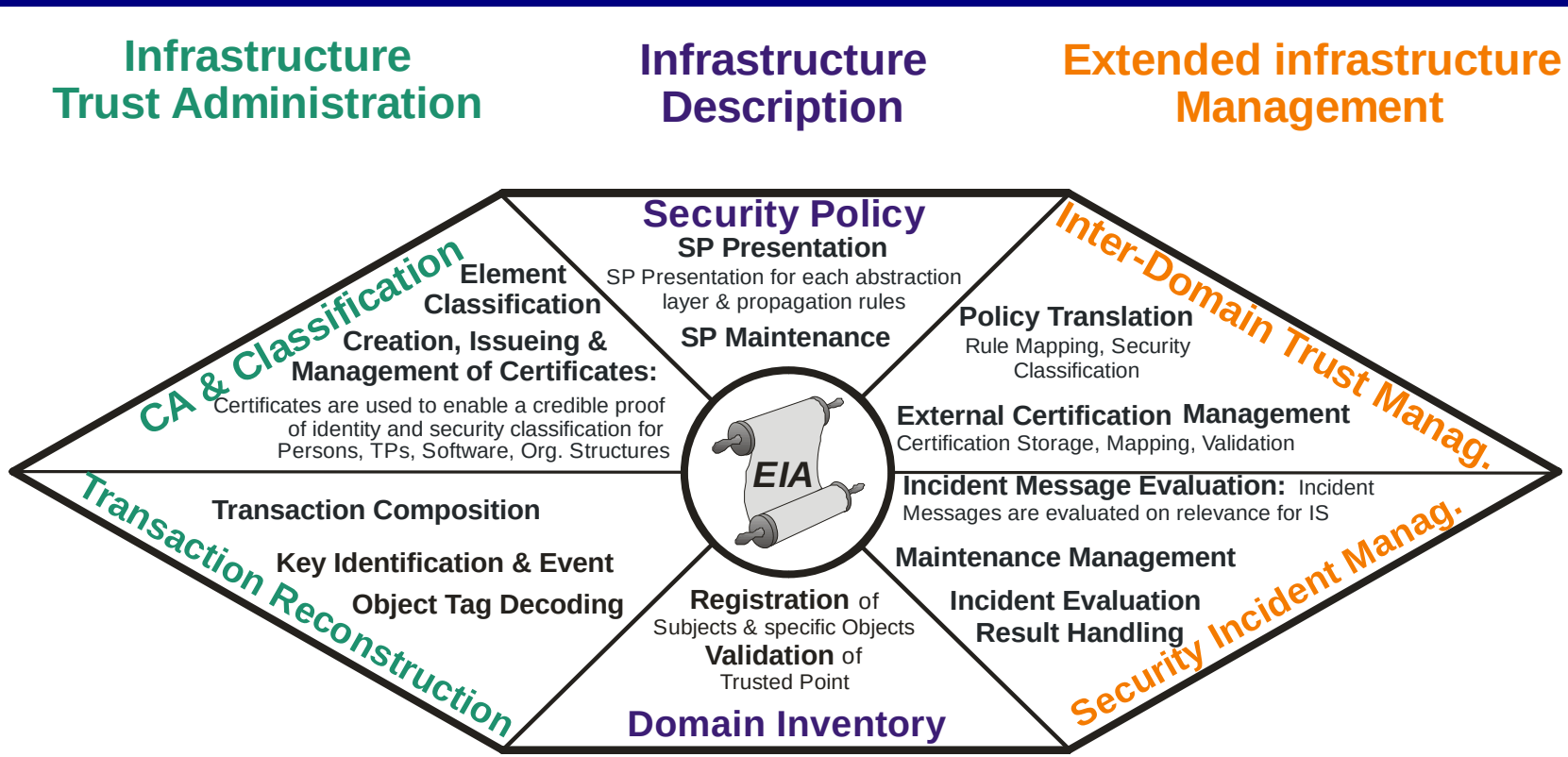
Methodik: Wirkungsisolierung



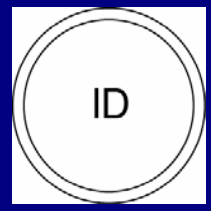
Architektur: Übersicht



Architektur: Element Identification Authority



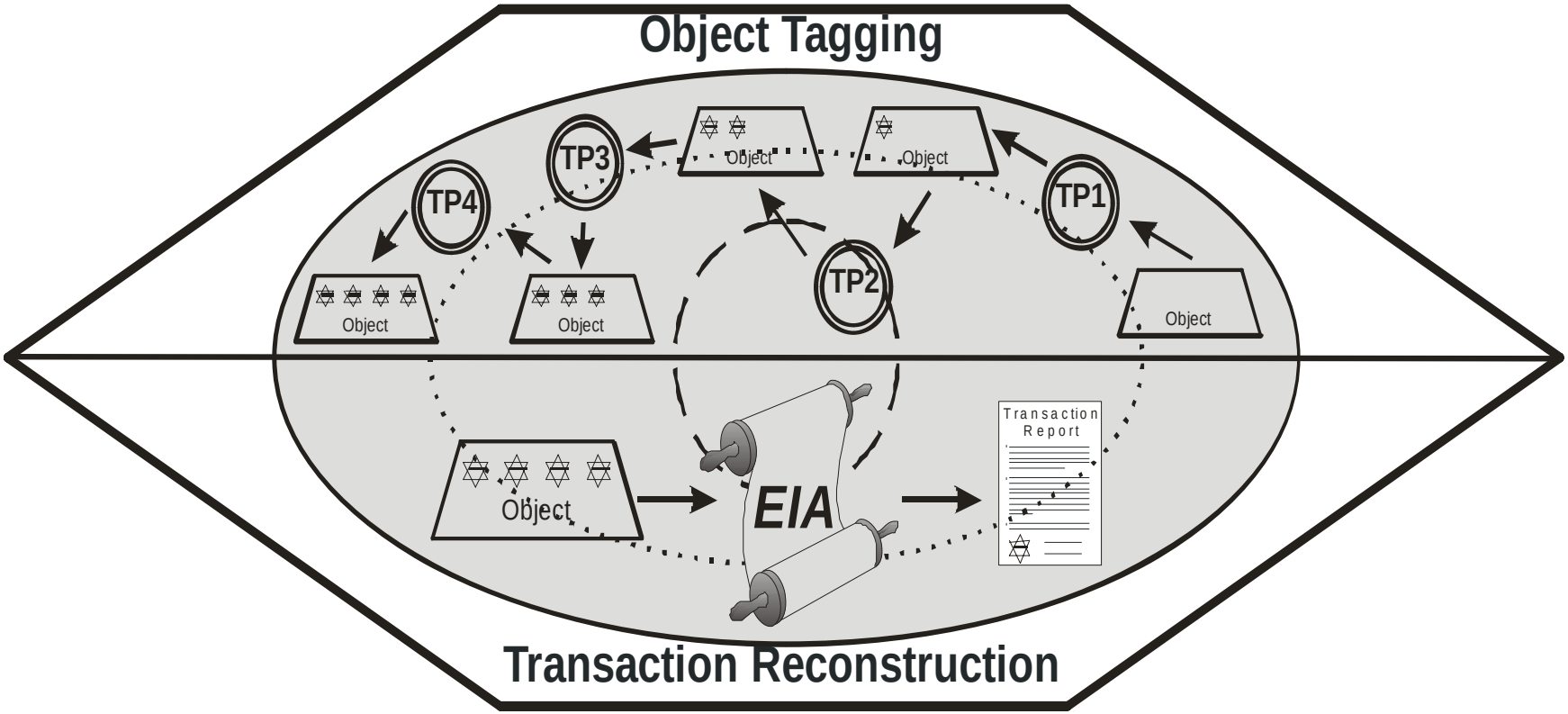
Wirkverbindliche Elemente (TPs)



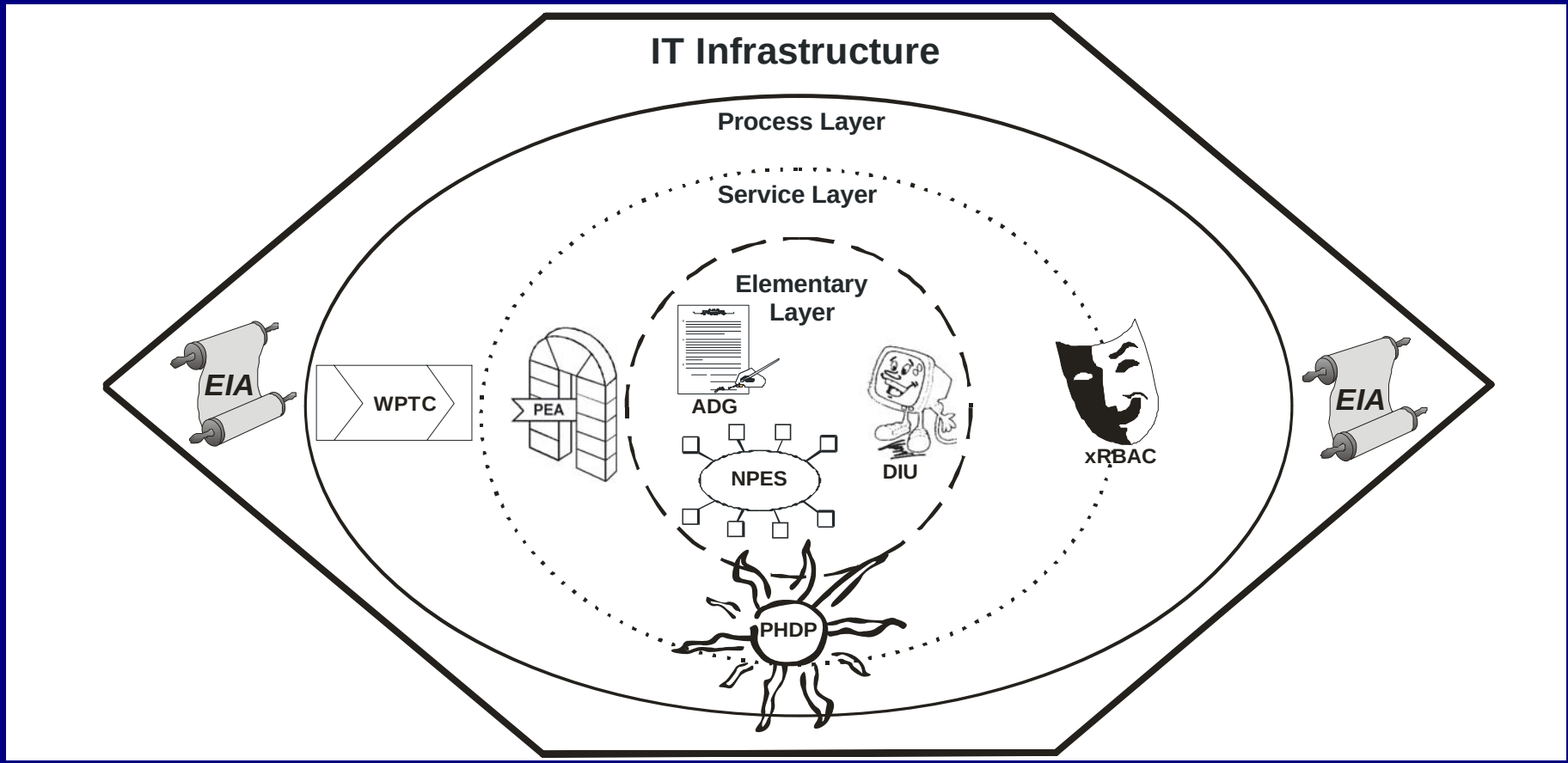
Wirkverbindliche Elemente sind Subjekte, die eine beschränkte, wohldefinierte und verifizierte Funktionalität verlässlich bereitstellen.
Sollte ihre funktionale Integrität nicht mehr gegeben sein, so stellen diese Elemente ihren Betrieb ein und zeigen ihre Kompromittierung für ihre Umgebung erkennbar an.

Sie sind vorzugsweise als geschlossene, dedizierte Systeme technisch realisiert.

Wirkverbindliche Elemente: Object Tagging



Architektur: Sicherungsverfahren, ADG

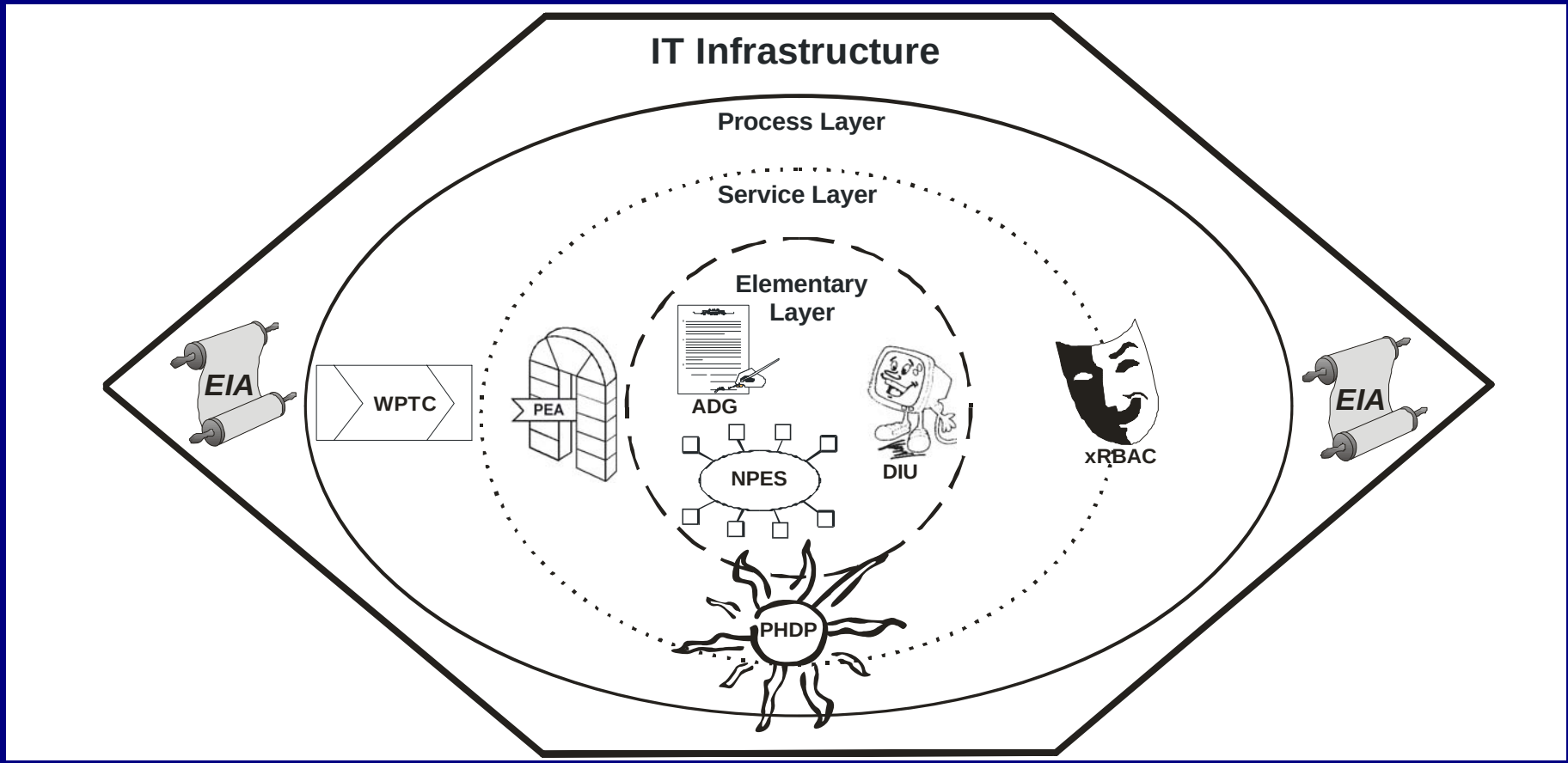


Architektur: ADG / ADD

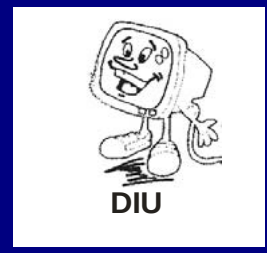
Authentisches Datenerfassungsgerät

- Authentische Darstellung von Daten zur Verifikation durch Personen
- Verbindliche digitale Signierung von Datendarstellungen
- Verbindliche Versendung von signierten Dokumenten

Architektur: Sicherungsverfahren, DIU



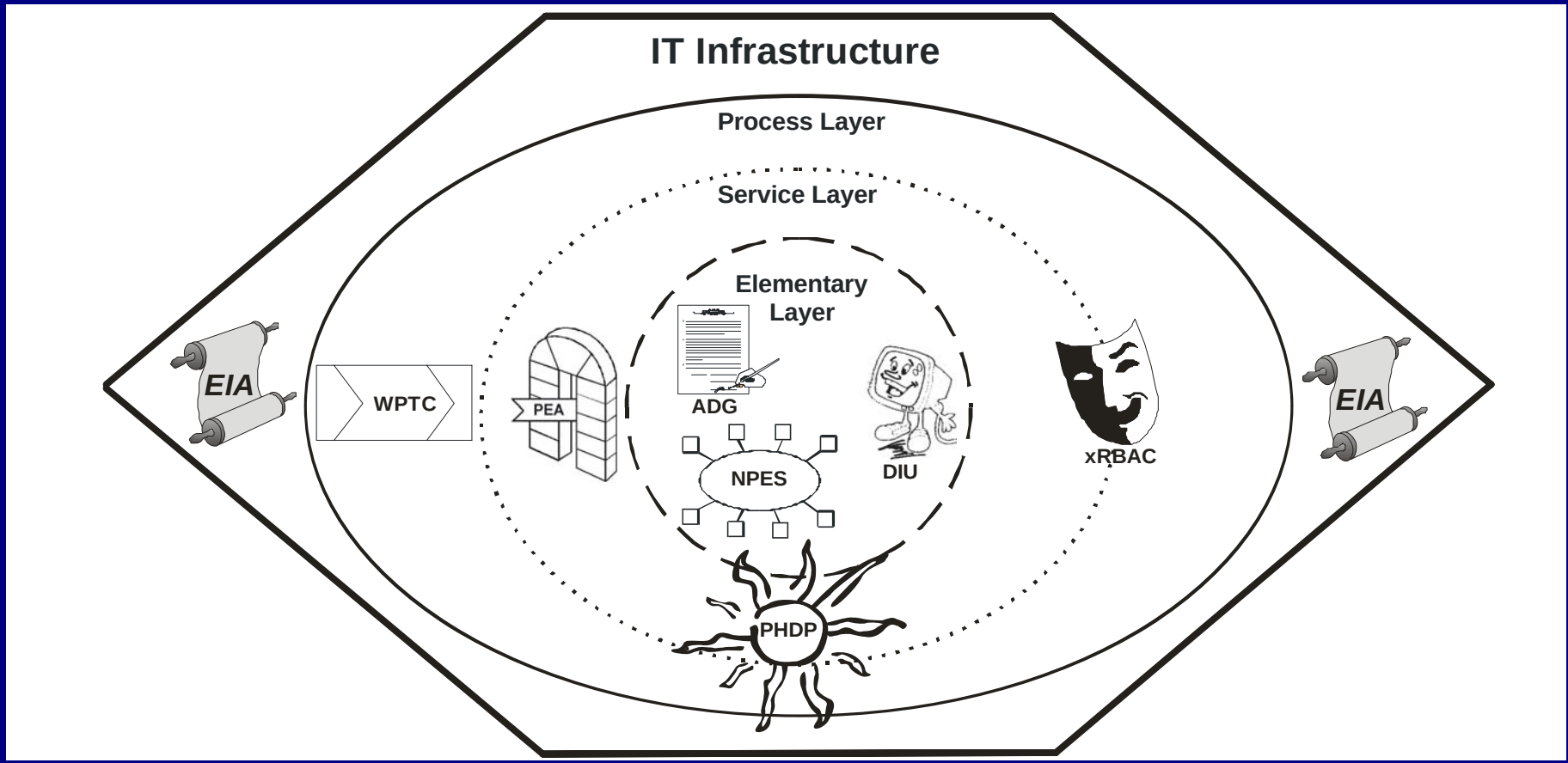
Architektur: DIU



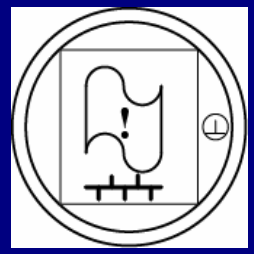
Device Identification Unit

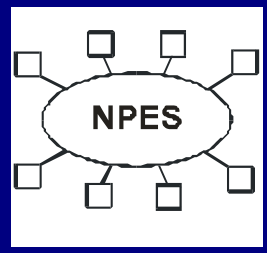
- Wirkungsverbindliche Identifikation von offenen Rechnersystemen
- Erkennung und Wahrung der Daten- und Systemintegrität offener Rechnersysteme

Architektur: Sicherungsverfahren, NPES



Architektur: NPES

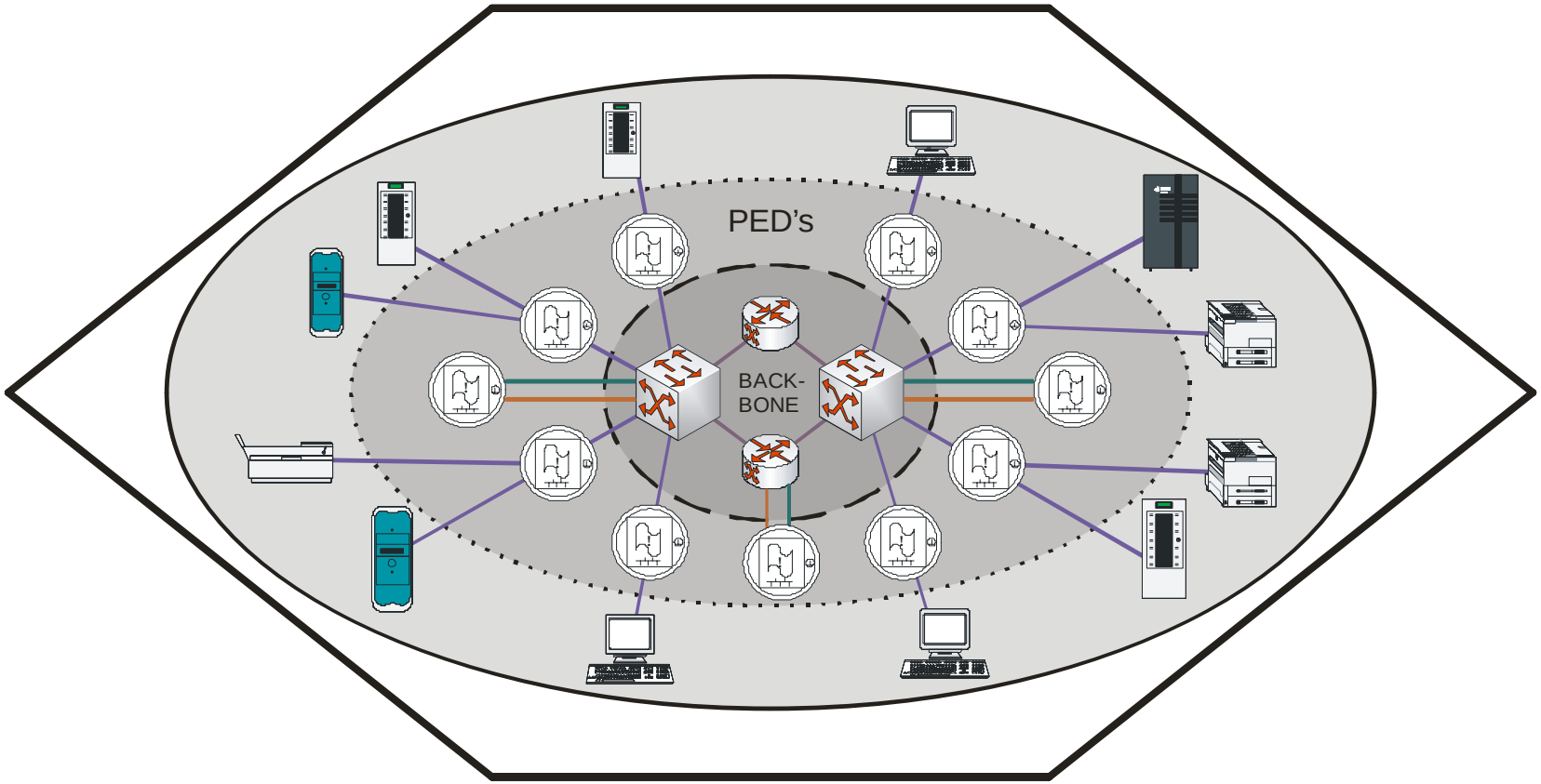




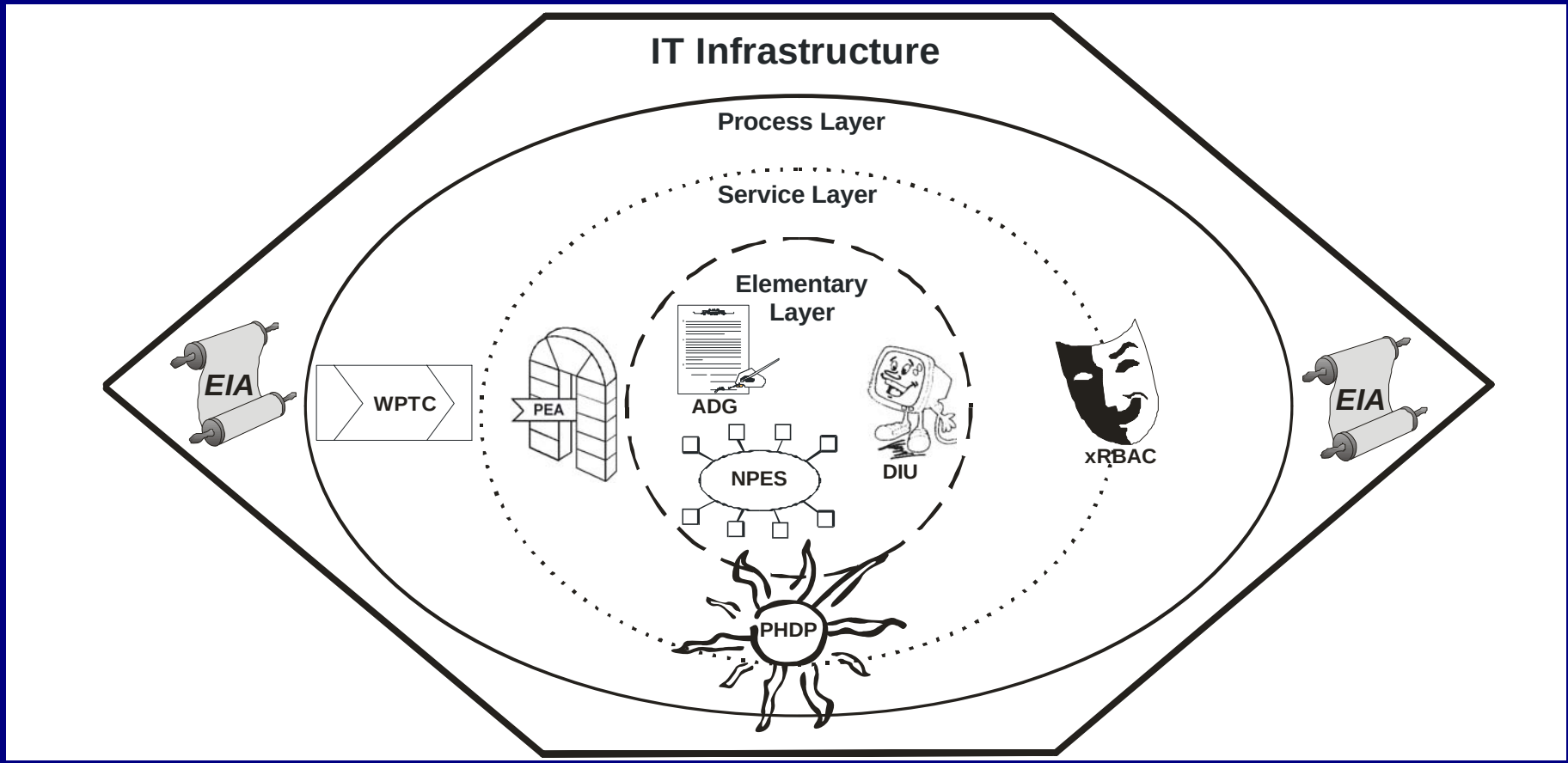
Network Policy Enforcement System

- Reduzierung der möglichen auf zugelassene Kommunikationsverbindungen
- Durchsetzung von Regeln zum Austausch klassifizierter Daten über die Netzinfrastruktur
- Basis für neuartige aktive Schutzmechanismen

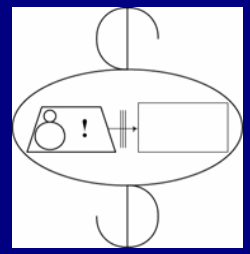
Architektur: NPES



Architektur: Sicherungsverfahren, PEA



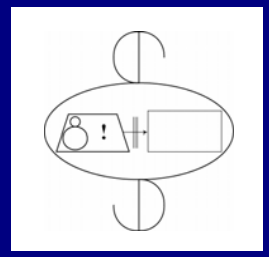
Architektur: PEA

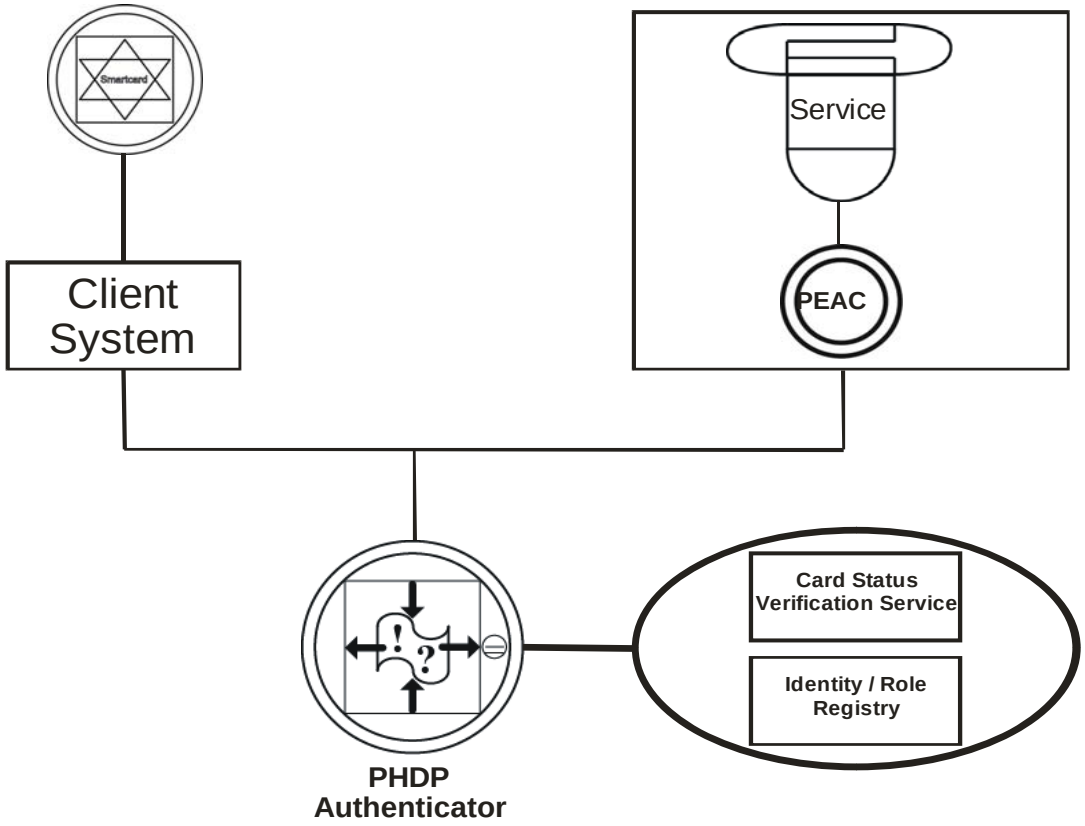


Privacy Enhanced Access Control System

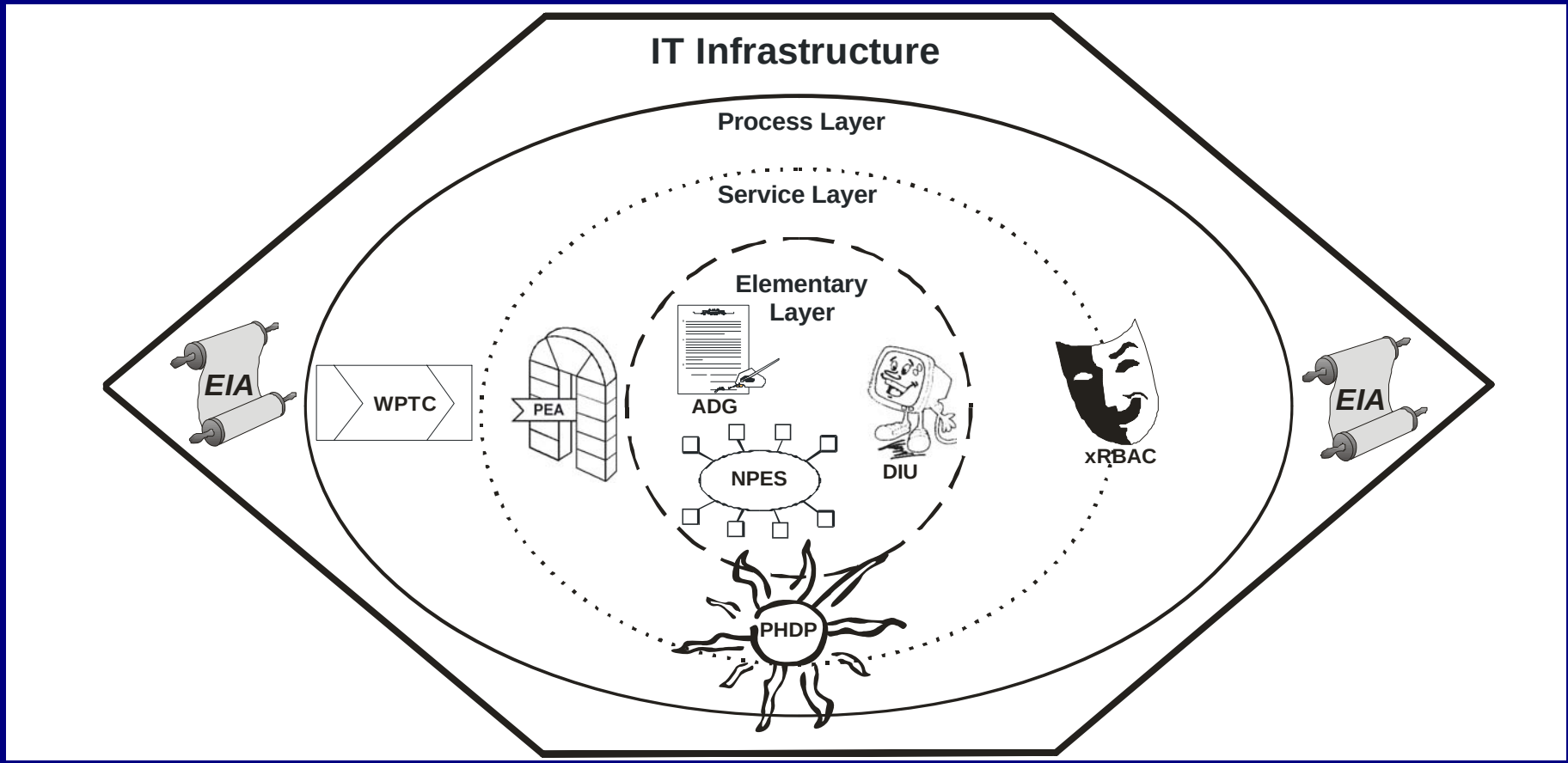
- Verbindliche und anonymisierte Zugangskontrolle zu Diensten
- Homogene Sicherungsniveaus heterogener Dienstinfrastrukturen mit skalierbaren Sicherheits-klassen
- Anwendungsspezifische Absicherung von Diensten

Architektur: PEA

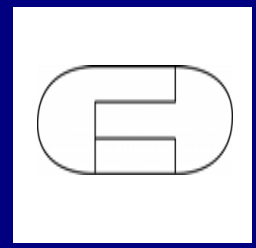




Architektur: Sicherungsverfahren, xRBAC



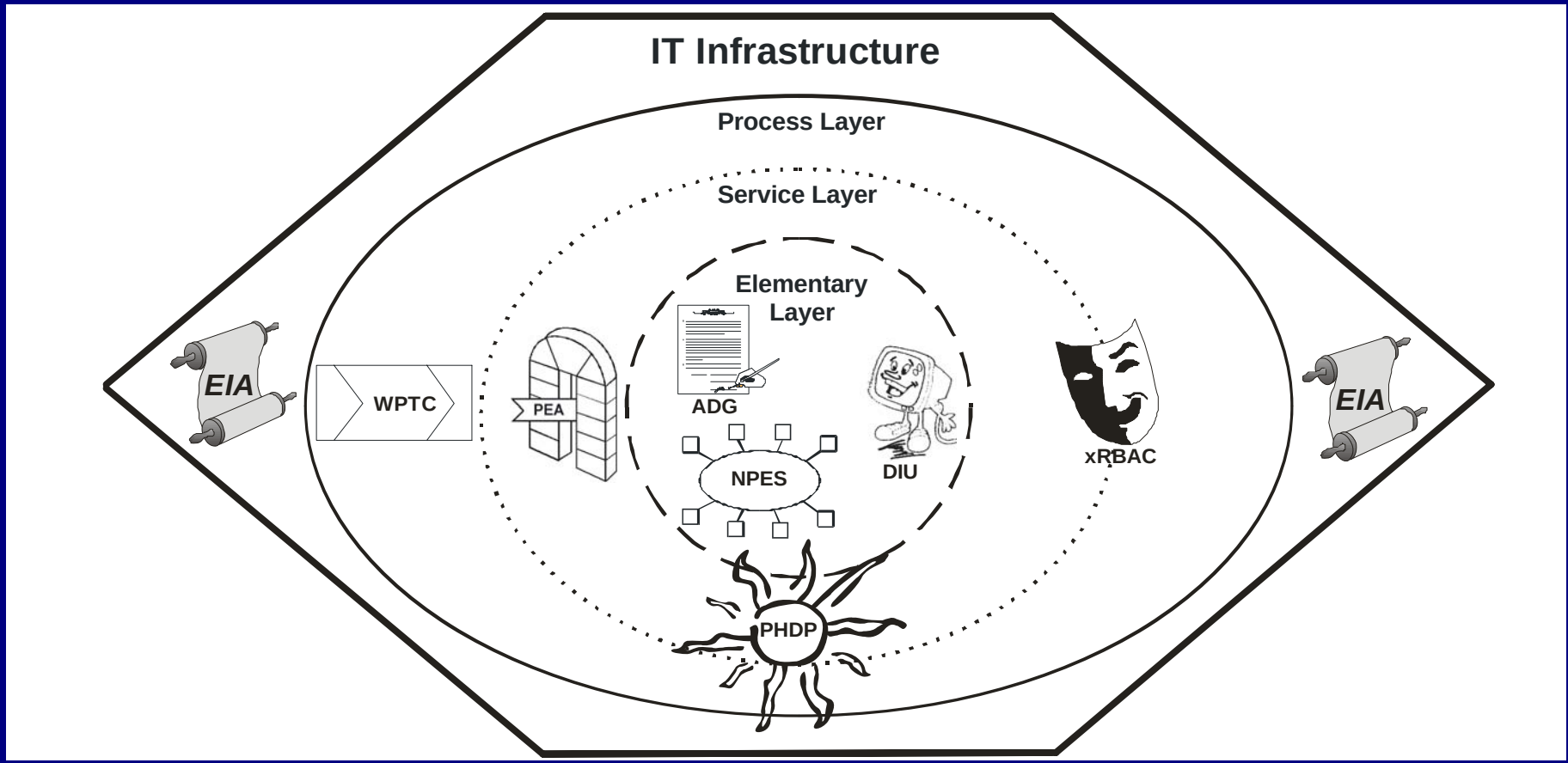
Architektur: xRBAC



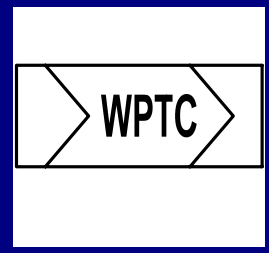
Realtime Enforced Role Based Access Control

- Homogene Abbildung und Durchsetzung von organisatorischen Strukturen und Kompetenzen auf technischer Ebene
- Homogene und umfassende Administration technischer Systeme und verbindliche Verantwortungszumessung bei Vorgängen

Architektur: Sicherungsverfahren, WPTC



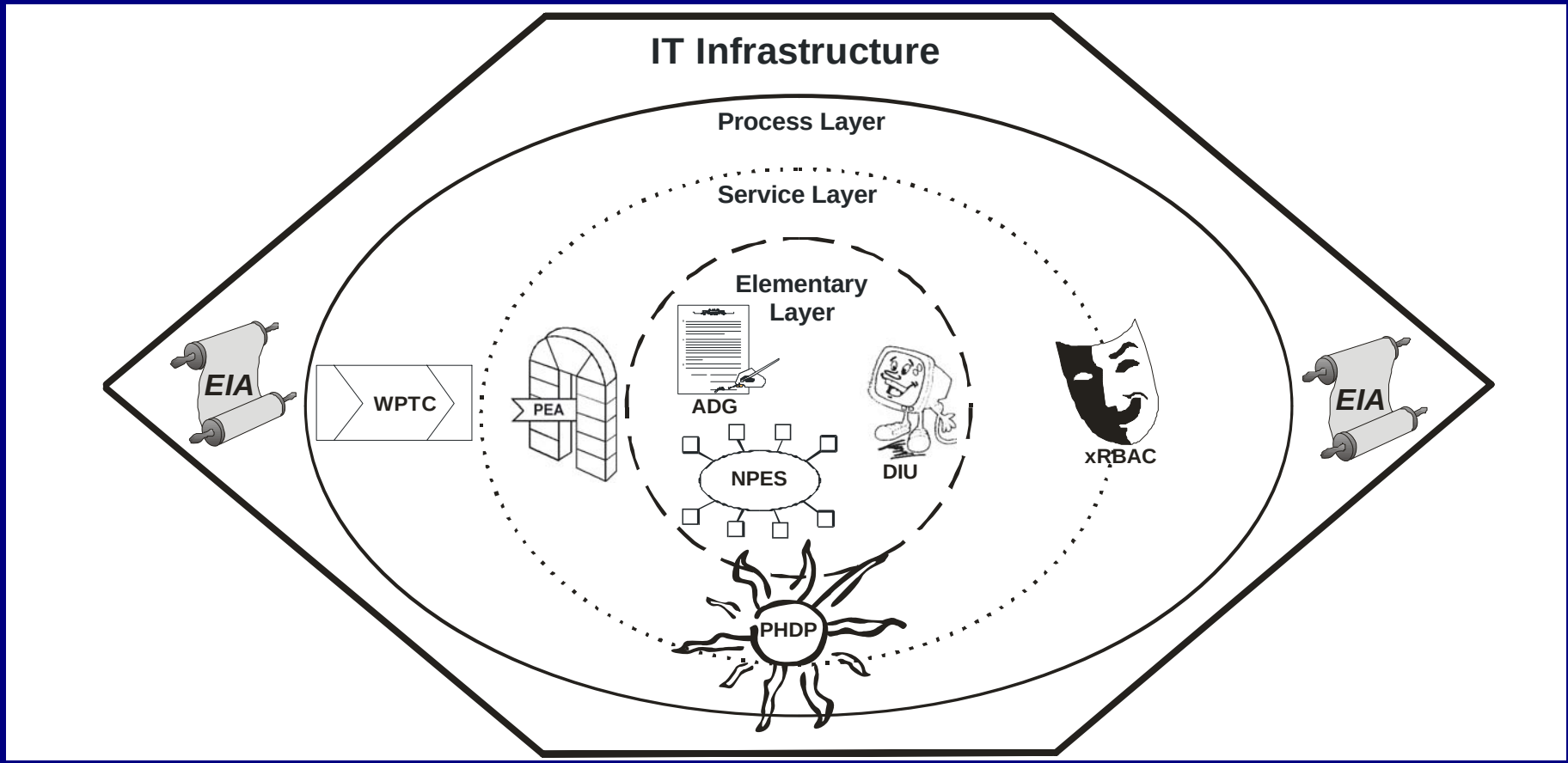
Architektur: WPTC



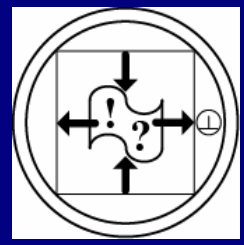
Workflow Process Transaction Controller

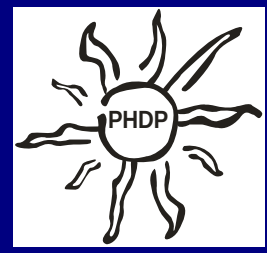
- Verbindliche Nachvollziehbarkeit bei der Abarbeitung von Geschäftsprozessen
- Koordinierung, Kontrolle und Erkennung von Sicherheitsrelevanten Situationen Arbeitsprozessen

Architektur: Sicherungsverfahren, PHDP



Architektur: PHDP





Policy Handling Distribution Point

- Verteilung der Regelwerke von der EIA zu den verschiedenen wirkverbindlichen Elementen
- Koordinierung der Situationsbehandlung in Interaktion mit den wirkverbindlichen Elementen
- Durchsetzung von Regeln bezüglich der Erweiterungs- und Instandhaltungsarbeiten an der IT-Infrastruktur

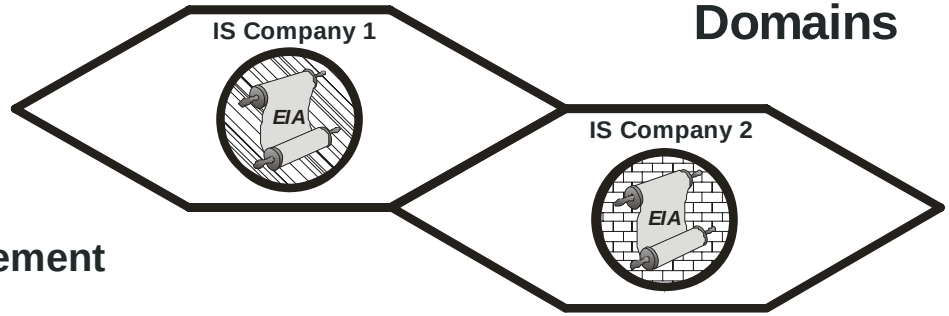
IT-Infrastrukturen Kopplung

Inter-Infrastructure Trust Establishment
- Exchange of Policy Rules and Explicit Restrictions
- Exchange of Certificates

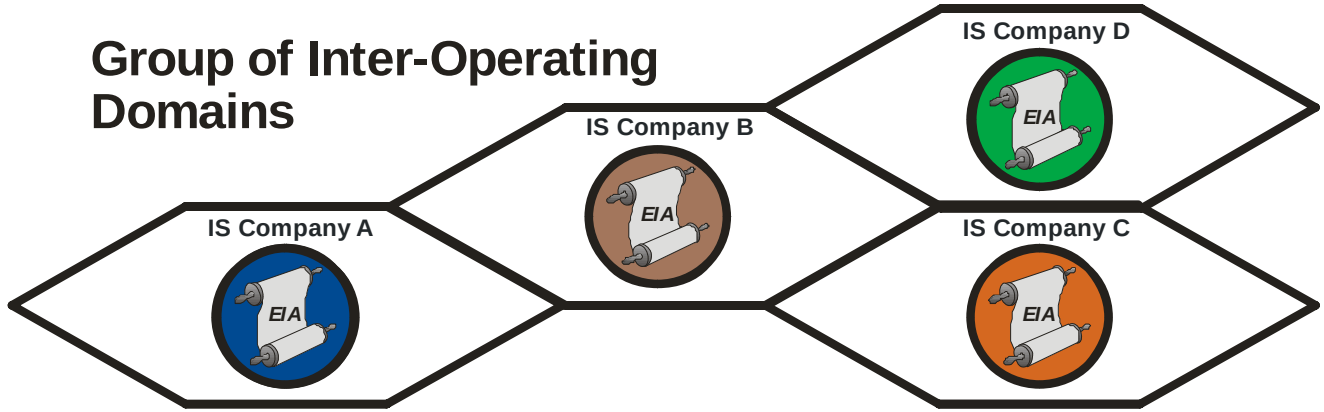
Policy Translation
- Exchange of Policy Rules & Explicit Restrictions
- Exchange of Certificates

External Certificate and Incident Management
- Certificate repository and control
- External Security Incident Message Handling

Couple of Inter-Operating Domains



Group of Inter-Operating Domains



Zusammenfassung (1/3)

- Voraussetzung zur Durchsetzung einer Sicherheitspolitik ist die Identifizierbarkeit von Elementen einer Infrastruktur
- Vorgänge mit hoher sicherheitstechnischer Relevanz dürfen ausschließlich auf wirkverbindlichen Elementen verarbeitet werden
- Für alle Abstraktionsebenen müssen ebenenspezifische Sicherungsverfahren zum Einsatz kommen

Zusammenfassung (2/3)

- Einheitliche Sicherheitsbezeichner und deren spezifische Bedeutungsfestsetzung für jede Abstraktionsebene bilden die Voraussetzung für eine vertikale Durchsetzung einer Sicherheitspolitik
- Horizontale und vertikale Wirkverzahnung von Sicherungsverfahren bilden die Voraussetzung zur verbindlichen Nachvollziehbarkeit von Vorgängen innerhalb von IT-Infrastrukturen

Zusammenfassung (3/3)

- Die vorgestellte Methodik und Architektur kann als Grundlage für die Realisierung moderner IT-Sichereits-paradigmen dienen
- IT-Sichereitsengineering muss bei der Absicherung von IT gestützten Anwendungen neben rein technischen Fragestellungen verstärkt das Anwendungsumfeld berücksichtigen

Ausblick

- Verfahren zur Durchsetzung von Regelwerken außerhalb der technischen Ebene von IT-Systemen (Context Related Security)
- Methodik für die umfassende und konsistente Anwendung des Instrumentariums der IT-Sicherheit
- Methodik zum angemessenen Einsatz von IT-Systemen, die Wirkung auf den zivilisatorischen Kontext entfalten können (IT-Security Engineering)

Kontakt

Ansprechpartner: Thomas J. Wilke
mailto@tjw.li
+49 (30) 74740929
www.Total-IT-Security.de