Total IT-Security

Anwendung der Kryptographie bei der Umsetzung neuer Paradigmen in der IT-Sicherheit

Thomas J. Wilke, tub@tjw.li

Gliederung

- IT-Sicherheit
- Paradigmen
- Wirkprinzipien
- Werkzeuge
- Anwendungen
- Ausblick

IT-Sicherheit: Begriffe

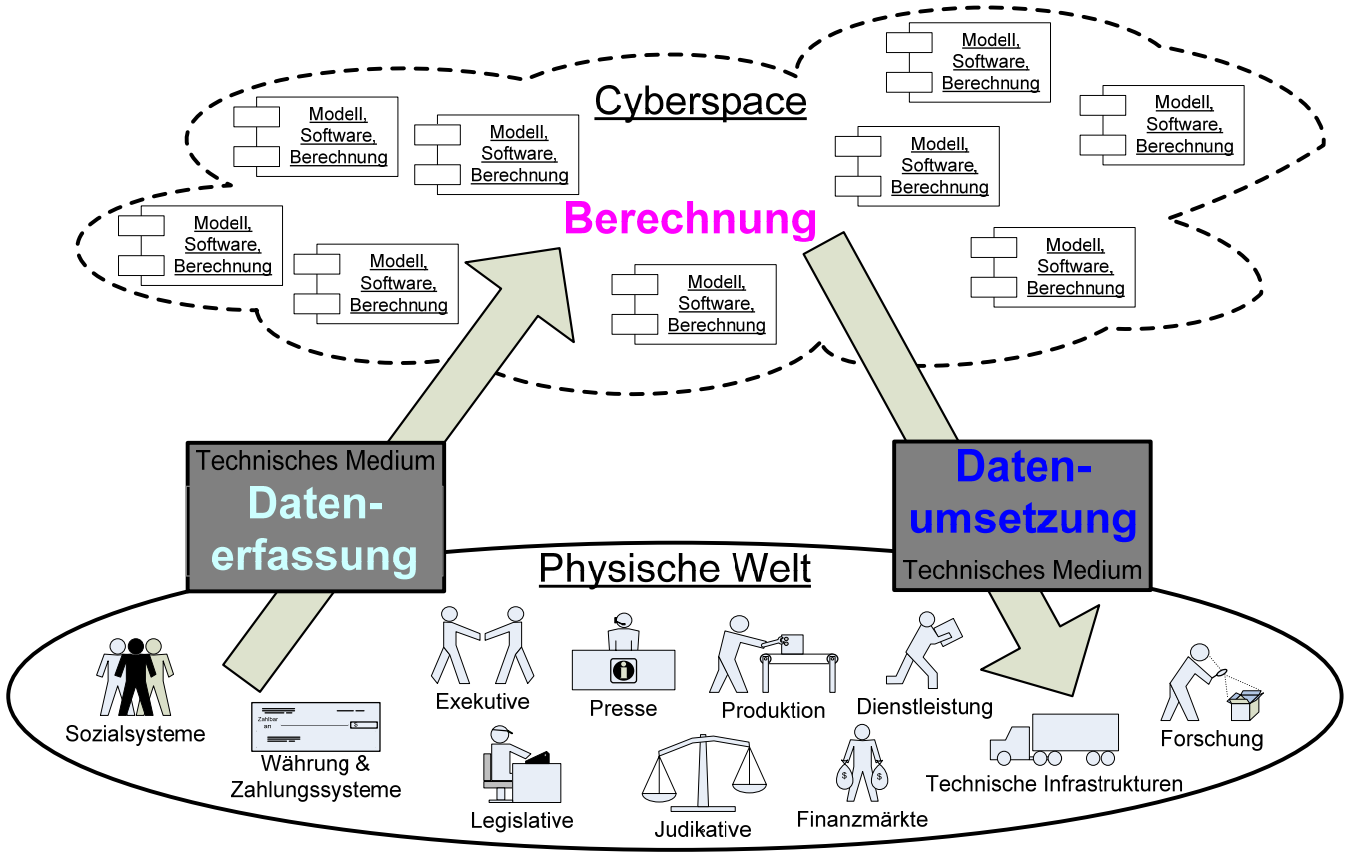
Sicherheit

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.

IT-Sicherheit

Sicherstellung der Funktionsweise von IT-Systemen, so dass die Systeme im Sinne der Einsatzintention der Betreiber und dem realen Gebrauchsverständnis der Nutzer korrekt und zuverlässig arbeiten, wobei die Anwendbarkeit der Regeln und Mechanismen des zivilisatorischen Umfelds für die IT basierte Vorgangsbearbeitung gewährleistet ist.

IT-Sicherheit: Cyberspace & physische Welt



IT-Sicherheit: In den frühen Tagen der IT

Umfeld

- Kompetente Benutzer: tiefgehendes Verständnis der Funktionsweise
- Geringe Zahl von Nutzern und identische Interessenslage
- Verhältnismäßig geringe Funktionskomplexität
- Software, die individuell für Anwendungen entwickelt wurde
- Begrenzter Zugang zu den Rechnersystemen

Maschine → Maschine

Verfügbarkeit

Korrektheit

IT-Sicherheit: Gegenwärtige Anwendungen

Komplexes Umfeld

- Benutzer mit in der Regel geringem technischen Verständnis
- Vielzahl von Nutzern mit unterschiedlichen Interessen
- Offene Systeme, hohe Funktionskomplexität und -vernetzung
- Nutzung von Standardsoftware für sehr unterschiedliche Einsatzbedingungen
- Darstellung und Verarbeitung von Werten mit Rechnersystemen

IT-Sicherheit: Gegenwärtige Anwendungen

Mensch → Maschine: Dienstnutzung

Schutz der Maschine vor einem Menschen

Mensch ↔ Mensch: Mehrseitige Sicherheit

Gegenseitiger Schutz der Menschen voreinander bei deren Interaktionen über Rechnersysteme

Mensch ↔ Maschine: Duale Sicherheit

Gegenseitiger Schutz einer Maschine vor einem Menschen und umgekehrt

IT-Sicherheit: Zielsetzung

Authentische Dualität von Cyberspace und physischer Welt

- Schutz von Werten innerhalb der IT-Systeme
- Verankerung von Mechanismen in IT-Systemen zur Wahrung wirtschaftlicher und 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

Paradigmen: Zielsetzungen

- Multi-Lateral Security:
  Angemessener technischer & organisatorischer Schutz der Parteien, die bei der Nutzung technischer Systeme betroffen sind.
- Strategic Information Distribution:
  Informationsverteilung zum Nachweis von Vorgängen und fortgeschrittenem Datenschutz
- Multi-Administrative Authorities:
  Direkte technische Abbildung und Durchsetzung von organisatorisch definierten Kompetenzen

Paradigmen: Zielsetzungen

- Dynamic Trust Relations:
  Aufbau und Nutzung begrenzter Vertrauensbeziehungen zwischen anonymen Interaktionspartnern.
- Functional Networking Complexity Reduction :
  Begrenzung der möglichen auf die benötigten Funktionen sowie der gegenseitigen Beeinflussungsmöglichkeiten
- Vertical and Horizontal Policy Enforcement :
  Homogene Abbildung und Durchsetzung von Sicherheitsregeln innerhalb einer Wirkebene sowie
  zwischen verschiedenen Wirkebenen

Wirkprinzipien

- Nutzung strategische Informationskontexte
- Indirekte Informationsverteilung
- Technisch verbindlich verifizierbare Identitäten
- Interessenbasierte Aufgabenverteilung
- Wirkungsverzahnte Sicherung
- Komplexitätsreduzierung

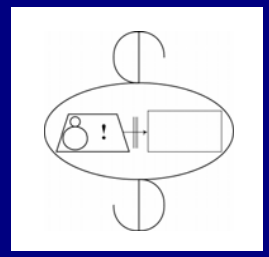
Werkzeuge: Kryptografie

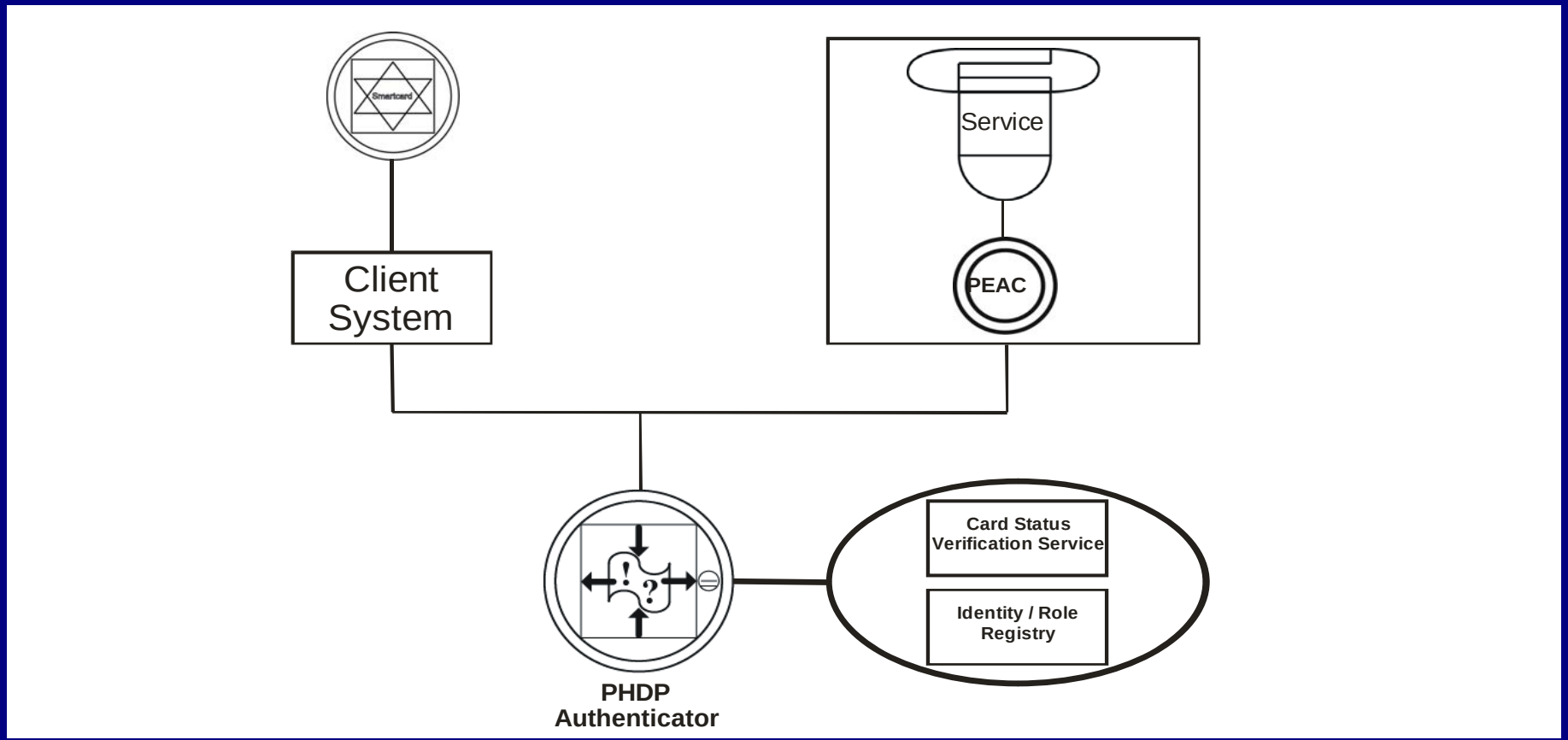
- Symmetrische Kryptografie
- Asymmetrische Kryptografie
- Hash-Funktionen
- Zufallszahlgeneratoren

Werkzeuge: organisatorische Mechanismen

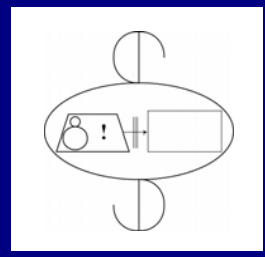
- Zeitversetzte Informationsverarbeitung & -speicherung
- Strategisch verteilte Informationsverarbeitung & -speicherung
- Strategische Sichtbarkeit & Nutzung von Informationen
- Zentralisierte & verteilte Organisationsstrukturen
- Strategische Positionierung wirkungsverbindlicher Subjekte

Anwendung: PEA





Anwendung: PEA



Aufteilung der atomaren Funktion von Authentisierung und Rechtezuweisung auf mehrere Parteien

Privacy Enhanced Access Control System

Eindeutige & anonyme ID

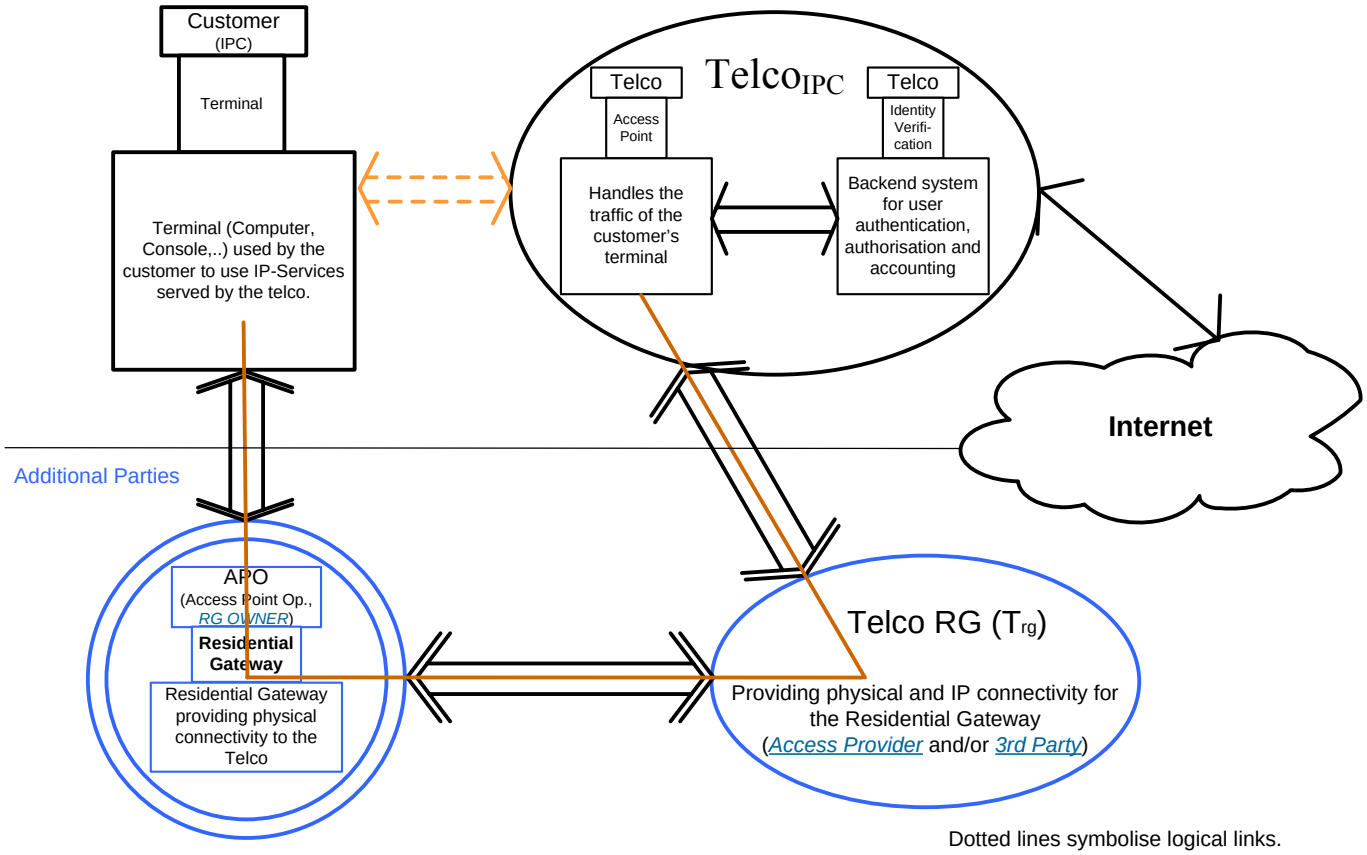
- je Client
- je Dienst

Campuskarten-Zugangs-kontrollverfahren

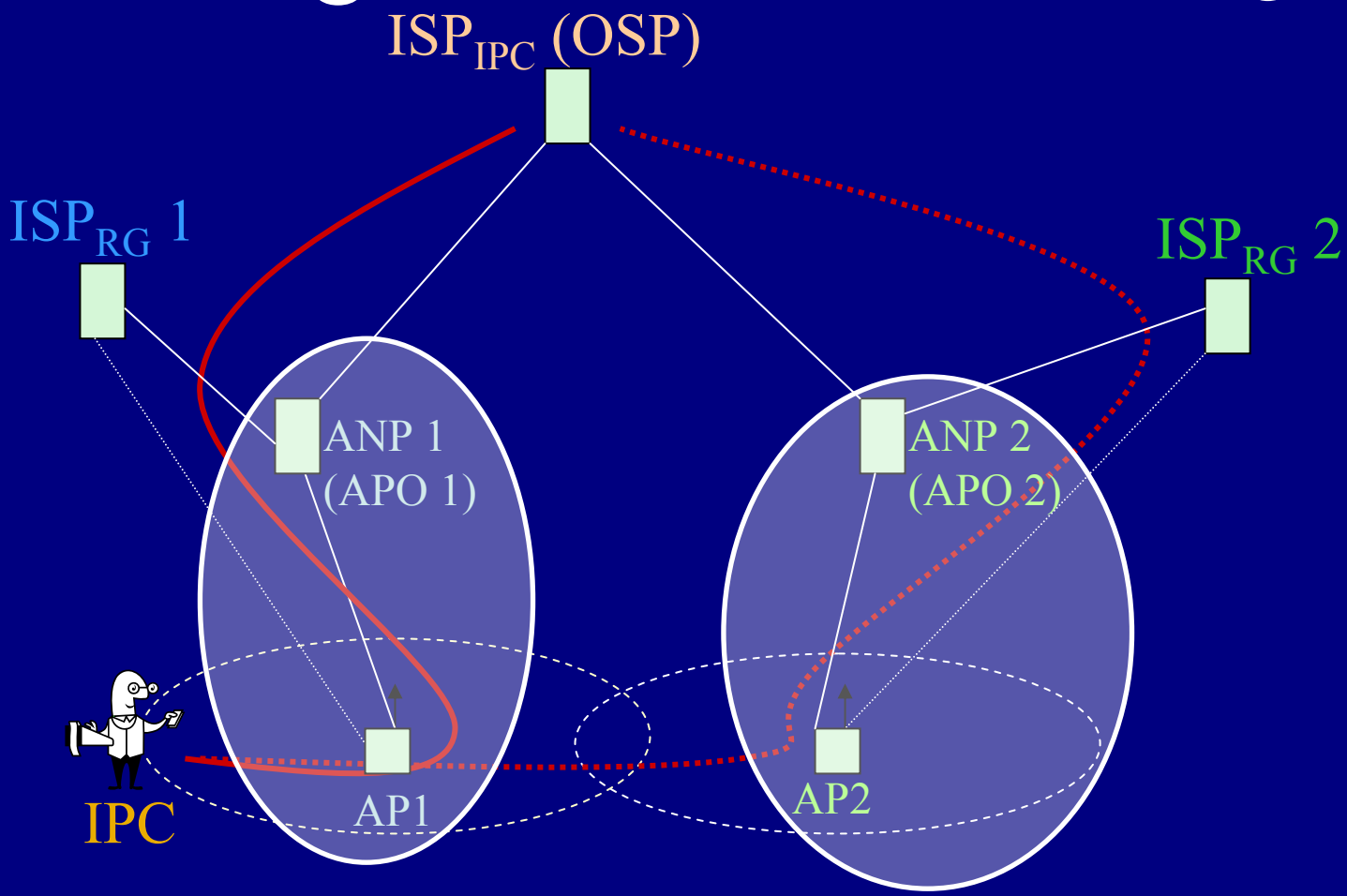
Eindeutige & anonyme ID

- je Client
- für alle Dienste der TUB

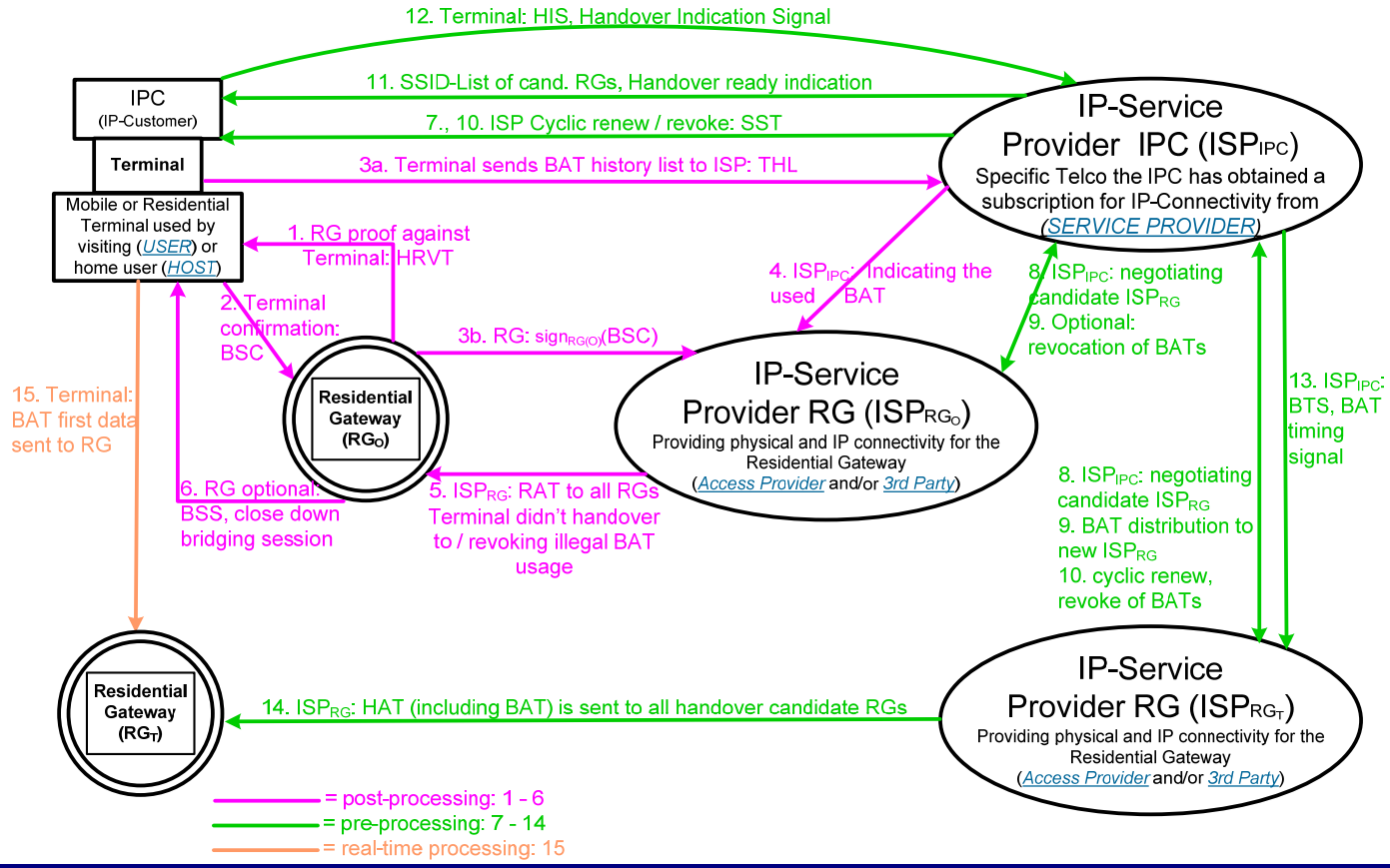
Anwendung: OBAN, Parteien



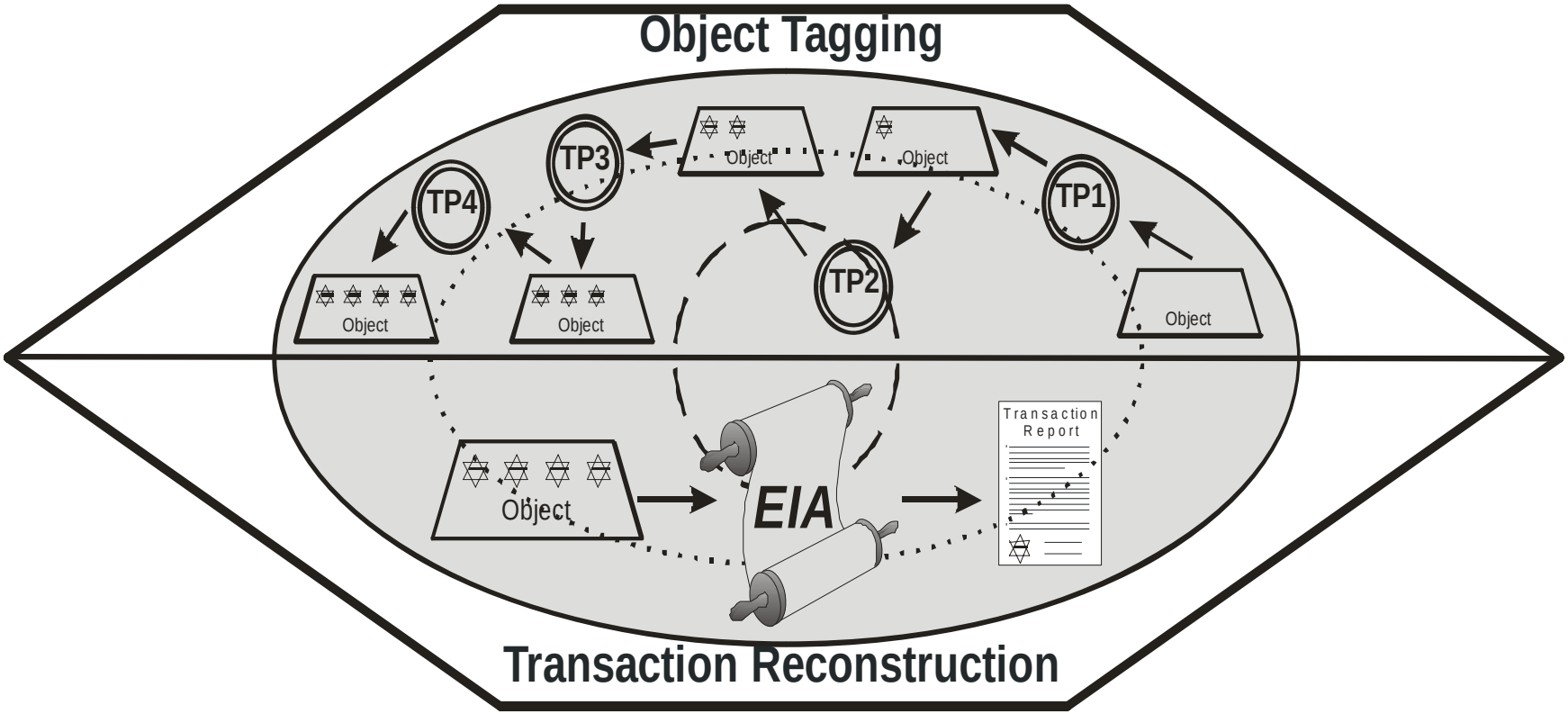
Anwendung: OBAN, Access Routing



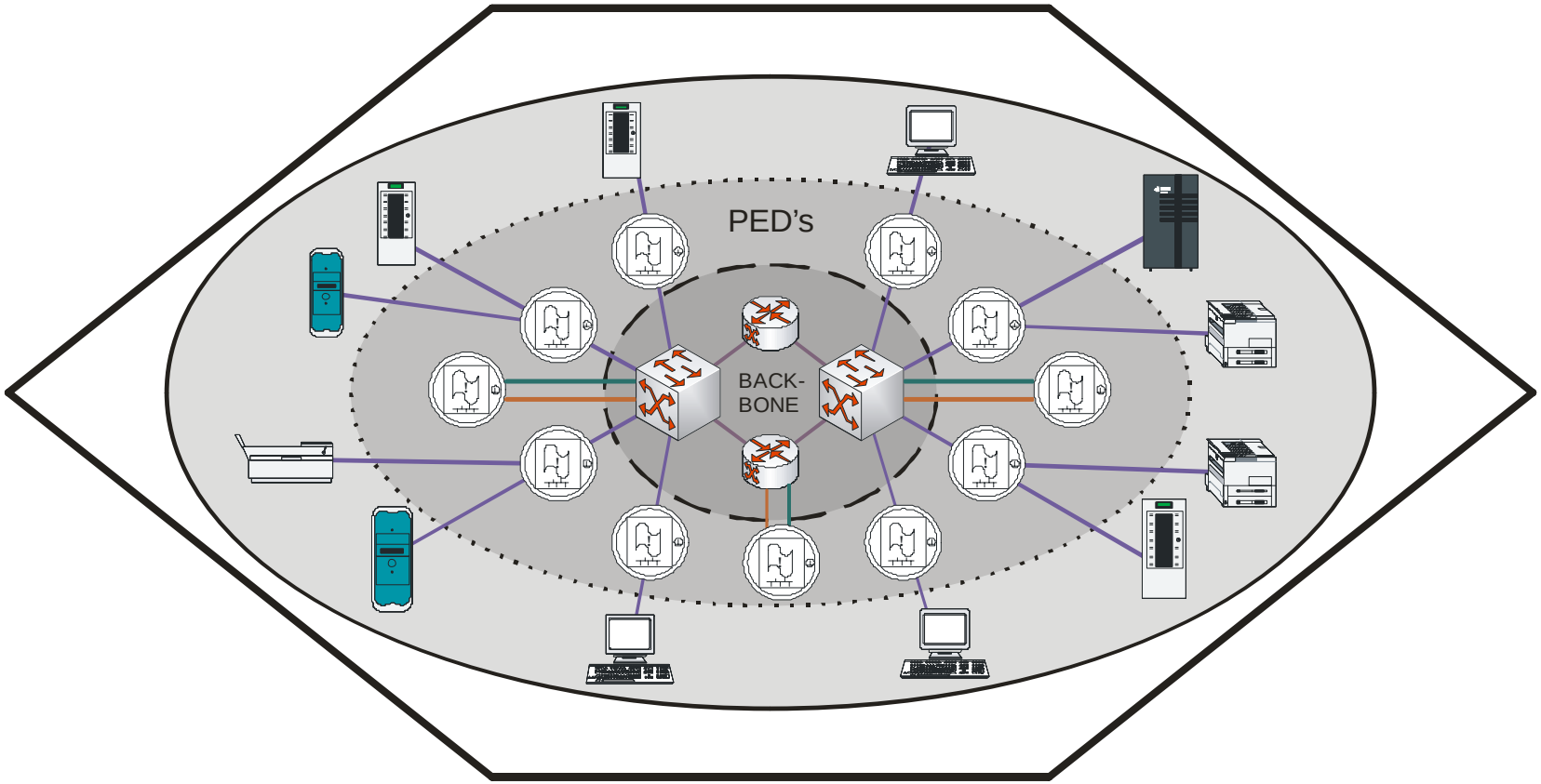
Anwendung: OBAN, Time Shifted AP



Anwendung: Object Tagging, Total IT-Security



Anwendung: NPES



Zusammenfassung

- Moderne IT-Sicherheit muss neben den anwendungsspezifischen funktionalen Sicherheitsanforderungen auch die Anforderungen des zivilisatorischen Kontextes sowie der beteiligten Partei berücksichtigen
- Problemstellungen bei Anwendung der Kryptographie : Schlüsselverteilung & -aufbewahrung, Verbrauch von Rechen- & Speicherressourcen
- Kryptographie **ein** wichtiges Werkzeug. Die Stärke von Sicherungsverfahren entwickelt sich jedoch erst im situationsangepassten Zusammenspiel der Kryptographie mit anderen Werkzeugen

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
tub@tjw.li
+49 (30) 74740929
www.tub.tjw.li