ABAC in der Theorie – Das Referenzmodell

Jochen Saßmannshausen

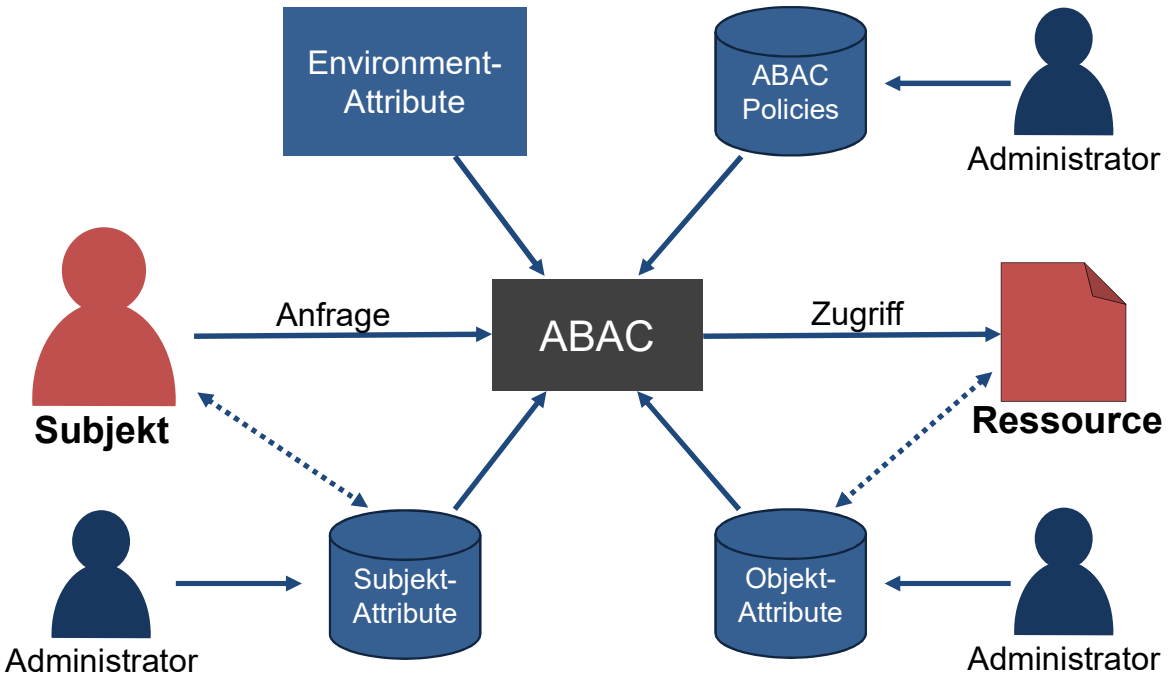
Lehrstuhl für Digitale Kommunikationssysteme
Universität Siegen

ABAC Workshop, 10. September 2020

Zugriffskontrolle – Allgemeines

- Zugriffskontrolle kommt zum Einsatz, wenn Subjekte (z.B. Benutzer, Maschinen, Prozesse) auf Ressourcen/Objekte (z.B. Dateien, Prozessdaten, Services, etc.) zugreifen.
- Authentifizierung des Subjekts ist notwendige Voraussetzung für wirksame Zugriffskontrolle.
- Zugriffskontrolle soll die Privilegien von Subjekten auf ein Minimum beschränken *(**Least-Privilege-Principle**)* und Interessenskonflikte berücksichtigen *(**Separation of Duties**).*
- Verschiedene Zugriffskontrollmodelle:
  Berechtigungsmatrizen, Benutzergesteuerte Zugriffskontrolle, Rollenbasierte Zugriffskontrolle (RBAC) und Attributbasierte Zugriffskontrolle (ABAC).

Attributbasierte Zugriffskontrolle – ABAC



- ABAC trifft Entscheidungen auf Basis von Zugriffsregeln (Policies).
- Subjekte, Objekte und die Umgebung (Environment) werden durch Attribute beschrieben
- Attribute und Policies werden durch befugte Instanzen administriert.

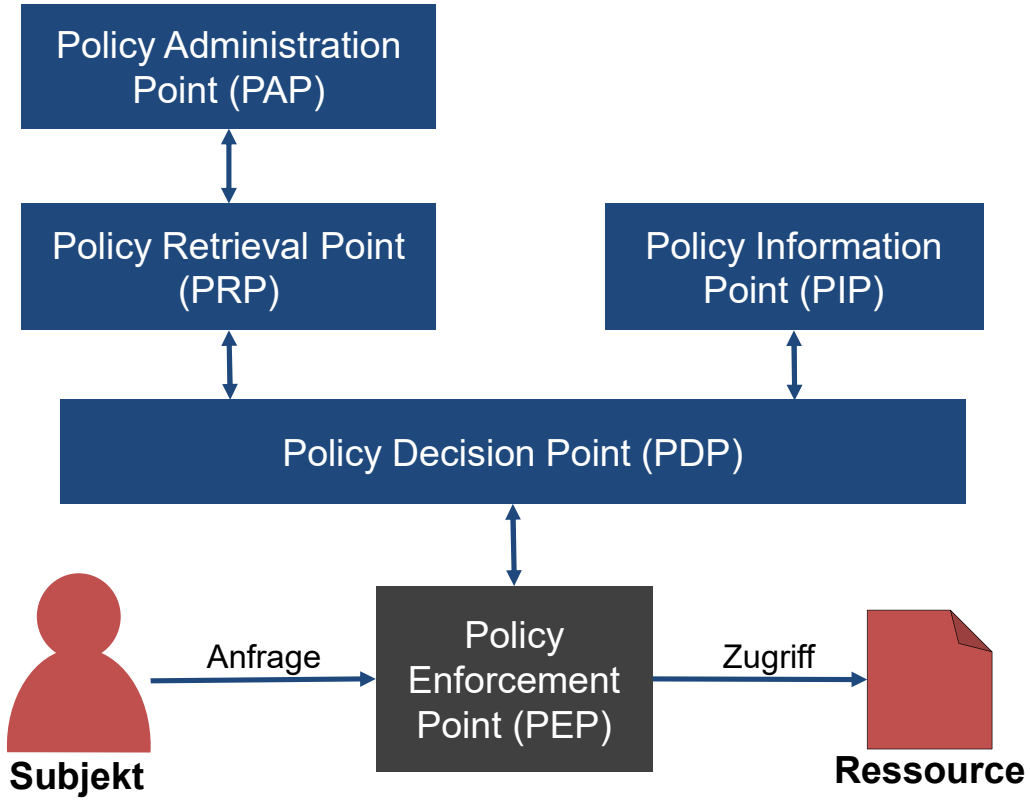
ABAC: Attribute und Policies – Beispiel

- In ABAC-Systemen werden Zugriffsentscheidungen (Permit/Deny) auf durch eine Policy auf Basis von **Subjektattributen**, **Objektattributen** und **Environment-Attributen** getroffen.

- **Eine ABAC-Policy könnte nun z.B. lauten:**

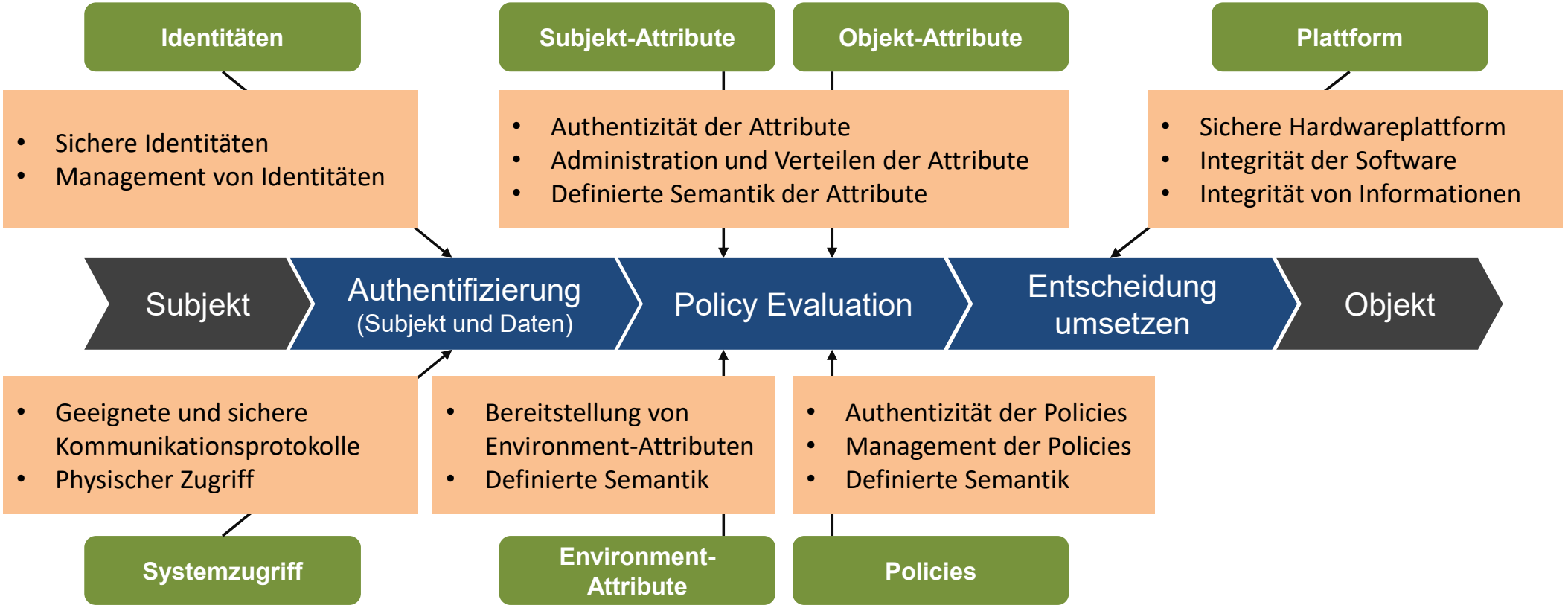
  „Subjekte mit **Rolle=ENGINEER** und dürfen Datenobjekte mit **Objekttyp=Konfigurationsdaten** ändern, wenn sich die Anlage im **Betriebszustand=Maintenance** befindet und sich das zu ändernde **Objekt** im **Zuständigkeitsbereich** des Subjekts befindet“.

ABAC – Typisches Datenflussmodell



- Policy Enforcement Point (PEP):
  - Setzt die Entscheidung (Permit/Deny) applikationsspezifisch um.
- Policy Decision Point (PDP):
  - Evaluiert die Zugriffsregeln.
- Policy Information Point (PIP):
  - Liefert benötigte Informationen, z.B. im Fall von ABAC benötigte Attribute.
- Policy Retrieval Point (PRP) + Policy Administration Point (PAP):
  - Management und Verteilung der Zugriffsregeln.

Security-Aspekte: Die „ABAC Trust Chain“



Standards und Guidelines (Auswahl)

- NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations:
  - Überblick über ABAC und Konzepte, führt einige Aspekte der ABAC Trust Chain ein.
- NIST SP 800-52r4: Security and Privacy Controls for Federal Information Systems and Organizations:
  - Behandelt unter anderem Zugriffskontrolle – Zwar nicht explizit ABAC, führt aber Sicherheitsanforderungen für Zugriffskontrollsysteme und Objekt-Attribute ein.
- OASIS eXtensible Access Control Markup Language (XACML):
  - Definiert eine XML-basierte Beschreibung von Policies und ihre Auswertung.
  - Definiert ein standardisiertes Format für Zugriffsanfragen und Evaluationsergebnisse.
  - Führt Standardattribute für verschiedene Zwecke ein (Subjekt-ID, Datum/Uhrzeit, Aktion, Objekt-ID)
- Domänenspezifische Standards – IEC 62351-8 und IEC TR 61850-90-19 (Zukunft)
  - IEC 62351-8 führt z.B. Attribute ein, die die Rolle und einen Zuständigkeitsbereich eines Subjekts beinhalten.
  - IEC 61850-90-19 wird Attribute definieren, die Eigenschaften von IEC 61850-Datenobjekten darstellen.

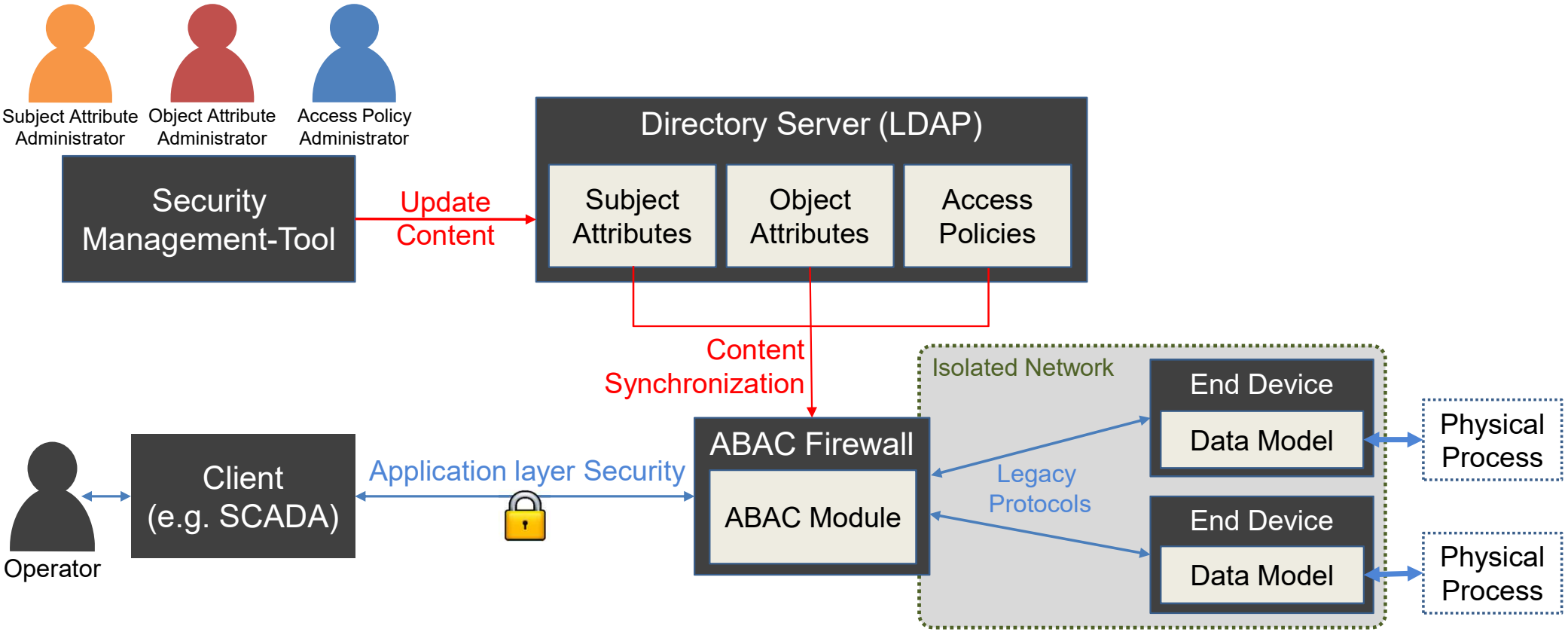
ABAC - Herausforderungen

- Management von Subjekt-/Objekt-Attributen
  - Attribute müssen von autorisierten Administratoren erstellt/bearbeitet/zurückgezogen werden.
  - Attribute müssen verifizierbar sein und auf sichere Weise an Subjekte/Objekte gebunden werden.
  - Attribute müssen vor Manipulationen geschützt sein.
- Environment-Attribute
  - Die „Umgebung“ hängt von vielen Faktoren ab (z.B. Prozessdaten).
  - Daten müssen ggf. von verschiedenen, heterogenen Systemen bezogen werden.
  - Die Umgebung muss auf definierte Weise dargestellt werden.
- Management von Policies
  - Ähnliche Anforderungen wie beim Attribute-Management
  - Der Policy-Designer muss Wissen über Syntax und Semantik der Attribute haben.

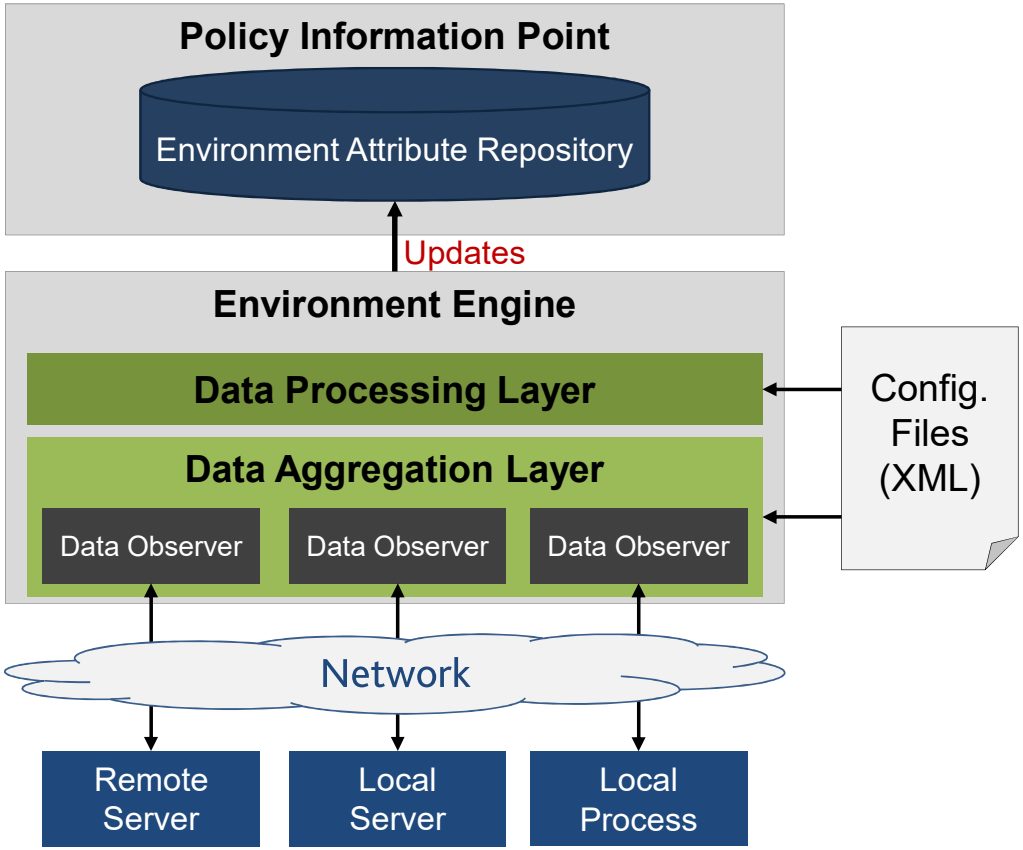
ABAC – weitere Aspekte

- Herausforderung: Auditability
  - Es kann unter Umständen schwierig sein, aus einem Regelsatz und vorhandenen Attributen die maximalen Berechtigungen eines Subjekts zu ermitteln.
  - Welche Privilegien hat ein bestimmtes Subjekt? Welche Subjekte haben ein bestimmtes Privileg?
  - Komplexität und Auditability hängen stark von dem Design der Attribute und Policies ab.
- Hybride Modelle: RBAC und ABAC
  - Hybride Modelle versuchen, Vorteile von RBAC und ABAC zu kombinieren.
  - Typisches Beispiel: Permissions werden durch eine Rolle an Subjekte gebunden. Individuelle Subjekt-Attribute (z.B. eine ***Area of Responsibility***) beschränken die Privilegien.
  - Weiteres Beispiel: Objekte werden durch Attribute beschrieben. RBAC-Policies definieren Privilegien auf Gruppen von Objekten mit bestimmten Eigenschaften.

Die Entwicklung der ABAC-Lösung – Gesamtübersicht



Die Entwicklung der ABAC-Lösung – Environment-Attribute



- Daten (z.B. Sensordaten) werden von einem **„Data Aggregation Layer“** aggregiert.
- Ein **„Data Processing Layer“** verarbeitet die bereitgestellten Daten zu definierten Attributen.
- Das Verhalten der beiden Layer ist durch den Policy Administrator definierbar.

Die Entwicklung der ABAC-Lösung – Subjekt-/Objekt-Attribute

- Ansatz: X.509-Attributzertifikate für Subjekt- und Objektattribute
  - Eigenes X.509-Attribut mit eigener OID zur Speicherung von Attributen
  - Einfache Anwendung für Subjekt-Attribute.
  - Neuer Ansatz für Objektattribute: Jedes Datenobjekt ist durch einen Directory-Eintrag repräsentiert und hat damit einen *Distinguished Name (DN).*

- **Vorteil: Ausnutzen von existierenden PKI-Mechanismen**
  - Verteilung der Informationen über ein Directory.
  - Kryptografische Mechanismen zur Wahrung der Integrität der Attribute.
  - Revocation-Mechanismen und Delegation von Zuständigkeiten.

Die Entwicklung der ABAC-Lösung – Policies

- Definition und Auswertung von Policies basierend auf XACML.
  - Hierarchische Struktur der Policies ermögliche effiziente Evaluierung.
  - Erhöhung der Performance durch Reduzieren der gleichzeitig anzuwendenden Policies und Attribute-Sets.
- XML-Signaturen zur Integritätssicherung und Verifizierbarkeit.
  - Nachweisbarkeit der Urheberschaft der Policies.
- Verteilung der Policies über LDAP.
  - Nutzt die gleiche Infrastruktur wie das Attribute-Management

Vielen Dank für Ihre Aufmerksamkeit!