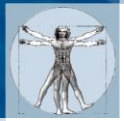


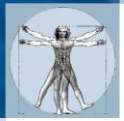
SIMPL

-

SimTech: Information Management, Processes and Languages

Authentifizierung und Autorisierung bei Web Services

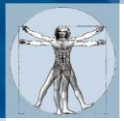
Michael Schneidt



Agenda

- Sicherheitsgrundlagen
- Authentifizierung
- Autorisierung
- Web Service Standards
- Sicherheit in BPEL Engines
- Zusammenfassung

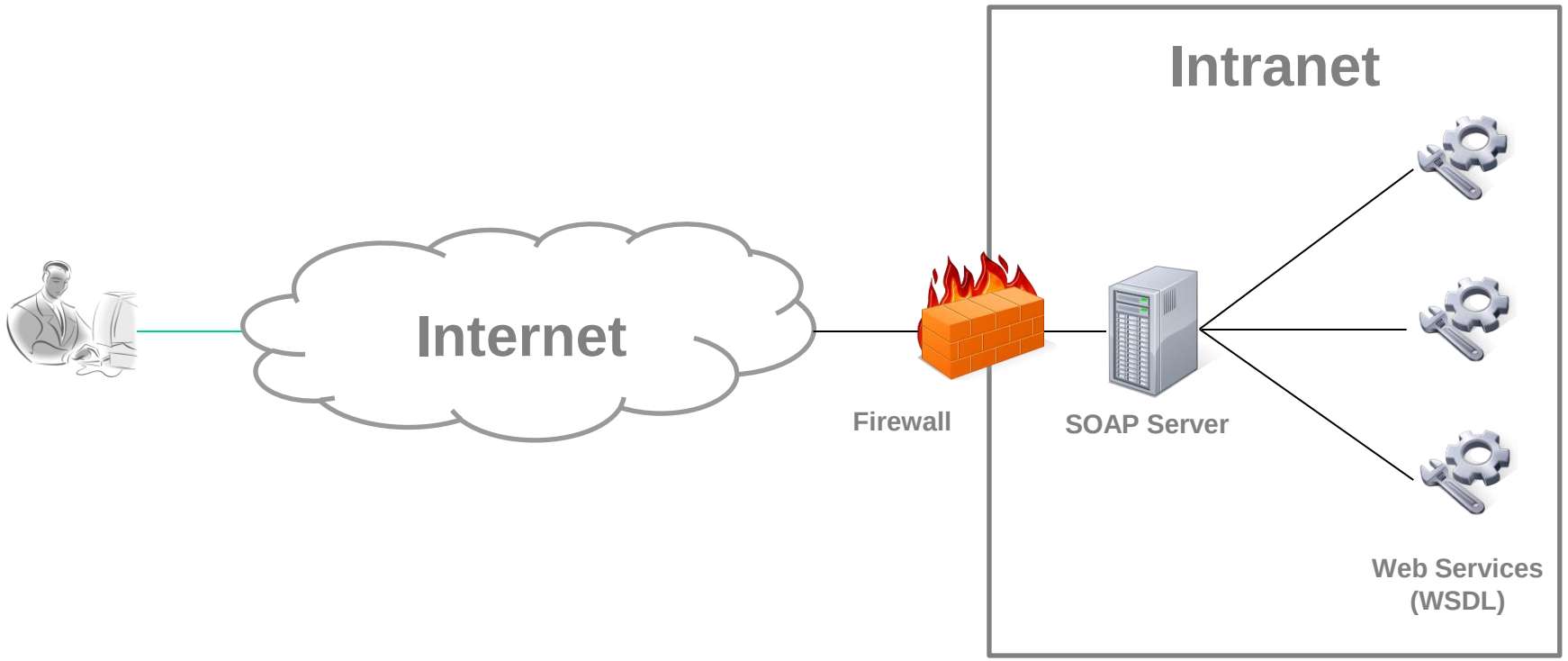
- Diskussion

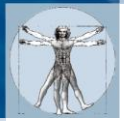


SICHERHEITSGRUNDLAGEN

KOMMUNIKATION, SICHERHEITSANFORDERUNGEN
SICHERHEITSTAXONOMIE

Kommunikation

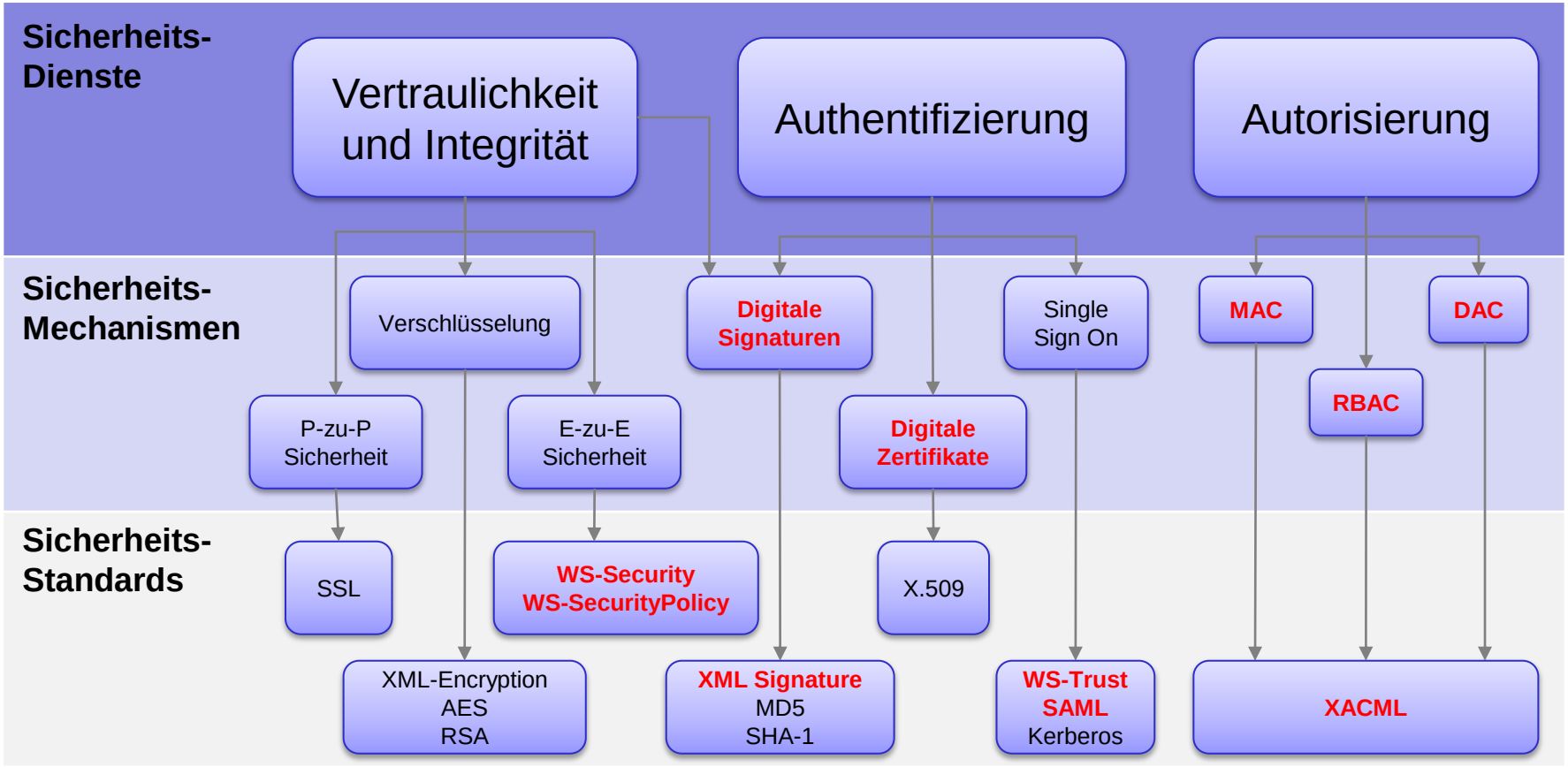


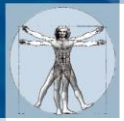


Sicherheitsanforderungen

- Authentifizierung
  - Wer ist der Benutzer?
  - Gegenseitiges Vertrauen zwischen Web Service und Benutzer
  - Nachweisbarkeit
  - Single Sign On (SSO)
- Autorisierung
  - Was darf der Benutzer?
  - Einschränkung der Zugriffe
  - Rechte vergeben und entziehen
  - Organisation (Gruppen, Hierarchien, Sicherheitsstufen)
- Integrität und Vertraulichkeit

Sicherheitstaxonomie



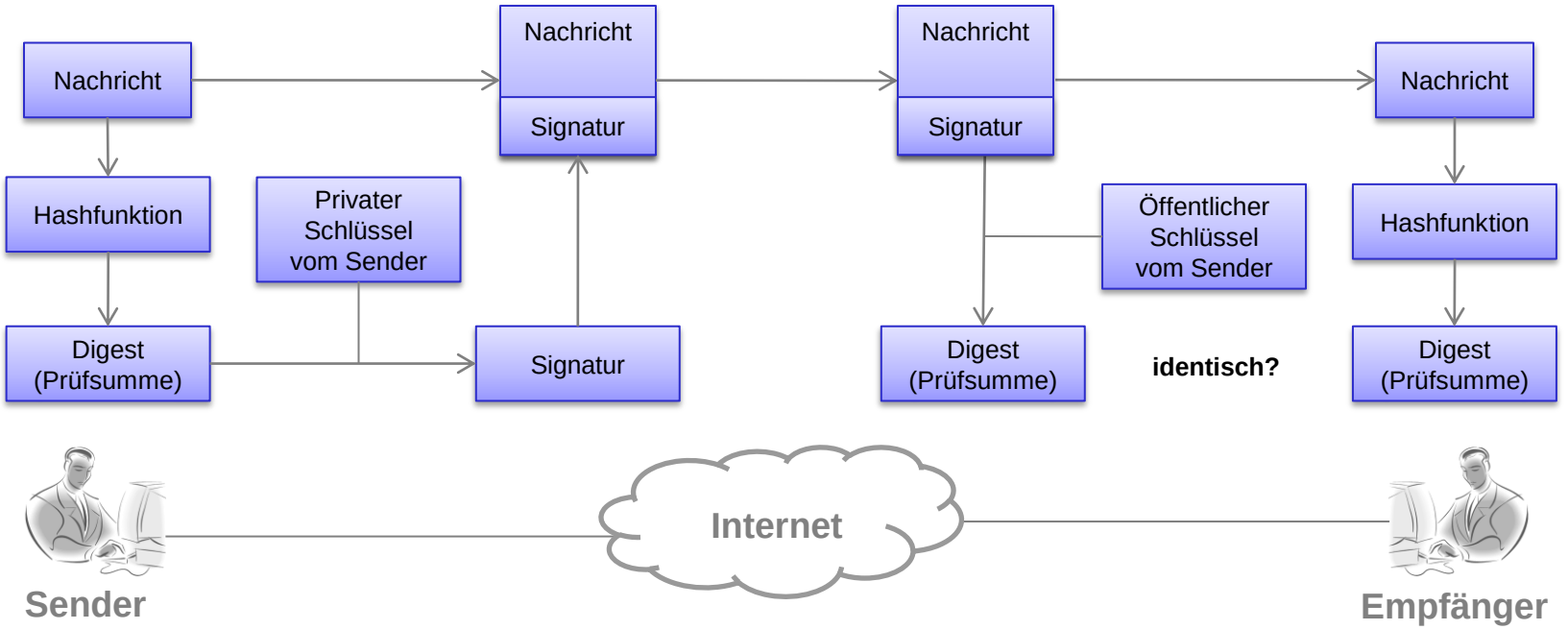


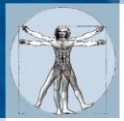
AUTHENTIFIZIERUNG

SIGNATUREN, ZERTIFIKATE, XML SIGNATURE, SAML

Signaturen

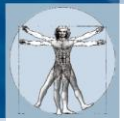
- Authentizität, Integrität
- Eindeutige Signatur aus Schlüssel und Daten (Digest)
- Signatur mit asymmetrischem Verschlüsselungsverfahren





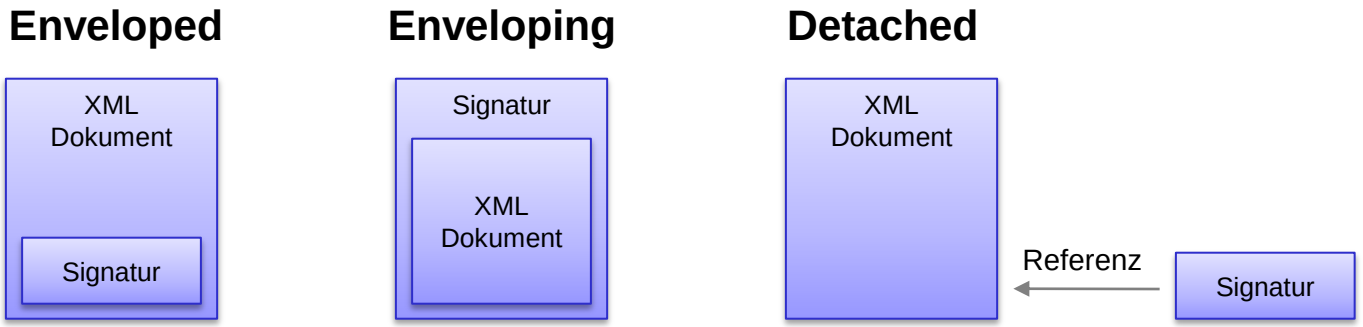
Zertifikate

- Nachweisbarkeit
- Öffentlicher Schlüssel mit Daten über Eigentümer
- Zertifizierungsstelle (z.B. GlobalSign, VeriSign)
- Werden mit dem privaten Schlüssel der Zertifizierungsstelle signiert
- Public Key Infrastructure (X.509)



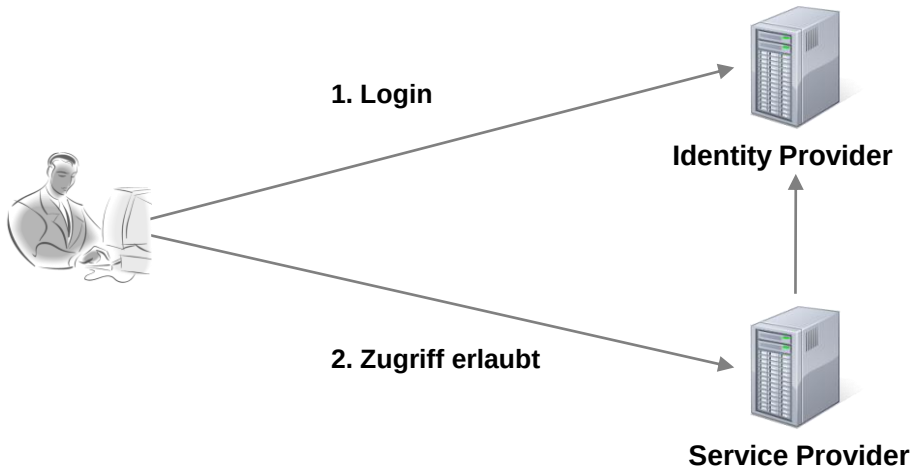
XML Signature

- Beliebige Daten signieren
- Kanonisierung vor der Signierung
- Verschiedene Arten der Signierung



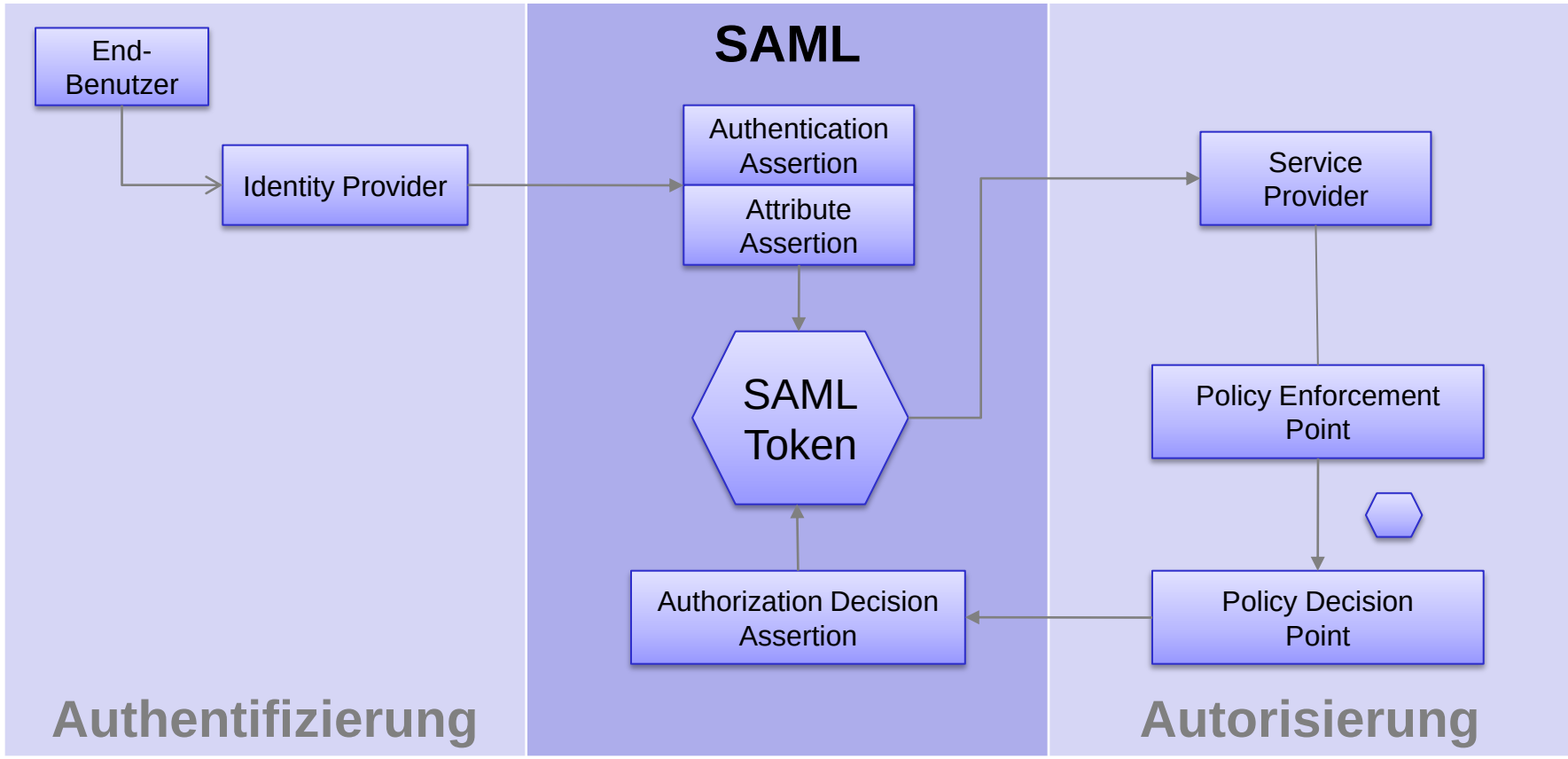
SAML

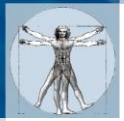
- Security Assertion Markup Language
- Formulieren von Informationen zur Authentifizierung und Autorisierung
- Kommunikation dieser Informationen über Organisationsgrenzen
- Single Sign On
- Trennung von Identity Provider und Service Provider



SAML Anwendungsfall

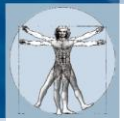
- Anwendungsfall





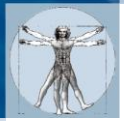
AUTORISIERUNG

ZUGRIFFSKONTROLLE, XACML



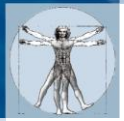
Zugriffskontrolle

- Discretionary Access Control (DAC)
  - Identitätsbasiert
  - (Subjekt, Objekt, Recht) → {ja,nein}
- Mandatory Access Control (MAC)
  - Identitäts- und Regelbasiert (Policy)
  - Multi-Level-Sicherheitssysteme (Stufen, Schichten)
- Role Based Access Control (RBAC)
  - Benutzer, Rollen, Gruppen
  - Identitätsmanagement-Systeme



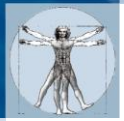
XACML

- eXtensible Access Control Markup Language
- Formulieren von Zugriffsberechtigungen
- Abfrage von Zugriffsberechtigungen
- Auswertung von Zugriffsberechtigungen
- DAC, MAC, RBAC umsetzbar
- Profile für andere Standards und Technologien (z.B. SAML)



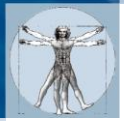
XACML Policy

- Target
  - Relevanz der Policy für den Zugriff
  - Definiert Attribute vom Typ Subject, Resource, Action
- Rules
  - Target, Effect, Conditions
- Rule Combining Algorithms
  - Auswertung der Regeln für finale Entscheidung (z.B. Deny-overrides)
- Obligations
  - Zusätzliche Operationen



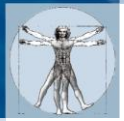
WEB SERVICE STANDARDS

WS-SECURITY, WS-SECURITYPOLICY, WS-TRUST



Web Service Standards

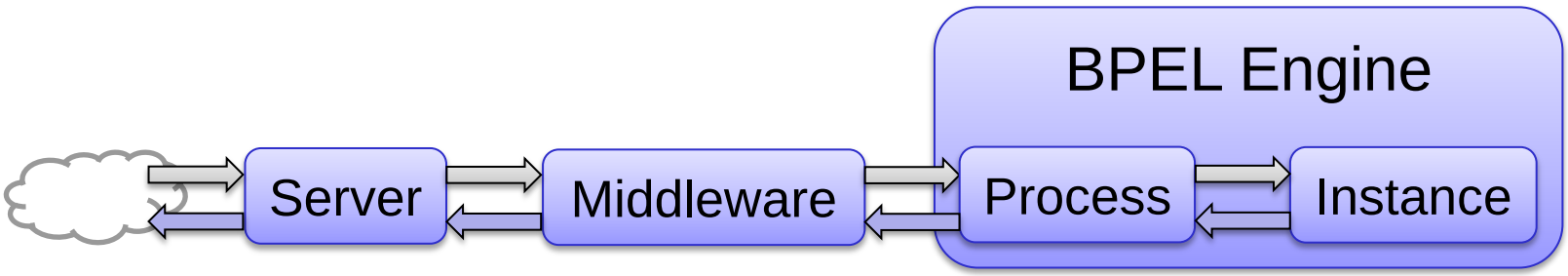
- WS-Security
  - Integrität, Authentizität und Vertraulichkeit für SOAP Nachricht
  - Verwendet XML Signature und XML Encryption
  - Security Tokens (unsigned, signed)
- WS-SecurityPolicy
  - Ergänzung zu WS-Policy
  - Sicherheitsanforderungen formulieren und bekannt machen
- WS-Trust
  - Security Token Service (STS) zur Herausgabe, Erneuerung und Validierung von Security Tokens
  - Konvertierung von Security Token
  - Überbrückung von Vertrauensdomänen



SICHERHEIT IN BPEL ENGINES

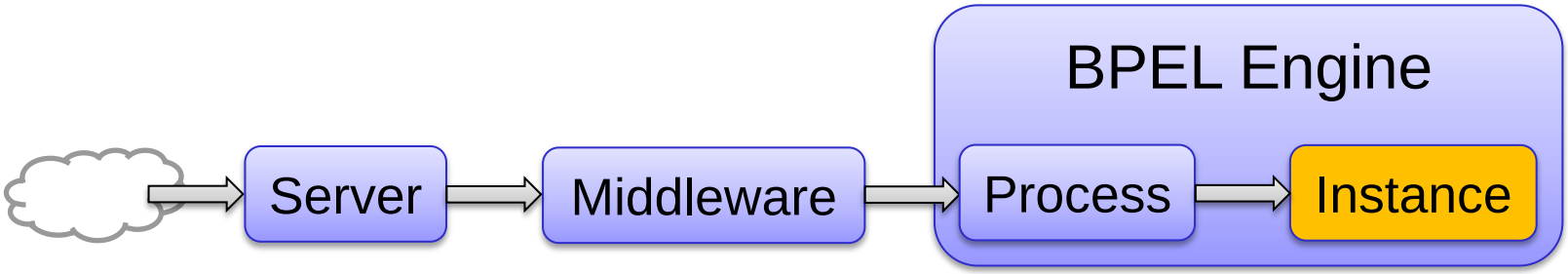
VERARBEITUNGSPROZESS, IMPLEMENTIERUNGEN

Verarbeitungsprozess



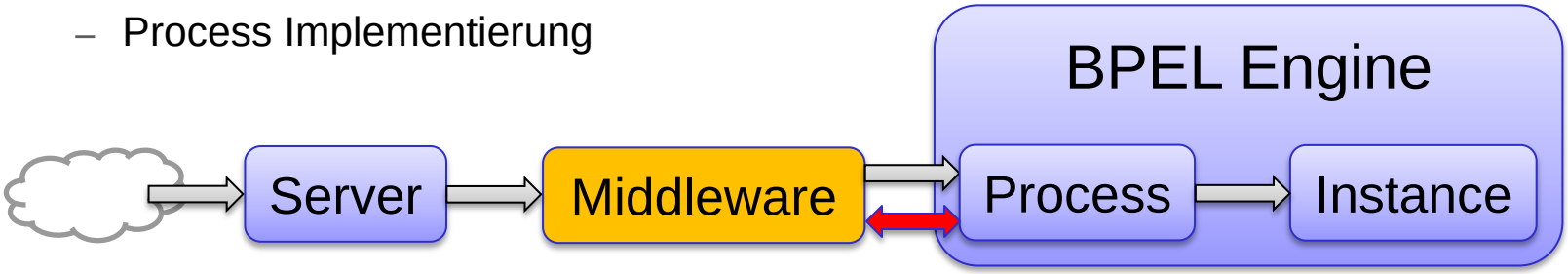
Instance Implementierung

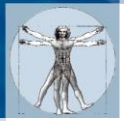
- Vorteile
  - Benutzerinformationen in Variable
  - Fehlgeschlagene Authentifizierung kann im Prozess abgefangen werden
  - Keine Erweiterung der BPEL Engine notwendig
- Nachteile
  - Vermischung von Prozesslogik und Sicherheitslogik
  - Redundanter Code
  - Unnötige Prozessinstanzen



Middleware Implementierung

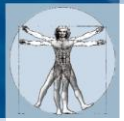
- Vorteile
  - Trennung von Prozesslogik und Sicherheitslogik
  - Verschiedene Authentifizierungsverfahren möglich
  - Wiederverwendung von Sicherheitsanforderungen
  - Keine unnötigen Prozessinstanzen
- Nachteile
  - Keine Benutzerinformationen im Prozess bei der Authentifizierung
    - **Erweiterung** der BPEL Engine oder der Middleware notwendig
  - Keine Prozessinformationen bei der Autorisierung
    - Process Implementierung



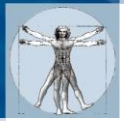


Zusammenfassung

- Sicherheitsgrundlagen
  - Kommunikation, Sicherheitsanforderungen, Sicherheitstaxonomie
- Authentifizierung
  - Signaturen, Zertifikate, XML Signature, SAML
- Autorisierung
  - Zugriffskontrolle, XACML
- Web Service Standards
  - WS-Security, WS-SecurityPolicy, WS-Trust
- Sicherheit in BPEL Engines
  - Verarbeitungsprozess, Instance und Middleware Implementierung

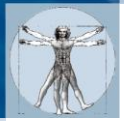


ZUSATZFOLIEN



Sicherheit

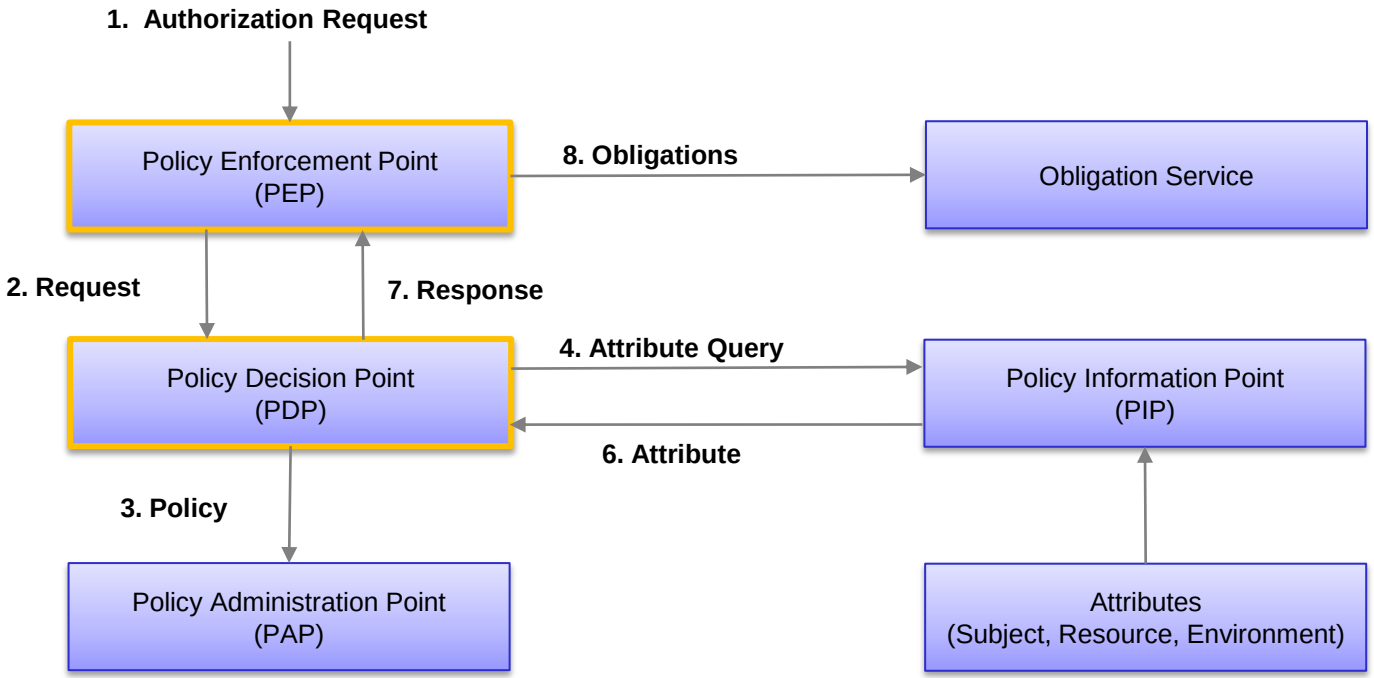
- Punkt-zu-Punkt Sicherheit
- Ende-zu-Ende Sicherheit
- Sicherheitsebenen
  - Transportebene
    - IP-Adresse, Ports
  - Meldungsebene
    - SOAP Nachrichten
  - Anwendungsebene
    - XML Dokumente



SAML Komponenten

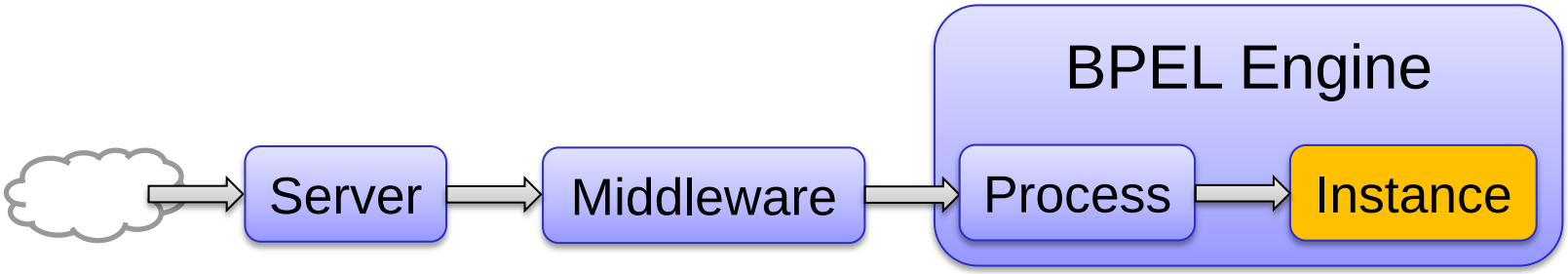
- Assertions
  - Authentication, Authorization Decision, Attribute
- Protocols
  - Kommunikation zwischen Service Provider und Identity Provider
- Bindings
  - Mapping von Protocols auf Standard-Nachrichten-Protokolle (z.B. SOAP)
- Profiles
  - Kombination von Assertions, Protocols und Bindings für versch. Anwendungsfälle
  - Abbildung von Attributen aus anderen Systemen (z.B. XACML)

XACML Anwendungsfall



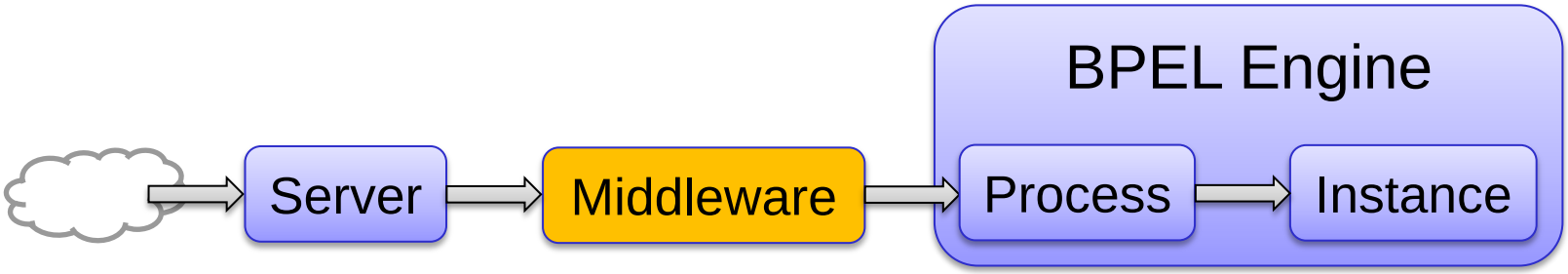
Authentication (1)

- Instance Authentication
  - Vorteile
    - Zugriff auf Identität in Variable
    - Fehlschlag kann in Prozess abgefangen werden
    - Keine Erweiterungen an der BPEL Engine notwendig
  - Nachteile
    - Vermischung von Prozesslogik und Sicherheitslogik
    - Redundanter Code



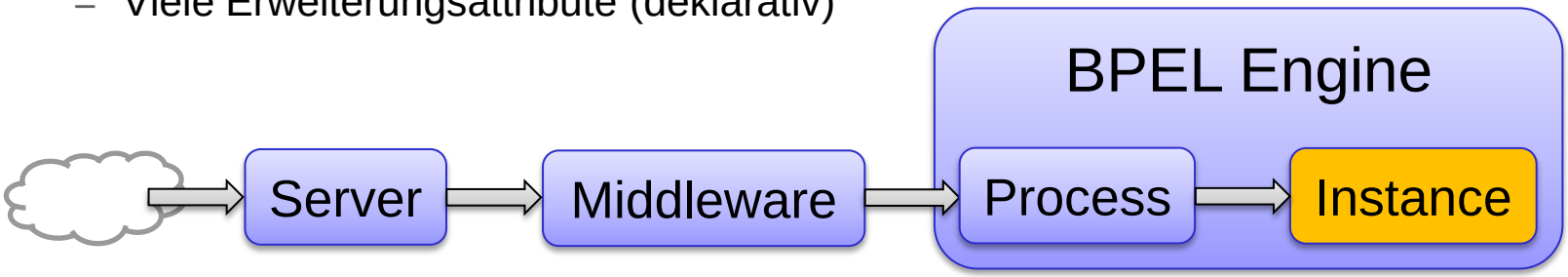
Authentication (2)

- Middleware Authentication
  - Vorteile
    - Trennung von Sicherheitslogik und Prozesslogik
    - Verschiedene Authentifizierungsverfahren möglich
    - Wiederverwenden von Sicherheitsanforderungen (WS-SecurityPolicy)
    - Keine unnötigen Prozessinstanzen
  - Nachteile
    - Benutzerinformationen nicht im Prozess verfügbar
    - Erweiterung der BPEL Engine oder Middleware nötig



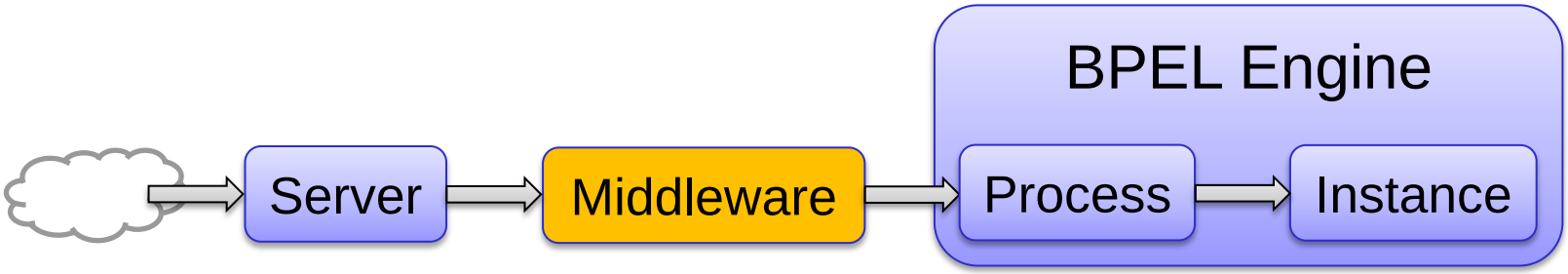
Authorization (1)

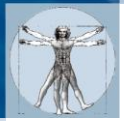
- Instance Authorization
  - Imperativ: bei einer Aktivität
  - Deklarativ : vor einer Aktivität
  - Vorteile
    - Größtmöglichste Flexibilität (imperativ)
    - Keine unnötigen Prozessinstanzen (deklarativ)
  - Nachteile
    - Vermischung von Prozesslogik und Sicherheitslogik
    - Unnötige Prozessinstanzen (imperativ)
    - Viele Erweiterungsattribute (deklarativ)



Authorization (2)

- Middleware Authorization
  - Middleware als PEP erstellt Decision Request (z.B. in XACML)
  - Authentication Service als PDP
  - Vorteile
    - Trennung von Sicherheitslogik und Prozesslogik
    - Wiederverwenden von Sicherheitsanforderungen (Policies)
    - Keine unnötigen Prozessinstanzen
  - Nachteile
    - Kein Zugriff auf Prozessinformationen bei der Autorisierung





END OF DOCUMENT