Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Sicherheitskonzepte in SOA auf Basis sicherer Webservices

Thies Rubarth

Agenda

What's going on...

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Service Oriented Architecture
- Sicherheitsanforderungen
- Sicherheitskonzepte
- Sichere Webservices
- Ausblick Masterthesis

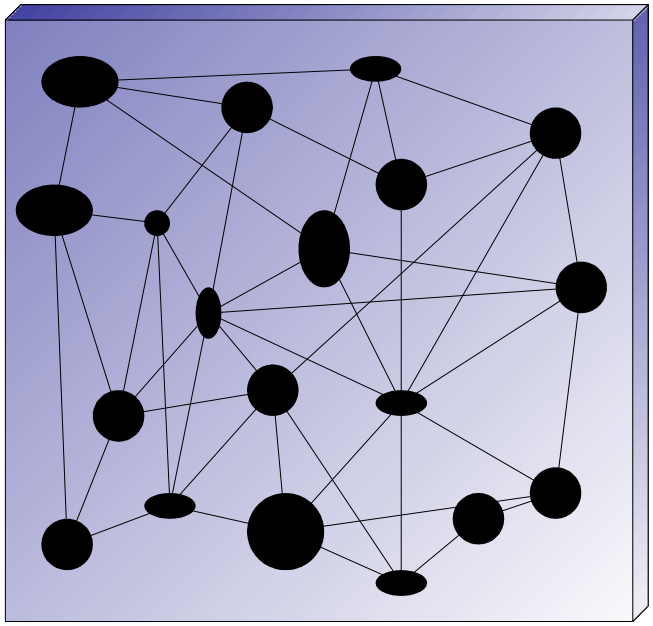
Agenda

Wo sind wir eigentlich?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- **Service Oriented Architecture**
- Sicherheitsanforderungen
- Sicherheitskonzepte
- Sichere Webservices
- Ausblick Masterthesis

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



Benutzerschnittstelle

Monolithische Anwendung

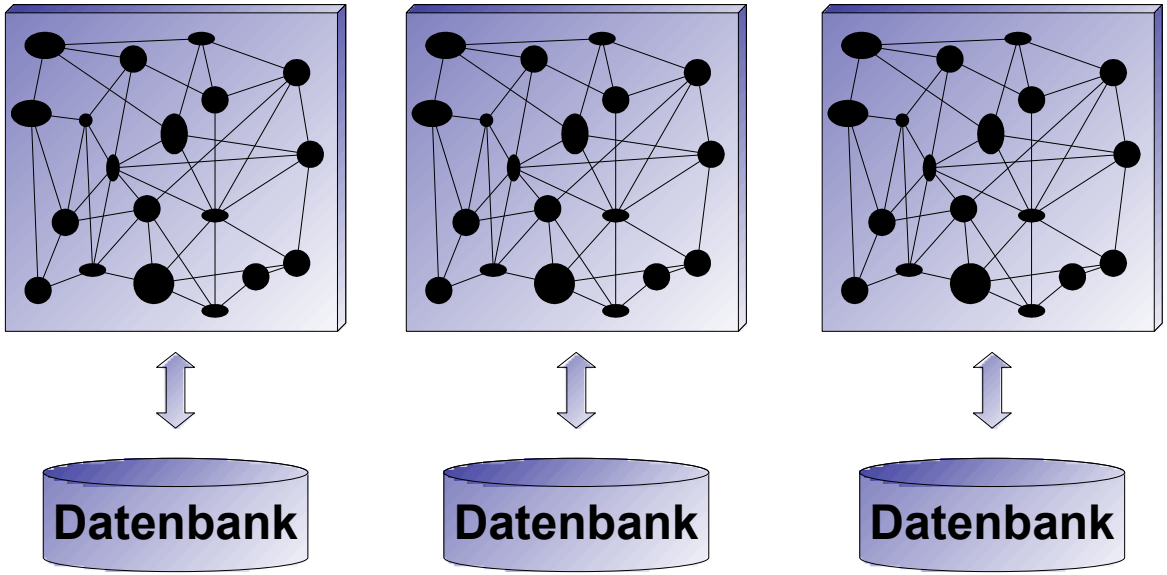
Daten in Dateien

- Monolithisches System
  - Schlechte Wartbarkeit
  - Logik & Daten eng miteinander verknüpft
  - Schnittstellen: Dateiexport

Service Oriented Architecture

... aber der Monolith brachte Probleme ...

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



Benutzerschnittstelle

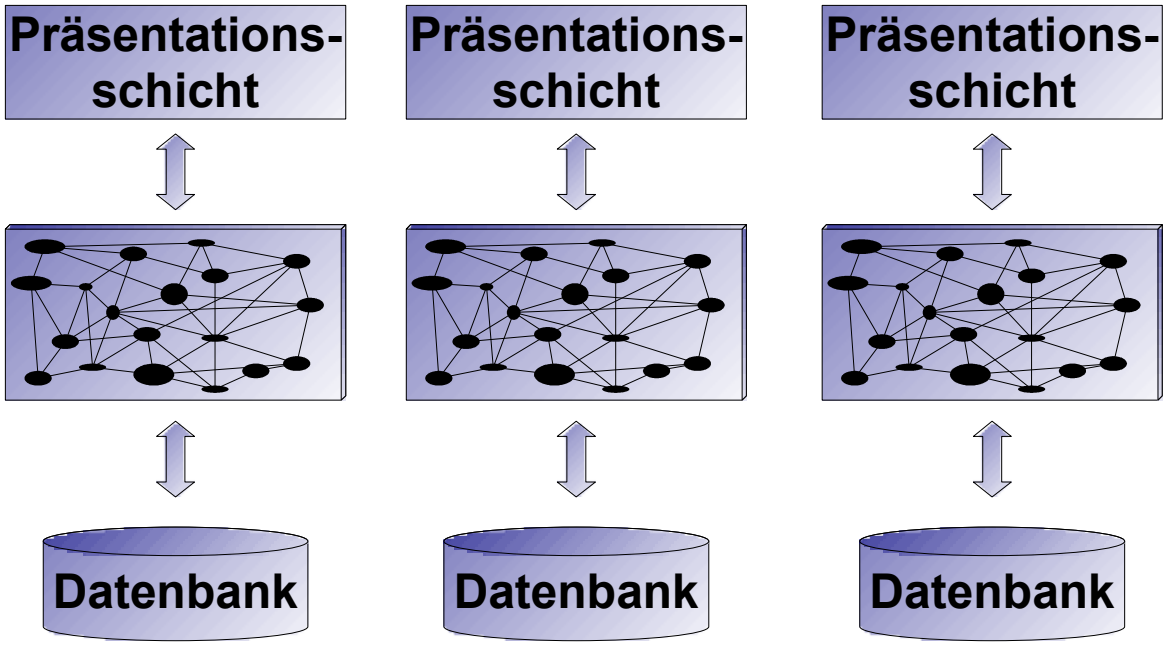
Monolithische Anwendung

- Zwei-Schicht-Architektur
  - Trennung von Daten und Logik
  - Schnittstellen auf Datenebene möglich
  - Enge Koppelung

Service Oriented Architecture

... die Drei-Schichten-Architektur schien perferkt ...

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



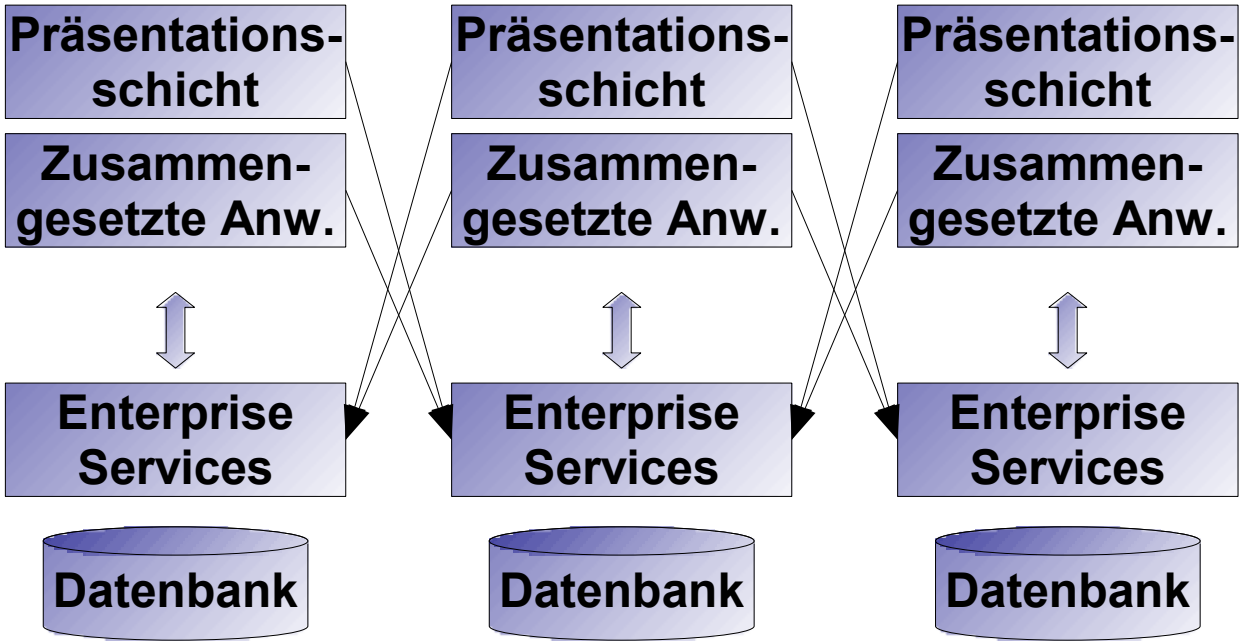
Monolithische Anwendung

- Drei-Schichten-Architektur
  - Trennung von Anwendungslogik und UI
  - Schnittstellen weiterhin durch enge Koppelung

Service Oriented Architecture

... aber die Koppelung musste weiter gelöst werden ...

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



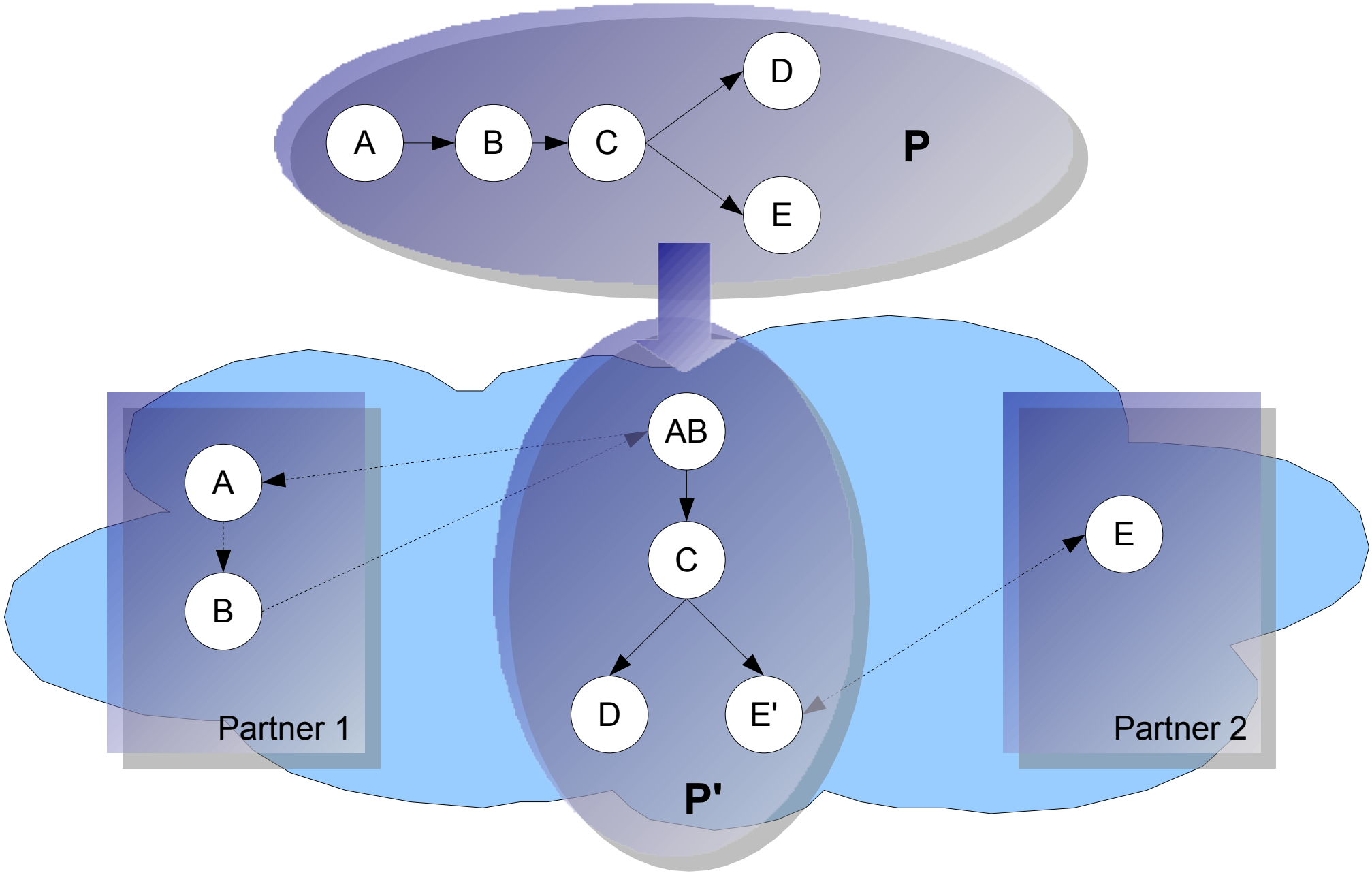
- Service Oriented Architecture
  - Lose Koppelung
  - Einfache Wiederverwendung von Komponenten

Service Oriented Architecture

... nur wozu das ganze?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- IT muss sich schnell und flexibel an neue Geschäftsanforderungen anpassen
- Einfaches einbinden von Alt-Systemen
- Heterogene IT-Landschaften fordern einfache Schnittstellen
- Entstehung von virtuellen Unternehmen


A
B
C
D
E
P
AB
C
D
E'
P'
A
B
Partner 1
E
Partner 2

- Webservices
  - Softwarekomponente, die über ein Netzwerk von anderen Anwendungen aufgerufen werden kann
  - Maschinenlesbar beschriebene Schnittstelle
  - Kommunikation über Internet-Standardprotokolle
    - HTTP als Transportprotokoll
    - Nachrichten im XML-Format (SOAP)

- Offene Infrastruktur
  - Leichtes abfangen der ausgetauschten Nachrichten
  - Viele potentielle Angreifer
- Unternehmensübergreifende Kommunikation
  - Größerer Sicherheitskontext
  - Neue Vertrauensmodelle werden benötigt

Agenda

Wo sind wir eigentlich?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Service Oriented Architecture
- **Sicherheitsanforderungen**
- Sicherheitskonzepte
- Sichere Webservices
- Ausblick Masterthesis

Sicherheitsanforderungen

Schutzbedarf

- Verstoß gegen Gesetze oder Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Auswirkungen
- Finanzielle Auswirkungen

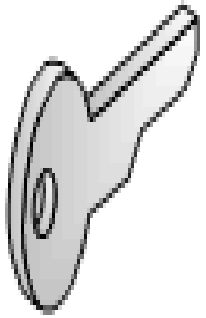
Sicherheitsanforderungen

Was braucht man für Schutz?

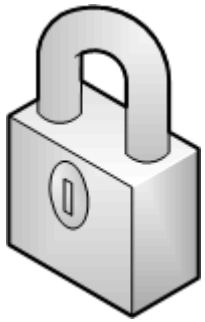
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Vertraulichkeit

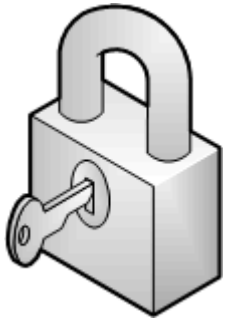
Authentifikation



Integrität



Autorisierung



Agenda

Wo sind wir eigentlich?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Service Oriented Architecture
- Sicherheitsanforderungen
- **Sicherheitskonzepte**
- Sichere Webservices
- Ausblick Masterthesis

Sicherheitskonzepte

Wie erreicht man Sicherheit?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

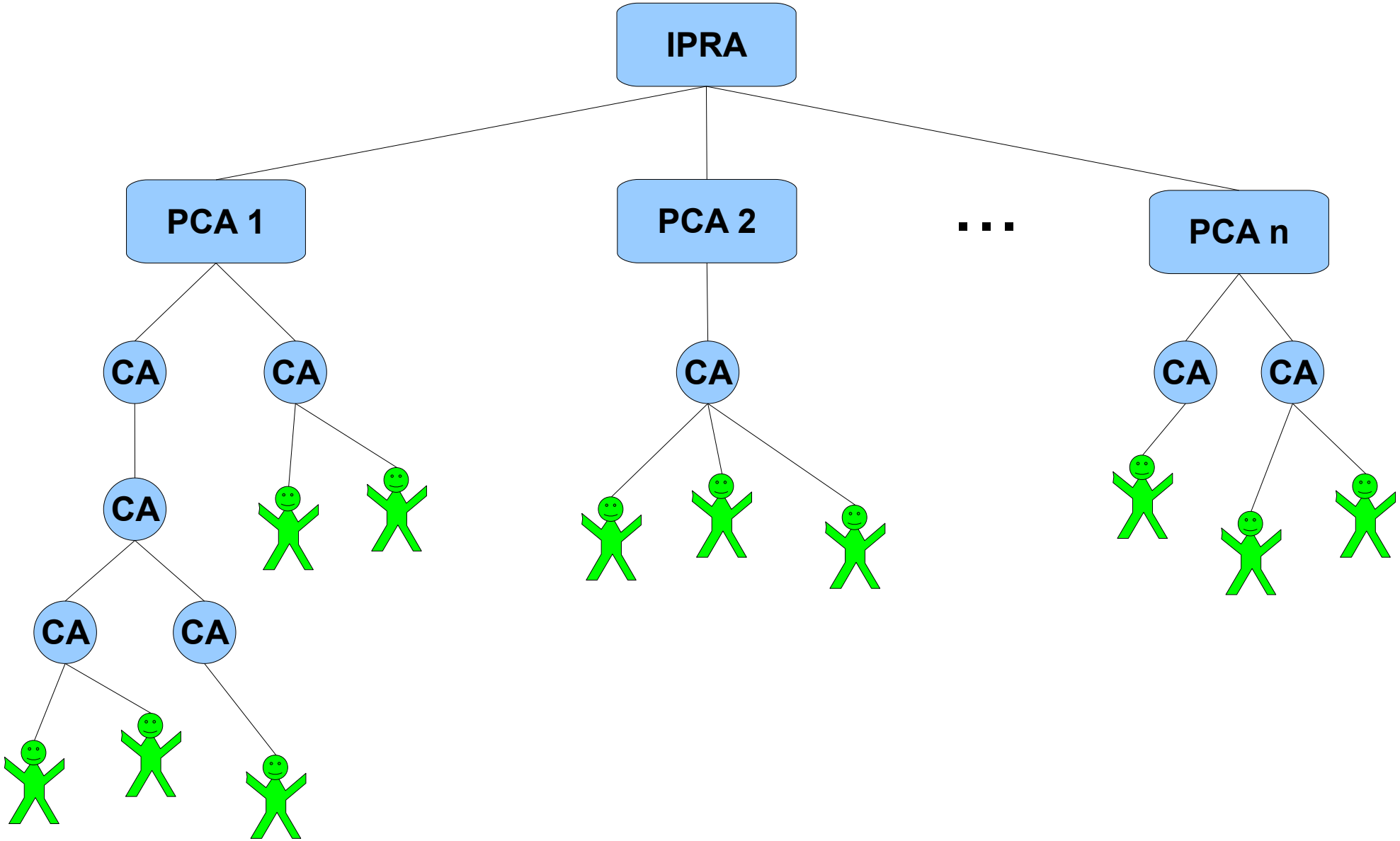
- Verschlüsselung
- Signierung
- Vertrauensmodelle
  - Public Key Infrastruktur
  - Kerberos

- Trust Center stellt Zertifikate aus
- Zertifikate binden öffentlichen Schlüssel an juristische oder natürliche Person
- Öffentlicher Schlüssel kann für verschiedene Zwecke autorisiert werden
  - Verschlüsseln
  - Signieren
  - Zertifizieren

Sicherheitskonzepte

Hierarchie von Zertifiierungsstellen

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

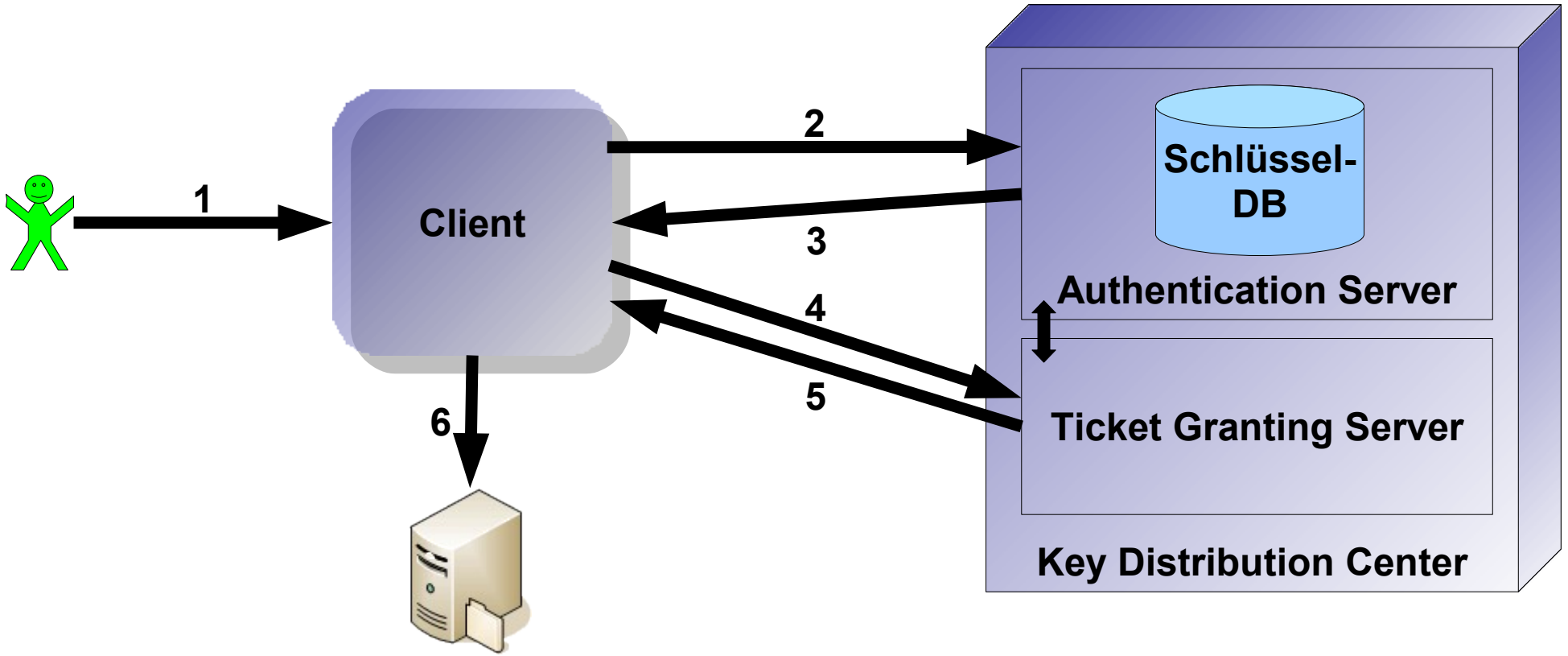


- Authentifikation über vertrauenswürdigen Server
- Key Distribution Center stellt Tickets aus
  - Initialticket durch Authentication Server
  - Tickets für Dienste innerhalb des Realms durch Ticket Granting Server
- Wechseln in andere Realms durch Ticketforwarding
  - Hierarchie von KDCs

Sicherheitskonzepte

Ablauf von Kerberos

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



1) Login mit Passwort
2) Anforderung des Initialtickets für den TGS
3) Auslieferung des Inititialtickets
4) Anforderung des Tickets für den Serverzugriff
5) Auslieferung des Tickets für den Serverzugriff
6) Serverzugriff

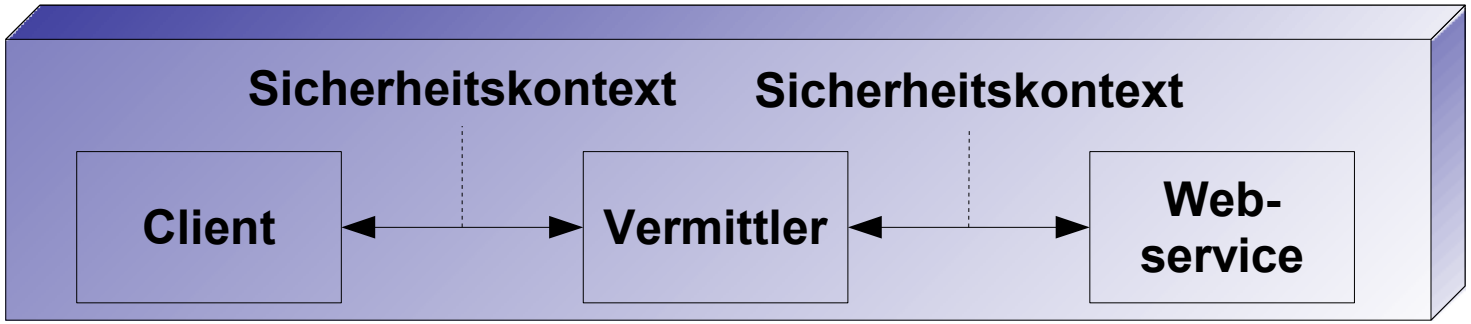
Agenda

Wo sind wir eigentlich?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Service Oriented Architecture
- Sicherheitsanforderungen
- Sicherheitskonzepte
- **Sichere Webservices**
- Ausblick Masterthesis

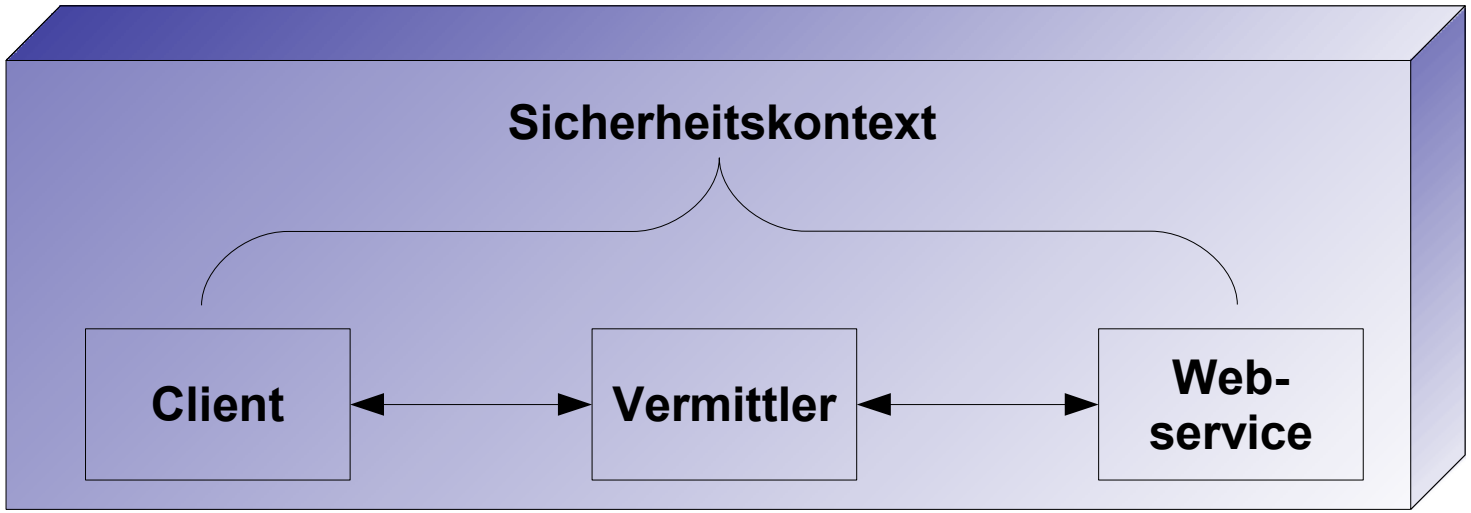
- HTTPS mit Secure Socket Layer (SSL)
  - Authentifikation des Clients und des Servers möglich
  - Verschlüsselung der Daten sichert Vertraulichkeit und Integrität
  - Sicherheitskontext nur zwischen zwei direkt kommunizierenden Partnern möglich



- WS-*-Spezifikationen für sichere Webservices
  - WS-Policy, WS-SecurityPolicy
  - WS-Security
  - WS-Trust
  - WS-SecureConversation
  - WS-Federation
  - Noch unveröffentlicht
    - WS-Privacy
    - WS-Authorization

- WS-Policy
  - Beschreiben von Anforderungen für einen Webservice
  - Verschachteln von Anforderungen
- WS-SecurityPolicy
  - Erweitern von WS-Policy für WS-Security, WS-Trust und WS-SecureConversation

- WS-Security
  - Definition von Security-Tokens
    - Benutzerinformation
    - Verschlüsselte Daten (XML Encryption)
    - Signierte Daten (XML Signature)
  - Sicherheitskontext zwischen Endknoten



- WS-Trust
  - Erzeugen von Vertrauen durch Security Tokens
  - Protokoll für
    - Anfordern von Tokens
    - Erstellen von Tokens
    - Austauschen von Tokens
  - Beispiele für Tokens
    - UsernameToken
    - X509Token
    - KerberosToken
    - ...

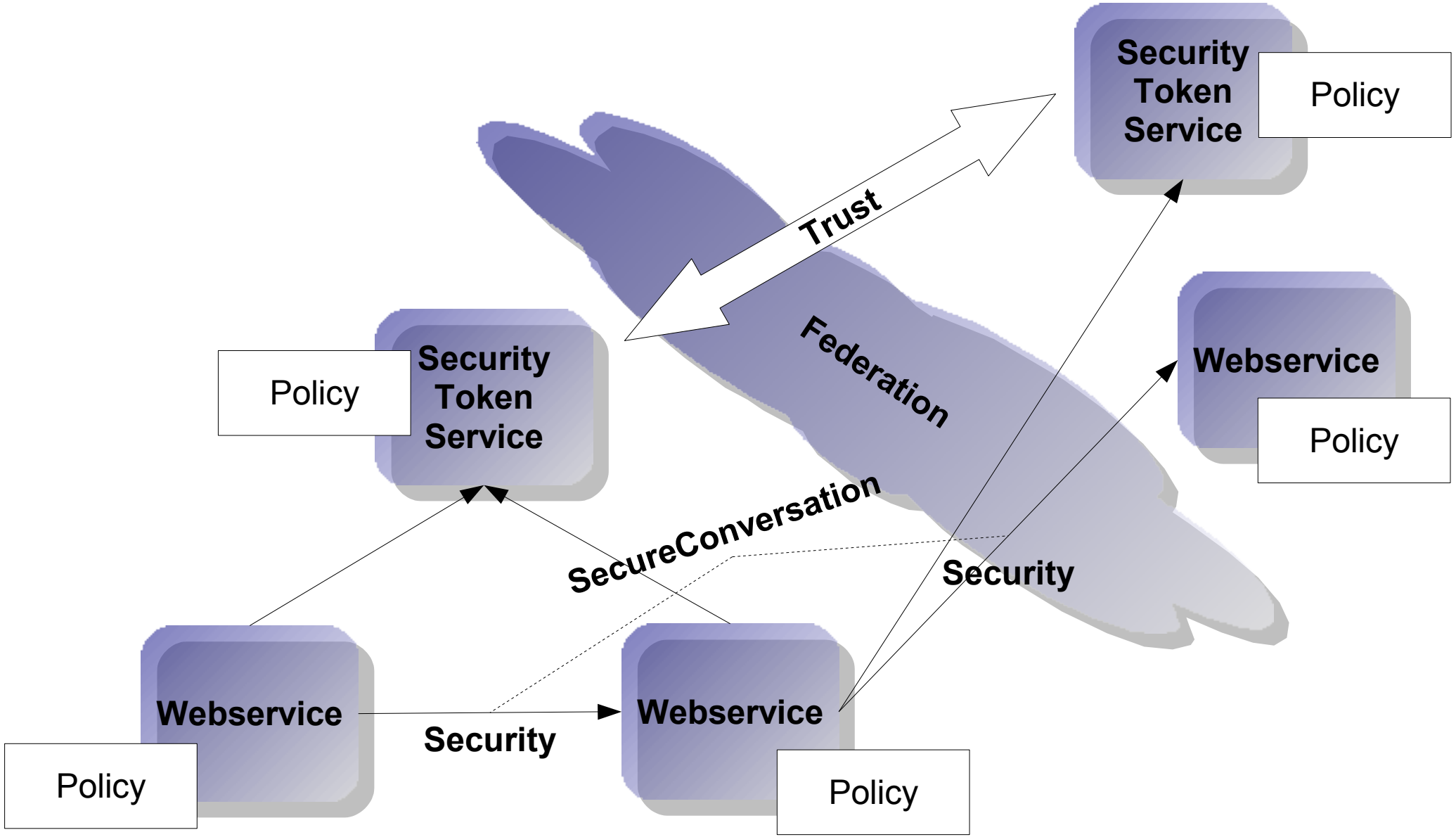
- WS-SecureConversation
  - Sichere Kommunikation über mehrere Webservice-Aufrufe
  - Sicherheitskontext
    - Erstellen
    - Erweitern
    - Ableiten von Schlüsseln zum Signieren oder Verschlüsseln

- WS-Federation
  - Ermöglicht Authentifiaktion und Autorisierung über mehrere „Realms“
  - Modell zur Kombination von WS-Security, WS-Trust und WS-Policy

Sichere Webservices

The Big WS-* Picture

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences



Agenda

Wo sind wir eigentlich?

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

- Service Oriented Architecture
- Sicherheitsanforderungen
- Sicherheitskonzepte
- Sichere Webservices
- **Ausblick Masterthesis**

Ausblick Masterthesis

Und nun?

- Das Big-Picture im Detail
  - Vertrauensmodell
  - Konfigurieren statt implementieren
  - Machbarkeit durch Prototyp(en) untersuchen
  - Skalierbarkeit
- Risiken
  - Riesige Menge an Spezifikationen und Unterspezifikationen
  - Es gibt keine (oder kaum) Praxiserfahrung in dem Gebiet

Literatur

Was man lesen sollte...

[1] Dan Woods – **Enterprise Service Architecture** – O'Reilly 2003

[2] Thomas Erl – **Service-Oriented Architecture** – Prentice Hall PTR 2005

[3] Sanjiva Weerawarana et. al. - **Web Services Plattform Architecture** – Prentice Hall PTR 2005

[4] Prof. Dr. Claudia Eckert – **IT-Sicherheit** (Studienausgabe) – Oldenbourg 2005

[5] Siddharth Bajaj et. al. - **Web Service Policy** - BEA, IBM, Microsoft, SAP, Sonic Software, VeriSign September 2004

[6] Giovannis Della-Libera et. al. - **Web Services Security Policy Language** – IBM, Microsoft, RSA, Versign Juli 2005

[7] Nadalin Antony et. al. - **Web Services Security: SOAP Message Security 1.1** – Oasis Nobember 2005

[8] Steve Anderson et. al. - **Web Services Trust Language** – IBM, Microsoft, Actional, BEA, Computer Associates, Layer 7, Oblix, OpenNetwork, Ping Identity, Reactivity, Verisign Februar 2005

[9] Siddharth Bajaj et. al. - **Web Services Federation Language** – BEA, IBM, Microsoft, RSA, Verisign Juli 2003

[10] Steve Anderson et. al. - **Web Services Secure Conversation Language** - IBM, Microsoft, Actional, BEA, Computer Associates, Layer 7, Oblix, OpenNetwork, Ping Identity, Reactivity, Verisign Februar 2005