Technische Universität Kaiserslautern
Lehrgebiet Datenverwaltungssysteme

Seminar: *Grundlagen webbasierter Informationssysteme*

Thema: ***Trust, Reputation, Privacy***

Bearbeiter:
Rafael Schirru

Betreuer:
Prof. Dr. Ing. Stefan Deßloch

Kaiserslautern, den 09.07.2004

Motivation:

Trust:

- Fehlender persönlicher Kontakt zwischen Geschäftspartnern im Internet
  → Methoden zur Etablierung von Vertrauen werden benötigt
- Trust und Trust Management als Elemente der Entscheidungsgrundlage

Reputation:

- Bewertung der Zuverlässigkeit von Agenten
- Minimierung des Risikos betrügerischer Geschäftsabschlüsse

Privacy:

- Welche Informationen werden bei der Nutzung eines Dienstes preisgegeben?
- Wer erhält Zugang zu den persönlichen Informationen?
  → Benutzer soll selbst entscheiden können, welche persönlichen Informationen er bekannt geben möchte

Gliederung:

1. Trust
    1.1. Trust Management
    1.2. WS-Trust
    1.3. WS-Federation

2. Reputation
    2.1. Interpretationen und Klassifikation
    2.2. Das eBay-Reputationssystem
    2.3. Der EigenTrust-Algorithmus

3. Privacy
    3.1. Der P3P-Standard
    3.2. Privacy bei Web Services

Gliederung:

1. Trust
    - 1.1. Trust Management
    - 1.2. WS-Trust
    - 1.3. WS-Federation

2. Reputation
    - 2.1. Interpretationen und Klassifikation
    - 2.2. Das eBay-Reputationssystem
    - 2.3. Der EigenTrust-Algorithmus

3. Privacy
    - 3.1. Der P3P-Standard
    - 3.2. Privacy bei Web Services

1.1. Trust Management

Motivation:

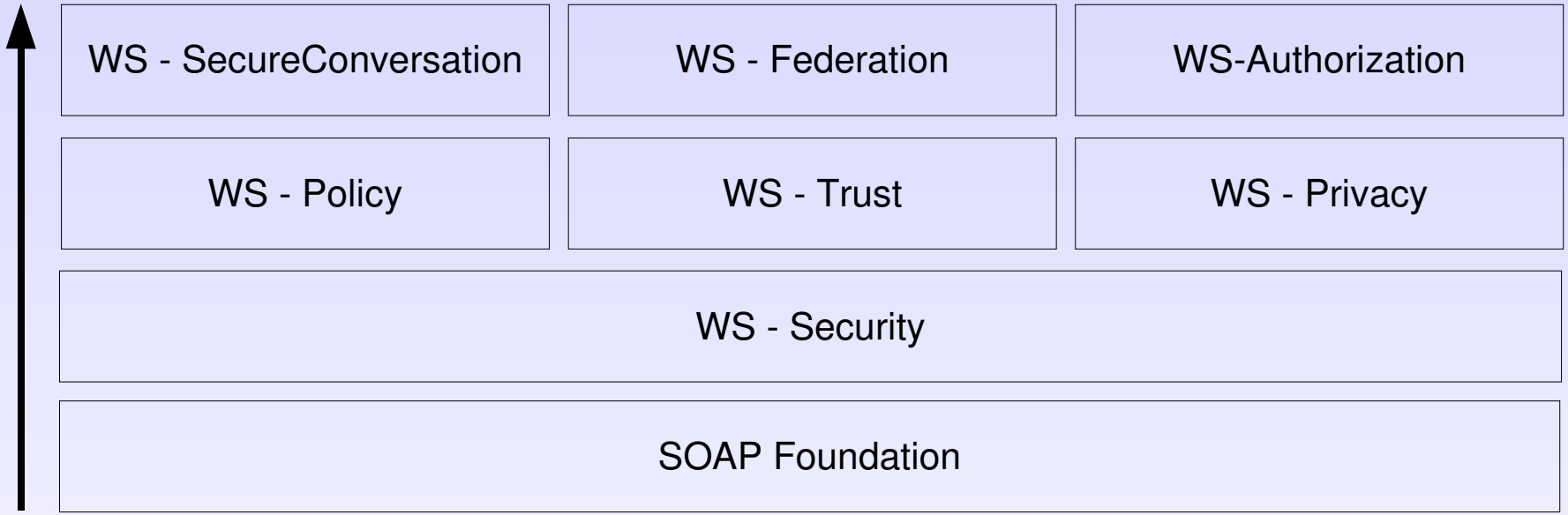
- Individuelle Sicherheitsbedürfnisse der Benutzer und Web Services sollen berücksichtigt werden
- Interoperabilität für Anwendungen in heterogenen Systemen
  - → die vorhandenen Sicherheitstechnologien der Organisationen sollen weiterhin benutzbar sein

Definition:

„A unified approach to specifying and interpreting security policies, cedentials, relationships which allow direct authorisation of security-critical actions.“ (Blaze et. al.)

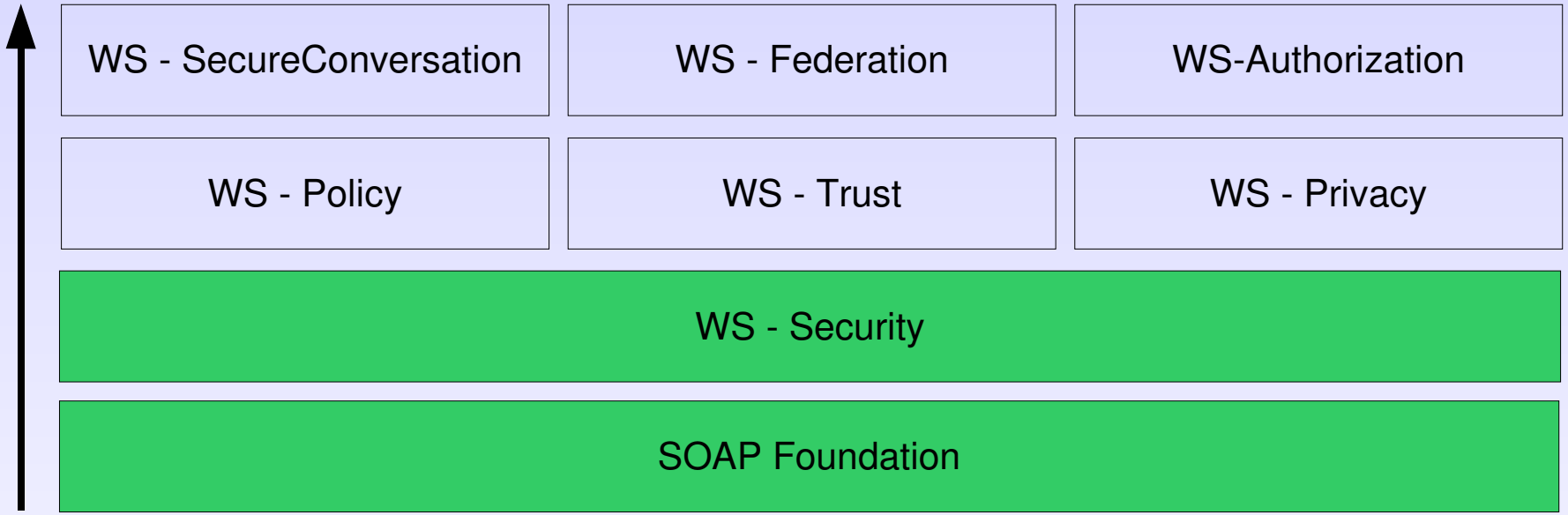
1.1. Trust Management

Einordnung: WS-Security-Spezifikation



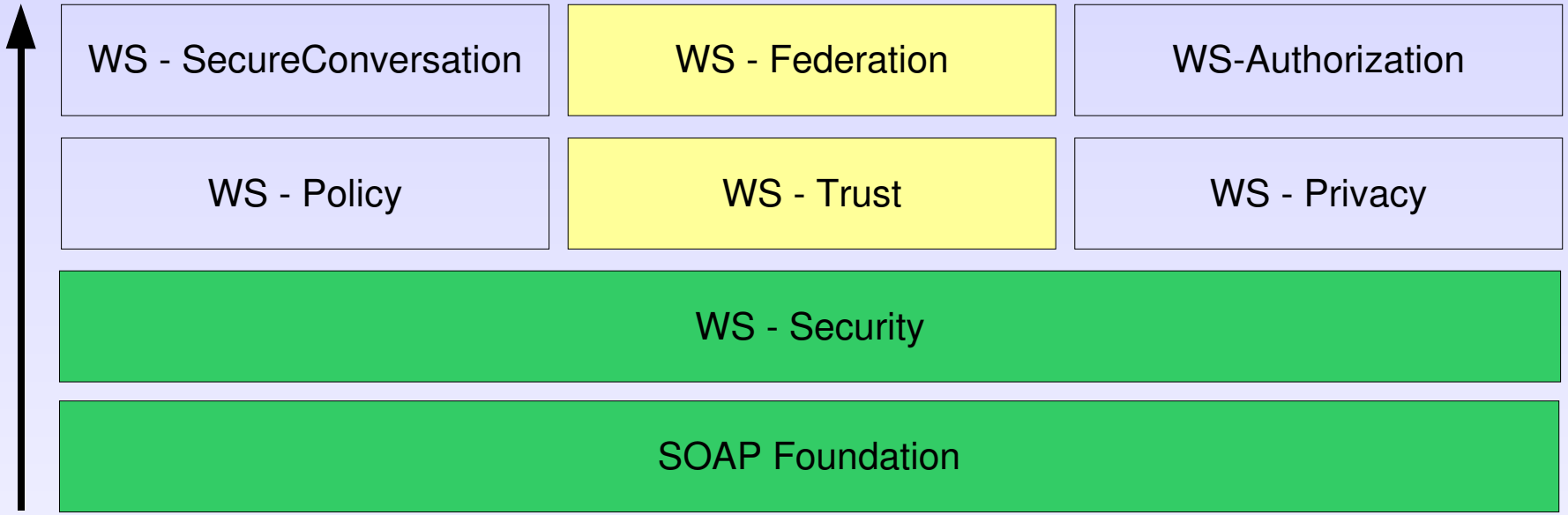
1.1. Trust Management

Einordnung: WS-Security-Spezifikation



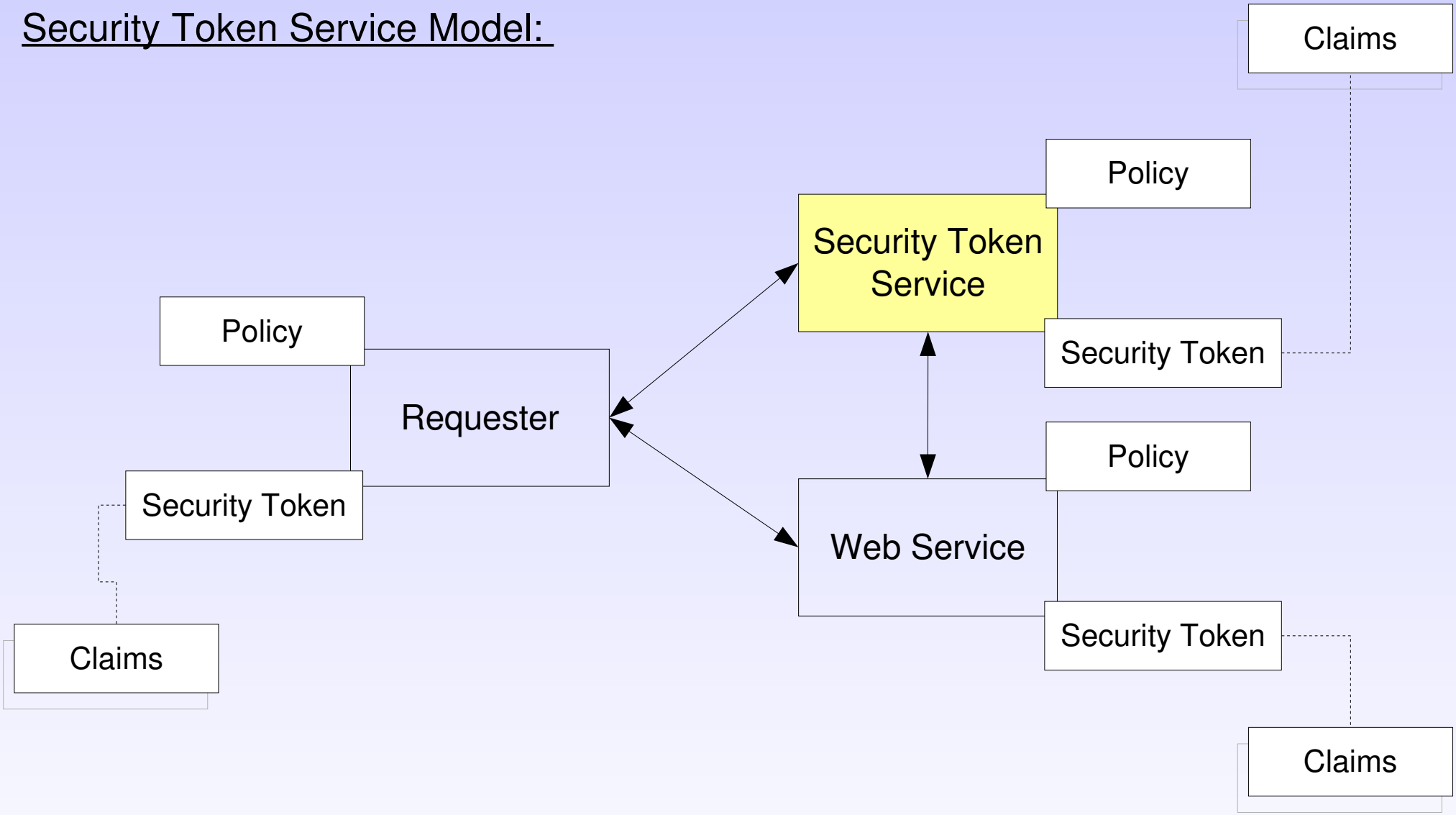
1.1. Trust Management

Einordnung: WS-Security-Spezifikation



1.1. Trust Management

Security Token Service Model:



1.2. WS-Trust

Etablierung direkter Trust-Beziehungen mittels:

A: Benutzername und Passwort unter Verwendung von TLS
B: Security Token zu denen direktes Vertrauen besteht

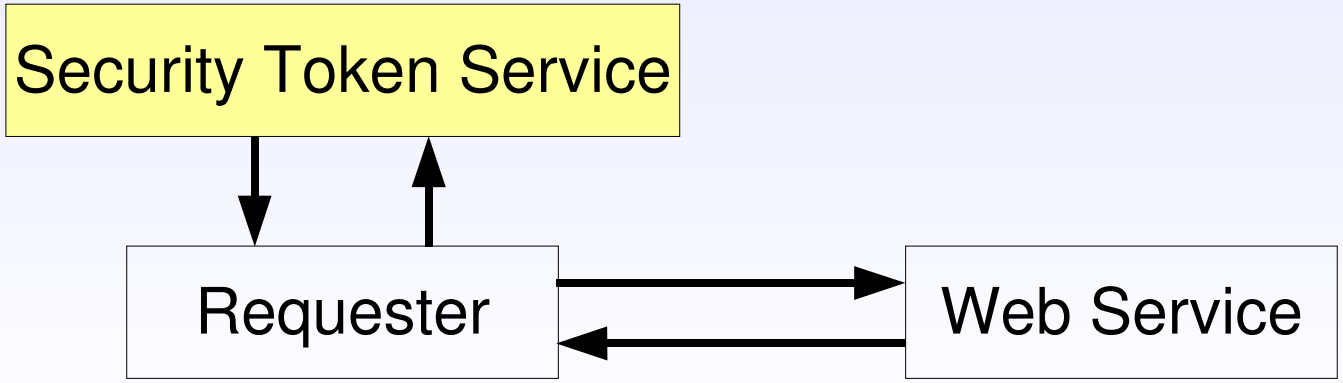
1.2. WS-Trust

Etablierung direkter Trust-Beziehungen mittels:

A: Benutzername und Passwort unter Verwendung von TLS
B: Security Token zu denen direktes Vertrauen besteht

Etablierung vermittelter Trust-Beziehungen mittels:

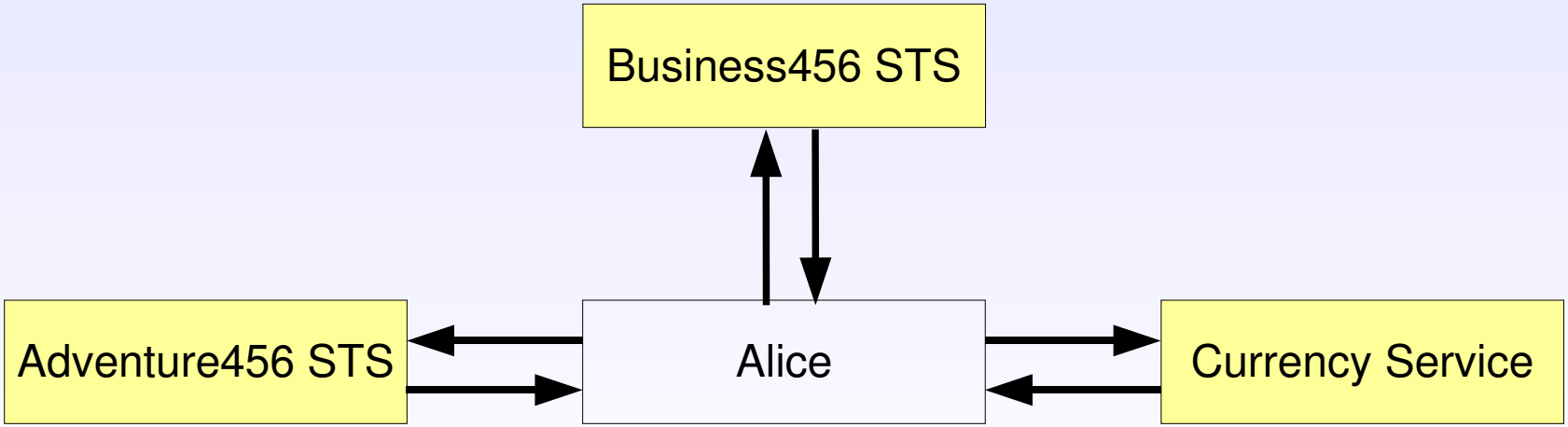
Authentisierung durch eine vertrauenswürdige Instanz



1.3. WS-Federation

Trust-Bündnis mittels Austausch von Security Token:

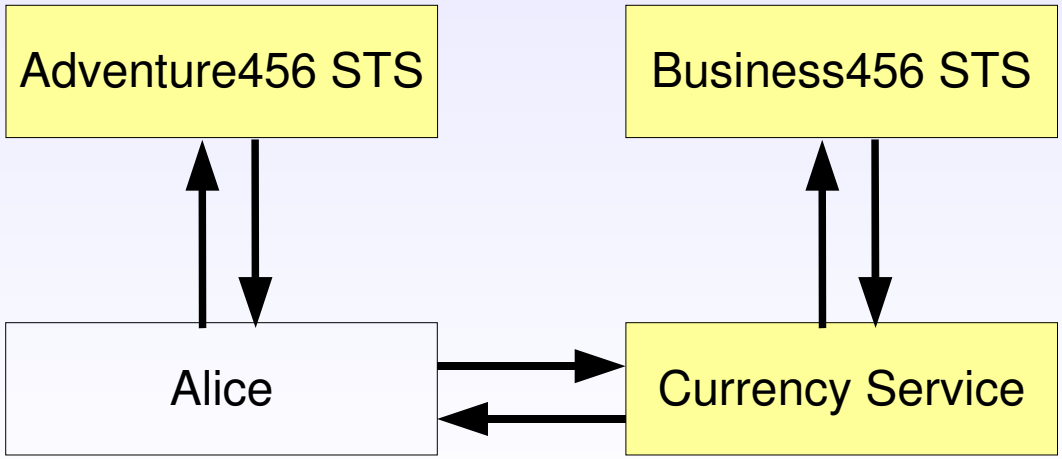
- Alice besitzt ein Adventure456 Security Token mit Angaben zu ihrer Identität
- Alice möchte den Währungs-Web-Service von Business456 nutzen
- *Der Währungs-WS akzeptiert nur Security Token, die von Business456 herausgegeben wurden*



1.3. WS-Federation

Trust-Bündnis mittels einer Trust-Kette:

- Alice besitzt ein Adventure456 Security Token mit Angaben zu ihrer Identität
- Alice möchte den Währungs-Web-Service von Business456 nutzen
- *Der Währungs-WS akzeptiert beliebige Security Token, die Anfrage wird jedoch erst bearbeitet, wenn der WS für das erhaltene Security Token ein Business456 Security Token erhalten konnte*



Gliederung:

1. Trust
    1.1. Trust Management
    1.2. WS-Trust
    1.3. WS-Federation

2. Reputation
    2.1. Interpretationen und Klassifikation
    2.2. Das eBay-Reputationssystem
    2.3. Der EigenTrust-Algorithmus

3. Privacy
    3.1. Der P3P-Standard
    3.2. Privacy bei Web Services

2.1. Interpretationen und Klassifikation

Allgemeines Verständnis der Reputation:

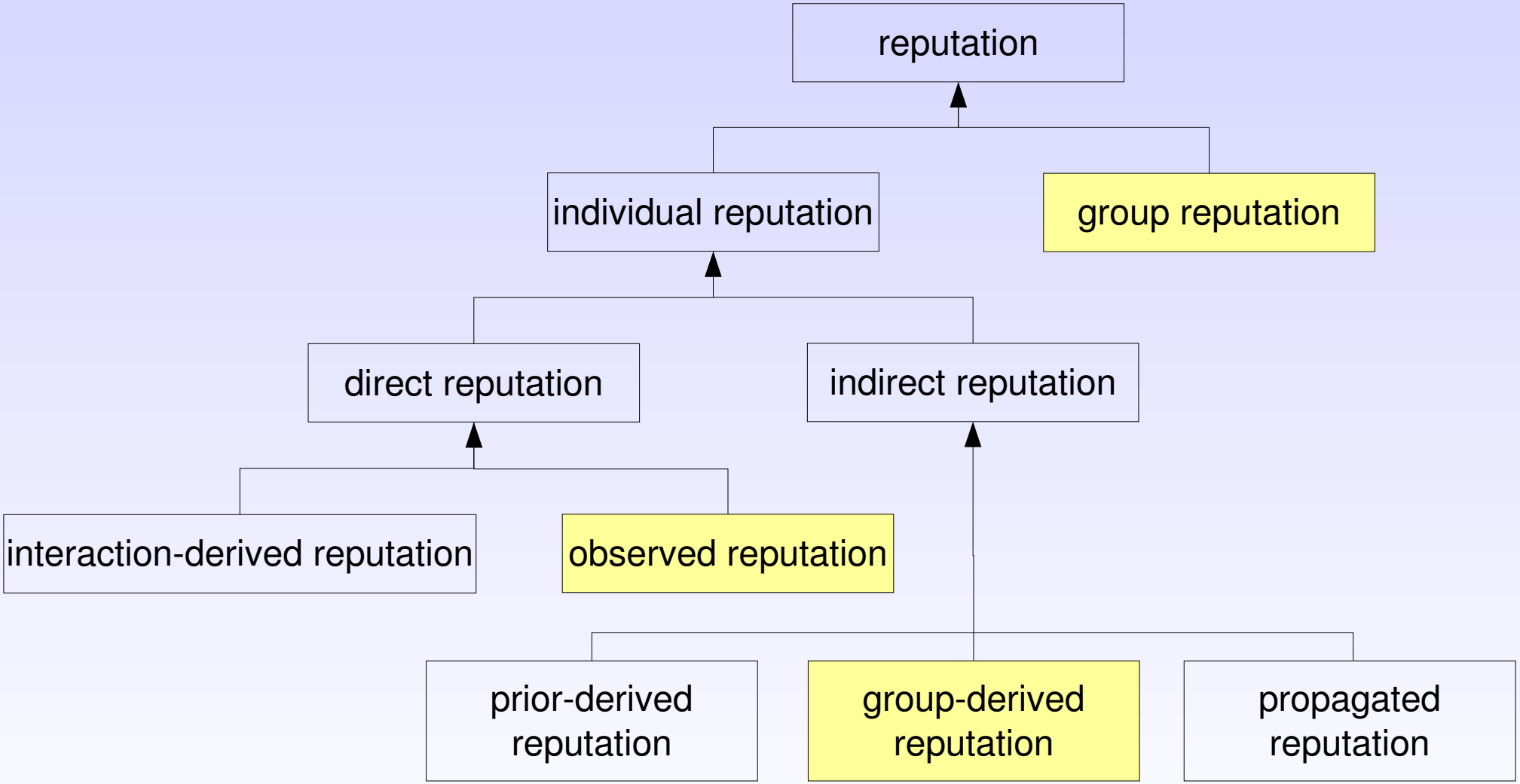
„Reputation refers to a perception that an agent has of another's intentions and norms“

Unterschiedliche Interpretationen von Reputation in der Informatik:

- Bewertungen, welche Agenten in Online-Communities von anderen Agenten erhalten (Zacharia und Maes (1999))
- „opinion or view of one about something“, berücksichtigt die individuelle, soziale und ontologische Reputation (Sabater, et al. (2001))
- Statistische Modelle: verwenden gewichtete, propagierte Reputationswerte der Nachbaragenten von Agenten, welche Bewertungen vornehmen (Mui, et al. (2001) und Yu, et al.(2001))

2.1. Interpretationen und Klassifikation

Hierarchische Reputationsklassifikation:



2.2. Das eBay-Reputationssystem

Zweck eines Reputationssystems:

- Entscheidungsgrundlage über Geschäftsbeziehungen zwischen gegenseitig unbekannten Geschäftspartnern

Arbeitsweise eines Reputationssystems:

Feedback über das Verhalten der Benutzer wird

- gesammelt
- aggregiert
- verbreitet

→ den Auswirkungen vergangener Transaktionen soll Relevanz für die Zukunft verliehen werden

2.2. Das eBay-Reputationssystem

Auftretende Probleme,

1. beim Sammeln der Information:
   - fehlende Motivation zum Ausfüllen der Formulare nach erfolgreichen Interaktionen
   - negatives Feedback ist schwierig zu entlocken
   - unehrliche Bewertungen

2. beim Aggregieren der Information:
   - keine Differenzierung zwischen Bewertungen von Agenten mit hoher bzw. niedriger Reputation
   - der Wert des Gegenstandes der Transaktion wird nicht berücksichtigt

3. beim Verbreiten der Information:
   - Möglichkeit der Namensänderung ist problematisch
   - mangelnde Portabilität zwischen den Reputationssystemen

2.3. Der EigenTrust-Algorithmus

Motivation:

Den Vorteilen von P2P-Filesharing-Netzwerken stehen einige Nachteile im Hinblick auf Sicherheit entgegen.

Anforderungen an das Trust Management im dezentralen Informationssystem:

- Bestimmung des globalen Trust-Modells, welches beschreibt, ob ein Agent vertrauenswürdig ist
- Definition eines lokalen Algorithmus zur Bestimmung von Trust
- Daten- und Kommunikationsmanagement: eine erweiterbare Implementierung soll erzielt werden

Idee:

- für jeden im Netzwerk befindlichen Peer i ist ein verteilt berechneter globaler Trust-Wert zu bestimmen
- Trust-Wert spiegelt die Erfahrungen der übrigen Peers mit i wider
- böswillige Peers sollen identifiziert und aus dem Netzwerk isoliert werden

2.3. Der EigenTrust-Algorithmus

Arbeitsweise:

- Peer i lädt eine Datei von Peer j und bewertet anschließend die Transaktion:

$$tr_{ij} = 1 \quad bzw. \quad tr_{ij} = -1$$

- Berechnung des lokalen Trust-Wertes des Peers i für Peer j:

$$s_{ij} = \sum tr_{ij}$$

- Berechnung des normalisierten Trust-Wertes des Peers i für Peer j:

$$c_{ij} = \frac{max(s_{ij},\ 0)}{\sum_{j} max(s_{ij},\ 0)}$$

- Berechnung des aggregierten Trust-Wertes des Peers i für Peer k:

$$t_{ik} = \sum_{j} c_{ij} c_{jk}$$

2.3. Der EigenTrust-Algorithmus

- Sei C die Matrix $[c_{ij}]$ und t_i der Vektor mit den Werten t_{ik}, so gilt:

$$t_i = C^t c_i$$

- Reputationswerte der Nachbarn der Nachbarn, etc. sollen mit einbezogen werden
- Trust-Vektoren t_i konvergieren gegen den Eigenvektor von C
  → t ist globaler Trust-Vektor

Der Algorithmus (ohne Berücksichtigung von Verteilungsaspekten) sieht dann wie folgt aus:

$$t^{(0)} = e;$$

$$repeat$$

$$\quad t^{(k+1)} = C^T t^{(k)};$$

$$\quad \delta = \| t^{(k+1)} - t^{(k)} \|;$$

$$until\,(\delta < \epsilon)$$

2.3. Der EigenTrust-Algorithmus

Zusammenfassung:

- Es wird ein globaler Trust-Wert für Peers berechnet
  → unter dessen Verwendung wird der Einfluss böswilliger Peers in P2P-Netzen minimiert

- Die Implementierung des Algorithmus ist erweiterbar und verteilt realisierbar

- Es kann empirisch nachgewiesen werden, dass die Anzahl an Downloads fehlerhafter Dateien in verschiedenen Threat-Szenarien sinkt

Gliederung:

1. Trust
    1.1. Trust Management
    1.2. WS-Trust
    1.3. WS-Federation

2. Reputation
    2.1. Interpretationen und Klassifikation
    2.2. Das eBay-Reputationssystem
    2.3. Der EigenTrust-Algorithmus

3. Privacy
    3.1. Der P3P-Standard
    3.2. Privacy bei Web Services

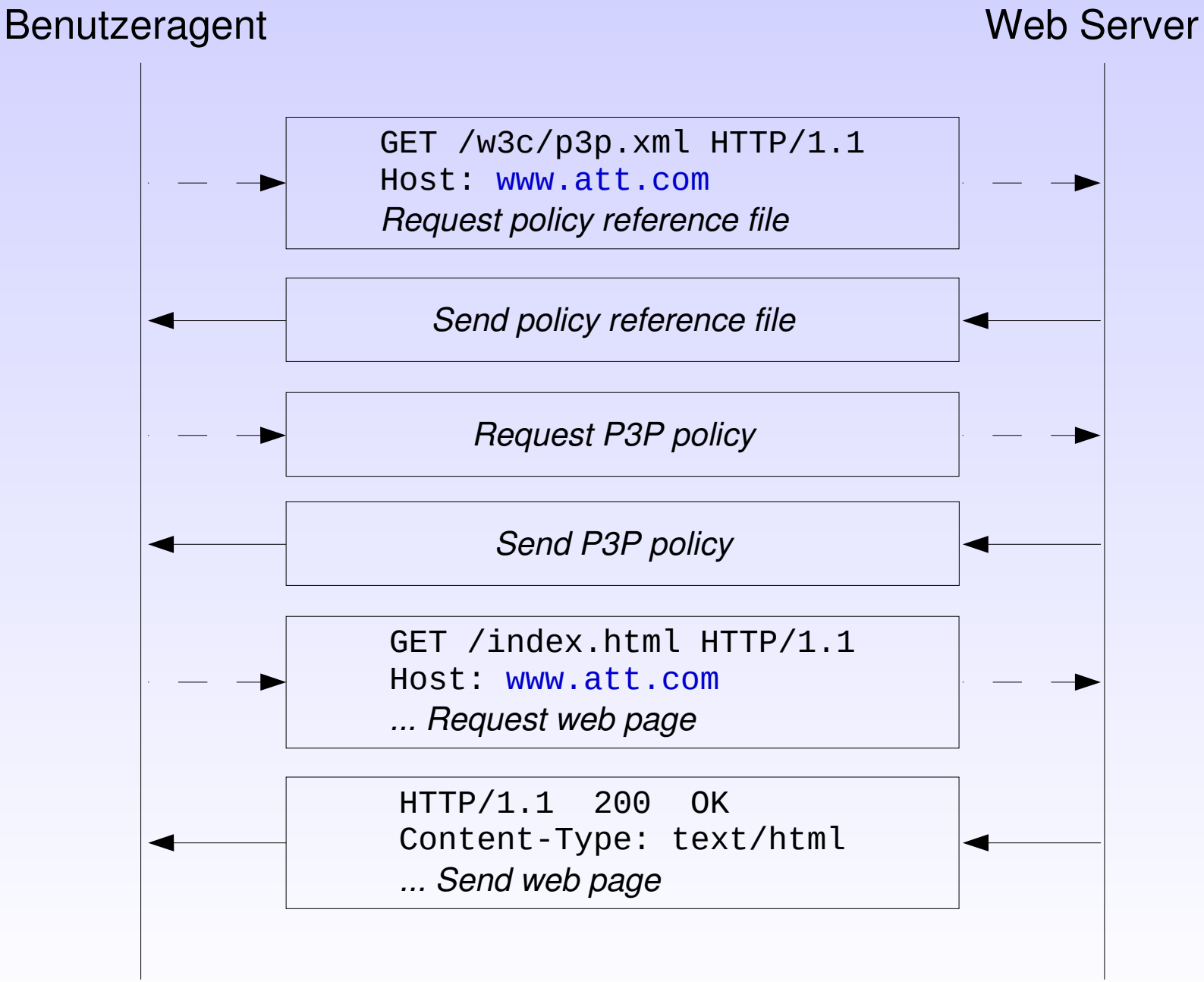
3. Der P3P-Standard

Motivation:

- Webseiten sammeln persönliche Informationen mittels Cookies
- Dienstanbieter geben über Privacy Policies bekannt, wie sie mit den persönlichen Informationen der Dienstnutzer umgehen
- Erhöhter Informationsbedarf der Dienstnutzer über die Privacy Policies der Dienstanbieter
  → P3P-Standard ermöglicht die automatische Verarbeitung der Privacy Policies durch den Computer

→ Entscheidungsgrundlage über den Austausch persönlicher Daten

3. Der P3P Standard



3. Der P3P-Standard

Gründe für den Einsatz von P3P:

- Dienstanbieter signalisieren, dass sie die Privacy-Bedürfnisse ihrer Kunden respektieren
  → Aufwertung der eigenen Marke

- Dienstanbieter erwarten, dass P3P ein Standard sein wird, dem Kunden Bedeutung beimessen werden

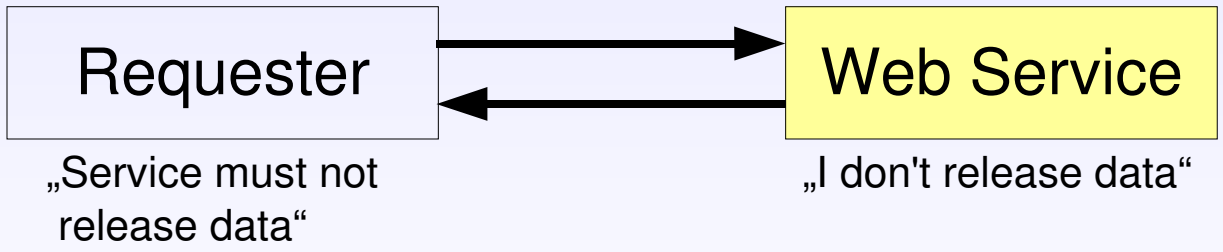
- Webseiten, die den P3P-Standard nicht erfüllen, können auf neuen Browsern teilweise nicht korrekt angezeigt werden

3.2. Privacy bei Web Services

Grundlegende Privacy-Fragen werden durch die Privacy Statements in der Service Policy geklärt.

Beispiel:

- Ein Agent beschreibt seine Privacy-Bedürfnisse
- Der Agent möchte einen Kalender-Web-Service nutzen
- Der Kalender-WS beschreibt seine Privacy Practice Rules
- Der Web Service vergleicht die Privacy-Bedürfnisse des Agenten mit seinen Privacy Practice Rules und entscheidet dann, ob die Nutzung seines Dienstes für den Agenten zulässig ist



Technische Universität Kaiserslautern
Lehrgebiet Datenverwaltungssysteme

Seminar: *Grundlagen webbasierter Informationssysteme*

Fragen?

Thema: ***Trust, Reputation, Privacy***

Bearbeiter:
Rafael Schirru

Betreuer:
Prof. Dr. Ing. Stefan Deßloch

Kaiserslautern, den 09.07.2004