



Vertrauenswürdige Aussagen im Semantic Web – Entwurf einer Sicherheitsinfrastruktur

Lutz Suhrbier (suhrbier@inf.fu-berlin.de)

AG Netzbasierte Informationssysteme (<http://nbi.inf.fu-berlin.de>)

FU Berlin, FB Mathematik und Informatik, Institut für Informatik

24. September 2007 (XML-Tage Berlin 2007)

Aspekte globalisierten Vertrauens

Vertrauen ist ein

- „Mechanismus zur Reduktion sozialer Komplexität“ (Luhmann)
- „riskante Vorleistung“ und potentiell unsichere Investition in die Zukunft
- „funktionales Equivalent“ zu Misstrauen (Überbetonung positiver/negativer Aspekte)
- immaterieller Wert, aber wichtiger Bestandteil der unsichtbaren Infrastruktur (soziales Kapital) einer Wirtschaft (Putnam)

Globalisierung verändert die

- Dynamik der Anpassung von Märkten
 - Immer mehr Entscheidungen in immer kürzerer Zeit
 - Immer mehr unzureichend überprüfbare Informationen
 - Explizites Wissen wird immer mehr durch Vertrauen (z.B. Geschäftspartner) ersetzt
- Wahrnehmung von Vertrauen in der Gesellschaft
 - System- und institutionelles Vertrauen verdrängt persönliches Vertrauen
 - Vertrauen bekommt immer weniger Zeit sich zu entwickeln, zu reifen
- Wertigkeit schnell verfügbarer, vertrauenswürdiger Informationen

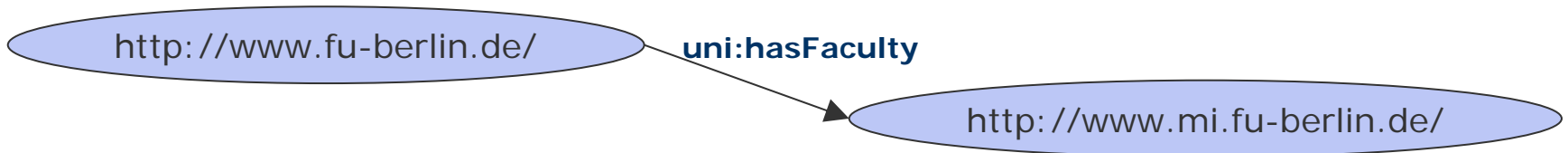
Semantic Web - Aussagen

Semantic Web

- Erweiterung des Web um maschinenlesbare *Meta-Informationen*
- Meta-Informationen beschreiben die Semantik von Webinhalten mit *RDF*

„Die **FU-Berlin** hat einen **Fachbereich Mathematik und Informatik**“

Subjekt *Prädikat* *Objekt*



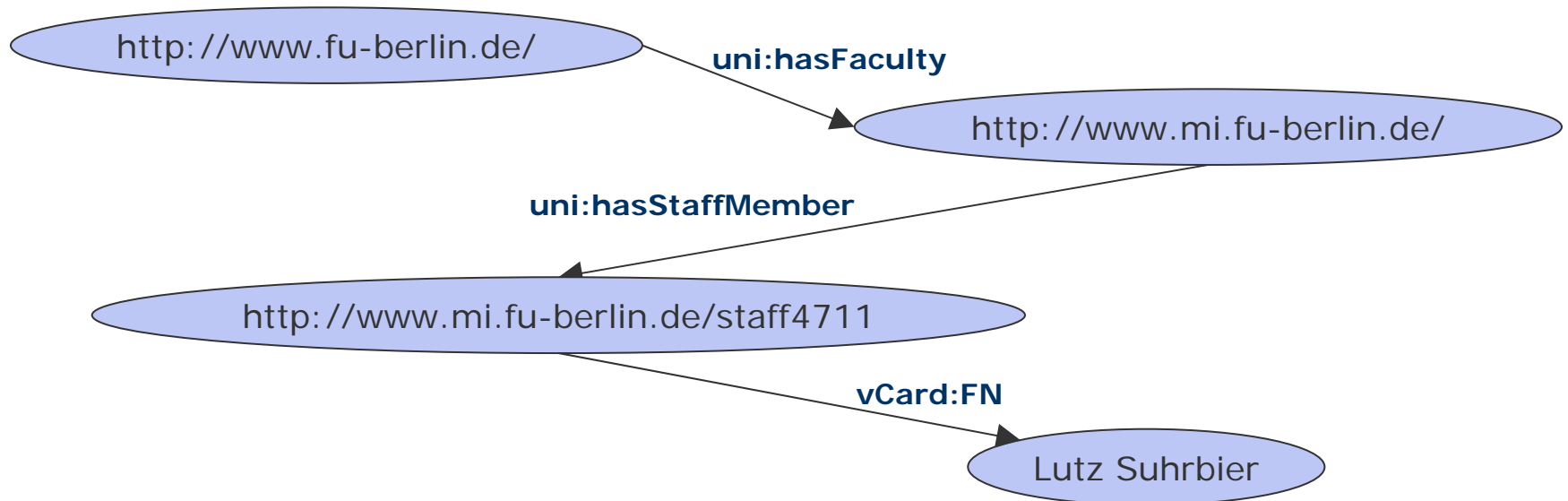
Resource Description Framework (RDF)

- Repräsentationsmodell für Meta-Informationen in Form von *Aussagen*
- Aussagen sind Tripel aus Subjekt, Prädikat (Eigenschaft) und Objekt
- Abbildung als gerichteter Graph

Semantic Web - Inferenz und Reasoning

Inferenz

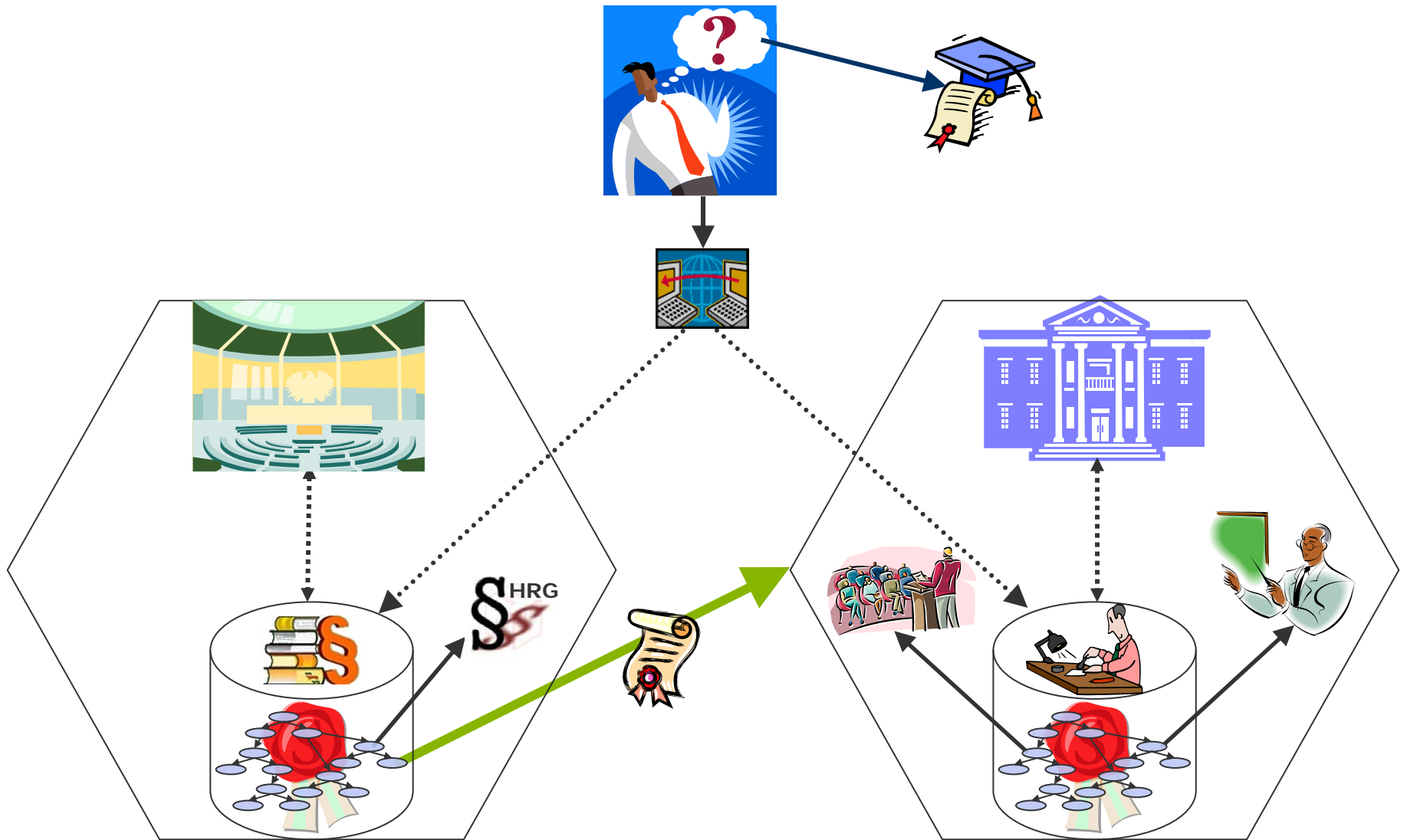
- Prozess der Ableitung neuen Informationen aus bereits Bekanntem
- Inferenzmaschine (inference engine)



Reasoning

- eine Art Inferenzmechanismus
- erlaubt automatisierte dynamische Erweiterung modellierten Wissens
- Redundanz-, Konsistenz- und Vollständigkeitsprüfungen

Beispielszenario



Motivation

● *Authentizität von (Meta-)Informationen*

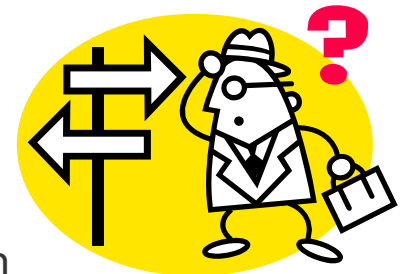
- Verlässlichkeit von Aussagen
 - Möglicherweise beeinträchtigt durch:
 - Übertragungsfehler, Fälschung von Informationen, (un-)bewusste Falschaussagen
- Mittel gegen RDF-Spam

● *Optimierung von Such- und Inferenzprozessen*

- Suchraumeinschränkung durch Bevorzugung vertrauenswürdiger Aussagen
- Steigerung der Ergebnisqualität durch Integration

● *Problemstellung*

- Sicherung der **Vertrauenswürdigkeit** von Aussagen
- Einfluss auf die **Verlässlichkeit** abgeleiteter Informationen



Vertrauenswürdige Aussagen (Eigenschaften)

- Jede Aussage besitzt einen Autor
- Autoren sind zweifelsfrei identifizierbar
- Autoren und Aussagen sind eindeutig einander zuzuordnen
- Integrität (Fälschungssicherheit) dieser Zuordnung
- Nichtabstreitbarkeit von Aussagen durch Autoren



Quelle: <http://www.cartoonfactory.com>

- Falsche Aussagen beeinträchtigen die Reputation des Autors

Lösungsansatz - Autorenbezogene Konzepte

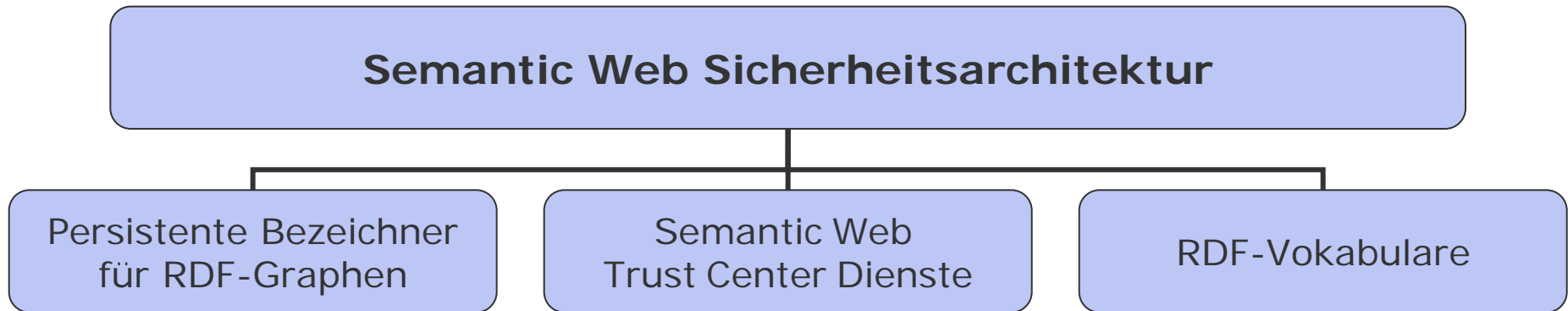
- Zuordnung von Aussagen und Autoren („Aussage X hat Autor Y“)
- Grundlegende Qualifizierung von Zuordnungen durch Prädikate:
 - **Bestätigung** („Aussage X wird (nicht) bestätigt durch Y“)
 - Basis für Bewertungsverfahren (Ranking, Reputationssysteme)
 - **Beglaubigung** („Aussage X wird amtlich beglaubigt durch Y“)
 - Veröffentlichung „atomarer Aussagen“ durch besonders gekennzeichnete Autoren
 - z.B. öffentliche Bekanntmachungen, Basis dynamischer Informationssysteme
- Erweiterte Qualifizierung durch Hinzufügen weiterer Prädikate

Lösungsanforderungen

- Absicherung der Vertrauenswürdigkeit autorenbezogener Konzepte
- Optionalität von Sicherheitsinformationen
 - Parallele Existenz mit nicht sicherheitsrelevanten Anwendungen
- Optionale Integration in Inferenz- und Reasoningmechanismen



Entwurf einer Semantic Web Sicherheitsarchitektur



Referenzierung von RDF-Aussagen

● *Persistente Bezeichner*

- Eindeutige Identifikation von RDF-Aussagen oder Graphen
 - Kryptographische Hashwerte über RDF-Aussagen (z.B. Carroll, Sayers)
 - Integration von Kontextinformationen (z.B. Algorithmus)
- URI-basiert
 - RDF beschreibt Ressourcen anhand von URIs
- Mögliche Realisierung: **Uniform Resource Name(URN)**
 - Schema Definition
- Vorteil: Stabile Referenzen bei Lokalitätsveränderungen von Aussagen

● *Semantic Web Integration über Named Graphs*

- Kennzeichnung beliebiger RDF-Graphen über URIs
- SPARQL unterstützt Named Graphs

● *Lokalisierung der RDF-Aussagen über persistente Bezeichner*

- Ideal: Globaler „Triple Space“
- Verzeichnisdienst (Lokalisierungsdienst)
 - Ermittelt auf Anfrage URL von RDF-Graphen zu persistenten Bezeichner
 - „Google“ für persistente Bezeichner

Semantic Web Trust Center Dienste

● *Public Key Infrastructure (PKI) für Semantic Web (RDF)*

- RDF-Signaturen
 - Sicherung autorenbezogener Konzepte
 - Integrität, Nichtabstreitbarkeit, Eindeutigkeit von Zuordnungen
- RDF-Zertifikate
 - zweifelsfreie Identifikation von Autoren
 - RDF-Signatur gebildet über RDF-Zertifikatsinformationen
- Vertrauenswürdige Instanzen (Certification Authorities)
 - Bereitstellung von Trust Center Diensten

● *Trust Center Dienste für Semantic Web*

- Ausgabe und Widerruf von RDF-Zertifikaten
 - Mögliche parallele Verwaltung von X.509- und RDF-Zertifikaten
- Statusabfrage für RDF-Zertifikate
 - Spezialisierter Verzeichnisdienst für RDF-Aussagen
- Verifikation von
 - RDF-Signaturen und RDF-Zertifikaten
 - autorenbasierten Konzepten (Urheberidentität)

RDF-Vokabulare für vertrauenswürdige Aussagen

● *Spezifikation von Vokabularen mittels RDF-Schema*

- Autorenbezogene Konzepte
- RDF-Signaturen
- RDF-Zertifikate
- ...

● *RDF-Schema*

- Klassenkonzept zur formalen Beschreibung der Semantik von RDF-Elementen
- Beschreibt Ressourcen, Eigenschaften und deren Relationen

Ziele

● „Proof of concept“

- Grundlegende Spezifikation und Implementierung von RDF Vokabularen
 - Autorenbezogene Konzepte
 - RDF-Signaturen und RDF-Zertifikate
 - Persistente Bezeichner
- Prototypenentwicklung der Basisfunktionalität folgender Dienste
 - Semantic Web Trust Center Dienste
 - Verzeichnisdienst für RDF-Aussagen und RDF-Zertifikate (?)
- Erweiterung einer ausgewählten Inferenzmaschine
 - Integration vertrauenswürdiger Aussagen
 - z.B. durch gewichtete Berücksichtigung autorenbasierter Konzepte
- Integration in ein „reales“ Semantic Web Anwendungsszenario
 - ...

● Vergleichende Analyse

- Performance
- Ergebnisqualität