



Perspektiven vertrauenswürdiger Aussagen im Semantic Web

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

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

FU Berlin, FB Mathematik und Informatik, Institut für Informatik

29. März 2006 (D•A•CH Security 2006)



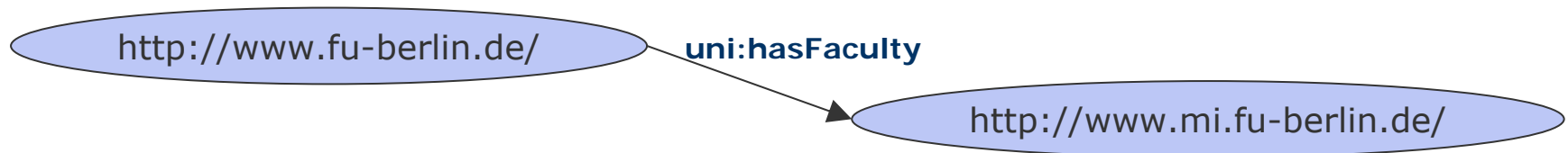
Semantic Web - Aussagen

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)

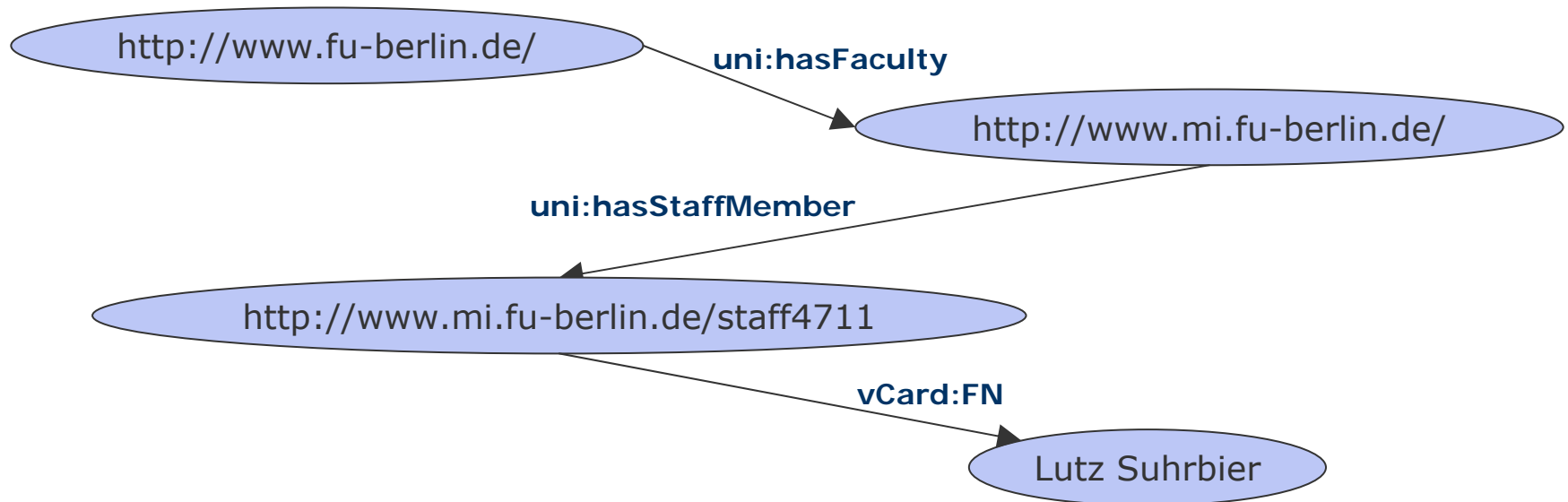
- Repräsentationsmodell für Meta-Informationen in Form von *Aussagen*
- Aussagen sind Tripel aus Subjekt, Prädikat (Eigenschaft) und Objekt
- Abbildung als gerichteter Graph



Semantic Web - Inferenz und Reasoning

Inferenz

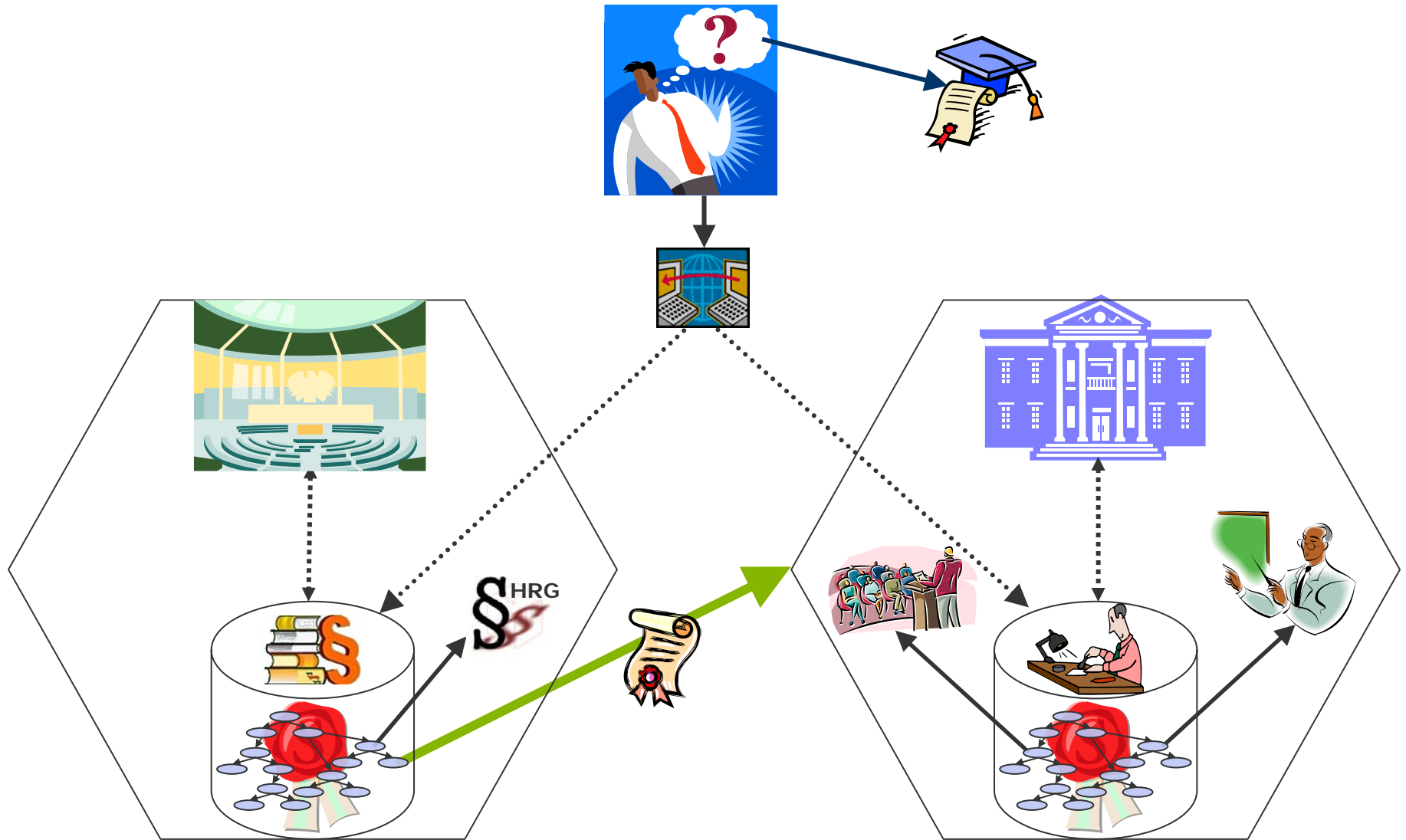
- Prozess der Ableitung neuen Wissens aus bereits Bekanntem
- Inferenzmaschine (inference engine)



Reasoning

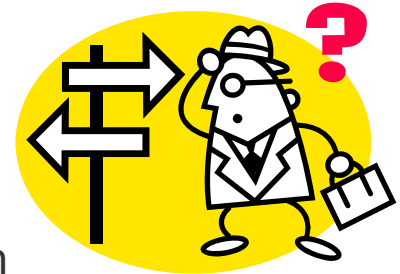
- eine Art Inferenzmechanismus
- erlaubt automatisierte dynamische Erweiterung modellierten Wissens
- Redundanz-, Konsistenz- und Vollständigkeitsprüfungen

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

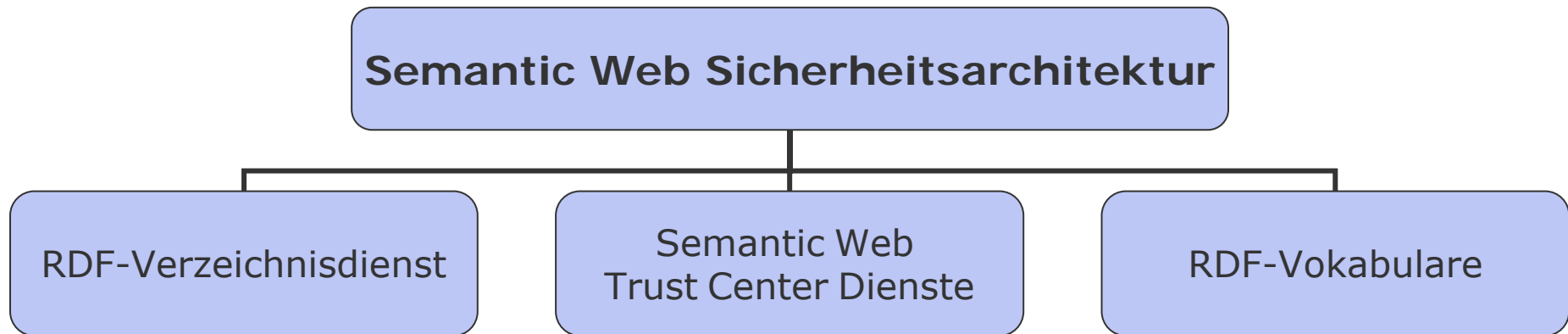
- Zuordnung von Aussagen und Autoren („Aussage X hat Autor Y“)
- Grundlegende Qualifizierung von Zuordnungen durch Prädikate:
 - **Bestätigung** („Aussage X wird (nicht) bestätigt durch Y“)
 - Basis für Bewertungsverfahren (Ranking, Reputationssysteme)
 - **Beglaubigung** („Aussage X wird amtlich beglaubigt 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
 - Identifikation durch Hashwerte über RDF-Aussagen (z.B. Carroll, Sayers)
 - Integration von Kontextinformationen (z.B. Verzeichnisdienst, Algorithmus)
- URI-basiert
 - RDF beschreibt Ressourcen anhand von URIs
- Mögliche Realisierung: **Uniform Resource Name(URN)**
 - Schema Definition
- Semantic Web Integration über *Named Graphs*
 - Kennzeichnung beliebiger RDF-Graphen über URIs
 - SPARQL unterstützt Named Graphs

● Verzeichnisdienst für RDF-Aussagen

- Verwaltung von Referenzen auf RDF-Graphen (persistente Bezeichner)
- Reduzierung redundanter Kopien von RDF-Graphen
- Mögliche Realisierung: **Persistent Uniform Resource Locator(PURL)**

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

Perspektiven

● „Proof of concept“

- Grundlegende Spezifikation und Implementierung von RDF Vokabularen
 - Autorenbezogene Konzepte
 - RDF-Signaturen und RDF-Zertifikate
 - Persistente Bezeichner
- Prototypenentwicklung der Basisfunktionalität folgender Dienste
 - Verzeichnisdienst für RDF-Aussagen und RDF-Zertifikate
 - Semantic Web Trust Center Dienste
- 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