Overview

• Introduction
• Definition of terms
  – Semantic Web
  – REST
  – Public Key Cryptography
• FOAF+TLS
• Conclusion
What are we talking about?

- **social networks**
  - [Facebook](https://www.facebook.com)
  - [wer-kennt-wen.de](https://www.wer-kennt-wen.de)
  - [StudiVZ](https://www.studievz.de)

**Register**
What would we like to have?

Single Sign-On System

One ID (URI)
Existing Single Sign-On Systems

Facebook Connect

NOT RESTful !!!
making meaning of information usable & machine-readable

- Formal description about objects
- Relation graph between subject and object:

subject → Predicate → object

This is a place.
Relations

- **Public key**
  - Generates
  - Ways of
    - PKI (hierarchical)
      - Generates
        - Web of Trust (decentralized)
          - Comparable

- **PKC securing communication**
  - Generates
    - PKI (hierarchical)

- **Single Sign-On**
  - Uses
    - WebID (URI)
      - Links to
        - Public key

- **WebID (URI)**
  - Uses
    - Single Sign-On
      - REST distribute hyper-media
        - Satisfies
          - FOAF
            - machine-readable social networks
              - Satisfies
                - TLS securing communication
              - Satisfies
                - REST distribute hyper-media

- **REST**
  - Distribute hyper-media

- **TLS**
  - Securing communication

- **PKC**
  - Securing communication

- **Web of Trust (decentralized)**
  - Generates
    - PKI (hierarchical)

- **PKI (hierarchical)**
  - Generates
    - Web of Trust (decentralized)

07.07.2009

Alexandra Wolyniec

Universität Koblenz, FB4
FOAF + TLS

Definition: REST (Representational State Transfer)

<table>
<thead>
<tr>
<th>Resource</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Book</td>
<td>ISBN</td>
</tr>
<tr>
<td>Website</td>
<td>URL</td>
</tr>
</tbody>
</table>

Operations:
- GET
- POST
- PUT
- DELETE
- HEAD
- OPTIONS
FOAF + TLS

Relations

- REST
  - distribute
  - hyper-media
- WebID (URI)
  - uses
- Single Sign-On
- Public key
  - generates
  - Ways of
- PKC
  - securing
  - communication
- PKI
- Web of Trust
  - Comparable
- FOAF
  - machine-readable
  - social networks
  - satisfies
- TLS
  - securing
  - communication
  - satisfies

Links to (hierarchical, decentralized)
Definition: Public Key Cryptography

- Secure communication
- *Encryption* or *Signing*
- Public/Private key:

  Client signs Certificate with private key

  Server verifies truthness with public key
FOAF + TLS

Definition: Public Key Cryptography

- **Public Key Infrastructure**
  - Hierarchical
  - Requires Certification authorities

- **Web of Trust**
  - Without Hierarchy
  - Every user can generate certificate

FOAF+TLS uses decentralized WoT in PKI way
FOAF + TLS

Relations

Public key

PKI (hierarchical)

PKC

Web of Trust (decentralized)

Ways of

generates

REST
distribute hyper-media

WebID (URI)

uses

Single Sign-On

 Links to

satisfies

FOAF
machine-readable social networks

satisfies

TLS
securing communication

Comparable

Single Sign-On uses WebID (URI) which links to Public key. Public key generates PKI (hierarchical) which is comparable to Web of Trust (decentralized). REST distributes hyper-media which satisfies FOAF machine-readable social networks. FOAF satisfies TLS securing communication.
• Provides privacy and data integrity
• TLS handshake:
  – Authentication and negotiation of encryption algorithm
  – If successful: server knows that client has corresponding private key
TLS (Transport Layer Security) Handshake Protocol

If finished, a secure communication is possible!
FOAF + TLS

Relations

- **Public key**
  - secures communication
  - generates PKI (hierarchical)
  - Web of Trust (decentralized)

- **PKI**
  - generates PKC

- **PKC**
  - securing communication

- **Single Sign-On**
  - uses WebID (URI)
  - links to REST

- **WebID (URI)**
  - uses REST

- **FOAF**
  - satisfies hyper-media
  - distributed social networks

- **REST**
  - distributes hyper-media

- **TLS**
  - securing communication

Comparable Ways of
Links to
Definition: FOAF

• Friend-of-a-Friend
• Machine-readable social network
  – Using RDFS
• Idea of antagonizing social network silos (Facebook, Studivz,...) is fulfilled
FOAF + TLS

Relations

- **Public key**
  - **PKI** (hierarchical)
  - **PKC**, securing communication
  - Generates ways of trust
  - **Web of Trust** (decentralized)

- **PKI** (hierarchical)
  - **Web of Trust** (decentralized)
  - **Single Sign-On** uses
  - **WebID** (URI)

- **REST**: distribute hyper-media
  - Satisfies **FOAF**: machine-readable social networks
  - Secures communication

- **TLS**: securing communication

- **FOAF**: machine-readable social networks
  - Satisfies **REST**: distribute hyper-media

- **Single Sign-On** uses **WebID** (URI)

- **Public key** links to **PKI** (hierarchical)

- **Comparable** ways of trust
What does all that mean for FOAF + TLS?

- Client needs 2 things, both containing public key:
  - An **own certificate** (with URI, that links to FOAF file)
  - A **FOAF file** (RDF document)
Authentication in FOAF+TLS:

1. URI
2. FOAF File
3. If public keys identical
   -> user is authenticated
The Difference:

In **PKI** server asks certification authority, who signed certificate, if certificate is true

In **FOAF+TLS** the server dereferences the URI, mentioned in the certificate (gets to the FOAF file) and checks, if the public key of FOAF file and certificate are equal
What did we want? And how did we reach it?

- Data that belongs to us
- One SSO system
- Link data/merge different aspects of different networks
- Secure communication

Global, distributed and open yet secure social network

- FOAF file in RDF scheme
- Certificates
- Semantic Web/REST
- TLS