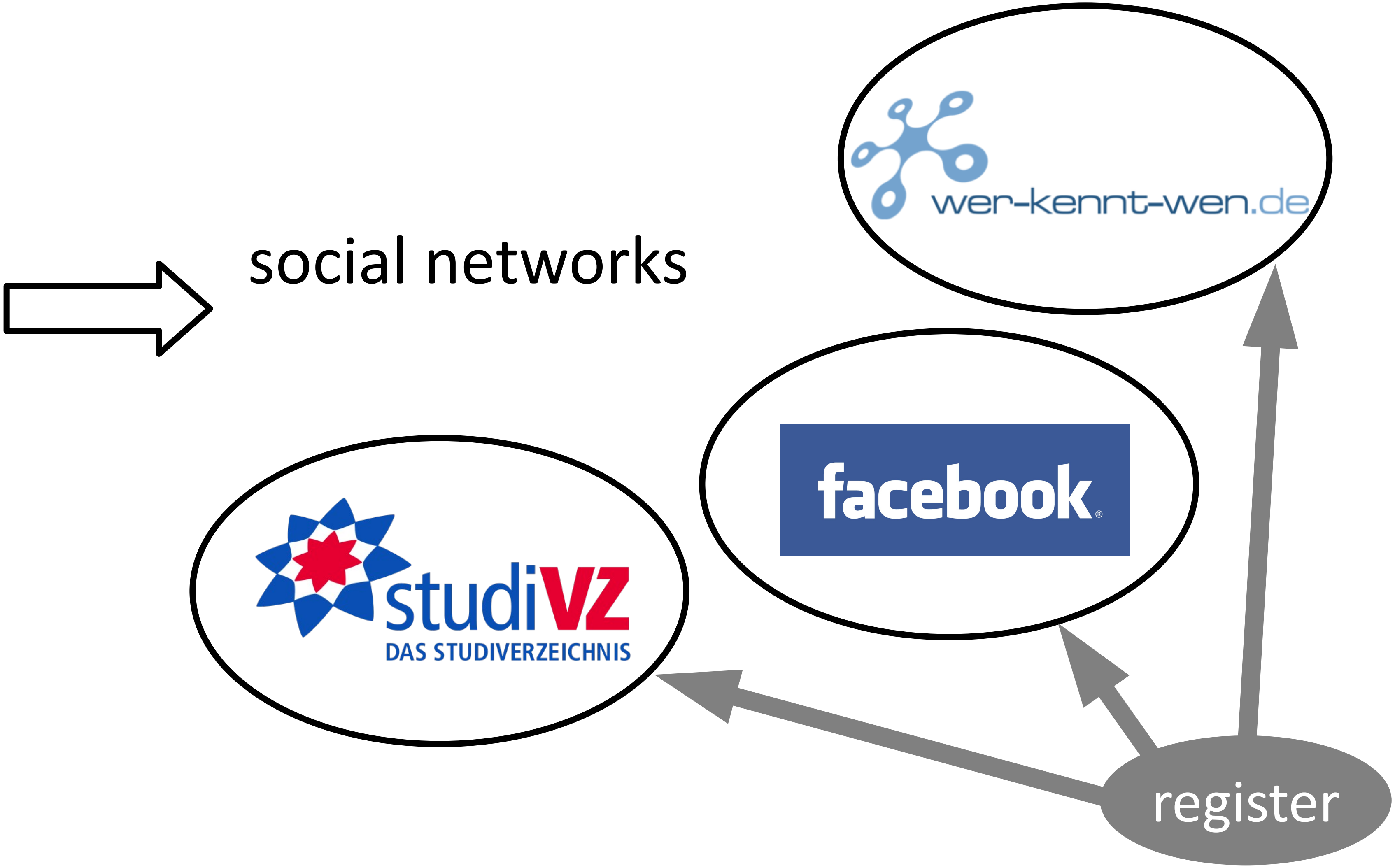
FOAF + TLS

Overview

- Introduction
- Definition of terms
  - Semantic Web
  - REST
  - Public Key Cryptography
- FOAF+TLS
- Conclusion

What are we talking about?



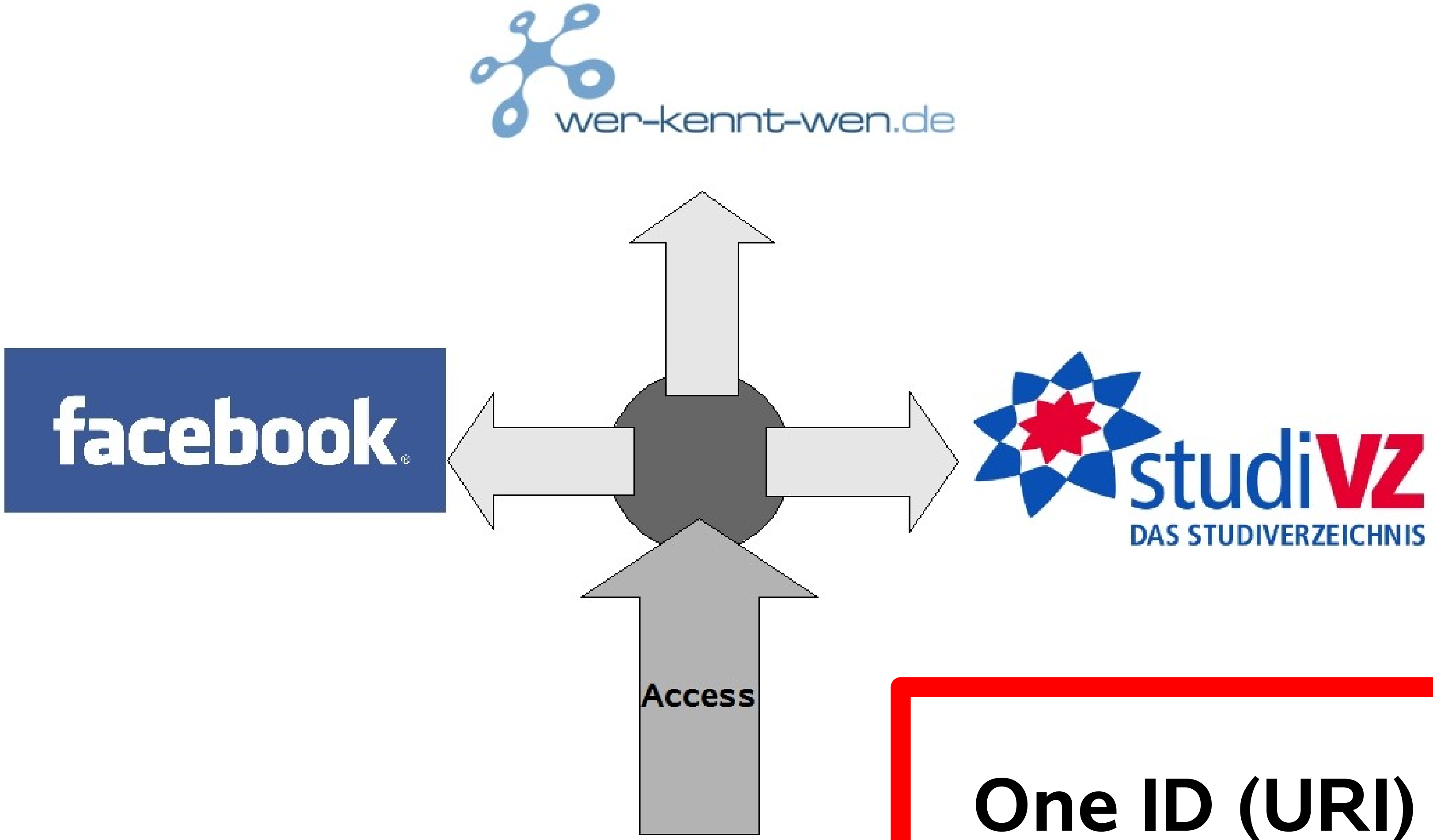
social networks

register

FOAF + TLS

What would we like to have?

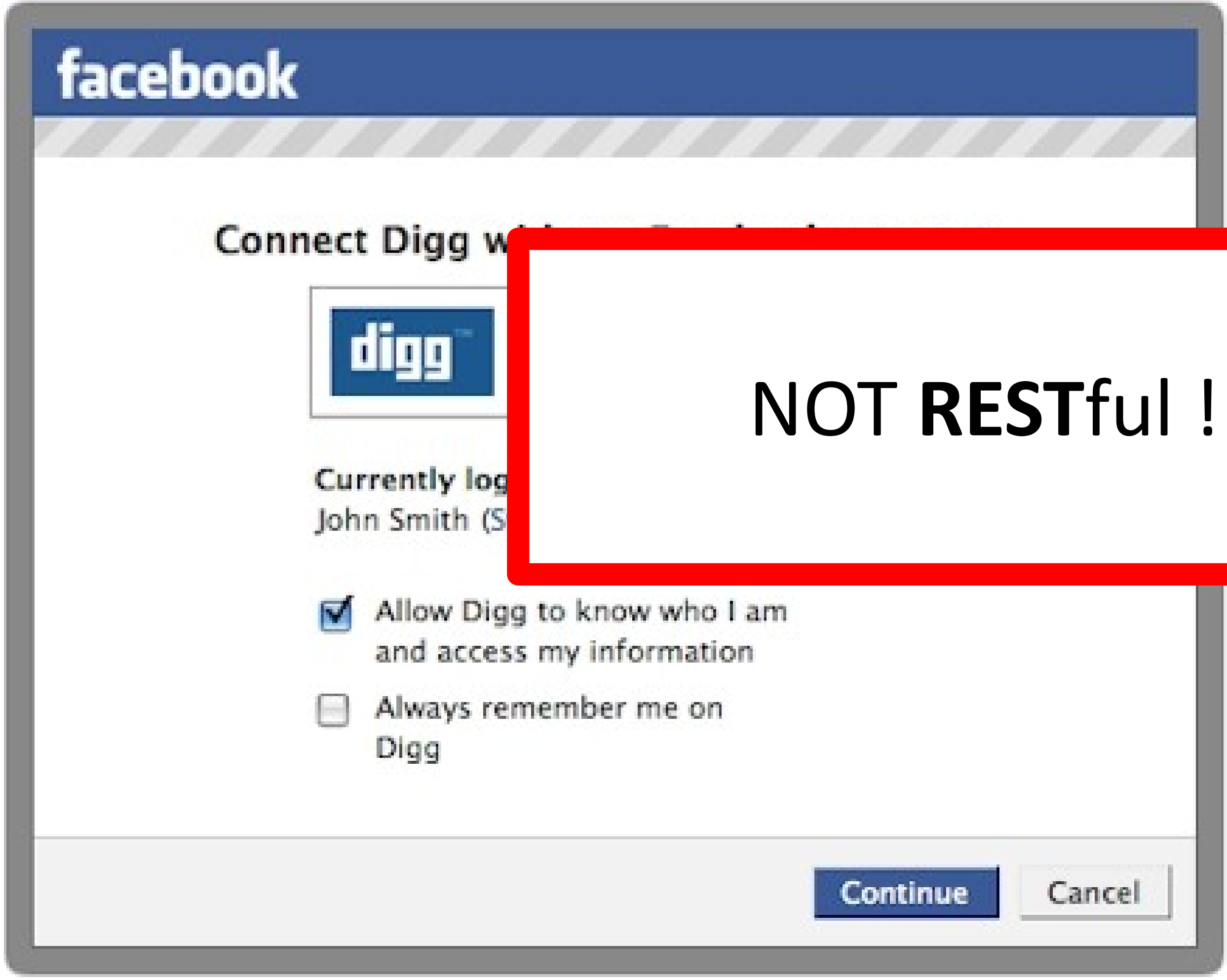
Single Sign-On System



One ID (URI)

Existing Single Sign-On Systems

Facebook Connect



facebook

Connect Digg w

Currently log
John Smith (S

☑ Allow Digg to know who I am and access my information

☐ Always remember me on Digg

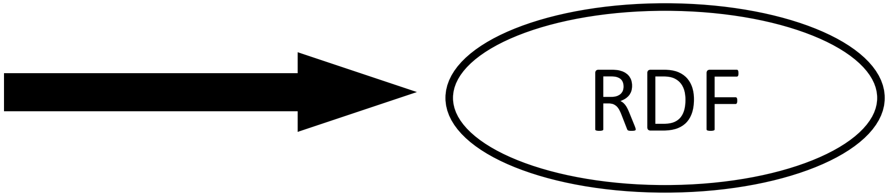
NOT **REST**ful !!!

hibboleth

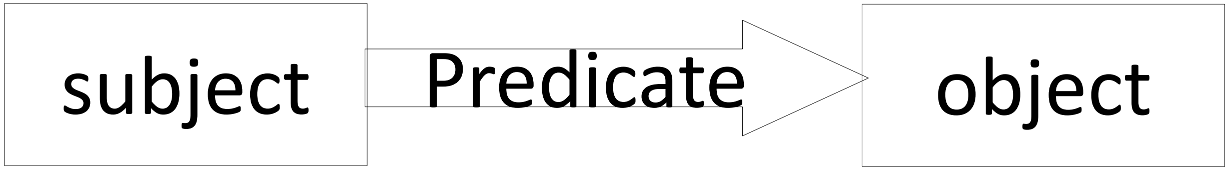
Definition: Semantic Web

making meaning of information usable

& machine-readable



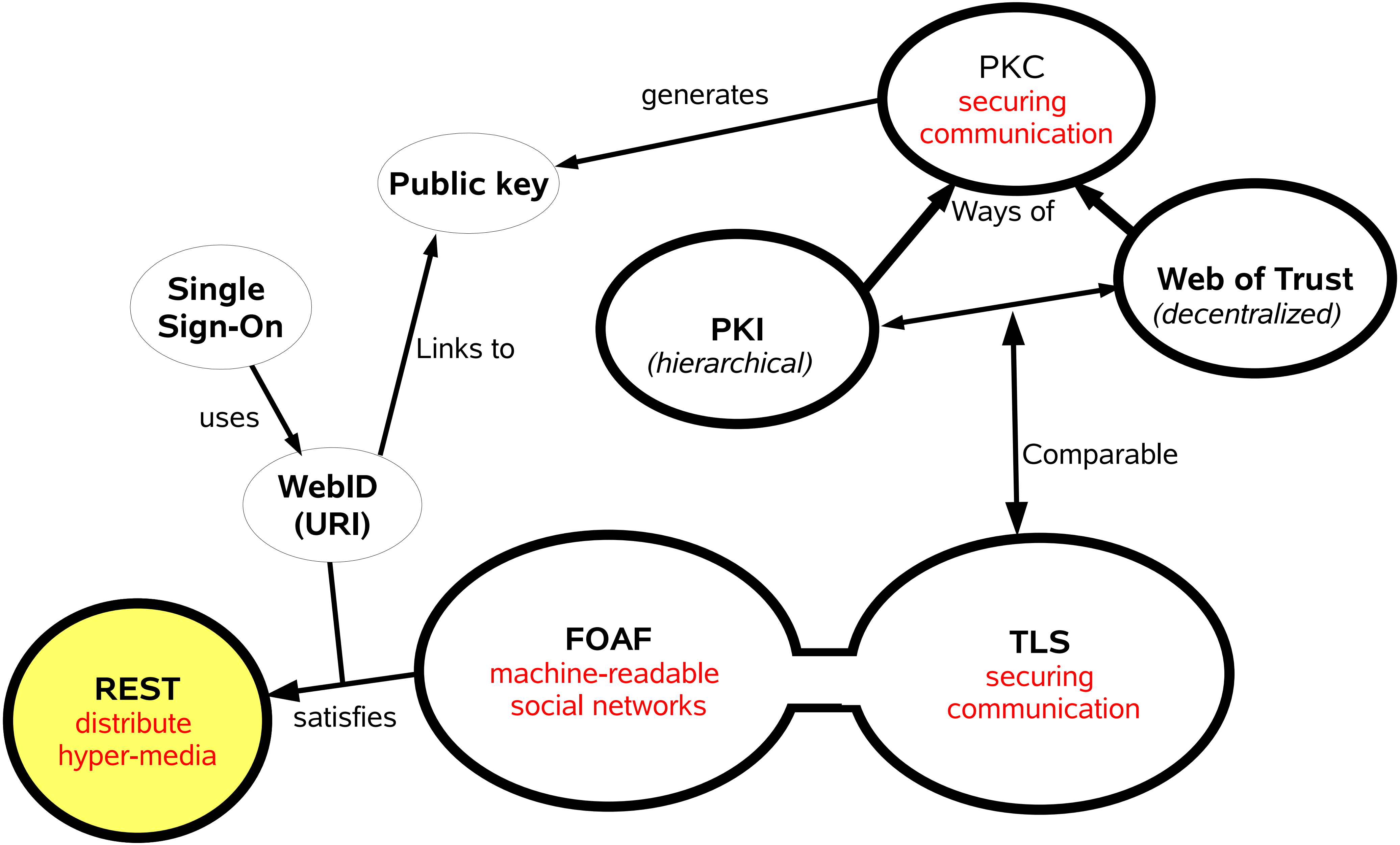
- Formal description about objects
- Relation graph between subject and object:



This is a place.

FOAF + TLS

Relations



Definition: REST (Representational State Transfer)

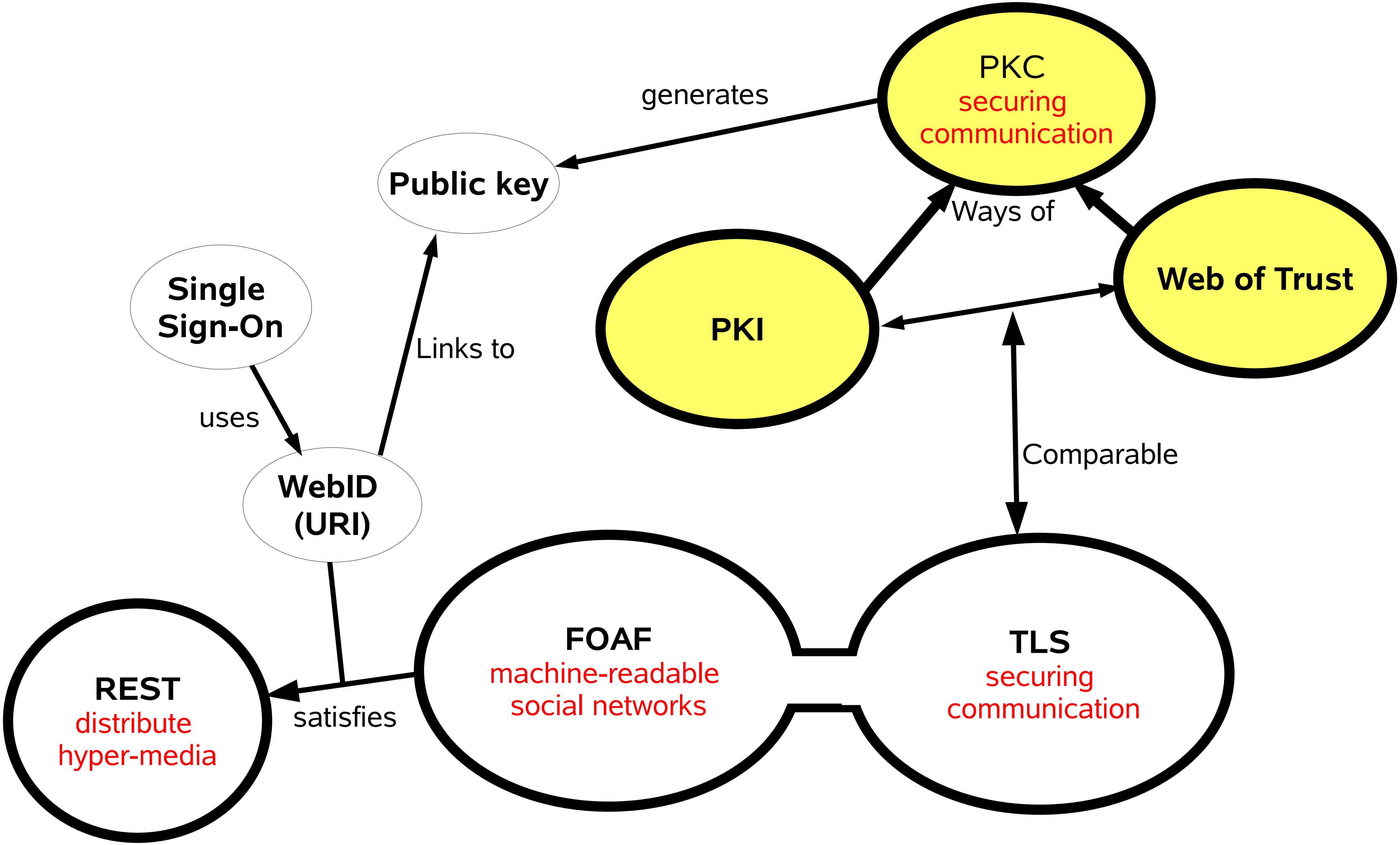
Resource	URI
Book	ISBN
Website	URL

Operations:

- **GET**
- **POST**
- **PUT**
- **DELETE**
- **HEAD**
- **OPTIONS**

FOAF + TLS

Relations



Definition: Public Key Cryptography

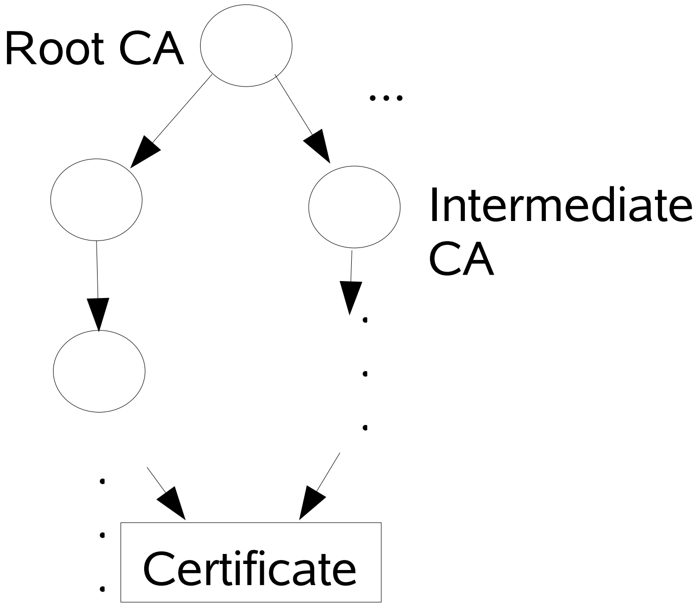
- Secure communication
- *Encryption* or *Signing*
- Public/Private key:

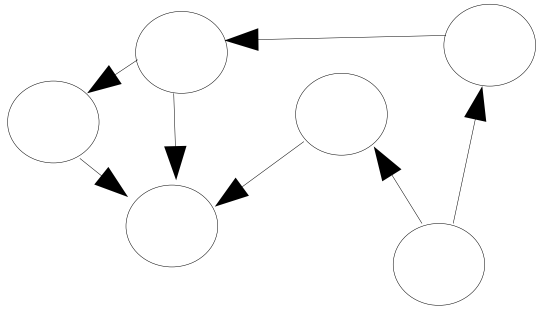
Client signs Certificate with private key

Server verifies truthness with public key

Definition: Public Key Cryptography

- **Public Key Infrastructure**
  - Hierarchical
  - Requires Certification authorities
- **Web of Trust**
  - Without Hierarchy
  - Every user can generate certificate

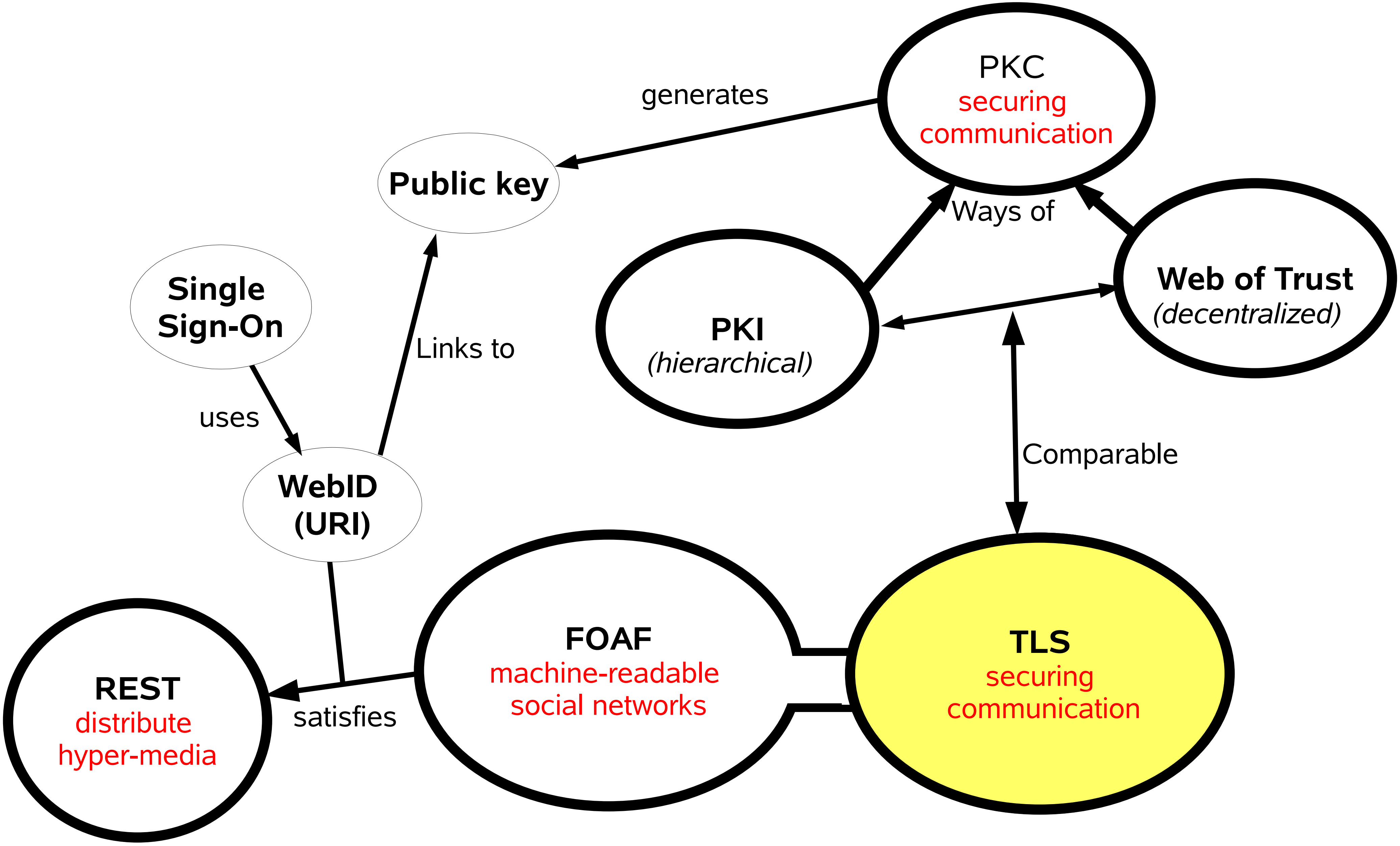




FOAF+TLS uses decentralized WoT in PKI way

FOAF + TLS

Relations

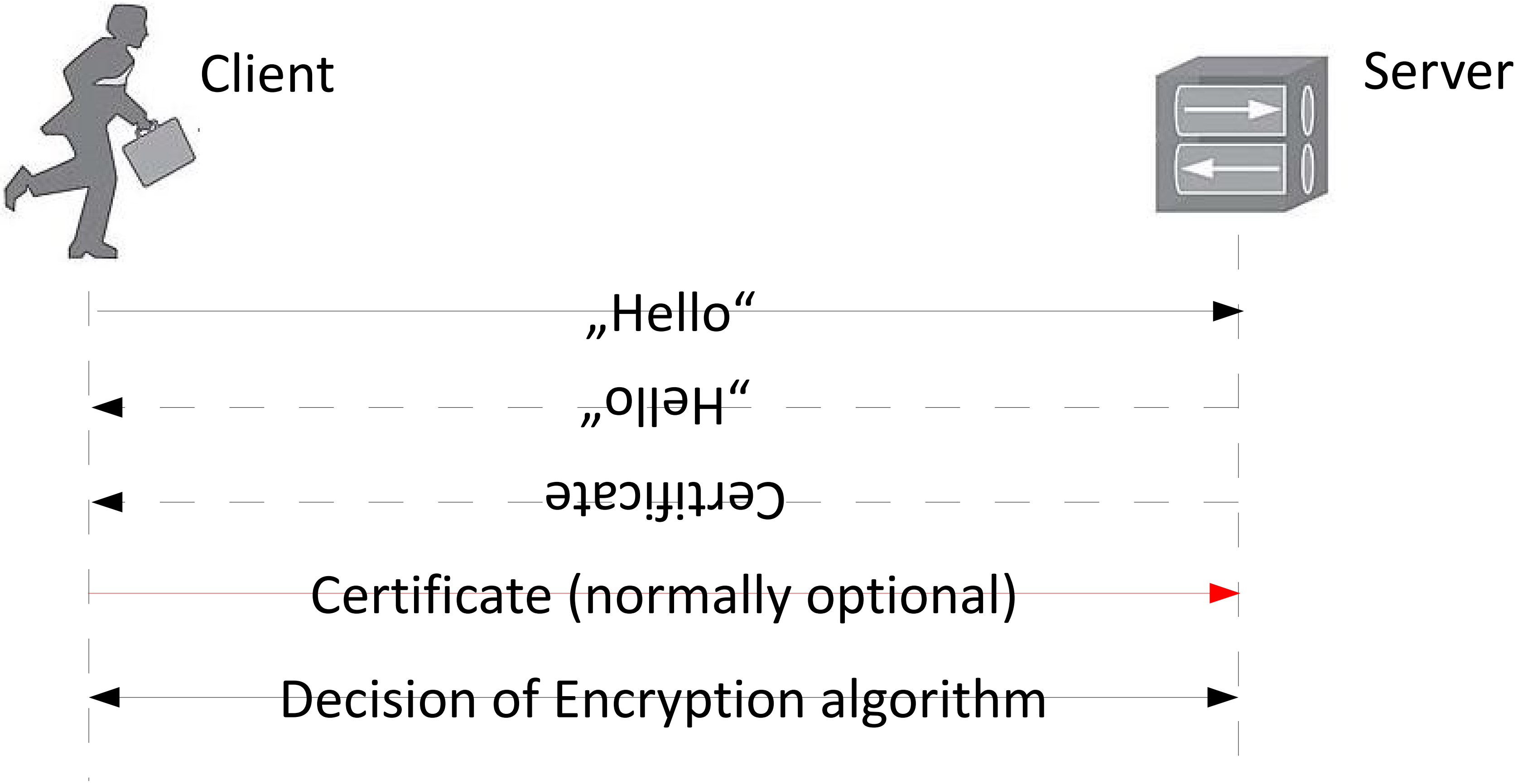


TLS (Transport Layer Security)

- Provides privacy and data integrity
- TLS handshake:
  - Authentication and negotiation of encryption algorithm
  - If successful: server knows that client has corresponding private key

FOAF + TLS

TLS (Transport Layer Security) Handshake Protocol



Client

Server

„Hello“

„Hello“

Certificate

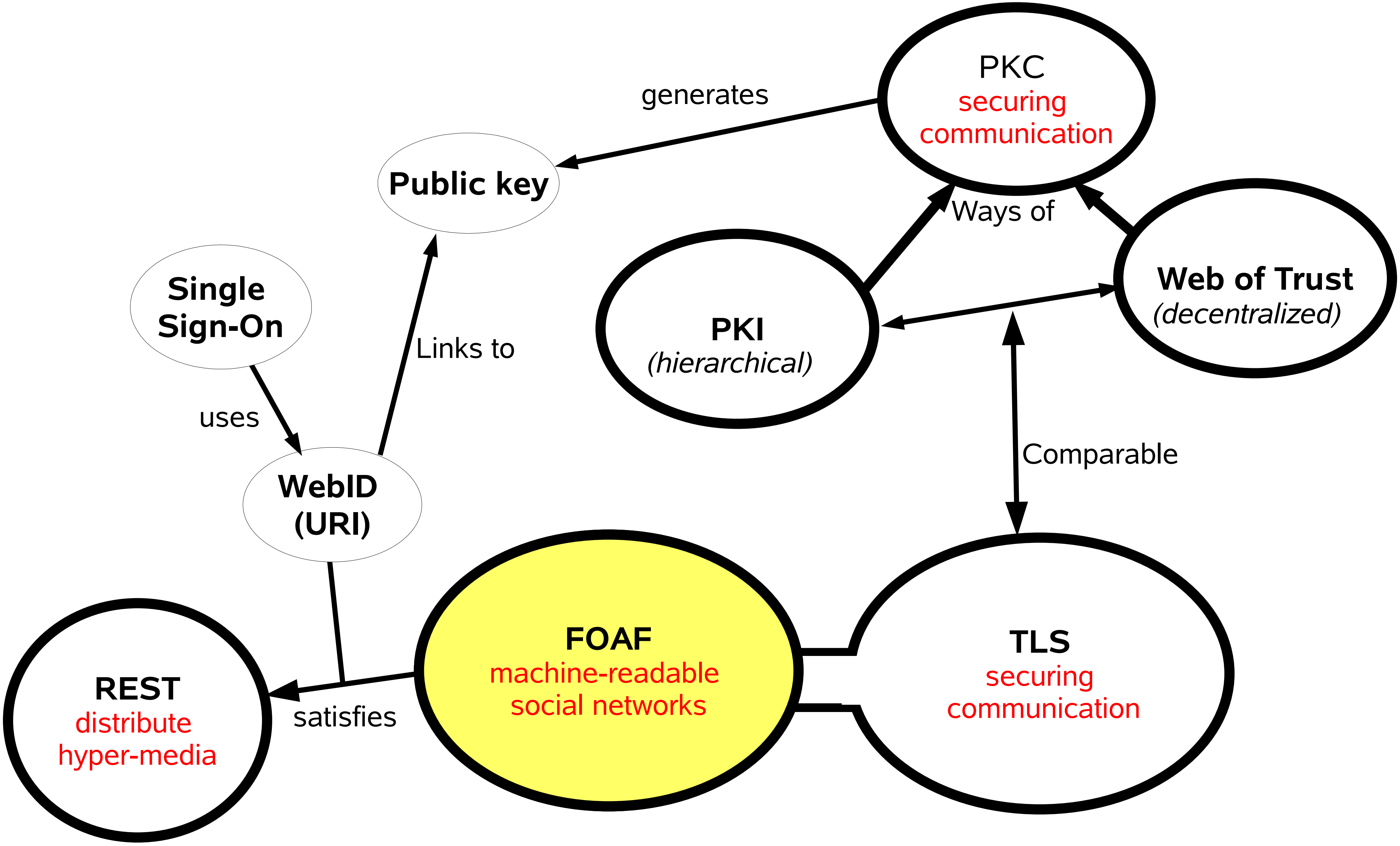
Certificate (normally optional)

Decision of Encryption algorithm

If finished, a secure communication is possible!

FOAF + TLS

Relations



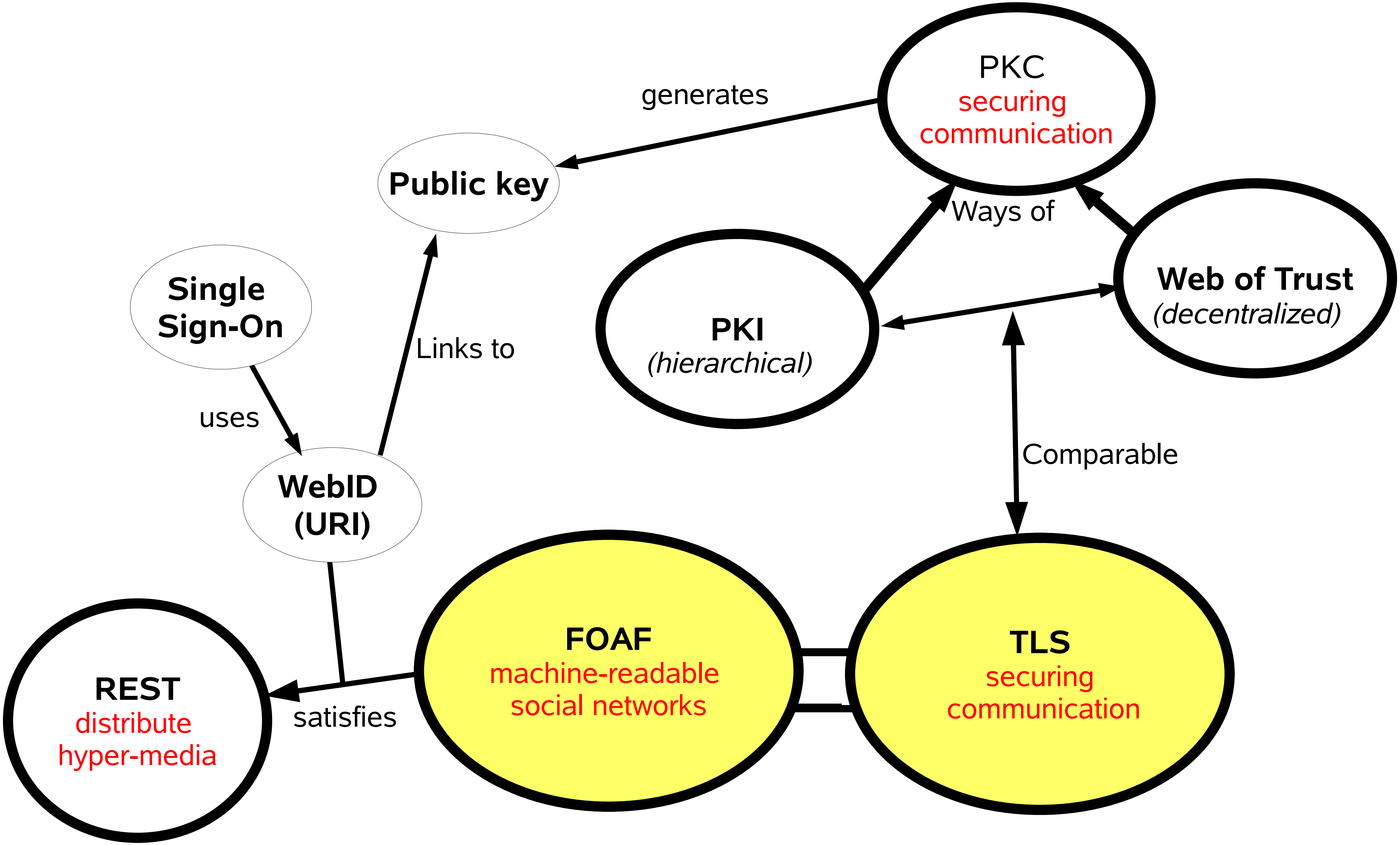
Definition: FOAF

- Friend-of-a-Friend
- Machine-readable social network
  - Using RDFS
- Idea of antagonizing social network silos (Facebook, Studivz,...) is fullfilled

FOAF File example

FOAF + TLS

Relations



What does all that mean for FOAF + TLS?

- Client needs 2 things,

  both containing *public key*:

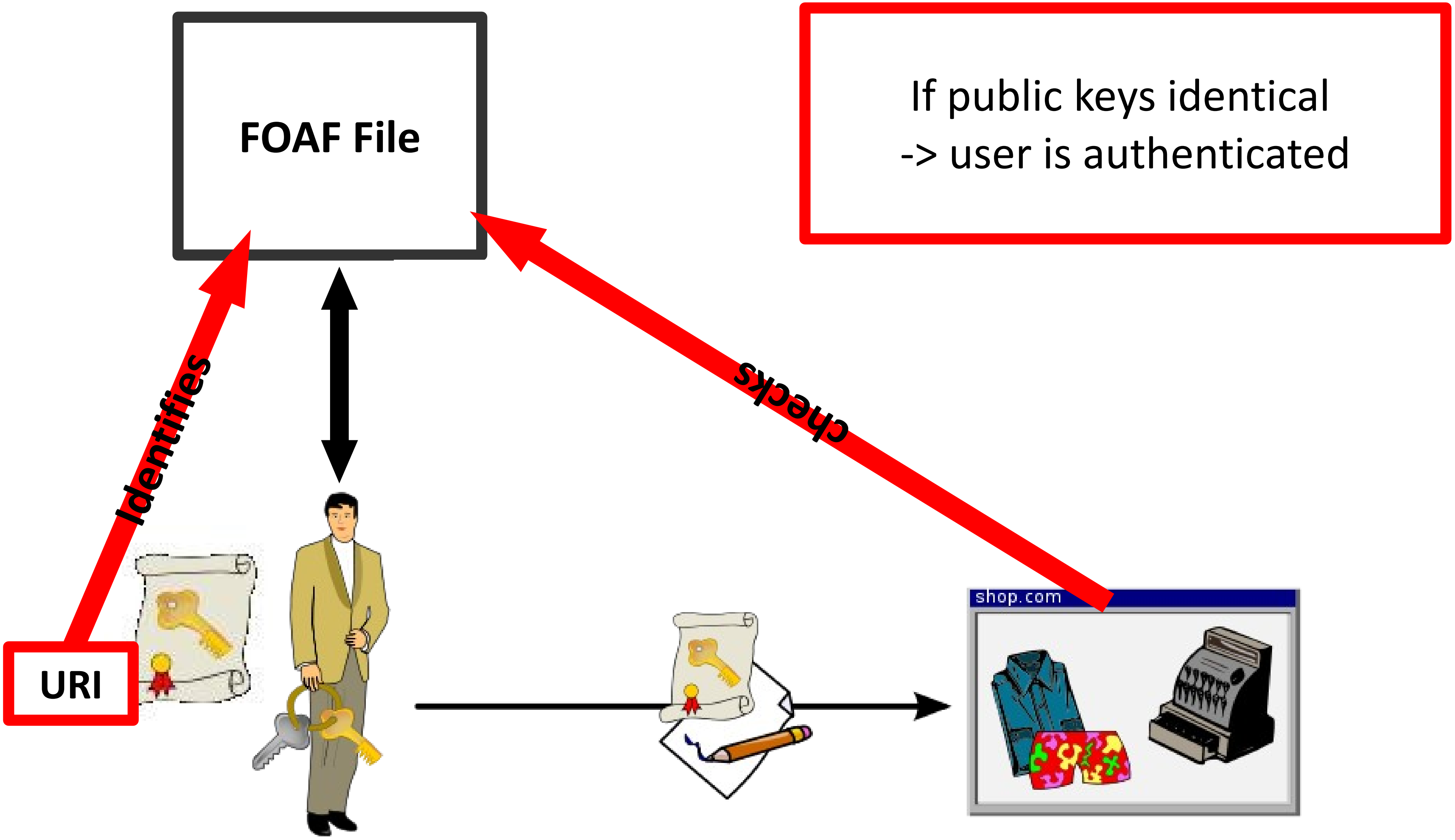
  - An **own certificate**

    (with URI, that links to FOAF file)

  - A **FOAF file** (RDF document)

FOAF + TLS

Authentication in FOAF+TLS:



If public keys identical
-> user is authenticated

FOAF + TLS

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

FOAF + TLS

What did we want? And how did we reach it?

- Data that belongs to us → FOAF file in RDF scheme

- One SSO system → Certificates

- Link data/ merge different aspects of different networks → Semantic Web/ REST

- Secure communication → TLS

⇒ Global, distributed and
open yet secure social network