Semantic Web

Vorlesung Informatik
Dr. rer. nat. Harald Sack
Institut für Informatik
Friedrich Schiller Universität Jena

Wintersemester 2006/2007

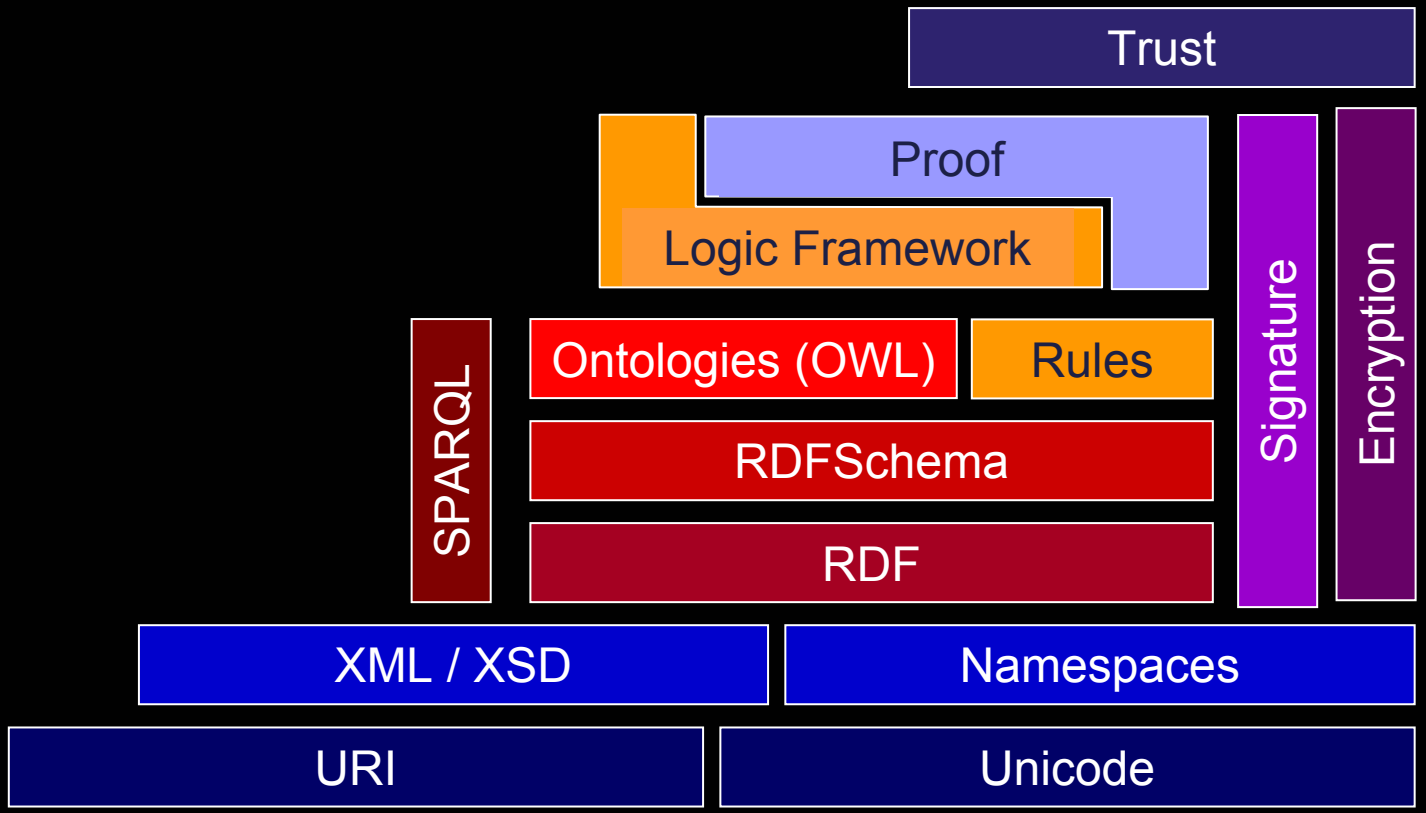
http://www.informatik.uni-jena.de/~sack/WS0607/semanticweb.htm

Semantic Web - Vorlesungsinhalt

1. Einführung
2. Die Sprachen des Semantic Web
3. Wissensrepräsentation
4. Ontology Engineering
5. **Web of Trust**
6. Semantic Web Anwendungen

5. Web of Trust

Semantic Web Architecture



Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.1.1 Sicherheitsziele

5.1.2 Kryptografische Verfahren

5.1.3 Digitale Signaturen

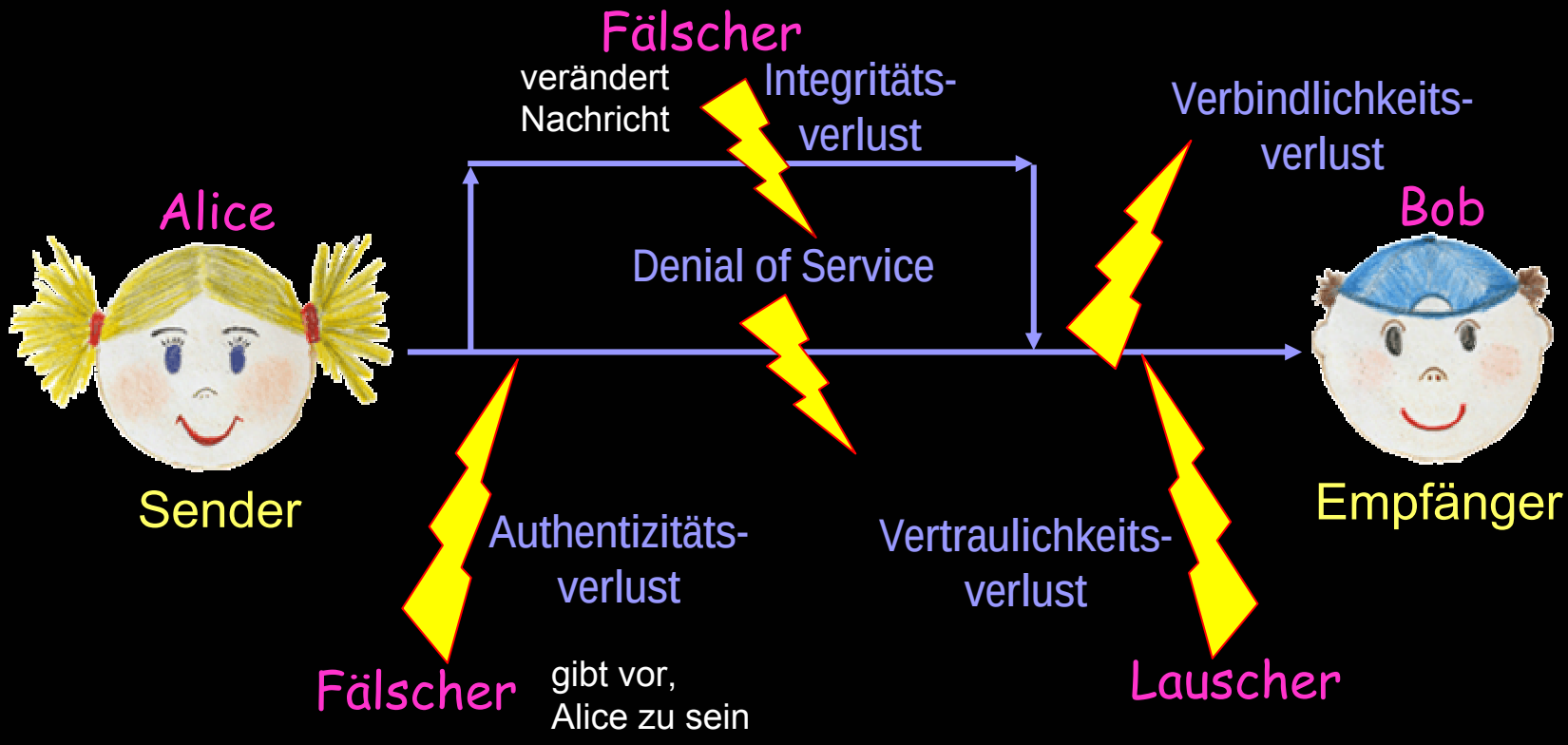
5.1.4 Zertifizierung

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5. Web of Trust
5.1 Kryptografische Grundlagen

- Sicherheitsziele



5. Web of Trust
5.1 Kryptografische Grundlagen

- Sicherheitsziele
  - **Verfügbarkeit**
    Die zuverlässige Funktionstüchtigkeit der zur Kommunikation verwendeten Medien darf nicht gestört werden können
  - **Datenintegrität**
    Die übertragene Nachricht muss den Empfänger im Originalzustand erreichen und darf nicht verändert werden
  - **Vertraulichkeit**
    Der Inhalt der übermittelten Nachricht darf nur für Sender und Empfänger, nicht für unbefugte Dritte lesbar sein.
  - **Authentifikation**
    Der Empfänger muss sich darauf verlassen können, dass der Absender der Nachricht diese auch tatsächlich verfasst hat
  - **Autorisation**
    Es muss sichergestellt werden, dass niemand anderes als der designierte Empfänger einer Nachricht die Berechtigung hat, diese zu lesen.

Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.1.1 Sicherheitsziele

5.1.2 Kryptografische Verfahren

5.1.3 Digitale Signaturen

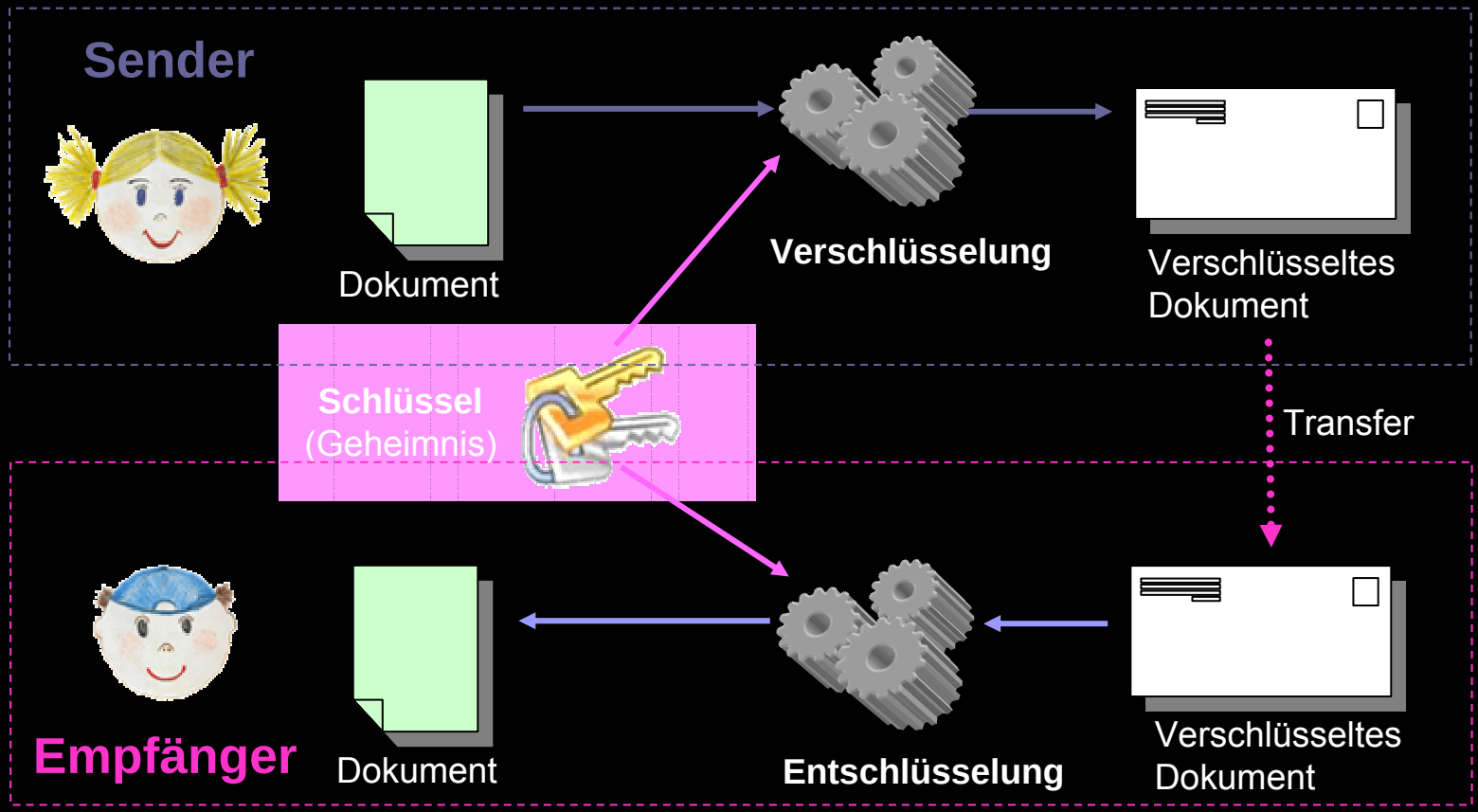
5.1.4 Zertifizierung

5.2 XMLEncryption und XMLSignature

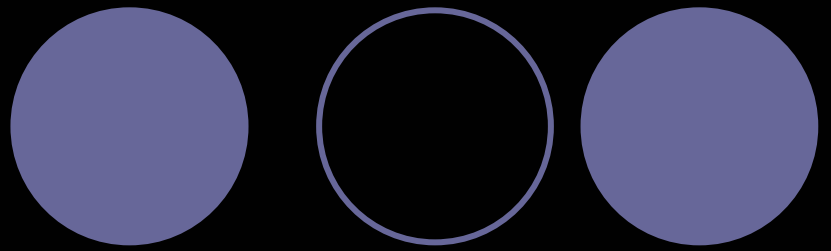
5.3 Voting-, Rating- und Reputationsysteme

5. Web of Trust
5.1 Kryptografische Grundlagen

- Symmetrische Schlüsselverfahren



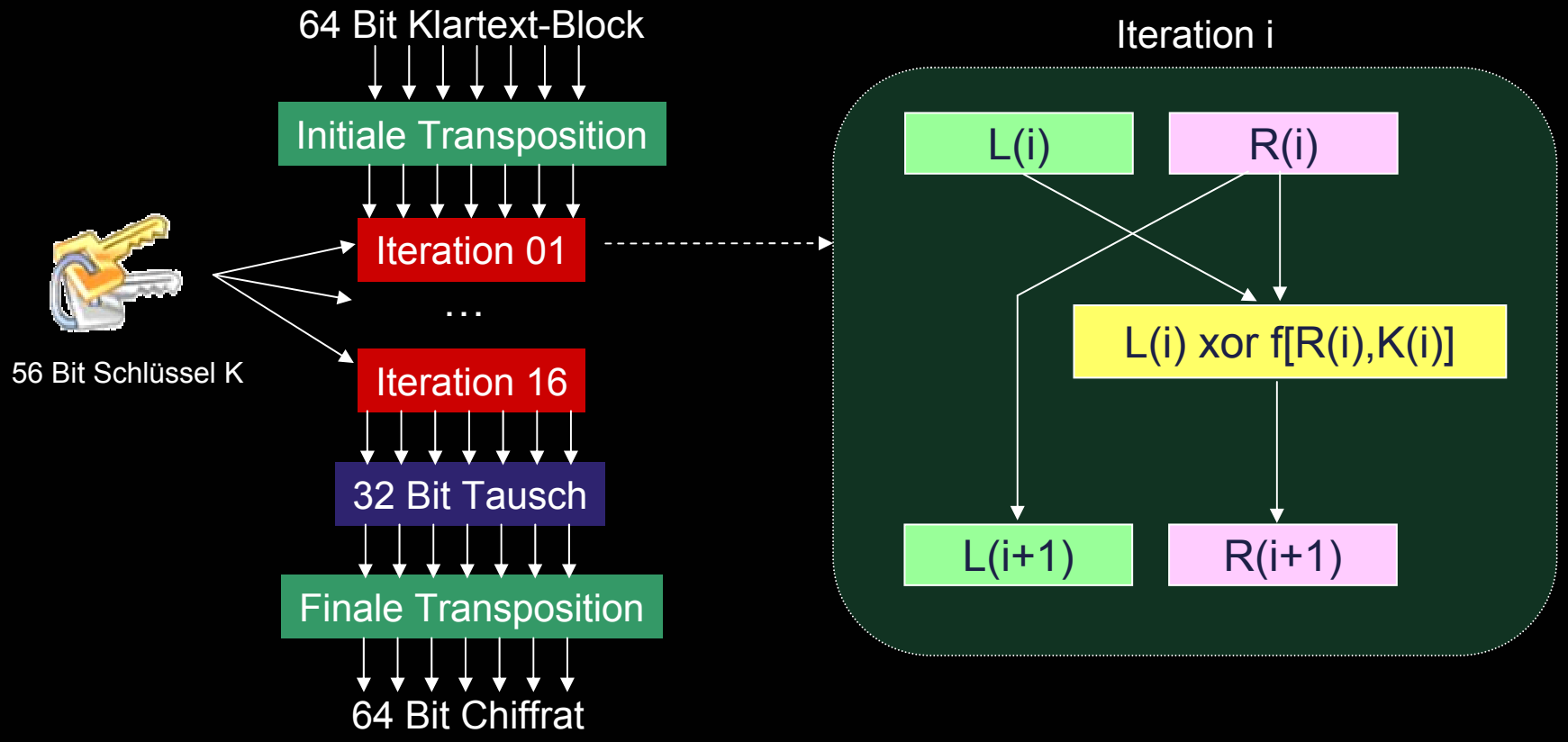
5. Web of Trust
5.1 Kryptografische Grundlagen



- Kryptografische Verfahren mit symmetrischem Schlüsselaustausch
  - Transpositionschiffre
  - Substitutionschiffre
  - Einwegchiffre
  - Blockchiffre und Stromchiffre
  - DES-Verschlüsselung
  - 3-DES
  - IDEA Verschlüsselung

5. Web of Trust
5.1 Kryptografische Grundlagen

- DES – Data Encryption Standard (1977 / 1993)



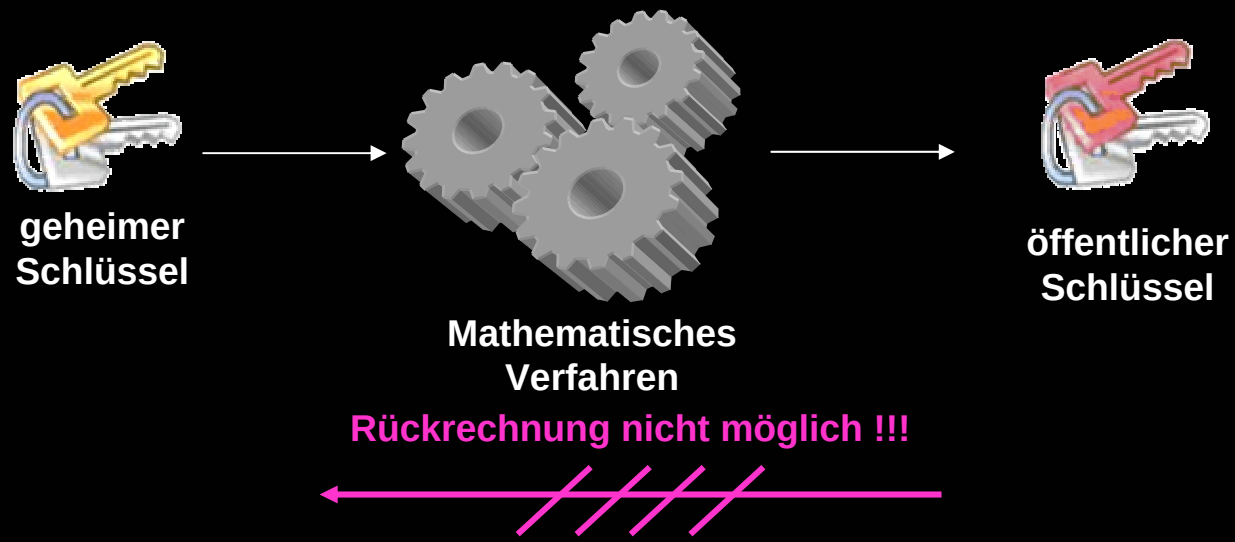
5. Web of Trust
5.1 Kryptografische Grundlagen

- Asymmetrische Verschlüsselungsverfahren
  - **Offene Geheimnisse – öffentliche Schlüssel**
    - Wie komplex die Verschlüsselungsverfahren auch sind, alle hängen bislang von einem **sicheren Austausch der** verwendeten **Schlüssel** ab
    - **Idee:**
      - Gibt es ein Verfahren zur Verschlüsselung, das ohne Austausch eines geheimen Schlüssels auskommt?
    - Kommunikation mit **öffentlichen Schlüsseln**
      - **öffentlicher Schlüssel** zum Verschlüsseln (kann von jedem genutzt werden)
      - **geheimer Schlüssel** zum Entschlüsseln (bleibt beim Besitzer)

Whitfield Diffie
Martin Hellmann
Ralph Merkle
(1976)

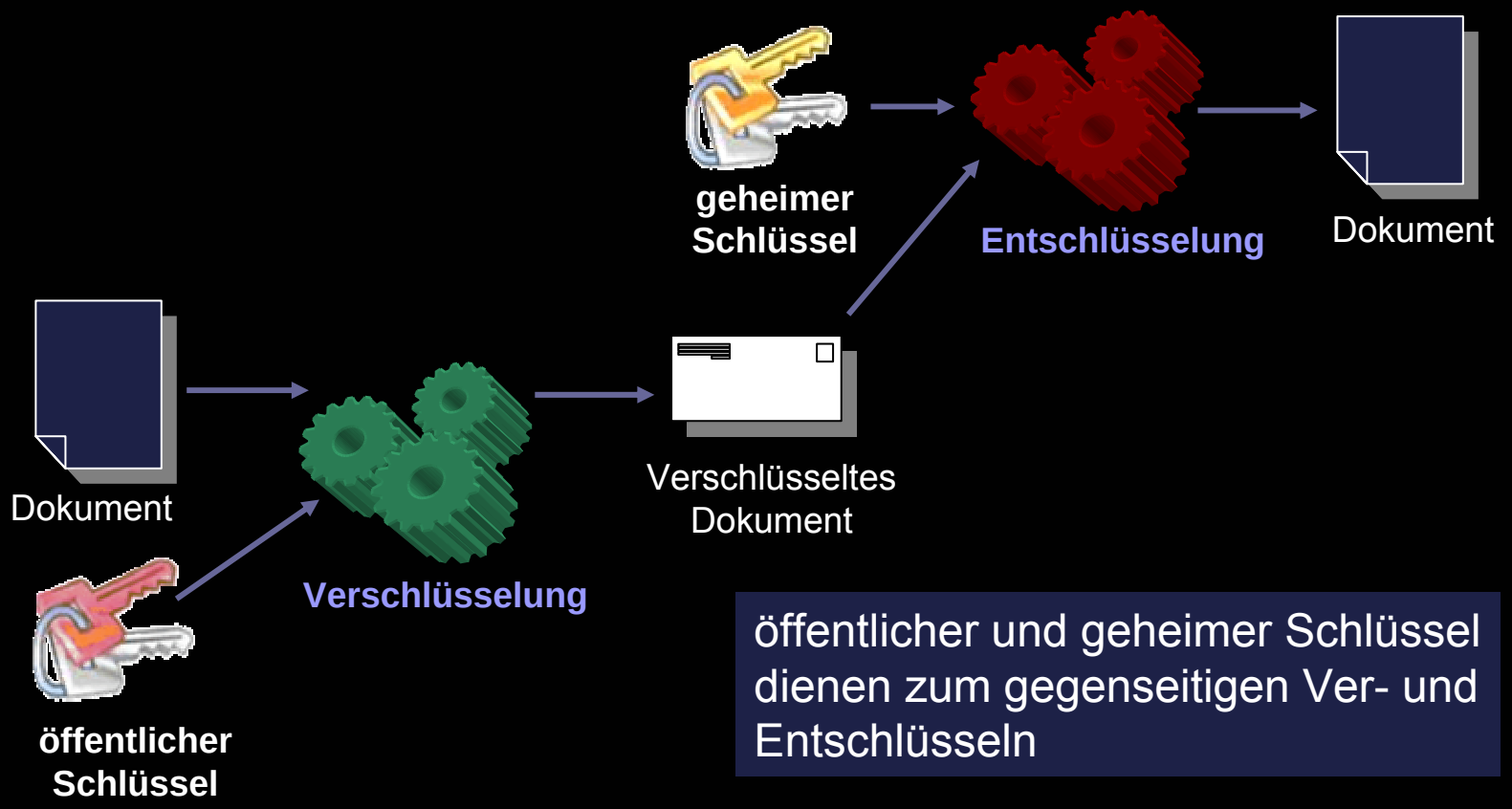
5. Web of Trust
5.1 Kryptografische Grundlagen

- Asymmetrische Verschlüsselungsverfahren
  - Voraussetzung dazu sind Funktionen/Verfahren, die (praktisch) **nicht umkehrbar** sind (z.B. Primfaktorenzerlegung im RSA-Verfahren)



5. Web of Trust
5.1 Kryptografische Grundlagen

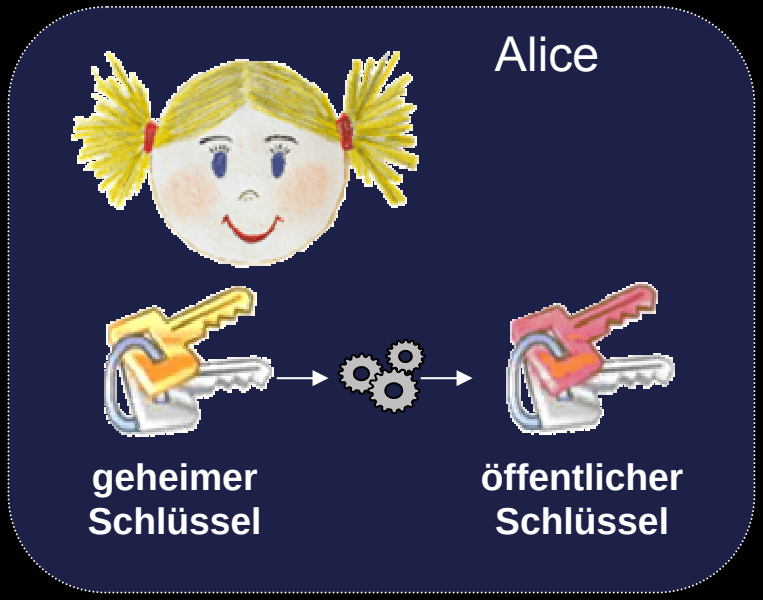
- Asymmetrische Verschlüsselungsverfahren

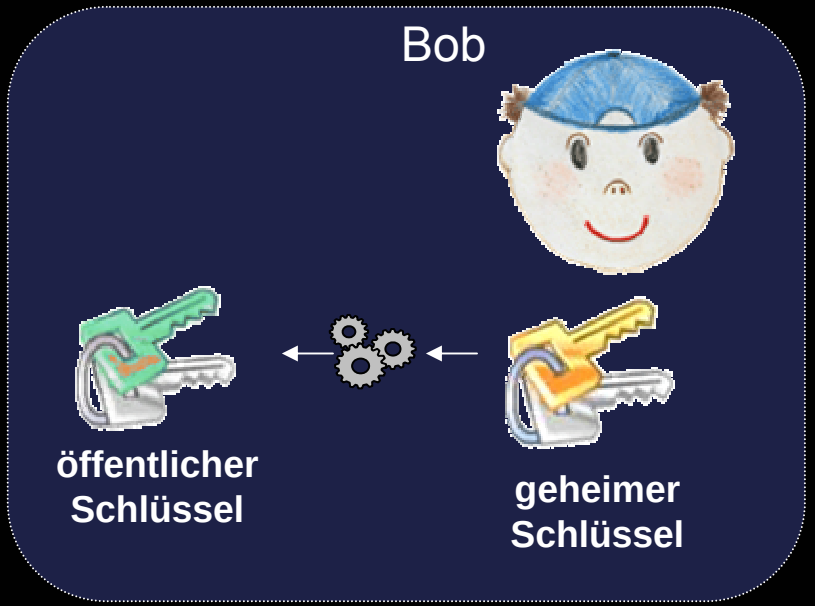


öffentlicher und geheimer Schlüssel dienen zum gegenseitigen Ver- und Entschlüsseln

5. Web of Trust
5.1 Kryptografische Grundlagen

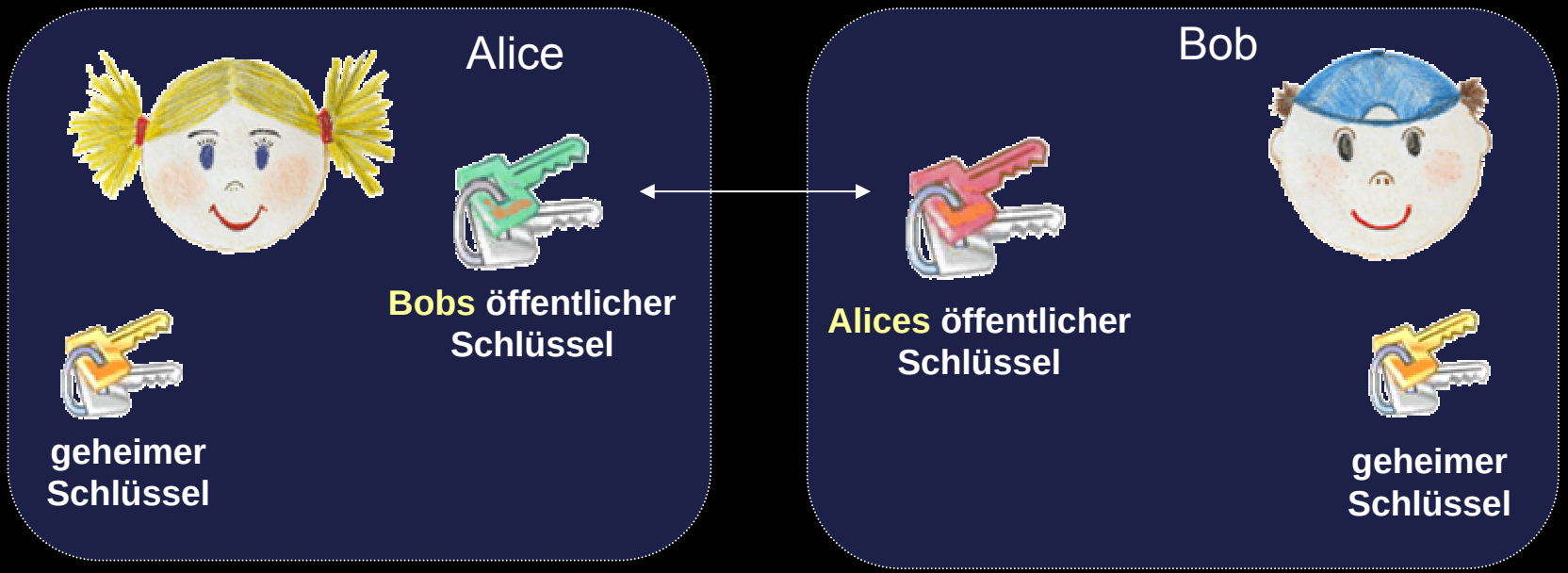
- Asymmetrische Verschlüsselungsverfahren
  - Sender **behält den geheimen Schlüssel** für sich
  - nur der **öffentliche Schlüssel wird an alle weitergegeben**, die mit dem Sender kommunizieren wollen





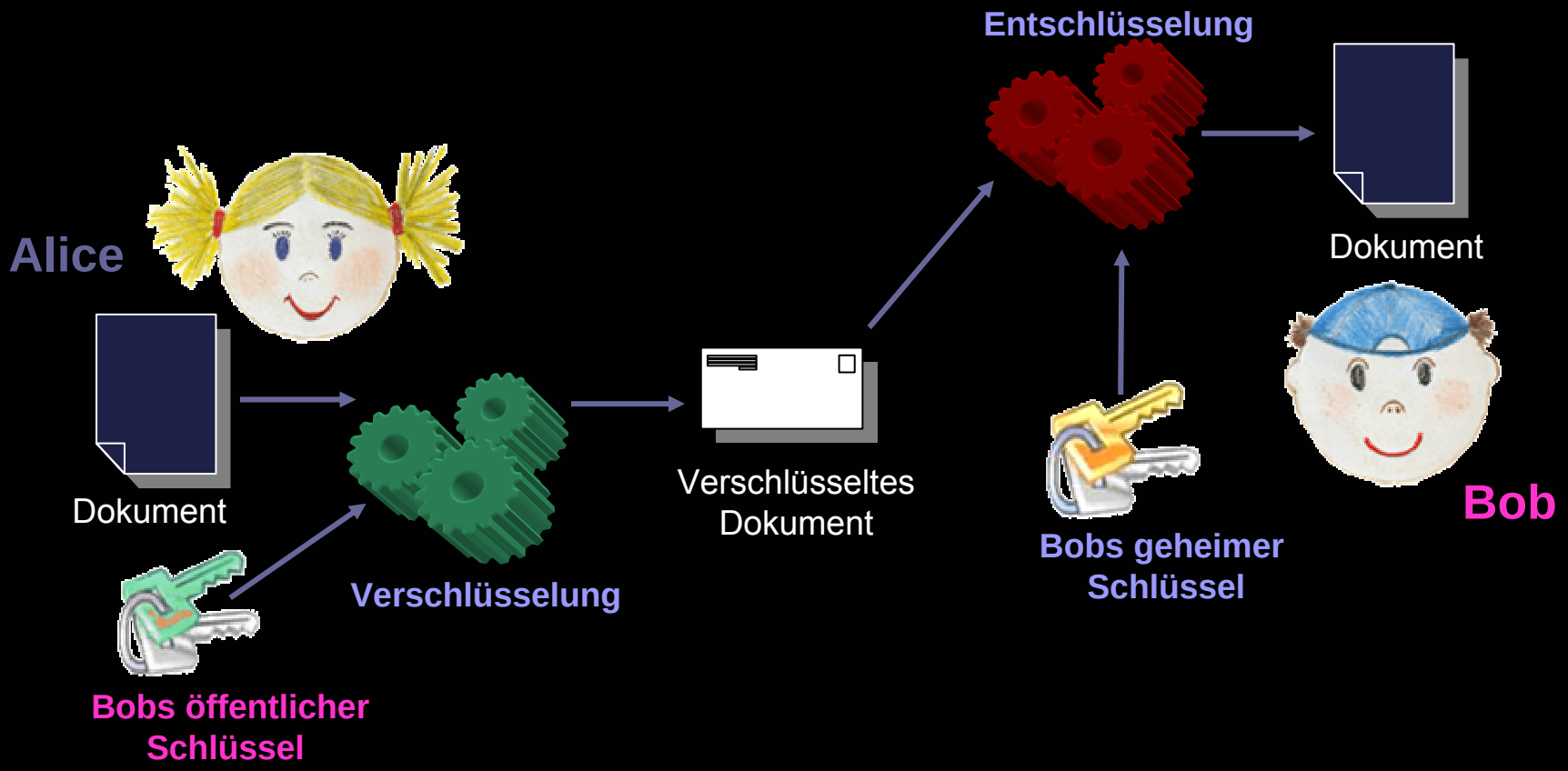
5. Web of Trust
5.1 Kryptografische Grundlagen

- Asymmetrische Verschlüsselungsverfahren
  - Sender **behält den geheimen Schlüssel** für sich
  - nur der **öffentliche Schlüssel wird an alle weitergegeben**, die mit dem Sender kommunizieren wollen



5. Web of Trust
5.1 Kryptografische Grundlagen

- Asymmetrische Verschlüsselungsverfahren



Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.1.1 Sicherheitsziele

5.1.2 Kryptografische Verfahren

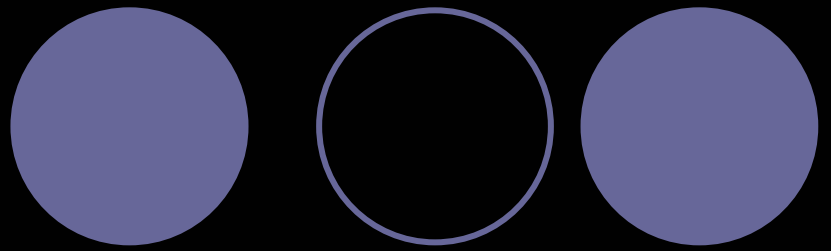
5.1.3 Digitale Signaturen

5.1.4 Zertifizierung

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

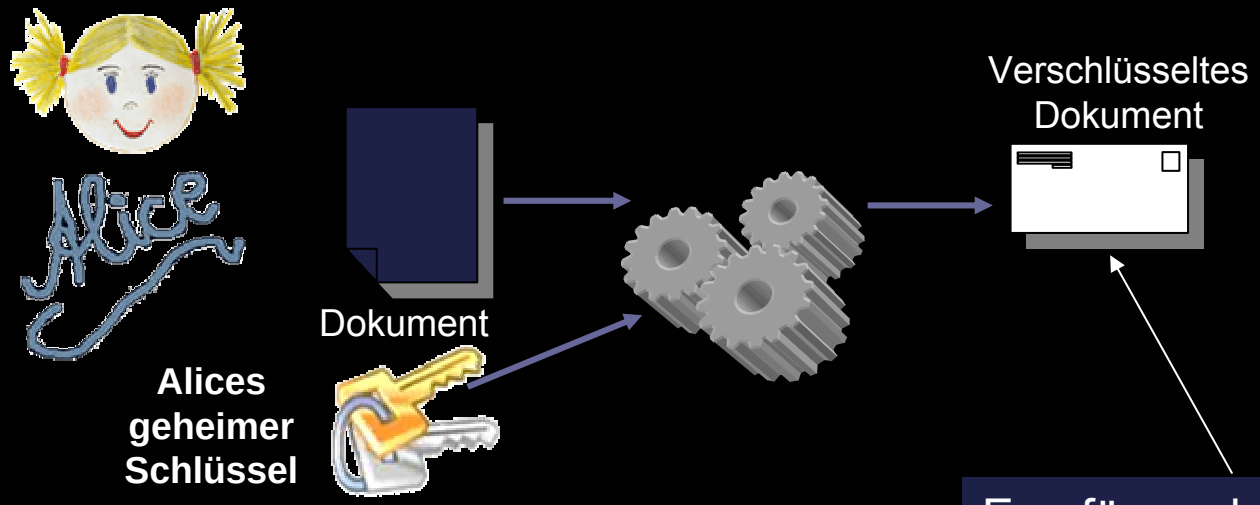
5. Web of Trust
5.1 Kryptografische Grundlagen



- Digitale Signaturen
  - Asymmetrische Verschlüsselung garantiert, dass nur der beabsichtigte Empfänger (Bob) tatsächlich die Nachricht entschlüsseln kann
  - Was aber, wenn Bob sicher gehen möchte, dass
    (a) die Nachricht tatsächlich von Alice stammt und
    (b) die Nachricht unterwegs nicht verfälscht wurde….
  - Idee: drehe das Verschlüsselungsverfahren mit öffentlichem Schlüssel einfach um:
    - Alice verschlüsselt eine Nachricht für Bob mit ihrem geheimen Schlüssel
    - Bob kann diese Nachricht mit dem öffentlichen Schlüssel von Alice entschlüsseln

5. Web of Trust
5.1 Kryptografische Grundlagen

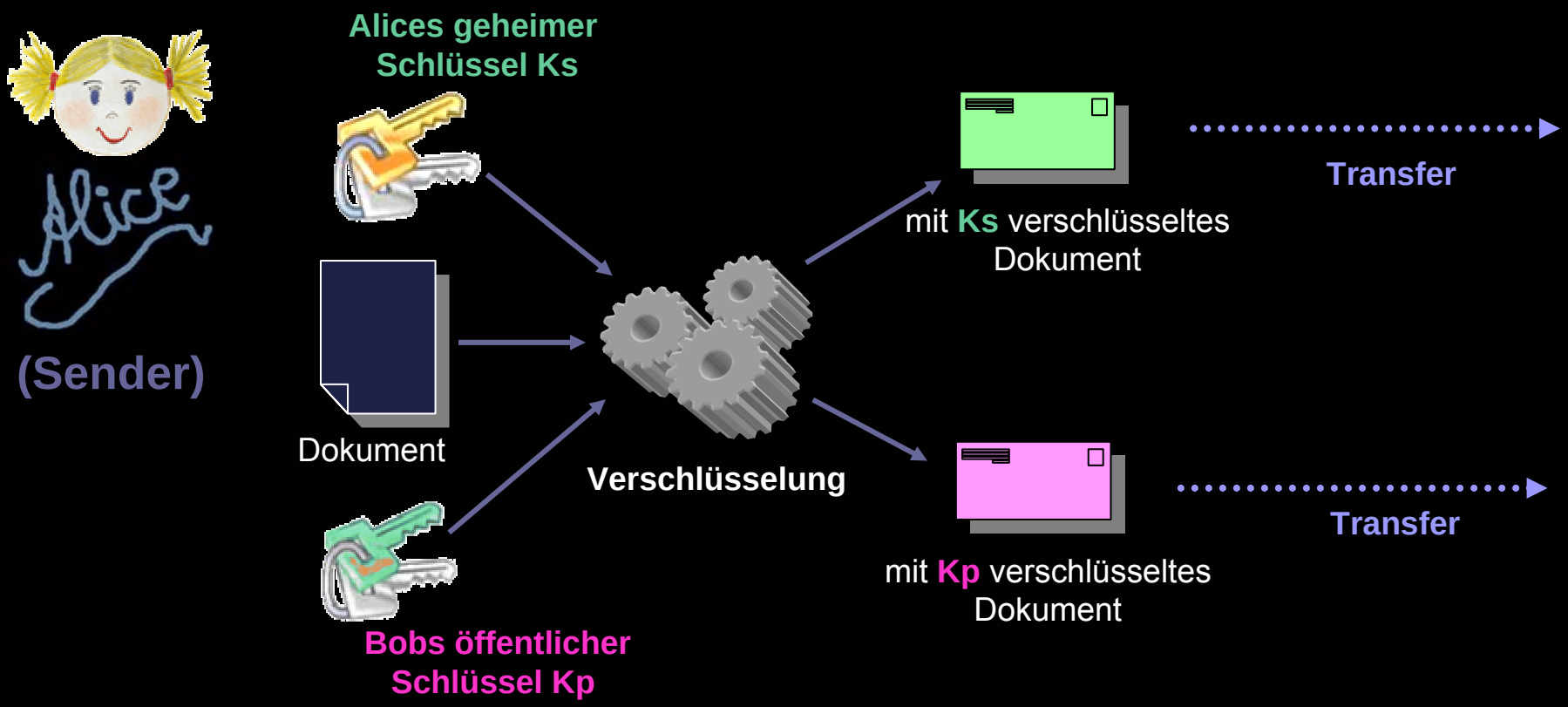
- Digitale Signaturen



Empfänger kann 100% sicher sein, dass **nur Alice** diese Nachricht verschlüsselt haben kann

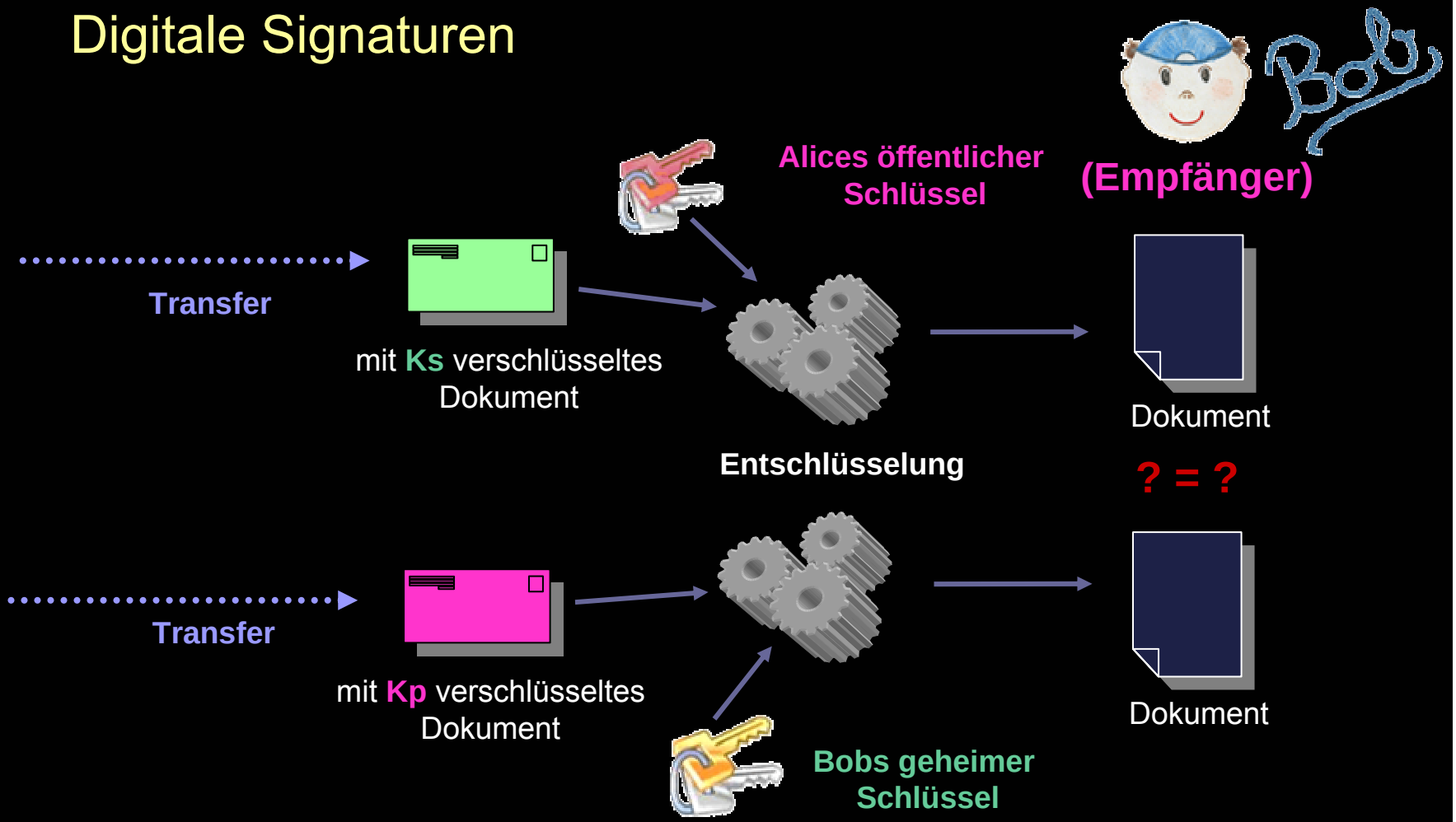
5. Web of Trust
5.1 Kryptografische Grundlagen

- Digitale Signaturen



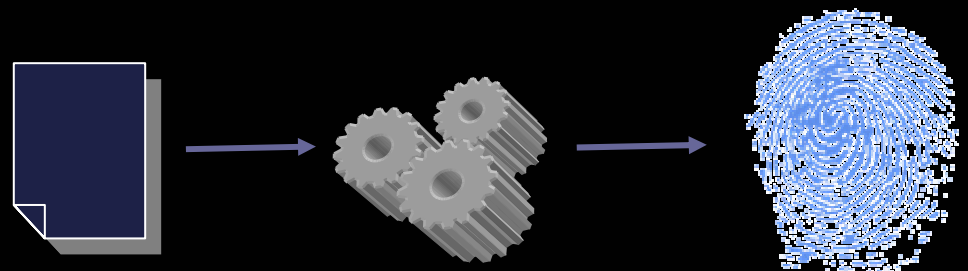
5. Web of Trust
5.1 Kryptografische Grundlagen

- Digitale Signaturen

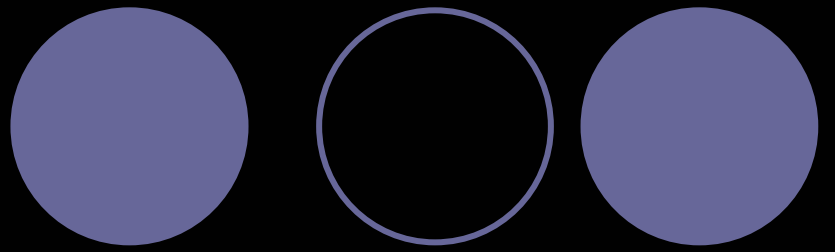


5. Web of Trust
5.1 Kryptografische Grundlagen

- Digitale Signaturen
  - Problem:
    Jeder, der Alices öffentlichen Schlüssel besitzt, kann das versendete Dokument lesen (→ Geheimhaltung)
  - Lösung:
    Versende nicht vollständiges Dokument, sondern nur „Fingerabdruck“ zum Vergleich



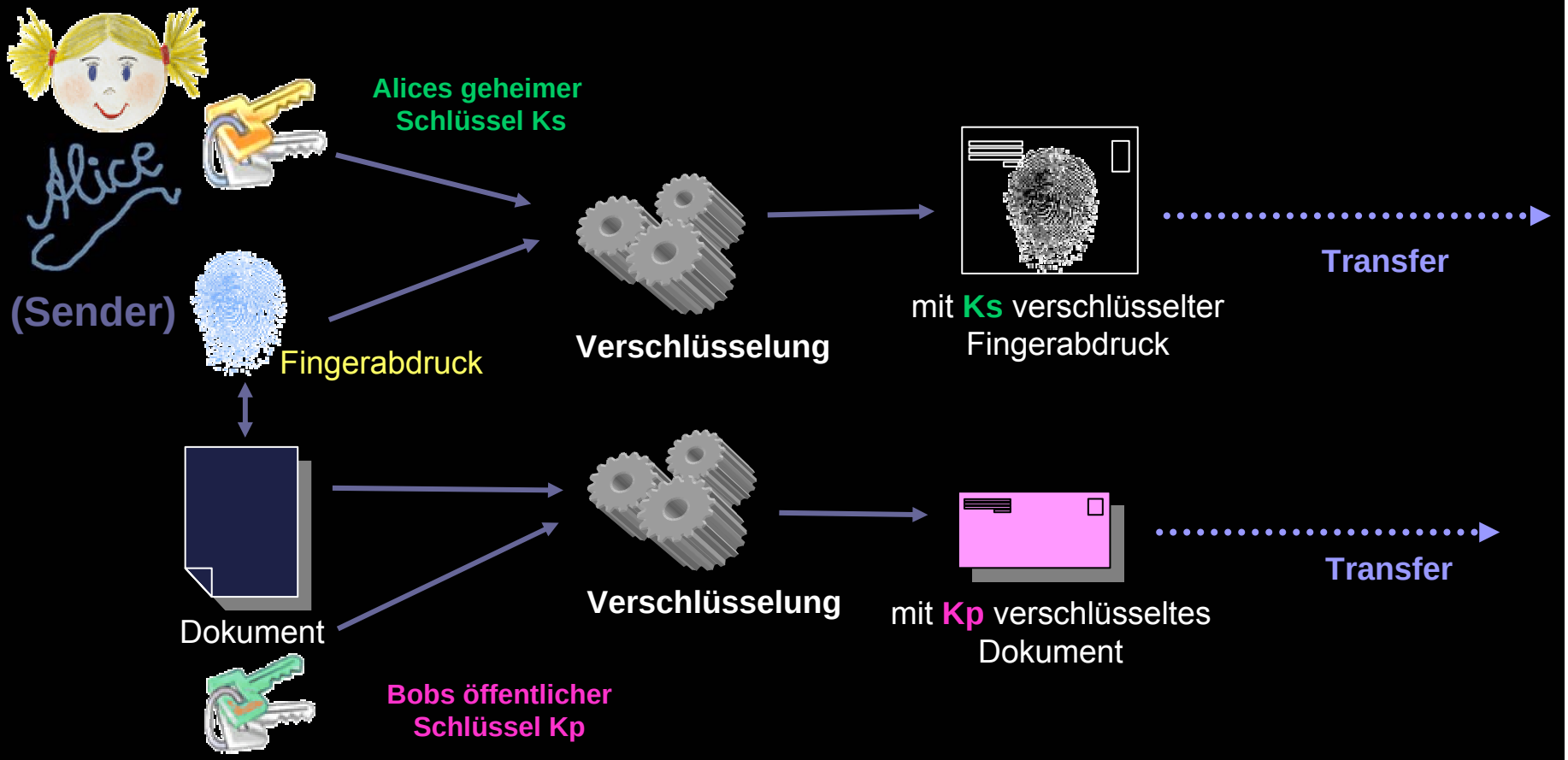
5. Web of Trust
5.1 Kryptografische Grundlagen



- Digitale Signaturen
  - Ein Fingerabdruck muss folgende **Eigenschaften** besitzen:
    - Er ist wesentlich **kleiner** als das Original (Komprimierung)
    - Er **identifiziert das Original** mit sehr hoher Wahrscheinlichkeit (Sicherheit), d.h.
    - die Wahrscheinlichkeit, dass zwei Originale denselben Fingerabdruck besitzen ist sehr, sehr gering (Kollisionsresistenz).
  - Aufgrund ihrer Eignschaften werden diese Funktionen auch als **Modification Detection Codes** (MDC) bezeichnet (Integrität).
    - Bsp.: MD5, SHA-1, RIPEMD-160
  - Wird ein MDC innerhalb eines Public Key Verfahrens mit dem geheimen Schlüssel des Versenders verschlüsselt

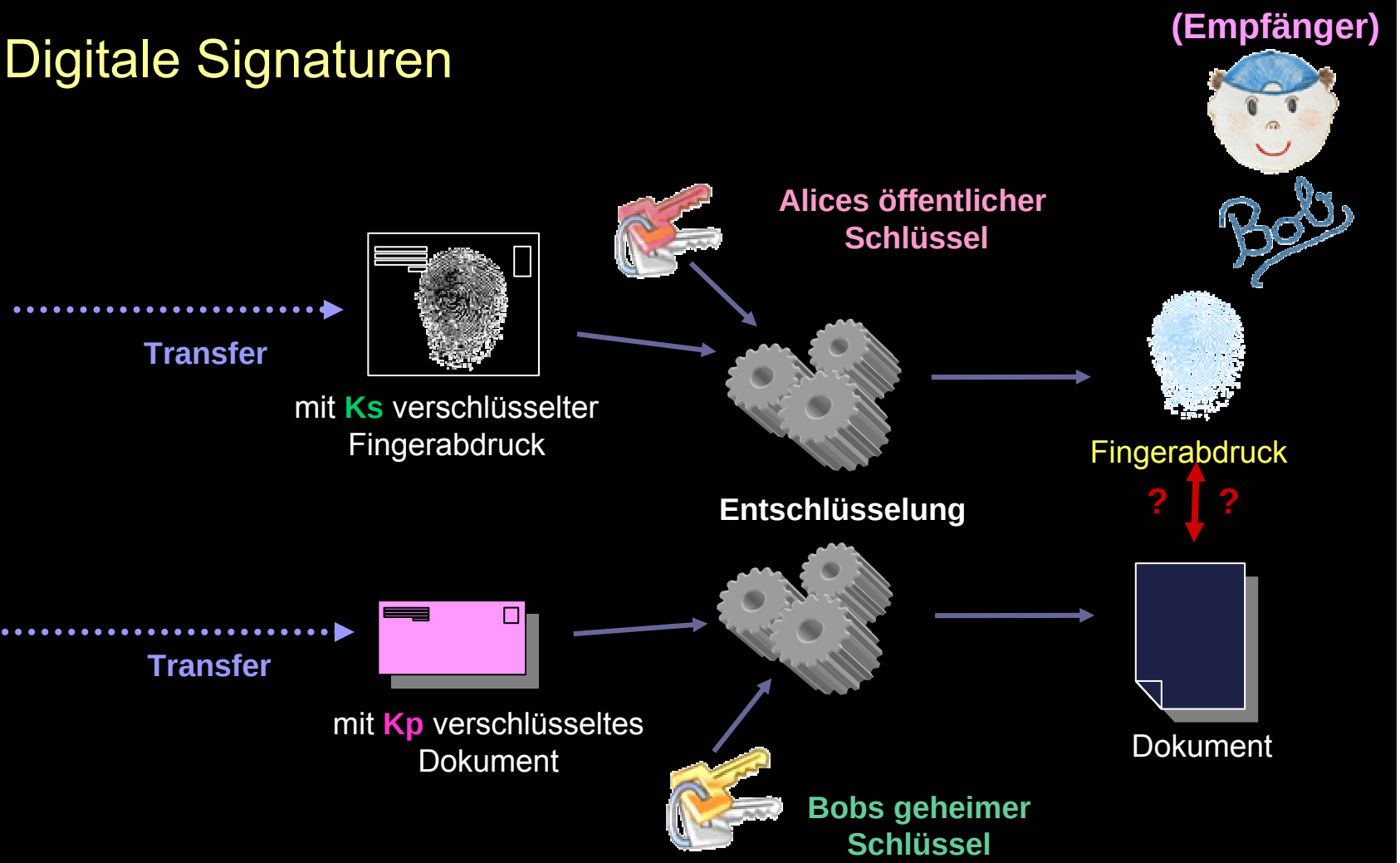
5. Web of Trust
5.1 Kryptografische Grundlagen

- Digitale Signaturen



5. Web of Trust
5.1 Kryptografische Grundlagen

- Digitale Signaturen



Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.1.1 Sicherheitsziele

5.1.2 Kryptografische Verfahren

5.1.3 Digitale Signaturen

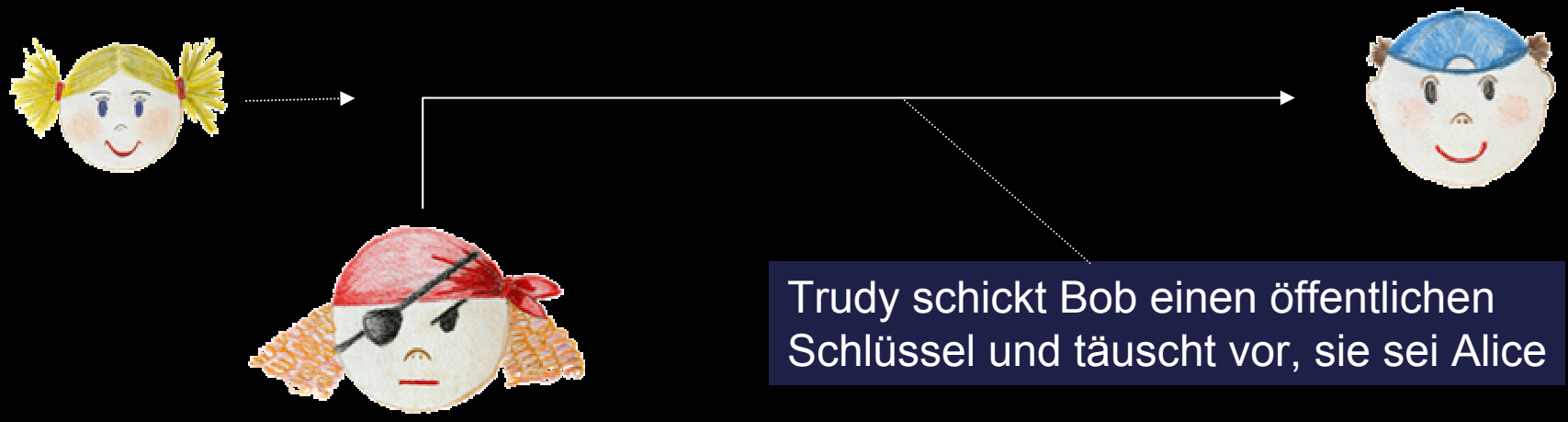
5.1.4 Zertifizierung

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5. Web of Trust
5.1 Kryptografische Grundlagen

- Zertifikate und Sicherheitsinfrastrukturen
  - Wie kann Bob eigentlich sicher sein, dass der öffentliche Schlüssel von Alice eigentlich tatsächlich Alice gehört??
  - Trudy könnte versuchen, Bob vorzutäuschen, sie sei Alice



5. Web of Trust
5.1 Kryptografische Grundlagen

- Zertifikate und Sicherheitsinfrastrukturen
  - **Zentrale Behörde (Zertifizierungsstelle / CA / Trust Center)**
    - **prüft Identität** der Kommunikationspartner und
    - **hinterlegt** deren **öffentliche Schlüssel**

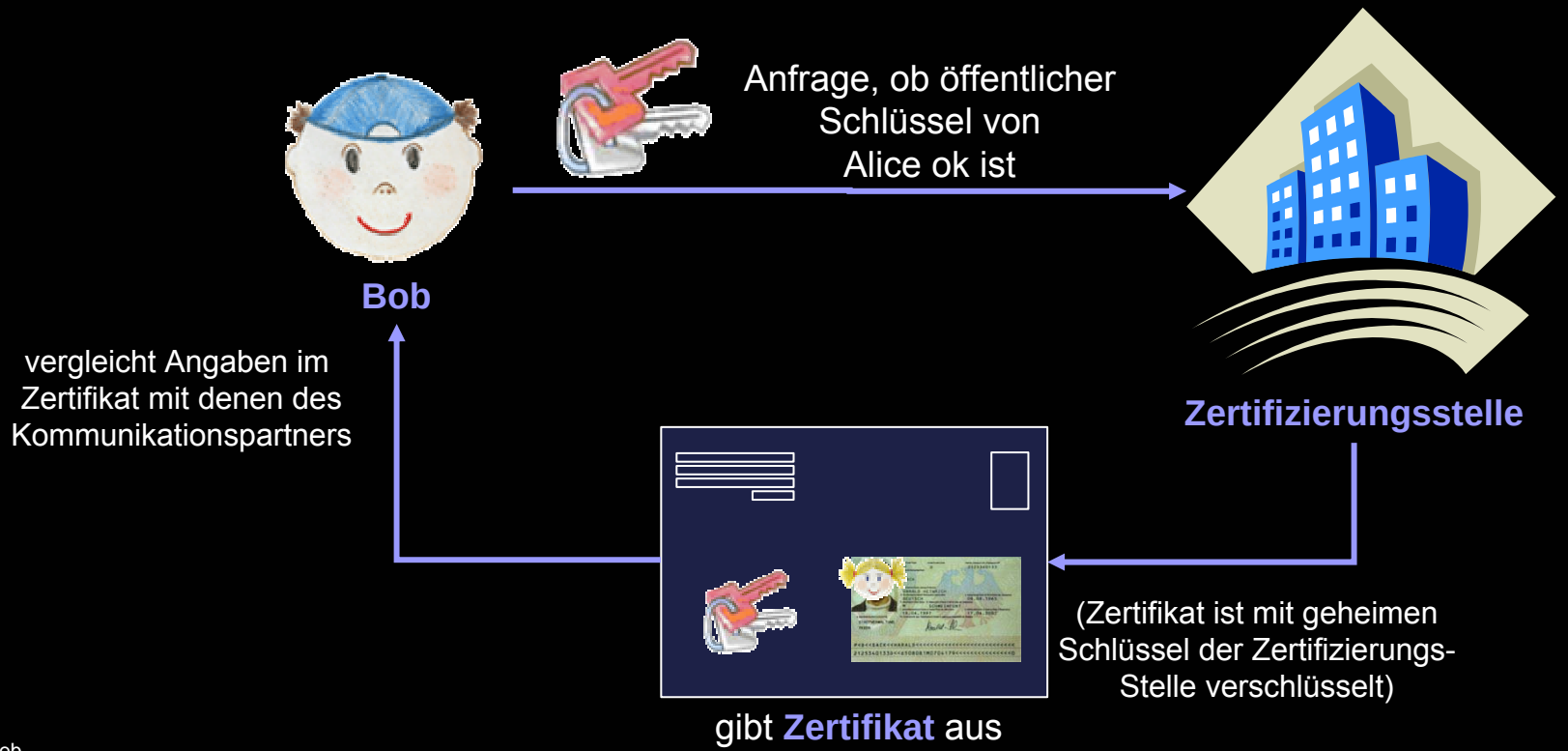
    - **vergibt** auf Anfrage hin einen angeforderten **öffentlichen Schlüssel**
    - **überprüft** auf Anfrage hin einen angefragten **öffentlichen Schlüssel**

5. Web of Trust
5.1 Kryptografische Grundlagen

- Zertifikate und Sicherheitsinfrastrukturen
  - **Zentrale Behörde (Zertifizierungsstelle / CA / Trust Center)**
    - Anmelden eines öffentlichen Schlüssels und Überprüfung der Identität des Besitzers

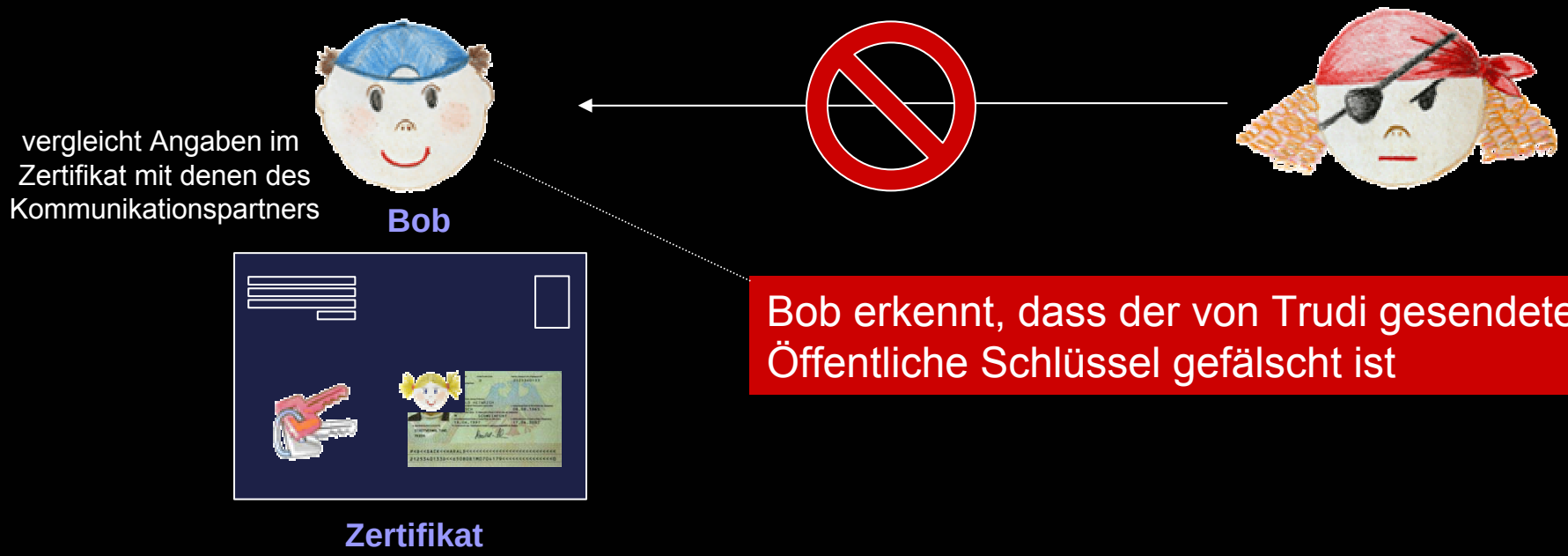
5. Web of Trust
5.1 Kryptografische Grundlagen

- Zertifikate und Sicherheitsinfrastrukturen
  - **Zentrale Behörde (Zertifizierungsstelle / CA / Trust Center)**
    - Überprüfung eines öffentlichen Schlüssels



5. Web of Trust
5.1 Kryptografische Grundlagen

- Zertifikate und Sicherheitsinfrastrukturen
  - **Zentrale Behörde (Zertifizierungsstelle / CA / Trust Center)**
    - Bob überprüft anhand des Zertifikats, ob der von Trudi gesendete öffentliche Schlüssel mit dem im Zertifikat angegebenen übereinstimmt



Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.2 XMLEncryption und XMLSignature

5.2.1 XMLEncryption

5.2.2 XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- Semantic Web und Kryptografie
  - Auf welche Weise kann Kryptografie das Semantic Web unterstützen?
    - Geheimhaltung / Vertraulichkeit
      durch unterschiedliche Verschlüsselungstechniken
    - Authentifikation / Autorisierung und Integrität
      durch asymmetrische Verschlüsselungsverfahren und digitale Signaturen
  - von Semantic Web Inhalten

Web of Trust

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption und XMLSignature
  - **Problem:**
    herkömmliche Verschlüsselungsverfahren erlauben nur die explizite Verschlüsselung von einzelnen **Ressourcen als Ganzes**
  - **Situation 1:**
    - Eine Ontologie, die in einer OWL-Datei vorliegt, kann nur über die Verschlüsselung der gesamten Datei gesichert werden
    - Unterschiedliche Nutzer sollen aber - je nach Berechtigung - unterschiedliche Teile dieser Datei lesen können
  - **Situation 2:**
    - Eine Semantic Web Ressource setzt sich aus Teilen zusammen, die aus unterschiedlichen Quellen stammen
    - Sind alle Teile der Ressource gleichermaßen vertrauenswürdig?

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption
  - 2002 W3C-Recommentation
  - erlaubt Verschlüsselung von XML-basierten Dokumenten auf unterschiedlichen Granularitätstufen
    - komplettes XML-Dokument
    - komplettes XML-Element inkl. Name, Inhalt und Kind-Elemente
    - Inhalt eines XML-Elements
    - Textinhalt eines XML-Elements ohne Kind-Elemente
  - Unterschiedliche verwendete Verschlüsselungsverfahren sind dabei via URI-Angabe frei wählbar

```
<EncryptedData type="uri">
  verschlüsselter Inhalt
</EncryptedData>
```

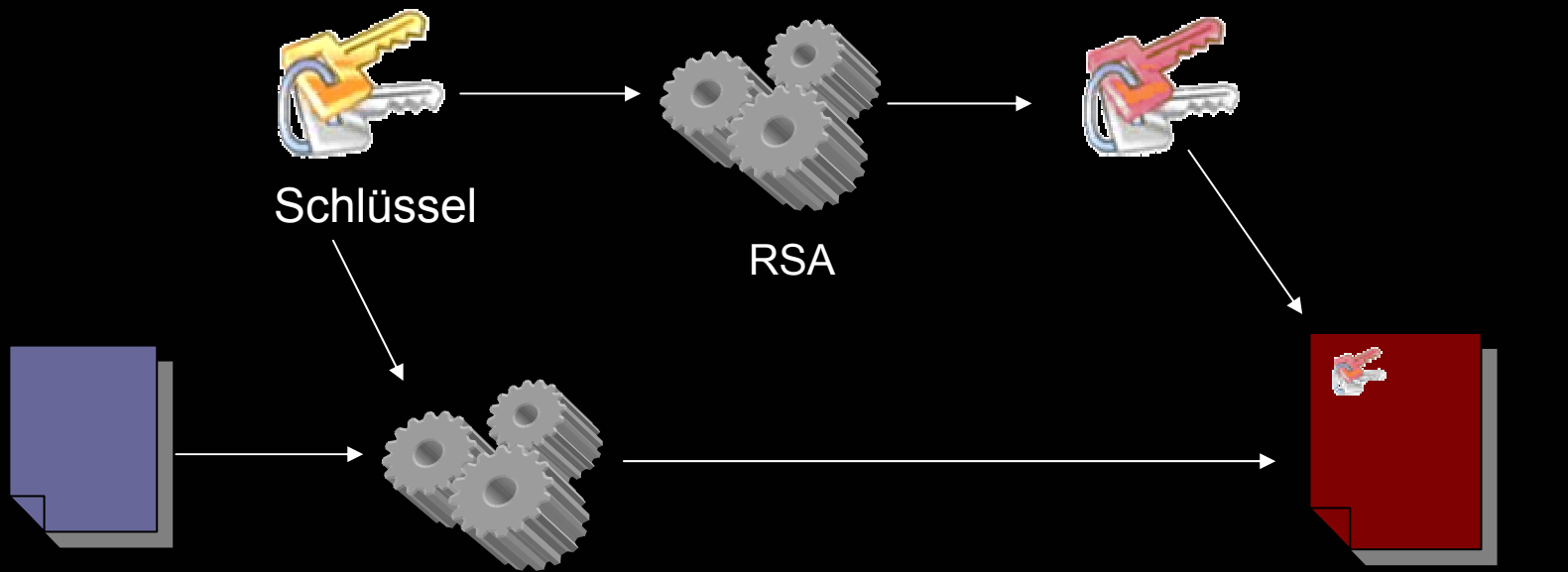
5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption
  - Ergebnis der Verschlüsselung ist <EncryptedData> Element
  - <EncryptedData> Element ersetzt ursprüngliches Element
  - <EncryptedData> Elemente dürfen nicht verschachtelt werden
  - <EncryptedData> Element kann wieder verschlüsselt werden
  - Über diese Superencryption hierarchische Zugriffsrechte definierbar

```
<EncryptedData Id Type MimeType Encoding>
  <EncryptionMethod/>
  <KeyInfo/>
  <CipherData/>
  <EncryptionProperties>
</EncryptedData>
```

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption
  - Beispiel



5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption
  - Beispiel

```
<EncryptedData Id="xy"
  type="http://www.w3.org/2001/04/xmlenc#Element"
  xmlns="http://www.w3.org/2001/04/xmlenc#">

   <EncryptionMethod Algorithm=
                          "http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
   <KeyInfo xmlns="http://www.w3.org/2001/04/xmldsig#">

     <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
       <EncyptionMethod Algorithm=
                          "http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
       <ds:KeyInfo xmlns:ds="http://www.w3.org/2001/04/xmldsig#">
         <ds:KeyName>Uni Jena</KeyName>
       </ds:KeyInfo>
   …
```

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLEncryption
  - Beispiel

```
…
        <CipherData>
           <CipherValue>afds45765(OZHKJFNSDK8ohkh8…</CipherValue>
        </CipherData>
     </EncryptedKey>
  </KeyInfo>

  <CipherData>
     <CipherValue>SDHFVUIK8ohkh847gzT454Kjghfjkjh56…</CipherValue>
  </CipherData>
</EncryptedData>
…
```

Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.2 XMLEncryption und XMLSignature

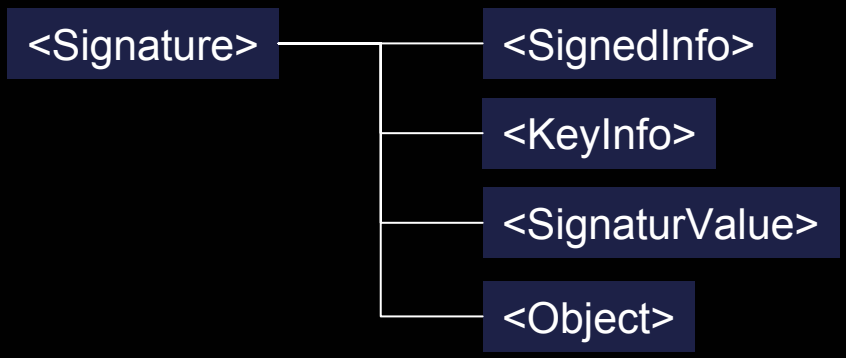
5.2.1 XMLEncryption

5.2.2 XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

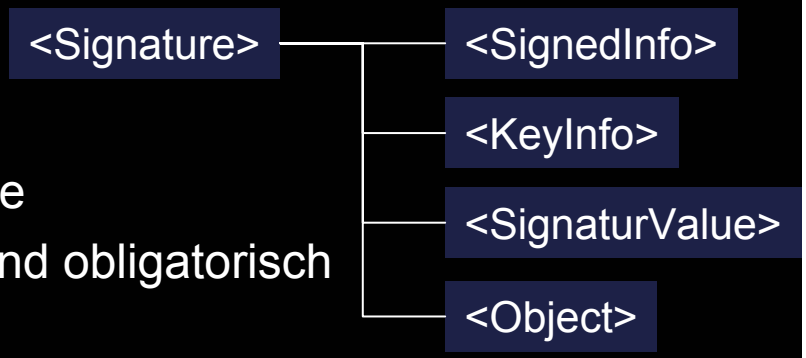
5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature
  - 2002 W3C Recommentation (älter als XML Encryption)
  - digitale Signatur für XML-Dokumente
  - zur Sicherung von Authentizität, Integrität und Verbindlichkeit



  - unterscheide
    - **Enveloped Signature**
      Signatur ist in das unterschriebene Objekt mit eingebettet
    - **Enveloping Signature**
      unterschriebenes Objekt ist in die Signatur eingebettet
    - **Detached Signature**
      unterschriebenes Objekt wird lediglich über URI referenziert

5. Web of Trust
5.2 XMLEncryption und XMLSignature

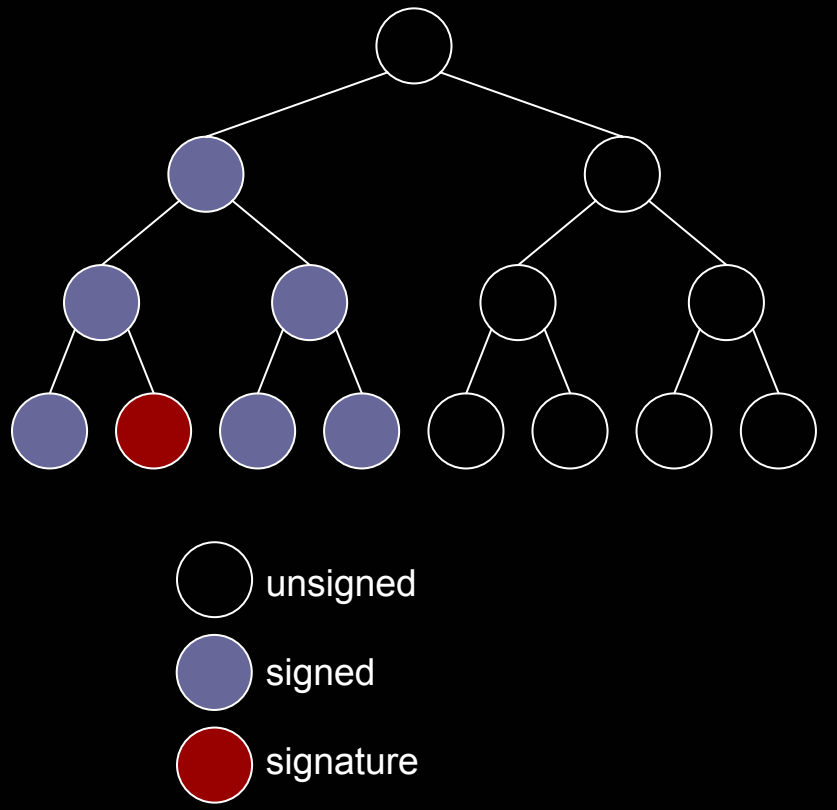


- XMLSignature
  - **Signature**
    - Wurzelelement von XML Signature
    - SignedInfo und SignatureValue sind obligatorisch
    - KeyInfo und Object sind optional
  - **SignedInfo**
    - enthält Kanonisierungs- und Signaturverfahren
    - enthält die Referenzen (Reference)auf die signierten Daten
  - **SignatureValue**
    - enthält Signatur (Base64) des SignedInfo Elements
  - **KeyInfo**
    - notwendig zur Validierung der Signatur beim Empfänger
    - enthält Informationen über Zertifikate, Schlüssel,Schlüsselnamen oder Public-Key-Management Daten
    - zeigt auf den öffentlichen Schlüssel oder enthält diesen

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature
  - **Enveloped Signature**
    Signatur ist in das unterschriebene Objekt mit eingebettet

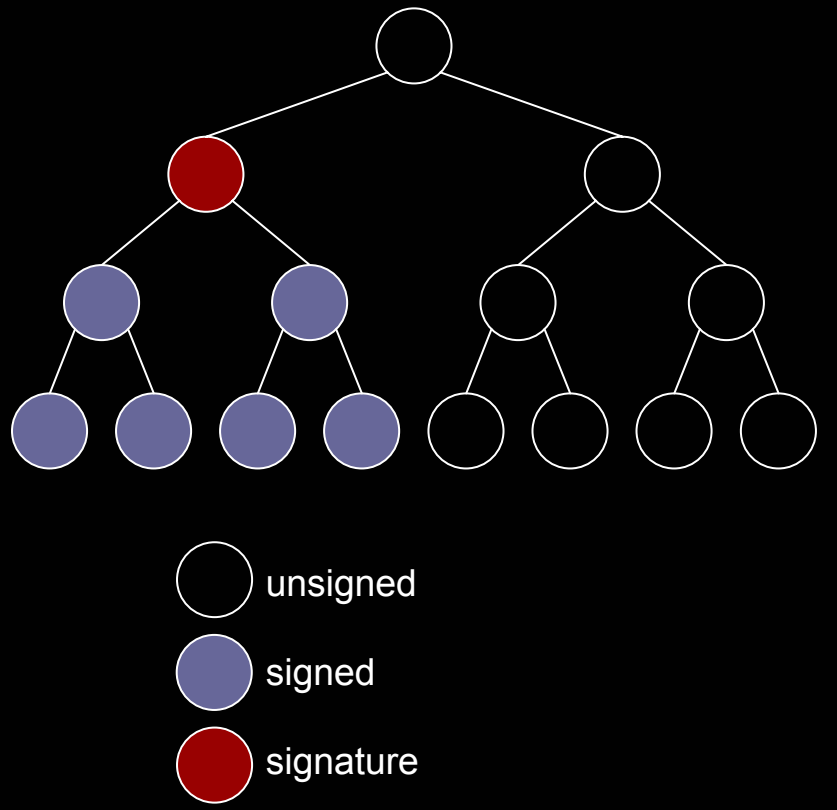
```
<dokumentPart Id="dok">
  <inhalt> … </inhalt>
  <Signature>
    …
     <Reference URI="dok"/>
    …
  </Signature>
</dokumentPart>
```



5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature
  - **Enveloping Signature**
    unterschriebenes Objekt ist in die Signatur eingebettet

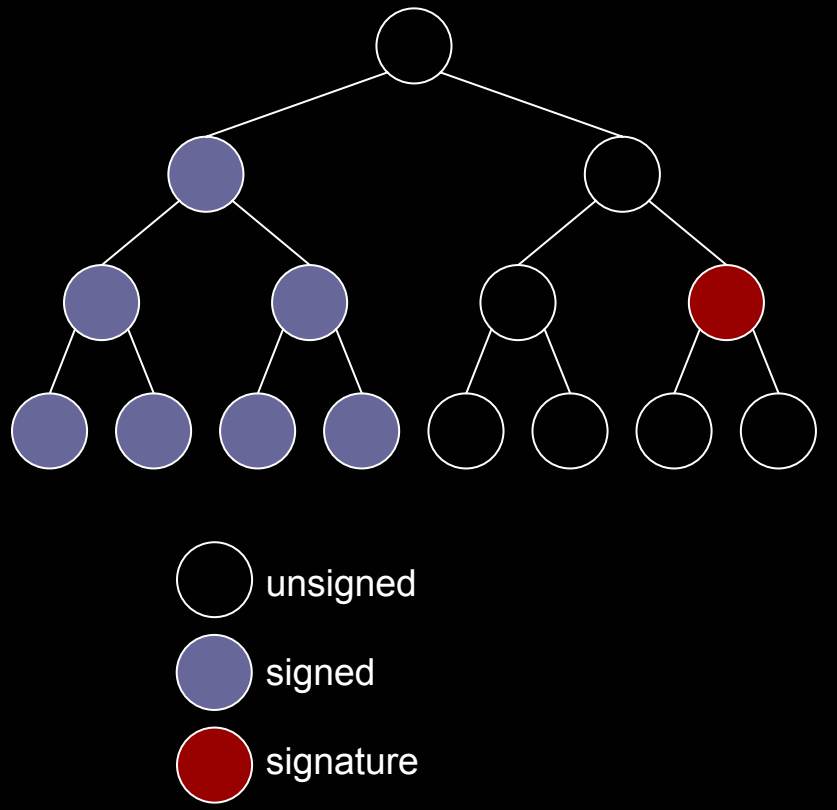
```
<Signature>
 …
  <Reference URI="obj"/>
 …
  <Object Id="obj">
    <dokumentPart>
    …
    </dokumentPart>
  </Object>
</Signature>
```



5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature
  - **Detached Signature**
    unterschriebenes Objekt wird lediglich über URI referenziert

```
<dokumentPart>
  <Signature>
   …
    <Reference URI="http://..."/>
   …
  </Signature>
</dokumentPart>
```



5. Web of Trust
5.2 XMLEncryption und XMLSignature

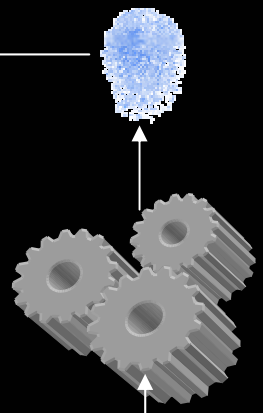
- XMLSignature
  - **SOAP Nachricht**
    - Digitale Signatur im SOAP-Header, die den Inhalt des SOAP-Body bzw. einzelne Teile davon signiert

SOAP HEADER

```
<Signature>
 <Reference URI="SEC"/>
  …
</Signature>
```

SOAP Body

```
<Object ID="SEC" …>
  …
<Object>
```



5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature – Ablauf
  - Unterscheide Generierung und Validierung der Signatur
  - Semantisch gleiche Dokumente können auf unterschiedliche syntaktische Weise beschrieben werden
  - Daher Kanonisierung notwendig, d.h. Elemente werden vorher in eine Normalform gebracht
  - Zudem können Transformierung definiert werden, d.h. Elemente werden in anderes Format umgewandelt
  - Nach Kanonisierung und ev. Notwendiger Transformierung kann die Signatur generiert werden

5. Web of Trust
5.2 XMLEncryption und XMLSignature

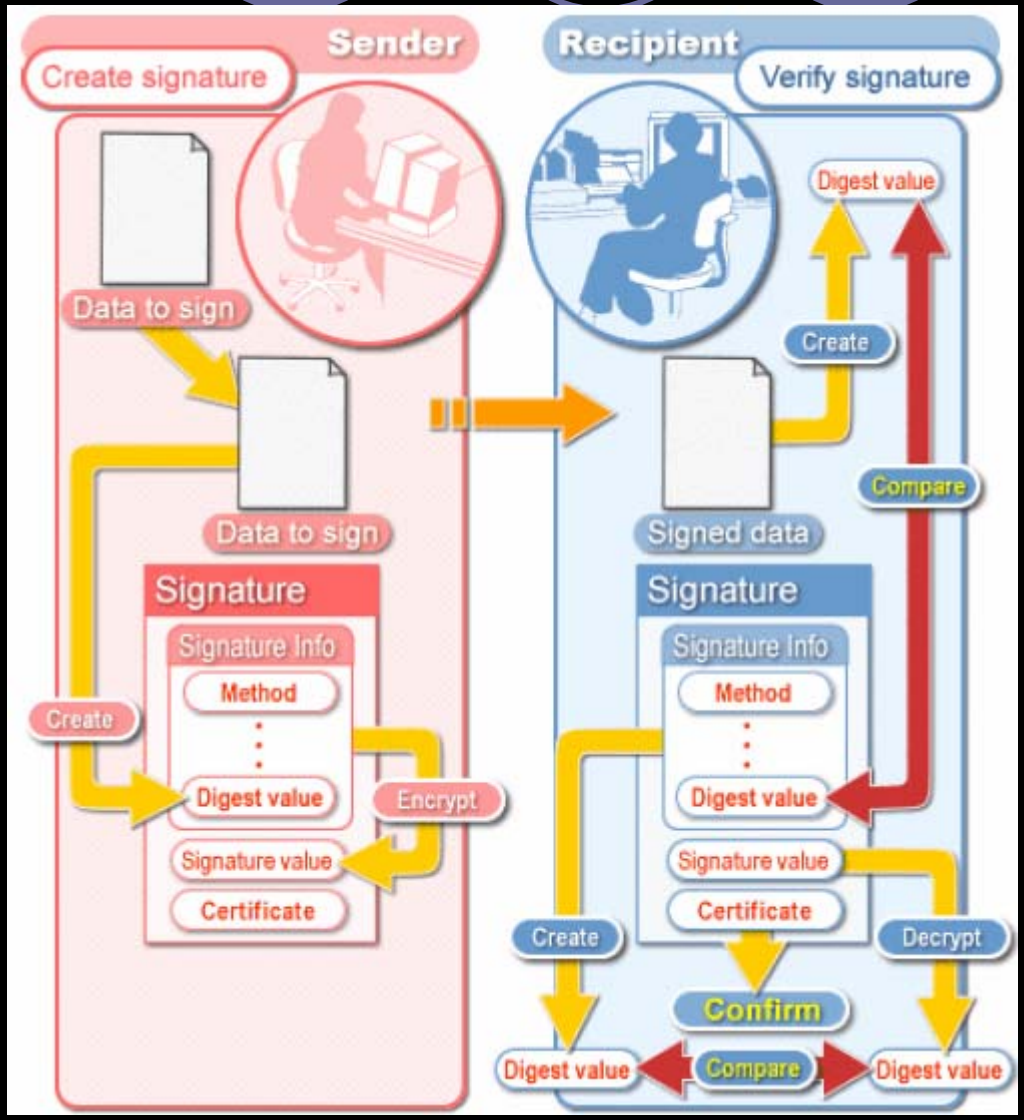
- XMLSignature – Ablauf
  - **Generierung**
    1. Erzeugen der **Referenzen** (für jedes zu signierende Element)
       1. Anwenden von Transformationen
       2. Darüber Fingerabdruck berechnen
       3. Erzeugen des Reference Elements (Identifikation,Transformationen, MDC, Fingerabdruck)
    2. Erzeugen der **Signatur**
       1. Erzeugen des SignedInfo Elements (mit obigen Reference Elementen)
       2. Kanonisieren des SignedInfo Elements, darüber Fingerabdruck berechnen und diesen verschlüsseln
       3. Erzeugen des Signature Elements (SignedInfo, KeyInfo, Signaturwert)

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature – Ablauf
  - **Validierung**
    - Validieren der **Referenzen** (SignedInfo kanonisiert)
      - Ermitteln der Daten (URI) und nötigenfalls Transformationen anwenden
      - Fingerabdruck laut DigestMethod berechnen
      - Diesen mit Fingerabdruck aus DigestValue vergleichen
    - Validieren der **Signatur**
      - Ermitteln des Schlüssels aus KeyInfo oder anderer Quelle
      - Ermitteln der kanonisierten Form der SignatureMethod, berechnen des Fingerabduck über SignedInfo, entschlüsseln des Fingerabdruck aus SignatureValue und beide vergeichen

5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature



5. Web of Trust
5.2 XMLEncryption und XMLSignature

- XMLSignature Beispiel

```
<Signature Id="MyFirstSignature„ xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/xml−c14n"/>
    <SignatureMethod Algorithm="http://www.w3.org/rsa−sha1"/>
    <Reference URI="http://www.foo .org/dsci1297.jpg">
      <DigestMethod Algorithm="http://www.w3.org/sha1"/>
      <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue> MC0CFFrVLtRlka4455 </SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509SubjectName> DN=Max Mustermann </X509SubjectName>
    </X509Data>
  </KeyInfo>
</Signature>
```

Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5.3.1 Grundbegriffe

5.3.2 Mathematisches Modell

5.3.3 Reputationsnetzwerke

5.3.4 Vertrauensstrategien

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Trust - Vertrauen

Vertrauen ist der individuelle Glaube an die positive Entwicklung von Ereignissen, meist im zwischenmenschlich-interaktiven Bereich, gebunden an die eigenen Wertvorstellungen und Erfahrungen….

Aus **systemtheoretischer Sicht**:
Vertrauen ist ein „*Mechanismus zur Reduktion sozialer Komplexität*“.

Dort wo die rationale Abwägung von Informationen (aufgrund unüberschaubarer Komplexität, wegen Zeitmangels zur Auswertung oder des gänzlichen Fehlens von Informationen überhaupt) nicht möglich ist, befähigt Vertrauen dennoch zu einer auf Intuition gestützten Entscheidung

(wikipedia.de)

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Trust - Reputation

Reputation bezeichnet die gesellschaftliche Wertschätzung einem Menschen oder einer Gruppe gegenüber….

In der **Marketingtheorie**: Summe von Einzelerwartungen und -erfahrungen über Vertrauenswürdigkeit und Kompetenz eines Anbieters

Nach chinesischer Denkweise hat jeder Mensch ein Gesicht.
Sein Gesicht wird ihm durch soziale Anerkennung gegeben oder durch Missachtung entzogen. Das Gesicht eines anderen zu wahren, heißt in erster Linie, seine Schwachstellen nicht bloßzulegen.
Wer Ansehen gibt, gewinnt damit zugleich selbst an Ansehen.
Wer einem Anderen das Gesicht nimmt, hat damit seines auch verloren.

(wikipedia.de)

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Web of Trust
  - Das Semantic Web ist (wie das Internet) ein **Open Publishing System**
    - Jeder kann publizieren
    - Keine Qualitätskontrolle
    - Keine zentrale Kontroll-Instanz

  → Erfordernis Informationen bezüglich Qualität/Verlässlichkeit zu filtern.

  - Grundlage dieser Filterung sind Voting-/Rating-/ und Reputationssysteme.

  - Aufgaben eines **Open Rating Systems**:
    - ***Aggregation*** von unterschiedlichsten Bewertungen aus unterschiedlichen Quellenzu einem einheitlichen Ranking
    - ***Meta-Ranking*** – Bewertung der Qualität der Bewertungen

Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5.3.1 Grundbegriffe

5.3.2 Mathematisches Modell

5.3.3 Reputationsnetzwerke

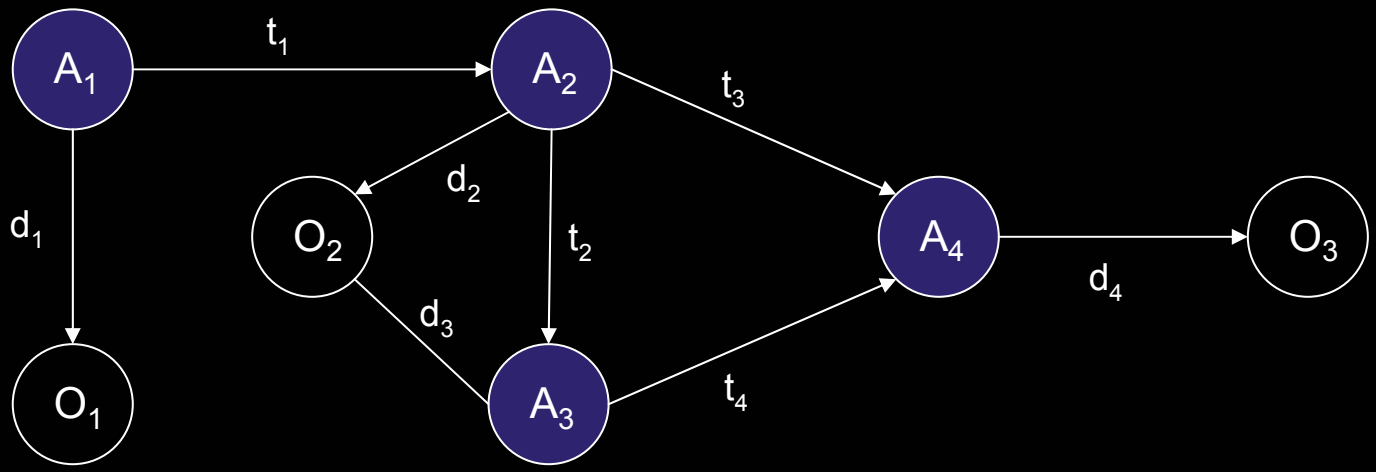
5.3.4 Vertrauensstrategien

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Meta-Ranking
  - Einfaches mathematisches Modell:
    - Objekte: $O := \{O_1, O_2, O_3, \ldots\}$
    - Agenten: $A := \{A_1, A_2, A_3, \ldots\}$
    - Bewertungen von Objekten: $D := \{d_1, d_2, d_3, \ldots\}$
    - Bewertungen von Agenten: $T := \{t_1, t_2, t_3, \ldots\}$
    - Partielle Funktion zur Bewertung von Objekten: $R: A \times O \rightarrow D$
    - Partielle Funktion zur Bewertung von Agenten: $W: A \times A \rightarrow T$

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Web of Trust

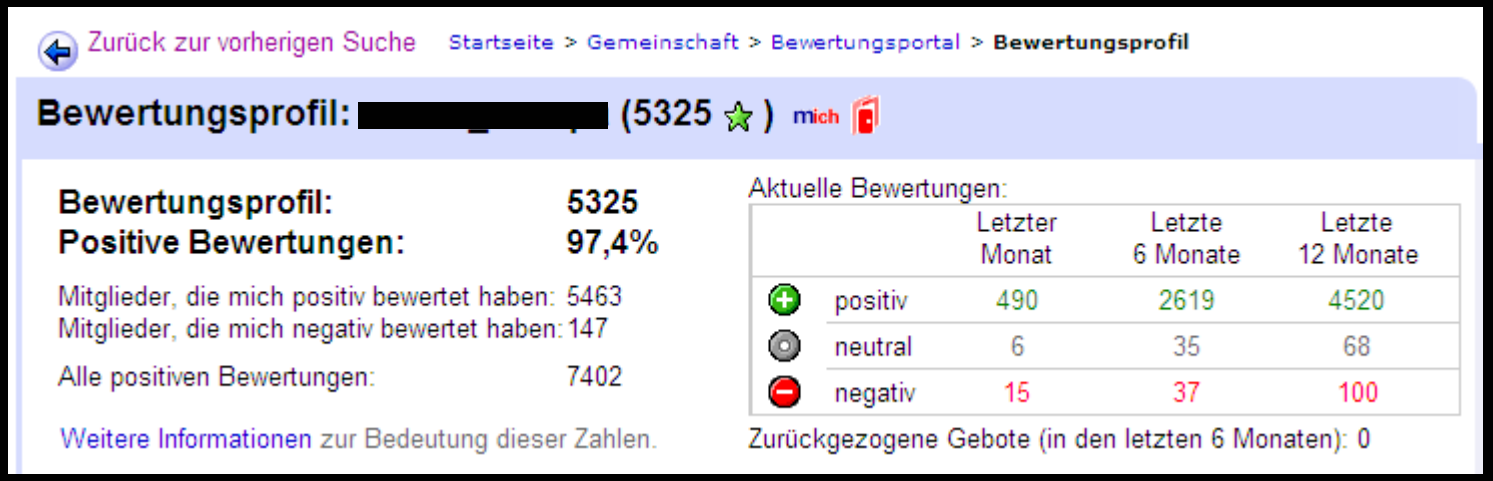


5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Web of Trust
  - **Rating-Problem**
    - Vervollständige die Matrix R mit Hilfe der Matrix W.
    - Wenn ein Agent ein Objekt nicht selber direkt bewertet hat, dann wird unter Ausnutzung von Vertrauensbeziehungen der Agenten untereinander berechnet, wie er dieses Objekt bewerten würde.
  - **Ranking-Problem**
    - Ordne eine Menge von Objekten aus der Sicht eines Agenten in die Reihenfolge gemäß ihrer Bewertung.
    - In den meisten Fällen reicht es, bezüglich der Reihenfolge die ersten N Objekte aufzulisten, daher **Top-N-Ranking-Problem**.

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Bsp. Ebay
  - Agenten werden von anderen Agenten hinsichtlich der Qualität eines Geschäftsablaufs bewertet
  - Ebay Bewertungen: {negativ, neutral, positiv}
  - Globales Rating wird einfach aus Anteil der positiven Bewertungen errechnet



5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Bsp. Modifizierter PageRank Algorithmus
  - Googles patentiertes Verfahren zur Ermittlung des globales Rankings einer WebPage über deren Relevanz
  - **Relevanzgewichtung**
  - Google unterscheidet „wichtige“ von „unwichtigen“ Dokumenten
  - **„Wichtig“**:
    1. ein Dokument ist um so „wichtiger“, je mehr andere Dokumente auf dieses Dokument via Links verweisen
    2. ein Dokument, auf das ein „wichtiges“ Dokument via Link verweist, ist selbst „wichtig“
    3. je mehr Links ein Dokument auf andere Dokumente enthält, desto „unwichtiger“ ist ein einzelner Link

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Bsp. Modifizierter PageRank Algorithmus
  - **Google Relevanz- und Gewichtungsmodelle**
    - aus 1-3 lässt sich eine Formel zur Berechnung der „Wichtigkeit“ (**PageRank**, **PR**) eines Dokuments gewinnen
      - sei **PR(A)** der zu ermittelnde PageRank des Dokuments **A**
      - seien $T_1 \ldots T_n$ Dokumente, die einen Link auf A enthalten
      - seien $PR(T_1) \ldots PR(T_n)$ die PageRanks der Dokumente $T_1 \ldots T_n$
      - sei $c(T_i)$ die Anzahl der ausgehenden Links in Dokument T_i
      - sei d ein Dämpfungsfaktor (0<d<1)

$$PR(A) = (1-d) + d\left(\sum_{i=1}^{c(A)} \frac{PR(T_i)}{c(T_i)}\right)$$

*Berechnung wird iterativ durchgeführt,bis sich ein stabiler Zustand (**Fixpunkt**) ergibt.*

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Bsp. Modifizierter PageRank Algorithmus
  - Übertragung auf Web of Trust:
    - Annahme: Bewertungen nehmen nur Wert positiv an.
    - Es entsteht Graph G := $R_P \cup W_T$ mit Agenten und Objekten als Knoten und Kanten, wenn Agent das Objekt positiv bewertet hat bzw. Agent anderem Agenten vertraut.
    - PageRank auf G angewendet ergibt **AORank** für Agenten und Objekte.
  - Anpassung, um negative Bewertungen zu berücksichtigen:
    - B_i = Menge von Agenten, die Objekt O_i negativ bewertet haben.
    - N_v = Anteil negativer Bewertungen, die ein Agent v abgegeben hat.

$$\mathrm{ModifiedPageRank}(O_i) = \mathrm{AORank}(O_i) - \sum_{v \in B_i} \frac{\mathrm{AORank}(O_i)}{N_v}$$

Semantic Web

5. Web of Trust

5.1 Kryptografische Grundlagen

5.2 XMLEncryption und XMLSignature

5.3 Voting-, Rating- und Reputationsysteme

5.3.1 Grundbegriffe

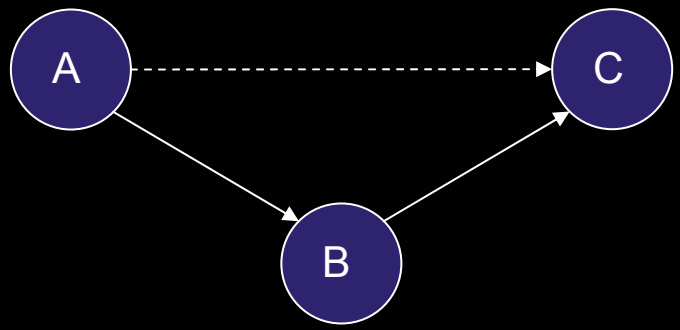
5.3.2 Mathematisches Modell

5.3.3 Reputationsnetzwerke

5.3.4 Vertrauensstrategien

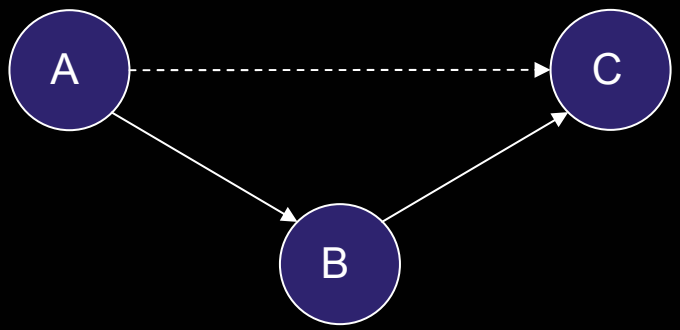
5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Reputationsnetzwerke
  - Lokales Ranking berücksichtigt Kontext
    (es wird immer nur die Reputation betrachtet, die ein Agent B in den Augen von Agent A genießt)
  - Eine Kante von Agent A zu Agent B bezeichnet die (direkte) Reputation, die B aus Sicht von A genießt.
  - Besteht zwischen den Agenten A und C keine Kante, kann eine (indirekte) Reputation über einen eventuell bestehenden Pfad von A nach B berechnet werden.



5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Reputationsnetzwerke
  - **Wie bestimme ich Reputation (A, C)?**
    - A = Quelle, C = Senke
    - A fragt jeden Nachbarknoten n_i , der eine gute Reputation besitzt, rekursiv nach Reputation (n_i , C)?
    - A akkumuliert die zurückgegebenen Reputationen (Durchschnittswert) und rundet diesen Wert kaufmännisch.



Unterscheiden gute und böse Knoten.
Gute Knoten haben gute Reputation.
Böse Knoten haben schlechte Reputation.
Böse Knoten bewerten die Reputation aller Nachbarknoten falsch.

→ Hier können Problematische Situationen entstehen…

Semantic Web

5. Web of Trust

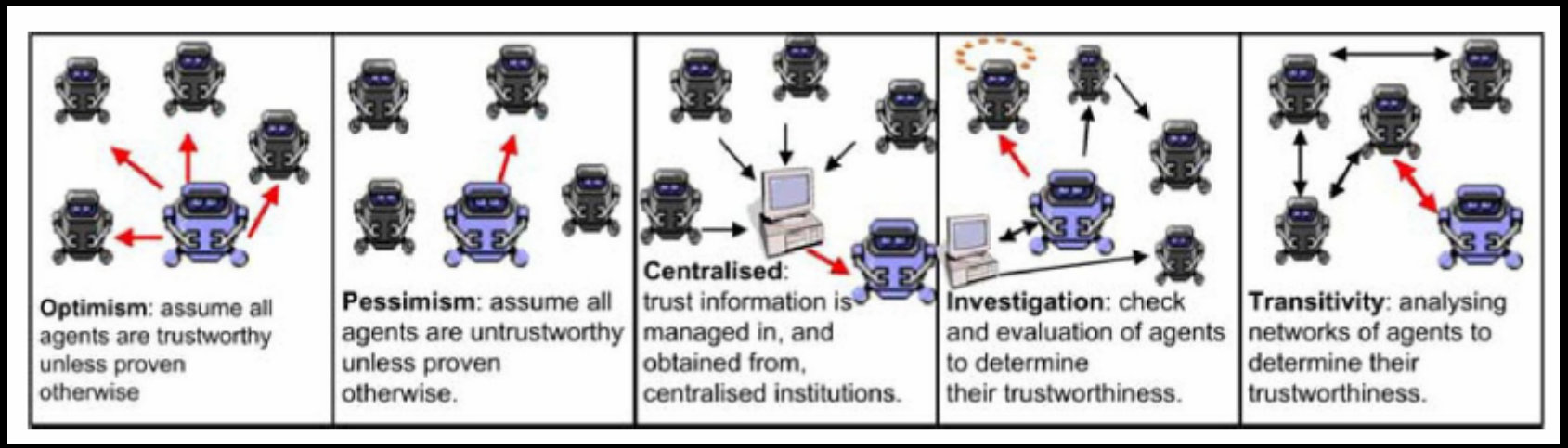
- 5.1 Kryptografische Grundlagen
- 5.2 XMLEncryption und XMLSignature
- 5.3 Voting-, Rating- und Reputationsysteme
  - 5.3.1 Grundbegriffe
  - 5.3.2 Mathematisches Modell
  - 5.3.3 Reputationsnetzwerke
  - 5.3.4 Vertrauensstrategien

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - Wie können Agenten miteinander interagieren?
    - Grundvoraussetzung ist Vertrauen.
    - Vertrauen bildet sich durch Informationsbeschaffung und Informationsauswertung.
    - Risiko sollte minimiert werden.
    - Interaktionsmöglichkeiten/Nutzen sollte maximiert werden.
  - **Strategie:**
    Die Strategie spiegelt die grundlegende Einstellung eines Agenten gegenüber einem anderen Agenten in einem System unter Unsicherheit wieder. Bei der Wahl der Strategie werden die relativen Kosten und der Nutzen der Interaktion mit dem entsprechenden Agenten berücksichtigt. Kombinationen und Wechseln der Strategien sind möglich.

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - Optimistische Strategie
  - Pessimistische Strategie
  - Zentrale Strategie
  - Recherche-Strategie
  - Transitive Strategie



5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - **Optimistische Strategie**
    - Vertraue per Default jedem Agenten.
    - Entziehe Vertrauen, wenn Gründe vorliegen.
    - Anwendbar, wenn..
      - Nutzen der Koorperation sehr groß.
      - Kosten/Risiko des Betrugs sehr gering.
      - schnelle Initialisierung des Netzwerks notwendig.
  - **Pessimistische Strategie**
    - Misstraue per Default jedem Agenten.
    - Schenke Vertrauen, wenn Gründe dafür vorliegen.
    - Anwendbar, wenn...
      - Es nicht vorteilhaft ist, jemanden zu vertrauen.
      - Kosten/Risiko des Betrugs hoch.

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - **Zentrale Strategie**
    - Zentrale Autorität sammelt Informationen über Agenten (Benutzerfeedback).
    - Zentrale Autorität zertifiziert Agenten.
    - Entscheidung über Ver-/Misstrauen fällt die zentrale Autorität.
    - Vorteil: Agent muss nur noch der Autorität vertrauen.
    - Bsp.: Ebay
  - **Recherche-Strategie**
    - Agenten erlangen vertrauen ineinander, indem sie schrittweise unter Aufsicht einer dritten Instanz, der sie vertrauen, eine Art Vertrag aushandeln.
    - Agenten agieren autonom und treffen Entscheidungen selbst.

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - **Transitive Strategie**
    - Basiert auf Bewertungen des Vertrauens der Benutzer/Agenten untereinander.
    - Problem:
      - Vertrauen ist nur **näherungsweise transitiv**.
      - Vertrauen wird meist nicht im **Kontext** betrachtet.

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - Welche Strategie soll gewählt werden?
    - Agenten sollen unter Unsicherheit miteinander agieren.
    - Risiko sollte minimiert werden.
    - Interaktionsmöglichkeiten/Nutzen sollte maximiert werden.
    - Zeit, bis gewisses Vertrauen erreicht (berechnet) wurde, sollte
    - Zeitschranke nicht überschreiten.
  - Risiko lässt sich in Form von anfallenden Kosten quantifizieren
    - Operationale Kosten
    - Opportunitätskosten
    - Ausfallkosten

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - Welche Strategie soll gewählt werden?
    - Agenten sollen unter Unsicherheit miteinander agieren.
    - Risiko sollte minimiert werden.
    - Interaktionsmöglichkeiten/Nutzen sollte maximiert werden.
    - Zeit, bis gewisses Vertrauen erreicht (berechnet) wurde, sollte
    - Zeitschranke nicht überschreiten.
  - Risiko lässt sich in Form von anfallenden Kosten quantifizieren
    - Operationale Kosten
    - Opportunitätskosten
    - Ausfallkosten

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - Operationale Kosten
    - Kosten die zur Realisierung (Durchführung) der Strategie anfallen
    - Proportional zur Komplexität der Strategie (Ressourcenbedarf)
    - Gering: Optimismus, Pessimismus (einfache Tests)
    - Hoch: Zentralisiert (Economie of Scale), Transitiv (hohe Nebenkosten), Recherchierend
  - **Oportunitätskosten**
    - Entstehen, wenn man Möglichkeiten, den maximalen Nutzen
    - zu erzielen, nicht wahrnimmt.
    - Gering: Optimismus
    - Mittel: Zentralisiert (Anzahl zertifizierter Agenten), Recherchierend (Agent hat beschränkte Ressourcen)
    - Hoch: Pessimismus, Transitiv (Netzwerkgröße)

5. Web of Trust
5.3 Voting-, Rating- und Reputationsysteme

- Vertrauensstrategien
  - **Ausfallkosten**
    - Fallen an, wenn sich Agent anders als behauptet verhält.

    - Gering: Pessimismus, Recherchierend
    - Mittel: Transitiv (Netzwerkgröße, selbstregulierend)
    - Hoch: Optimismus,
      Zentralisiert (Misstrauen in Autorität)

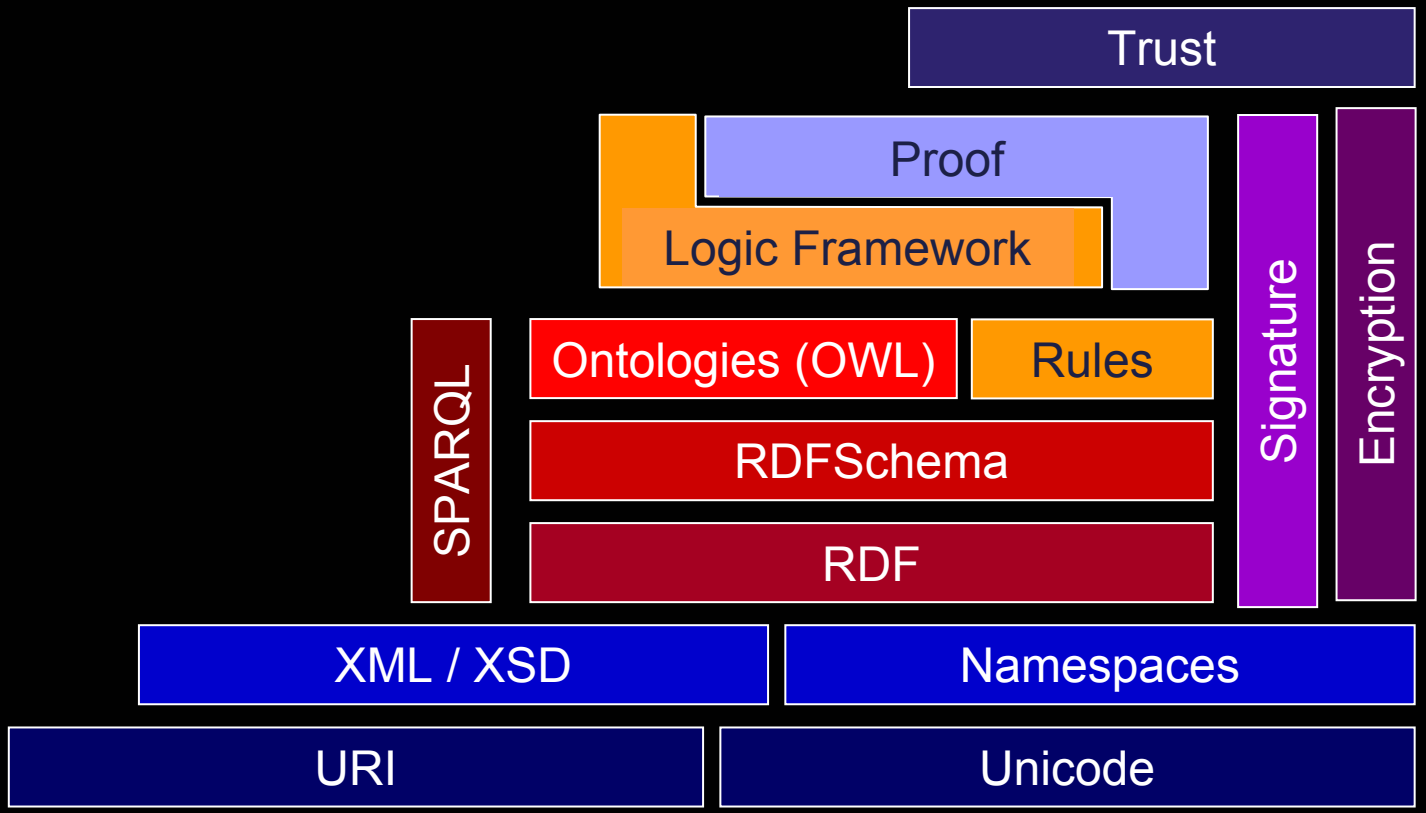
Semantic Web

5. Web of Trust

- 5.1 Kryptografische Grundlagen
- 5.2 XMLEncryption und XMLSignature
- 5.3 Voting-, Rating- und Reputationsysteme

5. Web of Trust

Semantic Web Architecture



5. Web of Trust

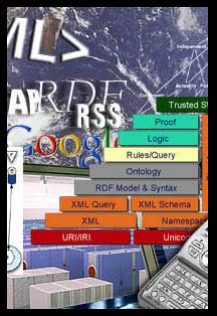
Literatur

- Ch. Meinel, H. Sack:
  WWW– Kommunikation, Internetworking, Web-Technologien,
  Springer, 2004.

- B. Schneier:
  Angewandte Kryptografie - Der Klassiker. Protokolle, Algorithmen und Sourcecode in C (2. Aufl.),
  Pearson, 2006.

5. Web of Trust

Literatur



- Materialien-Webseite
  http://www.informatik.uni-jena.de/~sack/WS0607/semanticweb-materialien.htm

- bibsonomy - Bookmarks
  http://www.bibsonomy.org/user/lysander07