Outline

1 The upper layers: Proof & Trust
   - Trust and Policy Management
     - Goals for Proof in the Semantic Web
     - Goals for Trust and Policy Management
     - Interaction dimensions between autonomous communicating parties
   - Examples
     - A trust framework for simple data transfer
     - Example of an extended transaction
     - Current Initiatives with participation of University of Hannover
The upper layers: Proof & Trust

- Trust and Policy Management
  - Goals for Proof in the Semantic Web
  - Goals for Trust and Policy Management
  - Interaction dimensions between autonomous communicating parties

- Examples
  - A trust framework for simple data transfer
  - Example of an extended transaction
  - Current Initiatives with participation of University of Hannover
The upper layers: Proof & Trust

Figure: http://www.w3.org/2000/Talks/1206-xml2k-tbl/slide10-0.html

Figure: http://www.w3.org/2002/Talks/09-lcs-sweb-tbl/slide19-0.html
The upper layers: Proof & Trust II

Figure: http://www.w3.org/2005/Talks/0511-keynote-tbl/
Goals for Proof

- proof that an answer found in the Semantic Web is correct
  - how has it been derived - logic
  - on which data - sources
  - by whom - chain of providers of data needs to be considered, too! (trust)

Goals for Trust and Policy Management

interoperability how to enable autonomous communicating parties to achieve bi-literal agreements?

scalability no single authority, no single operational model of trust management in the Web.
  → scalable systems must deal with variations in national, corporate and personal policy
Proof & Trust - Interaction dimensions between autonomous communicating parties

- Security [Sicherheit]
- Dependability [Zuverlässigkeit]
- Privacy [Privatsphäre], personal information is not disclosed or abused
- Policy [Regel zur Verständigung], rules for behaviour
- Provenance [Herkunft/Ursprung], information (metadata) about the source of some piece of data
- Trust [Vertrauen] belief in (expectation of) the behaviour of a party for some given purpose
- Authorization [Autorisierung], a decision about use of some mechanism or resource for a particular purpose
- Authentication [Authentifizierung], a mechanism, a receiver confirms the identity of a data sender
- Encryption [Verschlüsselung] a mechanism, a sender restricts who can receive data
- Access control [Zugriffskontrolle], a mechanism, controls access to a resource
- Exposure control [Ablieferungskontrolle] a mechanism, controls delivery of data to a recipient
- Negotiation [Verhandlung], a mechanism, determines what data is transferred
A simple transfer of data is between two parties, a sender and a receiver, and includes the following key steps:

- preparation of data
- transfer a copy of the prepared data
- use the copy of data received
More complex transactions:

**Needs of the sender:**

- access control can be used to restrict the sending of data
  authorization decisions based on
  - authentication
  - provenance
  - policy information
- encryption can be used to restrict who can receive the raw data, using
  - policy information
  - and knowledge of the intended recipient to guide the encryption process,
- negotiation can be used to obtain assurance that any data sent will be properly understood and usable, using
  - provenance
  - and policy information
  - and knowledge of the intended recipient to select the data sent,
- the sender must trust that the recipient will honour any restrictions on the use of any data transferred, such restrictions being indicated through provenance and policy information.
Needs of the recipient:

- authentication can be used to confirm the provenance of data,
- exposure control can be used to restrict data received, with authorization decisions based on
  - content inspection
  - provenance
  - and policy information
- the receiver may need to trust that the data received was appropriately originated consistent with any associated provenance information.
Trust and security interactions in a simple data transfer

- Original data
- Content generation policy
- Recipient capability/preference
- Recipient public key
- Generate data
- Encrypt
- Send
- Sign
- Access control
- Recipient id
- Sender private key
- Accepted data
- Trust in recipient
- Access policy
- Trust in sender
- Exposure policy
- Decrypt
- Receive
- Authenticate
- Recipient private key
- Sender public key
In the following, R is the receiver of transferred data and S is the sender:

1. R requests S to provide some information.
2. S requests information about capabilities of R, providing information about their privacy policy with that request.
3. R provides description of capabilities.
4. S selects and sends data.

Each of these steps corresponds to a simple data transfer, of the form described above!
R assumes or has prior knowledge that S can understand the form of the request, and can provide the required information. R trusts that S will not make inappropriate use of the fact that R has requested the resource (or does not care). The request might be encrypted to prevent disclosure to parties other than R or S. S makes few assumptions about the content of the request, and screens it carefully to ensure that it is a recognized, valid request. R may choose to authenticate the request data, and S may choose to check its authenticity.

If authenticity of the request is confirmed in step 1, S may check that R is authorized to receive the requested information. S also determines that one of several different forms of data may be provided, depending on the capabilities and/or preferences of R. S constructs a request for capability and preference information, including a description of the policy that S will use to govern use of that information. S probably has no concerns to constrain use of this policy information, so can assume no inappropriate use will be made. Based on the form of the request and other information from step 1, S assumes that R will understand the request for information and the privacy policy description. R makes few assumptions about the content of the capability request, and screens it carefully to ensure that it is recognized and valid; S may choose to authenticate the capability request data, and R may choose to check its authenticity.
Using information from step 2, R checks the request from S, including the privacy policy description and any authenticating or other provenance information against its own policies for release of capability information, resulting in an authorization decision whether or not to release the requested information. A decision to release information will depend on a degree of trust that the information will be used according to the policy declared by S for use of that information. R assembles a description of its capabilities and preferences, assuming that they can be understood by S, and sends them. The capability data might be encrypted to prevent disclosure to parties other than R or S. S makes few assumptions about the content of the capability description, and screens it carefully to ensure that it is recognized and valid; R may choose to authenticate the capability data, and A may choose to check its authenticity.
Using information from step 3, S analyzes the description of R’s capabilities, and selects a form of data to be sent. The decision to authorize access to this information was made at step 2, so it may be that no further authorization is needed. Alternatively, S may need to re-check its policy to ensure that R is permitted to access the particular version of data that matches R’s capabilities and preferences. Implicit in this authorization is a degree of trust that R will use the data in ways acceptable to S. The data might be encrypted to prevent disclosure to parties other than R or S. On receipt of the data, R may trust that the data is free of undesirable content (e.g. viruses, profanity), or may examine the content to ensure such freedom. If the data determined to be safe, R trusts that it does indeed correspond to the original request and use it accordingly.
Proof & Trust - Negotiated Transfer Interaction

**Receiver**
- R has belief and trust in S providing required information
- R authenticates S, checks privacy statement against local policy
- R trusts S privacy policy and sends capability information
- R trusts and uses data provided by S. R may or may not conform to trust expectations of S

**Sender**
- S authenticates R, checks authorization, determines capability info is needed.
- S constructs capability request with privacy policy statement
- S authenticates response, analyzes capability information
- S sends requested information in appropriate format that matches R capabilities

1. Request for information
2. Request capabilities, supply privacy policy
3. Provide capabilities
4. Send requested data
Secure Mime: **S/MIME** is an IETF standard for signing and encrypting MIME content, and providing other related security services.

**OpenPGP:** is another IETF standard for signing and encrypting data objects, and providing other related security services. It can be used to provide end-to-end security for arbitrary data objects.

**XML digital signatures: XMLDSIG** (or XML Signatures) is a joint IETF/W3C standard defining XML Signatures that can be used for signing arbitrary data, but with a particular view to XML content.

**XML encryption: XMLENC** is a W3C standard for encrypting arbitrary data and representing the result as XML. The result of encrypting data is an XML Encryption element which contains or references the cipher data.

**X.509 Public Key Certificates** is an ITU standard format for public key certificates. The purpose of a public key certificate is to distribute public key information in a secure, well-managed fashion.

**Internet X.509 Public Key Infrastructure (PKIX)** is an IETF standard profile of X.509 for Internet use.

**XML Key Management Services** is W3C protocol specification for verifying and accessing information about X.509 public key certificates (or other forms).
Kerberos ticket issuing systems is a widely used trusted third party authentication technology developed originally at MIT for Project Athena.

- To use an application service, a client must obtain a ticket for that service, from a ticket granting server. But to obtain a ticket, the client must obtain a ticket-granting-ticket from the Kerberos authentication server.

- Clients each share a secret key with the authentication server (AS), which is used to encrypt session keys generated by AS. AS also shares a secret key with the ticket granting server(s) (TGS), which is used to encrypt the ticket issued, so only TGS can access the content of the ticket to create service tickets.

- Ticket granting servers similarly share secrets with the services for which they issue tickets. This, in conjunction with a shared session key issued and encrypted by AS, allows TGS to create a service ticket for the client to present to gain access to a service.
Current Initiatives with participation of University of Hannover

REWVERSE: Reasoning on the Web with s and Semantics
http://www.reverse.net
KnowledgeWeb
http://knowledgeweb.semanticweb.org