Trusted Agent-Mediated E-Services via Semantic Web Rules Inference

Yuh-Jong Hu

May-2, 2002

jong@cherry.cs.nccu.edu.tw
http://www.cs.nccu.edu.tw/ENT
Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University Taipei, Taiwan
Talk Outline

✔ Research Background

✔ The Semantic Web

✔ Semantic Web Rules

✔ Agent-Mediated E-Services

✔ Trusted Agent-Mediated E-Services

✔ Research Challenges

✔ Summary
Research Background
Research Background

- Achieving the semantic web vision will be one of the emerging research areas for the academic community in the near future.

- We believe that software agents will be the prime beneficiary for the success of semantic web research.

- We focus on the agent trust issue for the semantic web research based on ontology (taxonomies + axioms) and security technologies.

- Agent-mediated e-services (or e-commerce) is one of the application domains to demonstrate the feasibility of our trust verification methodology.
The Semantic Web
The Semantic Web

A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities.

The Semantic Web will enable machines to comprehend semantic documents and data, not human speech and writings.

The explicit representation of the semantics of data, accompanied with domain theories (that is, ontologies), will enable a Web that provides a qualitatively new level of service.

Tim Berners-Lee, James Hendler, and Ora Lassila
Scientific American, May 2001
Ontology

An ontology is a **formal, explicit** specifications of a shared **conceptualization**.

The ontology for the Web has a **taxonomy** and a set of **inference rules**. The taxonomy defines classes of objects and relations among them. Inference rules in ontologies supply further power.

Some people treat ontology as a subset of logic, some treat logic as a subset of ontological reasoning, and others consider the terms disjoint.

Is the ontology equation shown to be: \( \text{Ontology} = \text{Taxonomies} + \text{Axioms} \)?
Ontology Language vs. Rule Language

Based on the language expressing power:

- RDF/RDF(S) ← ontology language
- OIL ← ontology/rule language
- DAML + OIL ← ontology/rule language
- RuleML ← rule language
- DAML-Rules ← rule language
# Ontology Languages for the Semantic Web

<table>
<thead>
<tr>
<th>Taxonomies</th>
<th>XOL</th>
<th>SHOE</th>
<th>OML</th>
<th>RDF(S)</th>
<th>OIL</th>
<th>DAML+OIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subclass of</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Exhaustive decompositions</td>
<td>-</td>
<td>-</td>
<td>+/-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Disjoint decompositions</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Not subclass of</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concepts</th>
<th>XOL</th>
<th>SHOE</th>
<th>OML</th>
<th>RDF(S)</th>
<th>OIL</th>
<th>DAML+OIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Issues</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partitions</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Documentation</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td><strong>Attributes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instance attributes</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Class attributes</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Local scope</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Global scope</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td><strong>Facets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default value</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Type constraints</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Cardinality constraints</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Documentation</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Asuncion Gomez-Peres and Oscar Corcho
## Ontology Languages for the Semantic Web (conti.)

<table>
<thead>
<tr>
<th></th>
<th>XOL</th>
<th>SHOE</th>
<th>OML</th>
<th>RDF(S)</th>
<th>OIL</th>
<th>DAML+OIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instances</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instances of concepts</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Facts</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Claims</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+/-</td>
<td>+/-</td>
<td>+/-</td>
</tr>
<tr>
<td><strong>Axioms</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First-order logic</td>
<td>-</td>
<td>+/-</td>
<td>+</td>
<td>-</td>
<td>+/-</td>
<td>+/-</td>
</tr>
<tr>
<td>Second-order logic</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Independent axioms</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Embedded axioms</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Relations and functions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n-ary relations/functions</td>
<td>+/-</td>
<td>+</td>
<td>+</td>
<td>+/-</td>
<td>+/-</td>
<td>+/-</td>
</tr>
<tr>
<td>Type constraints</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Integrity constraints</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Operational definitions</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Asuncion Gomez-Peres and Oscar Corcho
Agents and the Semantic Web

Many challenges of bringing communicating multiagent systems to the Web require ontologies. The integration of agent technology and ontologies could significantly affect the use of Web services and the ability to extend programs to perform tasks for users more efficiently and with less human intervention.

James Hendler
Agents and the Semantic Web (conti.)

The real power of the Semantic Web will be realized when people create many programs that collect Web content from diverse sources, process the information and exchange the results with other programs. The effectiveness of such software agents will increase exponentially as more machine-readable Web content and automated services (including other agents) become available. ⋯⋯

Tim Berners-Lee, James Hendler, and Ora Lassila
The “Original Layer Cake” for the Semantic Web

Tim Berners-Lee
The “Layer Cake” for the Semantic Web
The “Layer Cake” for the Semantic Web with Associated Ontology Language
FIPA Nomadic Application Support: Flow of Message Transport Protocol Negotiation
FIPA Nomadic Application Support:
Flow of Message Transport Protocol Negotiation (conti.)

(request
  :sender
    (agent-identifier
      :name A-AgentiM@mobile.com[10])
  :receiver (set
    (agent-identifier
      :name CaiM@mobile.com))
  :ontology FIPA-Nomadic-Application
  :language FIPA-SL0
  :protocol FIPA-Request
  :content
    (action
      (agent-identifier
        :name CAiM@mobile.com)
      (activate (sequence
        (transport-protocol
          :name x.uh.mdcp)
        (transport-protocol
          :name fipa.mts.mtp.wap.std
          :dest-addr wap://gateway.com:1234/acc))))


(agree
  :sender
   (agent-identifier
     :name CAiM@mobile.com)
  :receiver (set
   (agent-identifier
     :name A-AgentiM@mobile.com))
  :ontology FIPA-Nomadic-Application
  :language FIPA-SL0
  :protocol FIPA-Request
  :content
   
   ((action
      (agent-identifier
        :name CAiM@mobile.com))
  (activate (sequence
   (transport-protocol
     :name x.uh.mdcp))
  (transport-protocol
     :name fipa.mts.mtp.wap.std
     :dest-addr wap://gateway.com:1234/acc))))
true)
Ontology specifies the concepts and terms in a well-defined format for agents to refer and communicate.

If the ontology specifies that a particular class has a particular property and that the property has some restriction, then each agent can assume that the other has legal values for that property maintaining that restriction.

Agents that are not using the same ontology might still be able to communicate. If you can find a common ontology for each agent's ontology to map into.
Semantic Web Rules
RuleML

- RuleML is a rule markup language for the Semantic Web.

- RuleML rulebase exchange will require a taxonomy of the relations defined in the rulebase, where a relation with its arguments becomes a class with its slots.

- DAML+OIL taxonomies will require a rule system to derive/use certain implicit information that is not captured by the taxonomy alone.
A sophisticated software agent may be specified by

- an RDFS-based taxonomy for defining the schema of its mental state
- a set of RDF facts for specifying its factual (extensional) knowledge
- a set of RuleML integrity constraints for excluding non-admissible mental states
- a set of RuleML derivation rules for specifying its terminological and heuristic (intensional) knowledge
- a set of RuleML reaction rules for specifying its behavior in response to communication and environment events
DAML-OIL DAML-Rules and RuleML

- DAML+OIL is based on Description Logic (DL) and RuleML is based on logic programs (LP).

- DAML-Rules is a semantic rule markup language for Web resources and it builds on XML and RDF(S).

- DAML+OIL is an ontology language and RuleML is a rule markup language.

- No matter DAML+OIL, RDF(S)+RuleML, DAML-Rules, or DAML+OIL and RuleML, we need a consistent shared taxonomies and portable and interoperable axioms, and rules for agents to achieve autonomous, pro-active, reactive, and flexible service characteristics.
Axioms and Rules for DAML+OIL

Based on our observations, the DAML+OIL only provides axioms and rules for reasoning on the followings:

- **Ontology design**
  - Check class consistency and (unexpected) implied relationships
  - Particularly important with large ontologies/multiple authors

- **Ontology integration**
  - Assert inter-ontology relationships
  - Reasoner computes integrated class hierarchy/consistency
Axioms and Rules for DAML+OIL (conti.)

- Ontology deployment
  - Determine if set of facts are consistent w.r.t. ontology
  - Answer queries w.r.t. ontology, e.g. DQL

Are those axioms and rules enough for us to define our arbitrary trust validation rules once we have built the trust ontologies?
Combining Rules with Ontologies for the Semantic Web: DAML+OIL vs. RuleML

Two techniques for combination

- Meta-ontology: use DAML+OIL at a logical meta-level in order to describe classes of rules and rule sets.

- KR (Knowledge Representation) fusion: build rules on top of ontologies or build ontologies on top of rules.

Benjamin Grosof
The Web of trust is based on the proofs on the Web but very little has been done on this layer.

The proof will be a chain of assertions and reasoning rules with pointers to all the supporting material on the WWW.

A semantic Web will not require proof generation, i.e. find the path that constructs a valid proof, to be useful so proof validation will be enough.

This proof validation w.r.t. Web of trust is a decidable reasoning process.

An important facet of agents’ functioning will be the exchange of “proofs” written in the Semantic Web’s unifying language. (the language that expresses logical inferences made using rules and information such as those specified by ontologies).
Agent-Mediated E-Services
Web(or E)- Services

“Web Services are a new breed of Web application. They are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web. Web services perform functions, which can be anything from simple requests to complicated business processes. ⋯ Once a Web service is deployed, other applications (and other Web services) can discover and invoke the deployed service.”

IBM web service tutorial
Agent-Mediated E-Services (AMES)

The Semantic Web should enable users (or agents) to locate, select, employ, compose, and monitor Web-based services \textit{automatically}. So the primary motivations for Agent-Mediate E-Services (AMES) are:

- Automatic Web service discovery
- Automatic Web service invocation
- Automatic Web service composition and interoperation
Existing E-Services Frameworks

- WSDL/UDDI/SOAP
- ebXML
- RosettaNet
- BizTalk
Existing AMES Frameworks

- DAML-S + OAA
- RETSINA/LARKS
- IMPACT
- FIPA JAS
Ontologies for DAML-S Framework

DAML-S has the following ontologies but it lacks of trust ontologies to prove the trustworthiness of its AMES framework.

- Service ontology
- Process ontology
- Process control ontology (Not Ready Yet)
Trusted Agent-Mediated E-Services
Trusted Agent-Mediated E-Services

The trust issue will be one of the most important issues for the successful deployment of agent-mediated e-services framework.

People still do not know what are the specific trust issues need to be considered and resolved.

Security mechanisms can solve some of trust problems but not all of them so we need a total solution for the agent trust on the WWW.

We must find out what are the trust verification rules besides the security validation rules.
Why Trust Agent and Delegate our Authority?

The reasons for human (or agent) to trust their (peer) agents and delegate its authority to these agents are: efficiency, convenience, fault tolerance.

The most important one for agent’s delegation is that agents are cyberspace creatures.

If you fully(partially) trust your agent, then we assume you might delegate your complete(partial) authority to your agents.
Agent Trust Issues

There are at least two facets to deal with agent trust problem:

The trust on agent delegation must satisfy the “competence” (capability) and “disposition” (willingness) criteria.

- Do you (or your agent) trust agent (or another agent) so that the important mediation e-services authority can be granted to the delegatee agent?
- How do you make sure that agent can proceed and finish the task as your intention?
- Do you have to monitor and control your agent’s operations all the time to guarantee quality of trust?
Agent Trust Issues (conti.)

✔ The trust on access control for guardian agent must satisfy the “authorization” and “authorization” criteria.

✔ Once you trust your agents and delegate the access control authority for them to protect your precious resources, what kinds of methodologies are available for your guardian agent to ascertain the access control trust?

✔ Achieving agent trust on delegation and access control, we propose that the validation of agent’s authentication and authorization is an fundamental issue.

✔ What other issues are needed to consider for agent trust besides authentication and authorization criteria?
Complete authority delegation from principal $A$ to principal $B$ is denoted as either of the following:

✓ Principal $A$ says principal $B$(or $\text{threshold}(m, [B_1, \cdots, B_n])$) speaks for $A$ on some authority under conditions $\sim$.

✓ Principal $A$ delegates some authority to principal $B$ (or $\text{threshold}(m, [B_1, \cdots, B_n])$) under conditions $\sim$. 

Agent Delegation Logic:
Complete Authority Delegation
Agent Delegation Logic: Partial Authority Delegation

Partial authority delegation as role is denoted as:

Principal \( A \) says principal \( B \) (or \( \text{threshold}(m, [B_1, \cdots, B_n]) \)) speaks for \( A \) with role as \( \sim \) on some authority under conditions \( \sim \).
Agent-Oriented PKI
Identity Certificate

\[ ID_{CA\rightarrow p} - Cert = (Id_p, Pu_p, V, Option, Sig_{CA}) \]

where:

\( Id_p \): principal \( p \)'s distinguished identity.

\( Pu_p \): principal \( p \)'s public key.

\( V \): validation period for identity certificate.

\( Option \): optional information.

\( Sig_{CA} \): certificate signature signed by CA’s private key.
Attribute Certificate

\[ AT_{TA \rightarrow p} - Cert = (Id_p, Ar_p, V, Option, Sig_{TA}) \]

where:

- \( Id_p \): principal \( p \)'s distinguished identity.
- \( Ar_p \): principal \( p \)'s attribute information.
- \( V \): validation period for attribute certificate.
- \( Option \): optional information.
- \( Sig_{TA} \): certificate signature signed by \( TA \)'s private key.
Authorization Certificate

\[ AU_{p\rightarrow q} - Cert = (Pu_p, Pu_q, A, D, V, Sig_p) \]

where:

- \( Pu_p \): a public key for the issuer of principal \( p \) to grant authorization.
- \( Pu_q \): a public key for the subject of principal \( q \) to receive authorization.
- \( A \): expression for authorization.
- \( D \): delegation bit with value 0 or 1.
- \( V \): validation period for authorization certificate.
- \( Sig_p \): certificate signature signed by \( p \)'s private key.
Rule Certificate

\[ RU_{RA \rightarrow RS_i} - Cert = (RS_i, Assertions, Sig_{RA}) \]

where:

\( RS_i \): access authority for resource(or service)

\( Assertions \): a set of rules in Conjunct Normal Form (CNF) to indicate the requirements of both identity and attribute certificates to unlock the resource access authority \( RS_i \).

\( Sig_{RA} \): certificate signature signed by \( RA \)’s private key.
Closed Group Delegation Scenario

Internet bank Morgan-Trust provides customer $m_1$ with

✔ Valid customer citizenship ID $– Cert$

✔ Bank account’s AT $– Cert$

to perform a variety of transaction operations, such as check, withdraw, transfer, and deposit, on his account on the Internet. In this delegation scenario, all of the AT $– Cert$ issuers are the same as the resource owners so the attribute certificate verification process is a closed loop w.r.t the $RU_{Morgan-Trust} – agent$. 
Trust Establishment Scenario:
Granting Initial Authority for Service Requesting Agent
Rules

1. Morgan-Trust delegates the *issuing* operations for
   \[ ID_{HCA \rightarrow h} \rightarrow \text{Cert} = (?Id_h, ?Pu_h, ?V, Option, ?Sig_{HCA}) \text{ to } HCA \]
   If \( HCA \in (E - \text{Trust}) \).

2. Morgan-Trust delegates the *issuing* operations for
   \[ AT_{HTA \rightarrow h} \rightarrow \text{Cert} = (?Id_h, ?IsAccountOwner(?Id_h, ?Acc), ?V, Option, ?Sig_{HTA}) \text{ to } HTA \]
   If \( HTA \in (Morgan - \text{Trust}) \).

3. Morgan-Trust delegates the operations for
   \( \text{Check}(?Id_h, ?Acc), \text{Withdrawal}(?Id_h, ?Acc, ?Val), \text{TransferFrom}(?Id_h, ?Acc, ?Val), \text{Deposit}(?Id_h, ?Acc, ?Val) \) to \( \text{Name}(?Id_h) \)
   If \( ID_{HCA \rightarrow h} \rightarrow \text{Cert} \land AT_{HTA \rightarrow h} \rightarrow \text{Cert} \land \)
   \( \text{IsAccountOwner}(?Id_h, ?Acc) \land \)
   \( \text{IsAccountBalance}(?Val \geq 0, ?Acc) \).

4. Morgan-Trust says \( \text{PublicKey}(?Pu_h) \) *speaks for* \( \text{Name}(?Id_h) \)
   with role as \( \text{IsAccountOwner}(?Id_h, ?Acc) \) on the operations for
   \( \text{Check}(?Id_h, ?Acc), \text{TransferFrom}(?Id_h, ?Acc, ?Val), \text{Withdrawal}(?Id_h, ?Acc, ?Val), \text{Deposit}(?Id_h, ?Acc, ?Val) \)
   If \( \text{IsPublicKey}(?Pu_h, ?Id_h) \).
Access Control Facts for Morgan-Trust Bank

Facts

1. $IDE_{Trust} → m_1 - Cert = (Id_{m_1}, 12345, 2001/01/01 - 2002/12/31, Option, Sig_{E-Trust})$

2. $AT_{Morgan-Trust} → m_1 - Cert = (Id_{m_1}, IsAccountOwner(Id_{m_1}, B10234), 2001/02/02 - 2002/12/31, Option, Sig_{Morgan-Trust})$

3. IsPublicKey(12345, Id_{m_1})

4. IsPublicKey(45123, Id_{o_1})

5. IsPublicKey(51234, Id_{r})

6. IsPublicKey(23456, Id_{E-Trust})

7. IsPublicKey(34567, Id_{Morgan-Trust})

8. IsAccountOwner(Id_{m_1}, B10234)

9. IsAccountBalance($5000, B10234$)
A researcher $m_1$ is going to apply for financial support from the NSF (National Science Foundation)-Trust to participate in the AMEC 2002 conference. The NSF-Trust requirements for the approval of financial support must have the following digital certificates:

✔ an applicant must have a legal citizenship

✔ an applicant must be an faculty member at an MOE(Minister of Education) certified university

✔ an applicant must have full paper(s) accepted by the AMEC 2002 conference
Access Control Rules for NSF-Trust

Rules

1. NSF-Trust delegates the issuing operations for
   \[ ID_{HCA \rightarrow h} - Cert = (?Id_h, ?Pu_h, ?V, Option, ?Sig_{HCA}) \text{ to } HCA \]
   If \( HCA \in (US - Trust) \).

2. NSF-Trust delegates the issuing operations for
   \[ AT_{HTA \rightarrow h} - Cert_1 = (?Id_h, ?IsFacultyOf(?Id_h, ?Id_{HTA}), ?V, Option, ?Sig_{HTA}) \text{ to } HTA \]
   If \( HTA \ has \ AT_{MOE-Trust \rightarrow HTA} - Cert_2 \).

3. NSF-Trust delegates the issuing operations for
   \[ AT_{HTA \rightarrow h} - Cert_3 = (?Id_h, ?IsFullPaperAcceptedBy(?Id_h, ?Id_{HTA}), ?V, Option, ?Sig_{HTA}) \text{ to } HTA \]
   If \( HTA \in (ACM - Trust, IEEE - Trust, AMEC - Trust, \cdots) \).

4. NSF-Trust delegates the operation for
   \((UseTravelCredit(?Id_h, ?T - Amount) \land UseRegistCredit(?Id_h, ?R - Amount)) \text{ to Name(?Id_h)}\)
   If \( ID_{HCA \rightarrow h} - Cert \land AT_{HTA \rightarrow h} - Cert_1 \land AT_{HTA \rightarrow h} - Cert_3 \).

5. NSF-Trust says \( PublicKey(?Pu_h) \) speaks for \( Name(?Id_h) \) with
   role as \( IstheAuthorFor(?Id_h, ?Id_{HTA}) \) on the operations for
   \((UseTravelCredit(?Id_h, ?T - Amount) \land UseRegistCredit(?Id_h, ?R - Amount)) \)
   If \( IsPublicKey(?Pu_h, ?Id_h) \).
Access Control Facts for NSF-Trust

Facts

1. $ID_{US-Trust} \rightarrow m_1 - Cert = (Id_{m_1}, 12345, 2001/01/01 - 2002/12/31, Option, Sig_{US-Trust})$

2. $AT_{NCCU-Trust} \rightarrow m_1 - Cert_1 = (Id_{m_1}, IsFacultyOf(Id_{m_1}, Id_{NCCU-Trust}), 2001/02/02 - 2004/12/31, Option, Sig_{NCCU-Trust})$

3. $AT_{MOE-Trust} \rightarrow NCCU-Trust - Cert_2 = (Id_{NCCU-Trust}, IsCertifiedBy(Id_{NCCU-Trust}, Id_{MOE-Trust}), 2001/02/02-, Option, Sig_{MOE-Trust})$

4. $AT_{AMEC-Trust} \rightarrow m_1 - Cert_3 = (Id_{m_1}, IsFullPaperAcceptedBy(Id_{m_1}, Id_{AMEC-Trust}), 2002/02/02 - 2002/02/31, Option, Sig_{AMEC-Trust})$

5. IsPublicKey(12345, Id_{m_1})

6. IsPublicKey(54321, Id_{NSF-Trust})

7. IsPublicKey(56789, Id_{NCCU-Trust})

8. IsPublicKey(67891, Id_{MOE-Trust})

9. IsPublicKey(78912, Id_{AMEC-Trust})
Research Challenges
On-Going Research Issues

- Design and implement the trust ontology taxonomies and rules for agent-mediated e-services to evaluate agent’s authentication, authorization, delegation, and trust verification criteria.

- Establish the semantic web rules inference framework to execute our trust and delegation e-services rules on the Web.

- Use both the trust ontology taxonomy and semantic web rules inference to verify our trusted agent-mediated e-services model on the Internet.

- Build a generic trusted open agent e-services framework based on FIPA abstract agent architecture to serve a variety of e-service models.
Conclusion

☛ The **Semantic Web** is one of the important emerging research areas and the results are very promising in the near future.

☛ The real power of the Semantic Web will be realized when people create a lot of **software agent** programs to fulfill the agent characteristics for automated e-services.

☛ The relationships among **Semantic Web, ontology, agent**, and **trust** need to be established.

☛ The ontology equation: **Ontology = Taxonomies + Axioms (Rules)** needs to be verified.

☛ One of the challenge issues for the successful deployment of agent-mediated e-services is to resolve the **Web of trust** problem on the Semantic Web.

☛ The **trusted Semantic Web** has been done very little at this moment but people are very interested in achieving this objective.
References


Web Services Description Language(WSDL) 1.1, W3C Note 15, March 2001, http://www.w3c.org/TR/wsd1