Some Thoughts on Agent Trust and Delegation

Yuh-Jong Hu

June-1, 2001

http://www.cs.nccu.edu.tw/ENT
Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University
Taipei, Taiwan, R.O.C.

The Primary Objectives of This Research

- To build up, design and implement an agent-oriented Public Key Infrastructure(PKI) for software agents such that we might delegate our full(or partial)authority to our mediator agents to do cyberspace activities, such as E-Commerce in legalized manner.

- To study the Web trust problem, especial the agent trust problem so that we can handle both human vs. agent and agent vs. agent's trust, authentication, authorization, and delegation (all of them via certificates) issues.

- To consolidate the above research results and input these results to agent standard community, and Agent-Mediated E-Commerce (AMEC) community, such as FIPA .

Digital Certificate vs. PKI

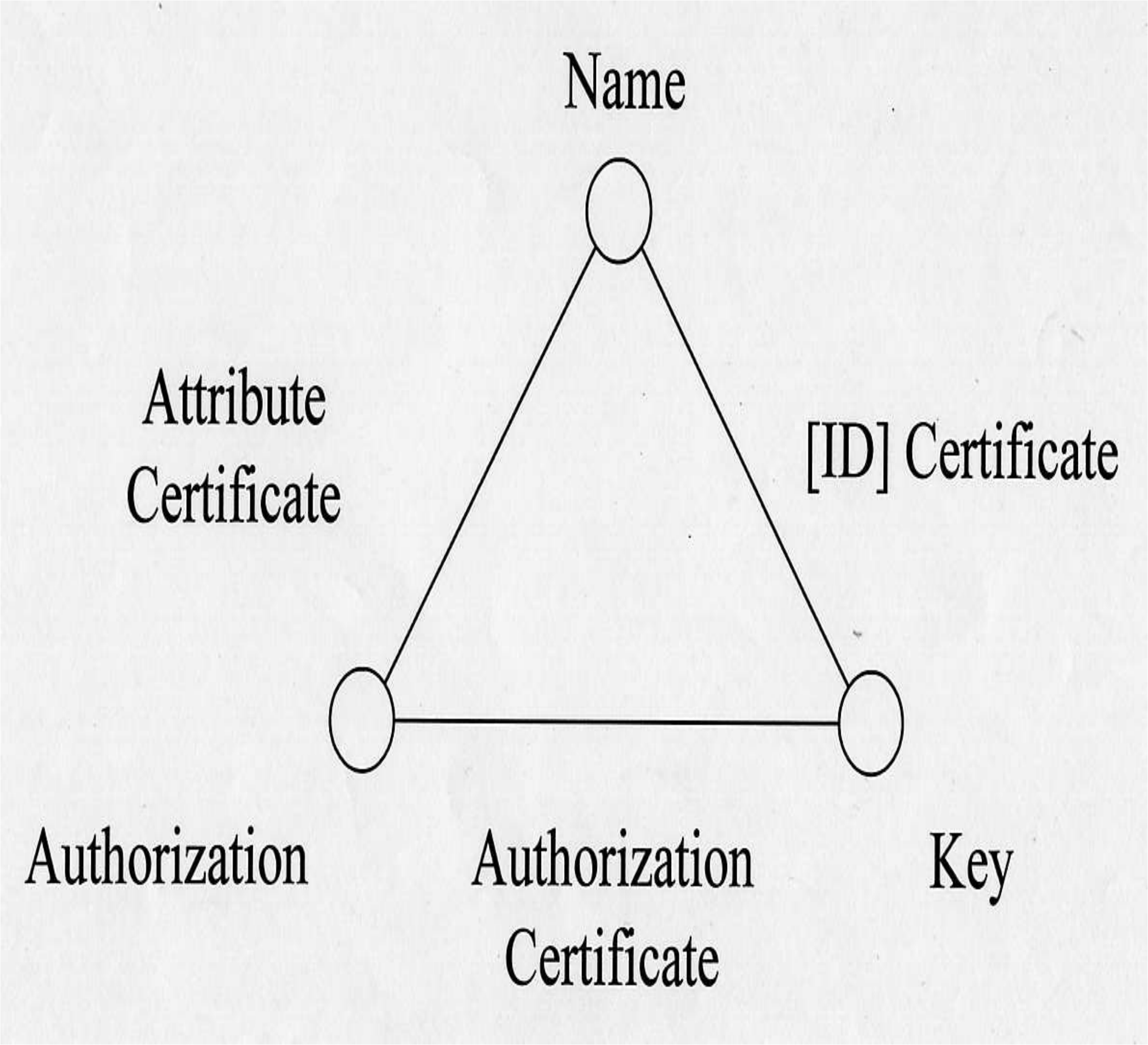
- A digital certificate(or digital credential) is a signed assertion about a public key binds with some other piece of personal identifier information, such as unique name.

- In fact, digital certificate might include identity certificate, attributed certificate, and authorization certificate and the binding problem for these three certificate categories is a very important research issue.

- A public key infrastructure(PKI) is an infrastructure for a distributed environment that centers around the distribution and management of public keys and digital certificates.

Digital Certificate vs. PKI(conti.)

Certificate Triangle Relationship



Agent Trust and Delegation

☛ We did not yet examine the trust issues before human and agent(trustors) are granting the authorization to the agents(trustees) so trust is normally *necessary* but not *sufficient* conditions for delegation.

☛ We are concerning about the verification of trustworthiness and validation of agent-oriented Public Key Infrastructure(PKI) with its issuing identity and authorization certificates.

Agent-Oriented PKI

- ☛ A solid foundation framework for agent trust and delegation via certificate theory.

- ☛ X.509-Based PKI is based on a very limited trust model.

- ☛ X.509-Based PKI only provides name-oriented identity certificate via binding public key of an entity with its symbolic name.

- ☛ SPKI/SDSI provides authorization certificate for authority delegation.

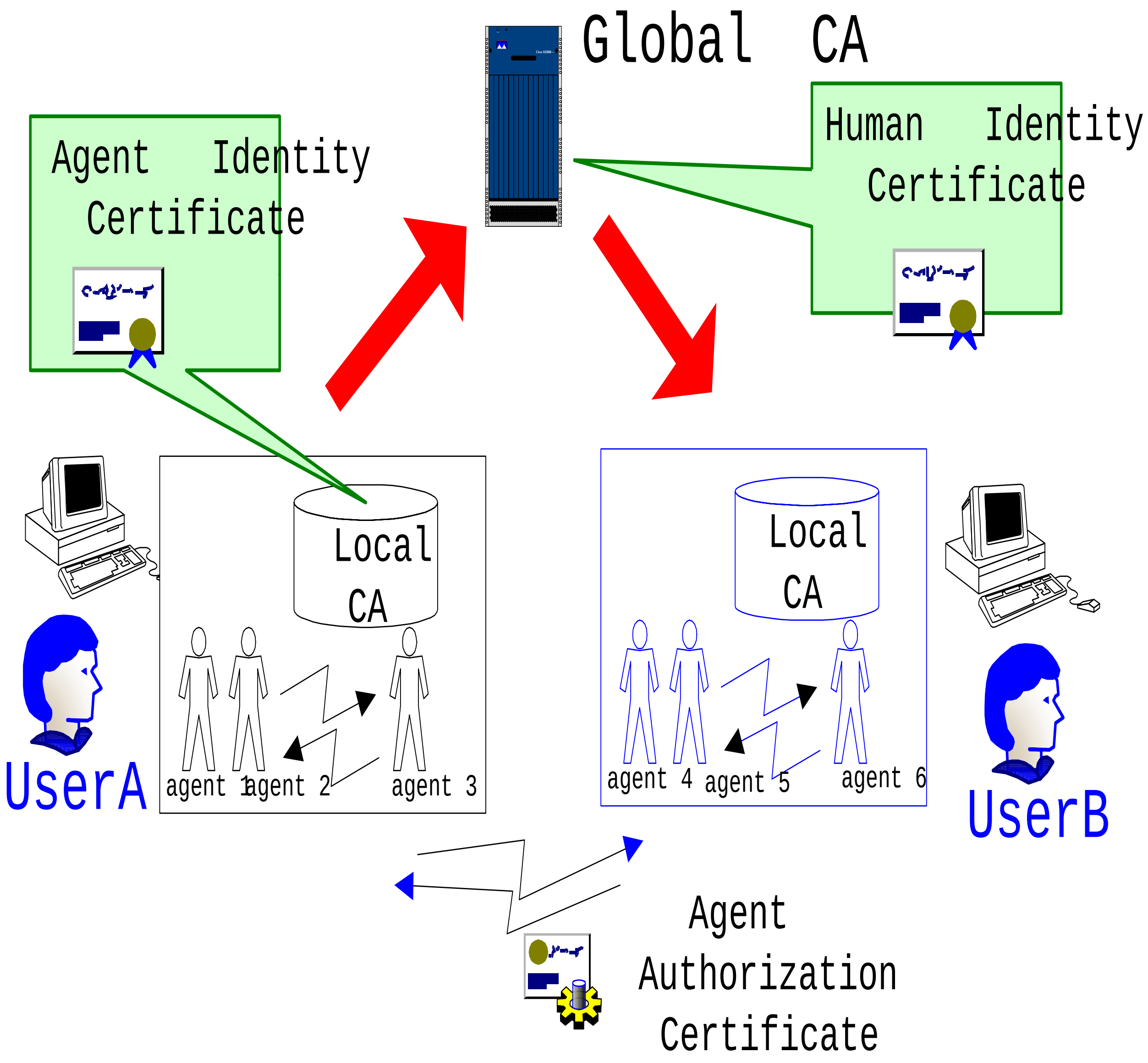
Agent-Oriented PKI(conti.)

- The global X.509 Certification Authority(CA) provides the identity certificate services for human.

- Local X.509 CAs provide agent’s identity certificate services.

- SPKI/SDSI authorization certificates are for both human/agent vs. agent/agent during authority delegation.

Agent-Oriented PKI


Global CA
Agent Identity Certificate
Human Identity Certificate
Local CA
Local CA
UserA
UserB
agent 1
agent 2
agent 3
agent 4
agent 5
agent 6
Agent Authorization Certificate

Human Identity Certificate

Human identity certificate $I_h - Cert$ is defined as:

$$I_h - Cert = (ID_h, PU_h, Options)$$

where:

ID_h:human unique symbolic name.

PU_h:unique public key for human.

$Options$:optional parameters for human profiles, such as email address, birth date, etc.

Agent Identity Certificate

Agent identity certificate $I_a - Cert$ is defined as:

$$I_a - Cert = (ID_h \# ID_a, PU_a, Options)$$

where:

$ID_h \# ID_a$:the concatenation of human unique symbolic name ID_h with agent symbolic name ID_a.

PU_a:unique public key for agent.

$Options$:optional parameters for agent profiles, such as agent name, network address , and validity life cycle, etc.

Human Authorization Certificate

The human authorization certificate $A_h - Cert$ is shown as a 5-tuple structure:

$$A_h - Cert = (PU_h, PU_a, A, D, V)$$

where:

PU_h:human's public key for granting authorization.

PU_a:agent's public key for receiving authorization.

A:authorization power for agent

D:delegation bit with 0 or 1 value.

V:validation period.

Agent Authorization Certificate

Agent authorization certificate can be shown as:

$$A_a - Cert = (PU_{a1}, PU_{a2}, A, D, V)$$

When each agent authorization certificate was issued, this certificate must be signed by issuer agent a_1 private key to ensure its legal status.

Agent Trust and Delegation via Certificates

- The reasons for human to trust their agents and delegate their 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 subjectively, then we assume you might delegate your complete(partial) authority to your agents.

Agent Trust and Delegation via Certificates(conti.)

- The trustor agent x tries to achieve a goal g via the delegation to trustee agent y.

- There are “competence” and “disposition” belief problems shown in the agent authority delegation.

- The authorization certificate itself is a “competence” token and the “disposition” belief is relative to the *willingness* of the trustee agent y to finish the task.

- The complete authority is denoted as speak for and the partial authority is denoted as speak for with role constraint as.

Certificate Chain Discovery Procedure

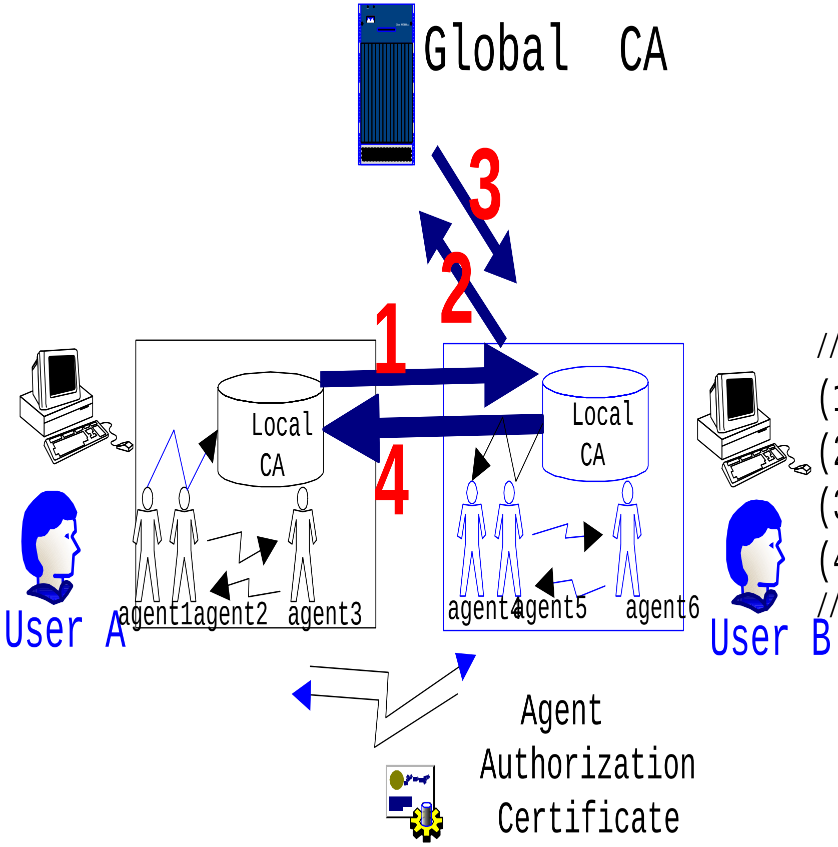
- Agent-oriented PKI must have a mechanism to provide the certificate chain discovery mechanism for any human(or agent) to discover the peer side human’s (or agent’s) public keys.

- We can easily verify the human/agent identity certificate and to do the delegation via human/agent authorization certificate.

- The trust of identity certificate is to trust the legal status of human/agent symbolic name with its public key.

- The trust of authorization certificate is to believe that the service request agent does have the authority with respect to the presented authorization certificates and these certificates are valid.

Certificate Chain Discovery Procedure(conti.)



Certicate Chain Discovery Procedure

//public key agent4 unknown

(1)User A ---> User B

(2) User B ---> Global CA

(3) Global CA ---> User B

(4)User B---> User A

//public key agent4 received

Issuer: Public Key Agent 1
subjectPublic Key Agent 4
Delegate TRUE
Authority *
Validity2001/04/05~2001/04/07

Chain-Ruled Delegation

☞ In the generic chain-ruled delegation, the authority delegation source is usually responsible for the final authority verification.

☞ The delegation mechanism allows the authority be delegated in a cascade style.

☞ the final service(authority) request agent does not necessarily to be the direct authority delegatee from the service(authority) source.

☞ This delegation type was also able to apply in the safe deals between strangers scenario and when the authority verification agent is different from the authority(or role) assignment agent.

Threshold Delegation

- ☛ Multiple agent delegation subjects are permitted from one agent delegation issuer. Thus, the issuer agent's authority can be split in this single delegation.

- ☛ The delegate agent subjects must coordinate with each other to perform the delegation authority.

Threshold Delegation(conti.)

General Manager Bob delegates the operations of *(check, transfer, withdraw, deposit)* to his agent G on Internet Bank *Morgan* with account ABC from 2001/04/05 to 2001/04/07.

Agent G says threshold $(2, [M_1, M_2, M_3])$ speak for agent G for the operations *(check, withdraw)* on Internet bank *Morgan* with account ABC from 2001/04/05 to 2001/04/07.

Conditional Delegation

Human(or Agent) delegates the operations of *(set of operations)* to agent G(or *threshold(*m*, [*A_1*,..,*A_n*])* on an *application* domain under the conditions that *satisfy* some regular conditional constraints within validation period.

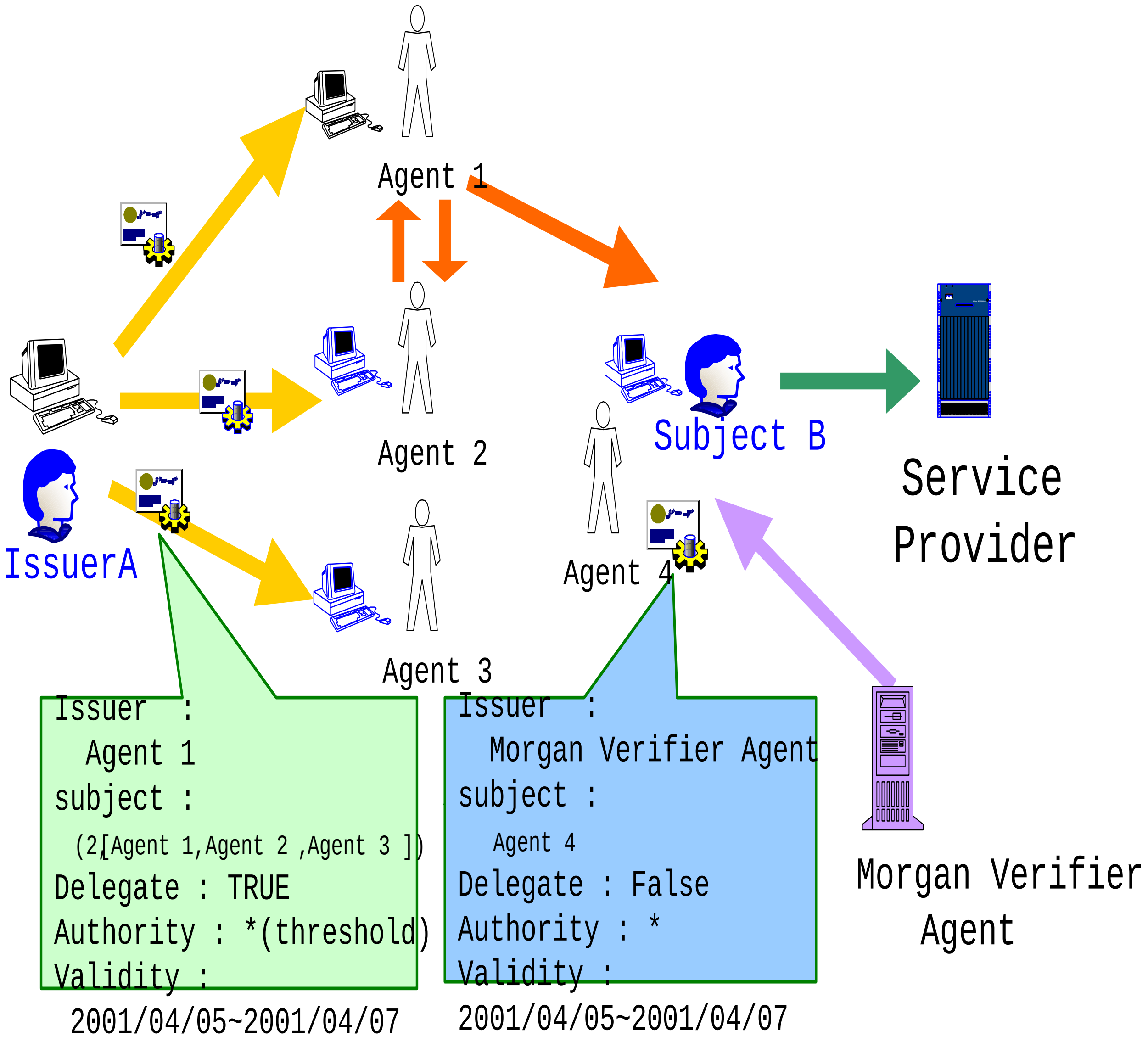
General Manager Bob delegates the operations of *(check, transfer, withdraw, deposit)* to his agent G on Internet Bank $Morgan$ with account ABC under the conditions that the amount of withdraw no more than NT$10,000 dollars in one day starting from 2001/04/06 within 2001/04/05 - 2001/04/07 validation period.

Agent Trust and Delegation Network

- The human(agent) trust and authorization problem consists of deciding whether the incoming collected certificates(or credentials) prove that a services(or resources) request complies with a human(agent) specified policies and facts.

- Consider the chain-ruled, threshold, and conditional delegation mechanisms can be dynamically and flexibly applied for distributed agent trust management in the mulit-agent systems.

Agent Trust and Delegation Network(conti.)



Issuer :
Agent 1
subject :
(2,[Agent 1,Agent 2 ,Agent 3])
Delegate : TRUE
Authority : *(threshold)
Validity :
2001/04/05~2001/04/07

Issuer :
Morgan Verifier Agent
subject :
Agent 4
Delegate : False
Authority : *
Validity :
2001/04/05~2001/04/07

Authority Verification Process

- The verification process ensure that each issuer agent in the delegation network should have the right authority declaration for re-delegation and all of the $A_a - Cert$s are within the validation period without any revocation status.

- Agent trust and delegation logic is based on the authority delegation policies(rules), delegation facts, and query:

  - Authority delegation rule can be shown as follows:

    ```
    H     if     F
    ```

    where H is a head statement and F is a body formula.

Authority Verification Process(conti.)

- Agent trust and authority delegation fact and query.
  - A clause with empty body is called a *delegation fact*.
  - A *query* takes the form: “F?” where F is a body formula.
- Usually a non-monotonic delegation logic was proposed to handle the certificate revocation problem so in this study we did not explicitly solve the certificate revocation problem.

Authority Delegation Rules

- Morgan delegates the operation *certify* of $I_h - Cert(?ID_h, ?PU_h, Options)$ to E-Trust.

- Morgan delegates the operation *certify* of I_a-Cert(?$ID_h \# ID_a$, ?PU_a, Options) to h-Trust.

- Morgan delegates the operations of *(check,transfer, withdraw, deposit)* to Owner(?ID_h) on Account(?Acc) if IsAccountOwner(?ID_h, ?Acc)

- Morgan says PublicKey(?PU_a) speaks for Name(?ID_h) if IsPublicKey(?PU_a, ?ID_h)

Authority Delegation Rules(conti.)

- Morgan says threshold(2,?S, E-Trust says belongTo(?S, BobOrg)) speak for Owner(?ID_h) on Account(?Acc) if Owner(?ID_h) delegates the operations *(check,transfer,withdraw,deposit)* to threshold(2,?S, E-Trust says belongTo(?S, BobOrg))

- Morgan says the operations *(transfer,withdraw)* on Account(?Acc) must less than Balance(?Acc)

Authority Delegation Facts

- E-Trust says
  $I_{Bob} - Cert = (ID_{Bob}, 123456, Options)$.

- Bob-Trust says $I_G - Cert = (ID_{Bob}\#ID_G, 783452, Options)$.

- Bob delegates the *(check, transfer, withdraw, deposit)* operations to agent G on Account(ABC) from 2001/04/05 to 2001/04/07.

- Agent G delegates the operations *(check,withdraw)* to agent threshold(2,(M_1,M_2,M_3)) on Account(ABC) from 2001/04/05 to 2001/04/07.

Authority Delegation Facts(conti.)

- Agent M_1 threshold-initiate the operations *(check, withdraw)* to agent M_2 on Account(ABC) from 2001/04/05 to 2001/04/07.

- Agent M_2 threshold-delegates the operations *(check, withdraw)* to agent M_1 on Account(ABC) from 2001/04/05 to 2001/04/07.

Authority Delegation Query

Do you allow agent M_1 withdraw(NT$10,000) on Account(ABC) on 2001/04/06?

Agent Delegation and Certificate in FIPA ACL

- FIPA standardization body has produced a set of specifications outlining a generic model for the architecture and operation of agent-based systems.
- FIPA has not produced X.509-Based identity certificate PKI for agent, so don't even mention about the agent-oriented PKI for agent identification, authorization, and trust management, etc.
- FIPA Security SIG Request For Information is an ongoing process.

Agent Delegation and Certificate in FIPA ACL(conti.)

- We are implementing the agent-oriented PKI in the FIPA-OS(Open Source) toolkits.

- Speech-act performatives for human/agent identity certificate management are certificate registration, query, and revocation:
  - $register - I_h - Cert/register - I_a - Cert$
  - $query - I_h - Cert/query - I_a - Cert$
  - $store - I_h - Cert/store - I_a - Cert$
  - $revoke - I_h - Cert/revoke - I_a - Cert$

Agent Delegation and Certificate in FIPA ACL(conti.)

- speech-act performatives for human/agent authorization certificate management are simple certificate delegation, threshold certificate delegation, certificate storing in the verifier rule base, etc.
  - $delegate - A_h - Cert/delegate - A_a - Cert$
  - $threshold - initiate$
  - $threshold - delegate$
  - $store - A_h - Cert/store - A_a - Cert$

ACL Outer Conversation Acts Encoded in XML

☞ The proposed new performatives for agent certificate management in this study are quite easy to embed to the XML DTD file in fipa.acl.rep.xml.std.

☞ The ACL encoded in XML only provides the syntax interoperability.

☞ The semantic interoperability feature of ACL in the agent state and in the agent content language must be done in XML/RDF.

ACL Inner Content Language Encoded in XML/RDF

- ☛ Facts and rules stored in our verifier agent's rule base can be expressed in fipa-rdf0 and fipa-rdf1.

- ☛ XML/RDF provides semantic interoperability that gives the agents interpret an RDF data model in the same way.

Inner Content Encoded in XML/RDF(conti.)

The fact E-Trust says $I_{Bob} - Cert = (ID_{Bob}, 123456, Options)$ might be shown as:

```
(store-I(Bob)-Cert
 :sender E-Trust
 :receiver Morgan
 :content(
 <?xml version="1.0">
 <rdf:RDF xmlns:rdf="http://www.w3.org/....."
      xmlns:s="http://desp/schema/">
     <rdf:Description ID="Bob Public Key">
     <s:pub-key>123456</s:pub-key>
     <!-- other optional profiles for Bob -->
     </rdf:Description>
     </rdf:RDF>)
     :language fipa-rdf0
     :signature efa23bcd)
```

Further Studies

☞ Agent trust and delegation problem is one of the very promising research areas for multi-agent system infrastructure.

☞ If we can not handle the above issues in technology and legal complete manner, then the dream of agent system to serve the entire human society can not be in reality.

☞ We are still exploring a generic global agent-oriented identity PKI with associated identity, authorization, and attribute certificates, which can support the agent trust and delegation process as well as relevant security, safety, and privacy issues.

☞ The general trust issues for human and agent will be clarified during certificates delegation and verification process to meet those requirements.

Conclusion

- We do believe that the agent trust and delegation problem is one of the most important research areas in agent-mediated cyberspace.

- At this moment, we did not handle all of the human vs. agent trust issues before the agent's authority delegation.

- Instead, an agent-oriented PKI was proposed to provide identification and authorization trust management.

- In this agent-oriented PKI framework, we have identity and authorization certificates operations under different delegation mechanisms, such as chain-ruled, threshold, and conditional, etc.

Conclusion(conti.)

- The agent trust and delegation logic was demonstrated in one specific Internet bank example.

- Finally, we propose some communicative acts for the identity and authorization certificate management and the related XML and XML/RDF encoding concepts were also briefly demonstrated.

- In general, we have to solve the agent trust and delegation problem via some sorts of binding from identity certificate, attribute certificate, and authorization certificate in our agent-oriented PKI.

References

1. Abadi, M., Burrows, M., and Lampson, B., A Calculus for Access Control in Distributed Systems. *ACM Transactions on Programming Languages and Systems,* 15, 4, (Sep. 1993), 706-734.

2. Aura, Tuomas, On the Structure of Delegation Network. *Proc. 11th IEEE Computer Security Foundations Workshop,* IEEE Computer Society Press, June 1998, 14-26.

3. Aura, Tuomas, Distributed Access-Rights Management with Delegation Certificates. *Secure Internet Programming: Security Issues for Mobile and Distributed Objects* LNCS 1603, Springer-Verlag, 1999, 213-238.

4. Brands, A. Stefan, *Rethinking Public Key Infrastructures and Digital Certificates Building in Privacy,* The MIT Press, 2000.

5. Castelfranchi, Cristiano and Falcone, Rino, Trust and Control: A Dialectic Link, *Applied Artificial Intelligence,* 14:799-823, 2000.

6. Clarke, Dwaine, et al., Certificate Chain Discovery in SPKI/SDSI(draft), MIT Lab for Computer Science, Nov. 1999.

7. Ellison, M. Carl, et al., SPKI Certificate Theory, RFC 2693, Internet Society, 1999,

8. *FIPA 97 Specification Part 2, Version 2.0, Agent Communication Language,* 1998.

9. *FIPA 98 Specification Part 10, Version 1.0, Agent Security Management,* 1998.

10. *FIPA ACL Message Representation in XML Specification,* 2000.

11. *FIPA RDF Content Language Specification,* 2000.

12. Ford, Warwick and Baum, S. Michael, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures & Encryption,* Prentice Hall, 1997.

13. Gerck, Ed, *Toward Real-World Models of Trust: Reliance on Received Information,* http://www.mcg.org.br/trustdef.htm.

14. Gladney, H., Safe Deals Between Strangers, *IBM Research Technical Report(draft),* IBM Almaden Research Center, August, 1999.

15. Grosof, N. Benjamin and Labrou, Yannis, An Approach to using XML and a Rule-based Content Language with an Agent Communication Language, *IBM Research Report,* RC 21491(96965) 28 May 1999.

16. He, Qi, Sycara, Katia, and Finin, Tim, Personal Security Agent: KQML-Based PKI. *Proceedings of the Second International Conference on Autonomous Agents,* May 1998.

17. Heckman, C. and Wobbrock, O. J., Liability for Autonomous Agent Design, *Autonomous Agents 98,* Minneapolis, MN USA, 1998, 392-399.

18. Herzberg, A., et al., Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers, *2000 IEEE Symposium on Security and Privacy,* 2000, 2-14.

19. Hu, Y. J., Some Thoughts on Agent Trust and Delegation, *Fifth International Conference on Autonomous Agents (Agents 2001)* Montreal, Canada, Monday 28 May - Friday 1 June 2001.

20. Jennings, R. N., Sycara, K., and Wooldridge M., A Roadmap of Agent Research and Development. *Autonomous Agents and Multi-Agent Systems,* 1, 7-38, 1998.

21. Josang, A., Pedersen, G. Ingar, and Povey, D., PKI Seeks a Trusting Relationship, *Proceedings of ACISP 2000,* Brisbane, Australia, July 2000.

22. Kimbrough, O. S. and Moore, A. S., On Automated Message Processing in Electronic Commerce and Work Support Systems: Speech Act Theory and Expressive Felicity, *ACM Tran. on Information Systems,* Vol. 15, No. 4, October 1997, 321-367.

23. Lampson, B., Abadi, M., Burrows, M., and Wobber, E. Authentication in Distributed Systems: Theory and Practice. *ACM Trans. Computer Systems,* 10, 4 (Nov. 1992), 265-310.

24. Li, N., Grosof, N. B., and Feigenbaum. J., A Logic-based Knowledge Representation for Authorization with Delegation, *IBM Research Report,* RC 21492(96966) 28 May 1999.

25. Li, Ninghui, Grosof, Benjamin, and Feigenbaum, Joan, A Practically Implementable and Tractable Delegation Logic, *IEEE 2000 Symposium on Security and Privacy,* 2000.

26. Moukas, A., Guttman, R., Zacharia, G., and Maes, P., Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective. *International Journal of Electronic Commerce, Vol. 4 , No. 3*, Spring 2000.

27. Nwana, S.H., et al., Agent-Mediated Electronic Commerce:Issues, Challenges and some Viewpoints. *Proceedings of the Second International Conference on Autonomous Agents 98*, 1998, 189-196.

28. Rivest, Ron and Lampson, Bulter, SDSI- A Simple Distributed Security Architecture, http://theory.lcs.mit.edu/ cis/sdsi.html.

29. Tschudin, F. C., Mobile Agent Security. *Intelligent Information Agents: Agent-Based Information Discovery and Management on the Internet,* Springer-Verlag, 1999, 431-445.

30. Wen, Wu and Mizoguchi, Fumio, An Authorization-Based Trust Model for Multiagent Systems, *Applied Artificial Intelligence,* 14:909-925, 2000.

31. Wong, H. C., and Sycara, K. Adding Security and Trust to Multi-Agent Systems. *Proceedings of Autonomous Agents '99 (Workshop on Deception, Fraud and Trust in Agent Societies)*. May 1999, Seattle, Washington, pp. 149-161.

32. Wooldridge, M., Semantic Issues in the Verification of Agent Communication Languages, *Autonomous Agents and Multi-Agent Systems,* 3, 9-31(2000).