

Supporting the Legal Identities of Contracting Agents with an Agent Authorization Platform

Dickson K.W. Chiu
Dickson Computer Systems
Hong Kong, P. R. China
+852 9357 2611
dicksonchiu@ieee.org

Irene Kafeza

Faculty of Law,
University of Hong Kong,
Hong Kong, P.R.China
kafeza.e@dsa.gr

Changjie Wang Ho-fung Leung
Department of Computer Science and Engineering,
The Chinese University of Hong Kong,
Hong Kong, P. R. China
{cjwang, lhf}@cse.cuhk.edu.hk

Eleanna Kafeza

Department of Marketing and Communications,
Athens University of Economics and Business,
Greece
kafeza@aueb.gr

ABSTRACT

New technologies have introduced new ways in business transactions where online contracting is complementing and even substituting traditional paper-based transactions. One of the major recent innovations of online contracting is the use of intelligent agents to make contracts among users and businesses around the globe. Despite recent legislations on electronic contracting, there are no legislations governing automatic agent transactions except one preliminary attempt in the USA. We identify the key problem rooted at the authorization management in agent delegation as well as the proper legal identity of agents. Therefore, we advocate solutions that consider both legal and technical aspects. Based on current legal and business practices, we develop a conceptual model for agent authorization and identity management. We propose an Agent Authorization Platform (AAP) for the enforcement of agent authorization during contract establishment as well as the maintenance of the legal identity of agents. The AAP also supports alerts and acknowledgment to further enforce the user's manifestation of assent to the contract terms. We also detail a required security scheme for the AAP based on Public Key Infrastructure (PKI) technologies to demonstrate the feasibility of our approach.

Categories and Subject Descriptors

K.4.4 [Computer and Society]: Electronic Commerce

General Terms

Economics, Security, Legal Aspects, Verification.

Keywords

Intelligent agents, e-Contract, agent certificate, legal identity, PKI, authorization.

1. INTRODUCTION

The use of Internet and new software technologies has resulted in legal problems and most existing legal framework is inadequate to deal with them. Although much work has been done in the area of developing intelligent software agents and machine to machine communication, there is a growing interest on legal aspects that arise when software agents are contracting. This transformation of the contracts landscape has raised some crucial legal issues and key regulatory challenges. In the process of the transition from offline to online, the contracting environment has changed markedly through the use of electronic agents. The legal framework has sought to keep up but the technology evolves fast.

As intelligent software agents perform deals and formulate contracts mainly in the open Internet environment, the notion of the protection is quite different from a closed one, especially with the complications due to the new technologies. If the agent does not act as the user's expectation, either based on the user instructions, either because of a malfunction of the agent, either because the agent can easily be manipulated by a third party, either because the user of the system did not estimate appropriately the benefit, etc., then it is not easy to decide who is liable for the damages.

The massive adoption of new technological advances in intelligent software agents depends on solving the legal issues first. From a business perspective, trade is not encouraged in such an environment where the rules are not clear and where technological innovation can be easily used as a means for fraud and deception. Inadequate legal response, international standards, and the cross-border nature of electronic trade make it even more difficult to resolve any possible disputes, thus discouraging people to use this new technology.

Based on the review of Kafeza et al. [13] on the recent legal framework for contracting with agents, we identify the main issues as the proper authorization management to ensure the user's manifestation of assent to the contract terms as well as the legal identity of agents. We try to bridge the gap between the technical and legal viewpoint about agents with common commercial and legal practices. With this objective, we detail a secure Agent Authorization Platform (AAP) as a solution and further suggest a security scheme based on the Public Key

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ICEC2005, August 15–17, 2005, Xi'an, China.

Copyright 2005 ACM 1-58113-000-0/00/0004...\$5.00.

Infrastructure (PKI) infrastructure. The contribution of this paper is a refined legal analysis of the requirements for establishing the legal identities of agents and to demonstrate that such requirements can be readily supported by existing technologies but with an ingenious design.

The rest of the paper is organized as follows. Section 2 presents some legal background that is relevant to the problem. Section 3 introduces the overview of an AAP, the requirements, and our proposed system architecture. Section 4 details our proposed secure AAP scheme for this purpose. We discuss the conclusion of this paper in Section 5 with directions of future work

2. LEGAL BACKGROUND AND PROBLEM OVERVIEW

The term contract is overloaded. In everyday life we use the term contract to refer to an agreement between two or more parties. An electronic contract extends this notion and refers to electronic agreements: agreements that are created through electronic means. In e-commerce, every time when intelligent software agents interact and agree upon the execution of a task, we have an electronic agreement. The question is whether this is a formation of a legally legitimate contract.

For a contract to be valid and enforceable, a further important requirement is that the contract must be drawn by persons with contractual capacity. It is accepted that such capacity is attributed to physical persons and legal persons. Since intelligent agents cannot be considered physical persons, they can only be regarded as legal persons in contracting. Bellia [2] and Lerouge [12] further believe that legal persons (such as a corporation, a government entity, a ship) exist only when they have assets.

One might consider that software agents serve the same function as human agents. According to common law principles, a human agent must accept his mandate, both parties have to consent, and as long as the person understands what he is doing, is capable to be an agent without himself having full contractual capacity. Similarly, in civil law the agency relationship arises when one person acts as a representative of another person, ordered or allowed by the law. The agent is not acting on its own behalf and therefore it is not necessary to have the full capacity to contract. In this sense, an incapacitated electronic agent may be an agent. However, the law limits the capacity of certain person to bind oneself to a promise, or to enforce a promise made to them such as minors, mentally disordered, etc.

To resolve the above ambiguity, let us consider the several stages for the formation of an electronic agreement: searching for the parties, negotiation, drafting of the contract, execution, control, and monitor of the contract. As defined in the American Law Institute's Restatement Second of the Law of Contracts, "a contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty."¹ As such, a contract consists of three essential elements: (1) an agreement, (2) an intention from both parties to be legally bound, and (3) a valuable and enforceable consideration.

¹ The definition of contract in most common and civil laws are very similar.

To determine whether the first element exists and an agreement has actually been concluded, it is necessary to examine whether the negotiations that have taken place between the parties (offerer / offeree) can be defined as an offer and acceptance. This is relatively straightforward by recording the information produced by the participating agents as non-repudiation evidence with an AAP.

The second element for a valid contract is that an agreement constitutes a binding contract when it is reasonably regarded as both parties intended to create legal relations. The general rule for testing the intention is to attribute to the preformed actions (such as speech-act for agents), but not what was in mind. In order to rule about one's intention, a judge asks questions and concludes from all the surrounding circumstances considering the subject's personality. The intention also requires that one has to be aware of the commitment. This is guaranteed only if one manifests assent of the terms. Many scholars in law point out that one manifests assent by conduct when using an electronic agent, especially when technological support can provide adequate evidence, such as the instructions and parameters given to the agent.

Lerouge [12] associates manifestation of assent by conduct with only the agent's opportunity to review the electronic record. He states that use of intelligent software agents to enter into contracts presumes the user's assent to the contract even though he may subjectively intent otherwise or does not know exactly the moment and the content of the contract. Middlebrook and Muller [16] state that the opportunity to review the record should be in a manner that would enable a "reasonably configured electronic agent" to react to the contract. Unless there exist international technical standards for specifying legitimate agent interactions, the concept of "reasonably configured electronic agent" will remain fuzzy and give ground for litigation. Kerr [9] also discusses this issue and states that a contract can arise only after the expressed or implicit *animus contrahendi*. Moreover, he states that the exchange of promises is not enough and a mutual assent on the nature and scope of the rights and obligations between the parties (i.e., meeting of the minds) is necessary. The underlying requirement of meeting of the minds is the voluntary nature of the contract. This is a result of the fact that each party has exercised its freewill and has chosen to trust and rely on the mind of the other party and thus assumes duties and obligations.

The above scholarly views are further supported by the recent Uniform Computer Information Transactions Act (UCITA) [20] of the USA,² which aims to provide a full set of commercial law for computer information transactions. An "Electronic agent" is defined as a computer program, electronic or other automated means, used by a person to initiate an action, or to respond to electronic messages or performances, on the person's behalf without review or action by an individual at the time of the action or response to the message or performance (Section 102, Definition 27). An electronic agent can in particular be relied to

² Section 107, Legal recognition of electronic record and authentication; use of electronic agents.

respond to a term in an electronic record if it is “conspicuous.”³ The person that employs an electronic agent for making an authentication, performance, or agreement, including the manifestation of assent,⁴ is bound by the operations of the electronic agent, even if the person was not informed or did not reviewed the agent’s operations or the results of the operations. UCITA also states that a contract can be formed by electronic agents,⁵ unless the court rules that it is a result from fraud, electronic mistake, or the like. As a result, the non-repudiation evidence provided with an AAP can provide strong evidence in accordance with the UCITA.

The third element of a legally enforceable contract is a consideration that is something must be given in exchange of a promise. An agent can be programmed to give specific consideration under specific defined situations. Thus, this aspect is relatively straightforward. However, the notion of enforceability (i.e., a party that does not fulfill its contractual obligation has a penalty) is not obvious when applied to an agent. That means, agents need to have legal personality if they are also delegated to execute the contract in addition to the negotiation and formation of a contract.

3. CONTRACT AGENT AUTHORIZATION PLATFORM

Based on the legal analysis in the previous section, the key contribution of technologies in agent contracting should aim at the proper authorization management in agent delegation and the proper legal identity of agents as well as providing such non-repudiation evidence, particularly for the manifestation of assent to the contract terms. Besides, our AAP also aims at a high reliability of agents programming, better communications infrastructure, and other technical improvements that can indirectly help the management of contract agent. We believe that a combination of legal and technical solutions would best serve the e-commerce community. In particular, we base our model on current legal and business practices and mimic such automation with agents in our implementation framework.

3.1 Scope of the Proposed Platform

We perceive that a high percentage of the solution relies on technological part and therefore a computer-supported solution with a controlled and customizable degree of authorization to agents might be more beneficial because of the diversity of requirements and situations.

Conceptually, we can create a hierarchy of authorization based on the legal analysis (see Figure 1). At the top authorization level are agents that the user assigns legal personality to them. At that level the agent is free to get involved to any contract formation where the other party accepts this level of authorization. In this kind of authorization, the agent can also convey its assets to the other agent in order to facilitate the decision of the agent to participate

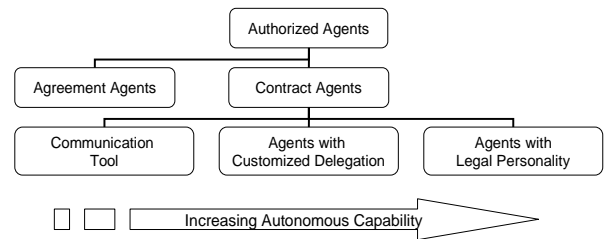


Figure 1. Overview of Agents Contractual Capability

in a contract or not. At the lowest level the agent can be a communication tool which makes the user liable for the agent’s action. If the agent is a communication tool then whatever arrangement the agent is doing the user is liable for it.

In between, an agent can have a customized degree of authorization and automation (i.e., delegation) based on the situation and the liability of their users. For example, a user may allow an agent to contract with other agents as long as a message reaches his/her mobile within a short period after the transaction. As another example, consider the case where an agent is programmed by the user to assume manifestation of assent by the other agent only in the case where the user of the agent sends an email stating that he read the contract and agrees.

In addition, we differentiate between two types of agents: the agreement agents and contract agents. Agreement agents are agents that perform agreements in the existing infrastructure or the users of the agents do not wish to be protected by giving contractual dimension to their transactions. These are cases where trust already exists. For example, it might be interesting from law point of view whether a user that requests from an agent to buy a book from amazon.com actually has a contract or not. But the user trusts that amazon.com will charge the credit card appropriately and do the delivery as agreed. In case amazon.com debits the card without delivery, the user has the alternative to sue under the tort of unjust enrichment. Contract agents are agents with contractual capabilities where the user wants to precede to agreements only if there is a legal contract between the participating parties.

3.2 Conceptual Model and Typical AAP Use Case

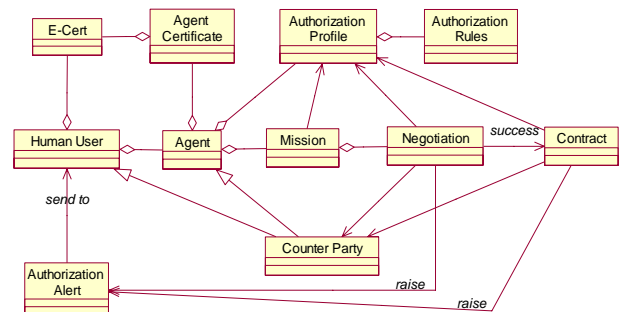


Figure 2. A Conceptual Model for Agent Authorization

³ Conspicuous means the agent cannot proceed without taking action with respect to the particular term or reference (Section 102, Def. 14(B))

⁴ Section 112, Manifestation of assent

⁵ Section 202, Formation in general; and Section 206, Offer and acceptance: electronic agents.

Figure 2 depicts our conceptual model for agent authorization in the Unified Model Language (UML [17]) class diagram to be supported in the AAP. The essential functions of the AAP include the following:

- Certification of agents
- Authentication of agents through electronic certificates
- Optional validation of agents' bids
- Witness of electronic contracts with validation to ensure contract terms are with the agents' authorization limits
- Alert the agents' user in case of authorization violations and seek for user approval
- Non-repudiation support

We explain the five phases of contract agent operation support in our AAP: user registration phase, agent registration phase, mission specification phase, negotiation phase, and contractual phase.

Before using the AAP, users must first certify their agents in the AAP, with each of their identity verified with a respective electronic certificate (*e-cert*). Users can specify various *authorization rules* for controlling their agents. Rules are organized into *authorization profiles* for potential reuse and customization. Users must also register each of their agents before delegating them to missions. A registration results in an *agent certificate* which captures the agent's descriptions, functions, the owner's e-cert, the agent's code, and other relevant information. Such information is digitally signed by the AAP.

When a user delegates an agent into a mission, the user may choose to override the agent's authorization profile with a *mission authorization profile*. Normally, the *mission authorization profile* is equal to the *contract authorization profile*. In some situations, a mission may comprise more than one contract, say, when the agent is delegated to buy some quantity of goods. However, for example, if the agent is not allowed to buy too much from a supplier, the user may set these two profiles different. In addition, the *negotiation authorization profile* may be set larger than *contract authorization profile* to increase the agent's flexibility and therefore the efficiency of the negotiation. However, if the contract exceeds the contract authorization as a result, then an alert will be sent to the user for approval to clarify legal responsibilities. All these authorization profiles should also be loaded into the agent's knowledge so that the agent can perform the delegation in accordance with its authorization.

In the negotiation phase, the agent may negotiate with one or more *counter-parties*, which may be humans or agents. Our AAP does not intend to interfere with the normal tasks of the agent because this may involve a large overhead and should be the responsibility of the agent's own running platform. However, counter-parties may obtain the following services from the AAP: 1) verify the authenticity of the agent certificate, 2) verify if the contract terms are under its authorization limit, and 3) optionally verify if an agent's bid is under its authorization limit. However, we cannot allow the counter-parties to directly access the authorization limits because this may expose sensitive information such as the reservation prices. Thus, before honoring authorization verification requests, the AAP must check if the bid

is really issued by the agent (by verifying the agent's signature on the bid).

Should the AAP detect a violation of any authorization limit, the agent's user is notified with an *alert* mechanism [4]. If the user confirms allowing such a deed of the agent, the AAP records this signed confirmation as evidence in case of future disputes and replies a positive result to the counterparty; otherwise a negative result is sent. Upon a negative verification, the counter-party should usually reject the bid or the contract.

Although an optimistic bidder (agent or human) need not verify every bid, contracts should be verified to ensure within the authorization limits. This is particularly important as users may change authorization limits during mission progress. Further, the AAP have to digitally sign the validated contract and then store it in a non-repudiation server. As such, the AAP much strengthens the legal protection against ambiguities in case of future possible disputes.

3.3 AAP System Architecture

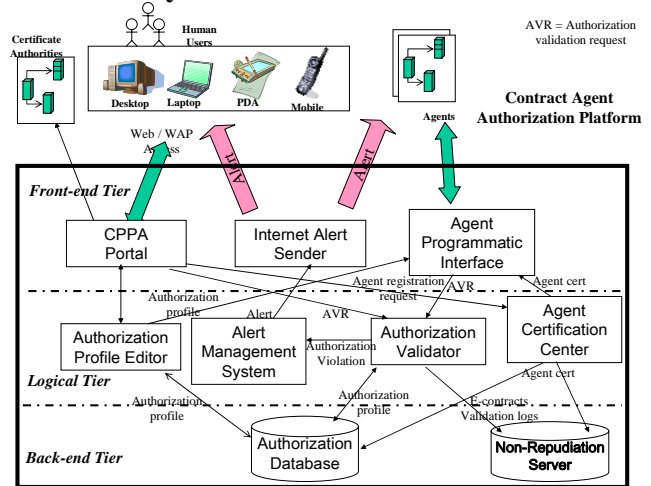


Figure 3. A Conceptual Model for Agent Authorization

Figure 3 describes an implementation architecture that consists of three tiers, namely the front-end tier, the logical tier, and the back-end tier. As we have identified a large number of legal issues are rooted from the proper authorization of agents and the provision of non-repudiation evidence for manifestation of assent to the contract terms. Therefore, based on PKI technologies, we propose an AAP as a foundation of a technical solution. We target to manage contract agents in our AAP, which is a trusted party to be operated by authorities.

The front-end tier interfaces with users and agents. The AAP Portal is a web-based interface for interactive user access to the AAP. The AAP authenticates users' identities with their e-cert from Certificate Authorities and register them to the system. The Internet Alert Sender sends alerts to agents and users with various mobile and Internet technologies [12] such as ICQ (I seek you), e-mail, Short Message Services (SMS), etc. The Agents Programmatic Interface supports interactions with agents through

established agent communication languages (ACL), such as that defined by the Foundation for Intelligent Physical Agents (FIPA), which has unambiguous clear formal definitions of the semantics for all the performatives as well as a well-defined syntax for communicative acts.

The logical tier implements all the necessary main programming logic for contract agent authorization. The Agent Certification Center creates agent certificates upon users' requests for certifying their new agents. The Authorization Profile Editor supports creation and maintenance of agent authorization rules and profiles, as well as binds them to agents at different scopes (namely, lifetime, mission, negotiation, and contract). The Authorization Validator checks if the bids or contracts violate the agents' authorization upon counter-parties' requests. Upon authorization violations, the Alert Management System generates alerts to notify the agents' owners for verification and confirmations as described in the previous sub-section. The agents' owners can then connect to the AAP Portal for further details and response to the alerts.

The back-end tier provides backing storage for the system. The Authentication Database keeps operational data such as the authorization rules and profiles, agent and user information, and so on. However, the Non-Repudiation Server is separated for sensitive legal evidence, such as e-contracts, validation logs, and so on.

4. An AAP Protocol

With reference to the framework proposed in the previous section, we propose to detail an AAP scheme for secure agent contracting in this section. We employ several cryptographic techniques based on PKI schemes. Figure 4 shows an overview of our proposed scheme. There are several roles involved in our scheme, named Customer, Agent Authorization Platform (AAP), Agent, and Seller. For the ease of illustration, we use the Internet buying and selling scenario as a running case study. The customer here could be anyone accessing through the Internet while the seller denotes any kind of targets that support agent-based electronic contracting. Finally, the Agent is the particularly certified software agent which takes the purchase information and authentication information of the customer. The agent may then negotiate on its own with Seller on behalf of customer, and help generate the final signed electronic contact, which may be subject to the final verification of the AAP and/or the approval of the customer.

4.1 Agent Request

Figure 5 shows the procedure for a human user C to request the AAP for using an agent. Before requesting, the customer C first generates a pair of keys (public key and private key) for the agent's use. Then, C sends to the AAP a signed request Req_C which is in the following form: $Req_C : \{request, Sig_C(request), Cert_C\}$. The request field includes the buying description, authorization profile, agent public key, and the agent code. $Sig_C(request)$ denotes the signature of the customer C on request, and $Cert_C$ is the public key certificate of C, which includes the public key of C.

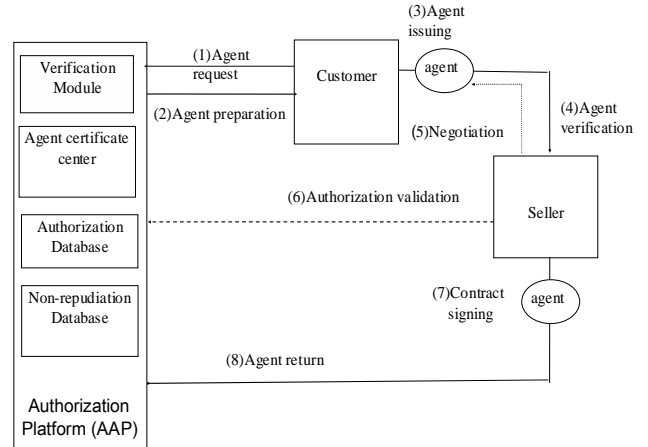


Figure 4. Overview of proposed secure AAP scheme

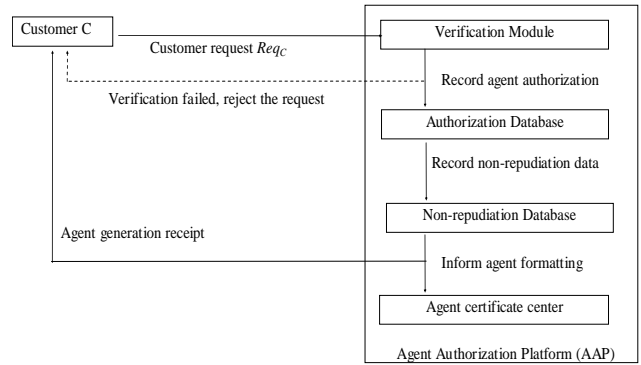


Figure 5. Agent request flow chart

On receiving the request Req_C , the AAP first checks the validation of the $Cert_C$ by verifying the signature of the Certification Authority (CA). Then it verifies C's signature on the request. In case of verification failure, the AAP rejects the request and report the possible fraud if necessary. If all the verifications succeed, the AAP records the request into the authorization database and $Sig_C(request)$ into the non-repudiation database. Finally, the AAP forwards the request to the agent certificate center for agent preparation and sends a confirmation receipt back to the customer. Note that the agent key pairs are generated on the customer side, and only the agent public key is submitted to the AAP, while the agent private key is kept secret by the customer.

4.2 Agent Certification

The agent certificate center module is in charge of preparing the software agent certificate $Cert_{Agent}$ according to the request. The agent certificate includes several fields, as shown in Figure 6.

Agent identification number (AIN)
Buying description
Authorization Profile
Time stamp and the period of validity
Agent public key
Other static data
Public Key Algorithm specification
$Sig_{AAP}(Above\ data)$
AAP certificate $Cert_{AAP}$

Figure. 6 Structure of a agent certificate

Here, the agent identification number is a random number which help identify the agent uniquely. The buying description describes the items to be bought and may include details such as a maximum bid price or quantity, depending on the customer's strategy. The time stamp marks the system time when the agent is generated and the period of validity defines the life time of the agent. The agent public key is then generated and submitted by the customer. There are also some other possible static data, such as further descriptions and non-functional requirements. The AAP then generates a digital signature on all of the above data (denoted as M) as: $Sig_{AAP}(M)$. Finally, the certificate of the AAP should be attached so that anyone can get the corresponding public key to verify the related signatures. Then, the AAP attach the agent certificate to the agent code to generate the final agent. Note that the AAP also need to sign all the agent data, including the execute code part, so that the customer can verify the integrity of the agent.

4.3 Agent Issuing and Negotiation with Host

After preparing the software agent, the AAP sends the agent back to the customer. On receiving the certified agent, the customer first install the agent private key. The agent can then start to negotiate with the other sellers according the customer's request. A seller first needs to verify the identity of the agent before and during the negotiation to protect the seller from any possible cheating or fraud transactions. To achieve this, the agent should firstly initiate the negotiation procedure and send the following handshake request to the seller as:

$$\{ Request_{Handshake}, Sig_{Agent}(Request_{Handshake}), Cert_{Agent} \}$$

Here, $Request_{Handshake}$ includes AIN, buying request, and a random number N_r , which is used for resisting replay attack. The host then verifies the following items:

- The certificate $Cert_{AAP}$ and $Cert_{Agent}$ using the public key of CA and AAP, respectively.
- The signature $Sig_{Agent}(Request_{Handshake})$ using the public key of Agent, which is included in the $Cert_{Agent}$.

If all the verifications succeed, it means that the agent is really certified by the AAP. The agent is then authorized to start negotiation. Subsequent negotiation messages, as usual, should be signed by the party bidding it. Note that a seller can also proof his identity to the agent with his public key certificate if necessary.

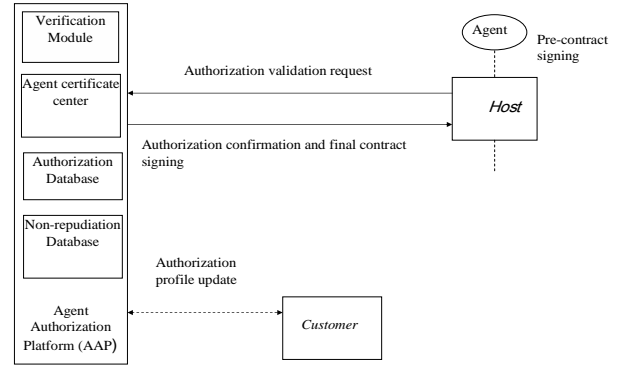


Figure. 7. Authorization validation protocol

4.4 Electronic Contracting and Authorization Validation

After reviewing a seller's offer, the agent can perform the electronic contracting if the offer is acceptable. In this paper, we employ the role of AAP that makes our scheme more flexible for a customer to choose the authorization level according to different transaction. Recall that the authorization profile could contain different authorization level as described in section 3.2. At least there are two levels option in our scheme, i.e., full authorization level and partial authorization level. At the full authorization level, the customer authorizes the agent the ability to perform the final contract signing without further approval from the customer. This mode is usually used for low-risk (low-value) transactions such as CDs, books, etc. At the partial authorization level, the agent cannot sign the electronic contract directly. The final contract requires the verification of the AAP, which involves an authorization validation protocol among the seller, the AAP, and the customer (as shown in Figure 7).

For an agent with only partial authorization level, the seller needs to verify the authenticity of the agent as well as whether the agent's bid and other terms of contract are under its authorization limit. A *pre-contract* between the seller and agent can be generated as:

$$pre-contract : \{ content || Sig_{Agent}(content) || Sig_{seller}(content) \}$$

where the content should include the agent identify number(AIN), the item description, the bid price, and other applicable terms in order to proof the manifestation of assent. Both of agent and the seller should sign on the above content. Since the agent is only partially authorized for this contract, the seller has to submit a request including the *pre-contract* to the AAP for authorization validation. Upon receiving the request, the AAP needs to verify the following:

- The signature $Sig_{Agent}(content)$ and $Sig_{host}(content)$ in *pre-contract*, and
- Whether the bid price and terms in *pre-contract* is consistent with the corresponding authorization profile recorded in authorization database.

If all above verifications hold, the AAP signs on the pre-contract to generate the final electronic contract as:

$$\text{Contract} : \{ \text{content} \parallel \text{Sig}_{\text{Agent}}(\text{content}) \\ \parallel \text{Sig}_{\text{host}}(\text{content}) \parallel \text{Sig}_{\text{AAP}}(\text{content}) \}$$

If verification (a) does not hold, the AAP rejects the validation request and inform the seller to re-submit the validation request. If verification (b) does not hold, the AAP inform the seller that the agent has exceeded the authorization limit and also notify the customer about the agent's deed. If the customer allows such change of authorization profile, he should send a signed confirmation to the AAP for recording into the non-repudiation database. Finally, the AAP should also sign as witness on the contract, and send it to both parties.

5. DISCUSSIONS AND SUMMARY

In this paper, we have analyzed the key legal issues that arise when intelligent software agents are used for e-commerce contracting in contrast to traditional human agents where the legal framework is built upon face-to-face transactions. Based on our legal analysis, we have identified that many of these issues are rooted from the legal identity of agents and the authorization management in agent delegation. Therefore, as a technical solution to such legal requirements, we propose the use of an Agent Authorization Platform (AAP) that also supports user alert and acknowledgment. Based on current legal and business practices, we mimic such automation with agents into a design. Therefore, we have naturally developed a conceptual model for agent authorization and illustrated an AAP architecture with typical use cases of the platform. We have further detailed a security scheme based on the widely-adopted PKI technology and demonstrate the practicability of our technical approach to fulfill such legal requirements. The comprehensive functions of the AAP can support the legal identities of the agents through agent certificates. Further, the AAP validates the final electronic contract against the agents' authorization or with the users' explicit consent with non-repudiation evidence to avoid any violation of the agents' authorization limit, therefore establishing a solid legal foundation for the agents' contract.

Only when the major issue of enforceable trust can be established allows the widespread adoption of agent-based electronic trade. In our approach, we do not intend to solve all the legal issues immediately but we propose a solid and extensible foundation for establishing enforceable trust between agents' communications by providing some fundamental platforms that can help clarify them. We argue that as long as a global standard governing agent interactions does not exist, a customized solution based on user preferences could be adopted. This approach is based on the general rule of freedom of contract where each party has the freedom to choose to enter into a contract on whatever terms it may consider advantageous to its interests.

To the best of our knowledge, there are no other attempts to support the legal requirements with a comprehensive platform for establishing the legal identities of contracting agents through proper authorization management. The only close technical-oriented attempt is Hu's [8] proposal of agent certificates for just authentication but without addressing the problem of authorization limits verification, which is legally crucial

especially for the manifestation of assent of the terms. Other researches on agent contract mainly focus on the logical notion instead of legal issues.

With the recent technical maturity, adoption, and diffusion of PKI and electronic certificate infrastructures, we believe our AAP proposal is a direct and viable extension. However, a main technical challenge and effort is the specification of authorization limits. This involves a proper encoding of users' requirements, intention, and preferences. To streamline the procedure for this as well as negotiation and other phases of electronic contracting, we are developing methodologies involving the notion of electronic contract templates [3] as well as the use of ontology [5] from Semantic Web technologies [21]. We are also extending this methodology for more general specification agent authorization limits with constraints and authorization verification in the form of the Constraint Satisfaction Problem [19] and Belief-Desire-Intention (BDI) agent architecture [6], both of which are widely adopted in artificial intelligence and agent computing. However, based on our experience, we observe that the first phase of deployment in electronic marketplaces and other common Internet trading scenarios are relatively straightforward (as opposed company or real estates acquisitions) because the number of negotiation issues and variables are small and the consideration of each transaction is relatively small. In particular, customer-to-customer markets involving only a small to medium amount of considerations are probably the most attractive for pioneering AAP-service because automatic bidding agents are useful in assisting the users in tedious negotiations.

Although there are no AAP-like services today, we perceive a gradual but successful adoption of the AAP or related platforms in the near future. This is because our approach not only helps in legal issues, but also technical issues (such as agent reliability as the AAP guide against constraint violations, which is another direction of our ongoing research) as well as social issues (such as the build up of trust and a positive image of technical reliability). Only after technical validation and success can further legislation be studied and enacted. However, the successful experience in electronic transactions with PKI can serve as a good reference and starting point.

There are several open issues that need to be resolved. We envision that a combination of enactment of legislation with the support of technical solutions is eventually required to resolve further ambiguities and to help establish strong user trust. For example, if the user wishes to fully authorize the contracting agent, legislation can be enacted to give legal personality to the agent. However, users are responsible to transfer adequate assets (or equivalent insurance) to the agents and the other parties can go against the agents' assets upon dispute. Then, agents can use solutions in artificial intelligence to make "their own" decisions based on user preferences. If agents own assets, their users are protected because the decision of the agents out at stake the specific assets, while the other parties are also protected because they can go against the agents. Assets granting and management for agents is therefore an important direction for future research to further enhance the notion of legal identity for agents as discussed in Section 2.

In addition, electronic communication can be used in an efficient way to facilitate the performance of a contract. For example, in real life a breach of contract can occur because a party fulfills its

contractual obligation inadequately. Our proposed AAP can be extended to solve such problems. Critical points of the execution can be identified and messages can be sent to the parties on time to remain of the contractual capabilities and request progress reports. Associated legislation should stipulate that if a party receives the pre-obligation messages, then unless otherwise proved, the party was fully informed, aware, and had the appropriate time to fulfill the obligation. Further for the promotion of international laws of electronic agents and avoid other ambiguities in contracting, we need to investigate a systematic way for digital unification of concepts (i.e., ontology), such as through Semantic Web technologies.

In our future work, we are also addressing specific jurisdictions and developing agent models that can adhere to the existing laws. We are also considering the legal and technical aspects of delegation, network of trust, and authorization chains. Investigations in cultural and trust issues are also in our agenda.

6. REFERENCES

- [1] T. Allen and R. Widdison, "Can Computers make Contracts?", *Harvard Journal of Law*, 1996
- [2] Anthony J. Bellia, "Contracting with electronic agents," *Emory Law Journal*, 2001.
- [3] D.K.W. Chiu, S.C. Cheung, and S. Till., "An Architecture for E-Contract Enforcement in an E-service Environment," In *HICSS36*, CDROM, 10 pages, IEEE Computer Society Press, Jan 2003.
- [4] D.K.W. Chiu, Benny Kwok, Ray Wong, E. Kafeza and S.C. Cheung, "Alert Driven E-Services Management," *HICSS37*, IEEE Computer Society press, CDROM, 10 pages, Jan 2004 (*Best Paper Award, Decision Technologies track*).
- [5] D.K.W. Chiu, J.K.M. Poon, W.C. Lam, C.Y. Tse, W.H.T. Siu, W.S. Poon. "How Ontologies Can Help in an E-marketplace," In *European Conference on Information Systems* (ECIS 2005), May 2005.
- [6] M. He, N.R. Jennings and H.-f. Leung, "On agent-mediated electronic commerce," *IEEE TKDE*, 15(4):985- 1003, July-Aug. 2003.
- [7] B. Hermans, "Intelligent Software Agents on the Internet: An Inventory of Currently Offered Functionality in the Information Society and a Prediction of (near-)Future Developments" (1996), http://www.firstmonday.dk/issues/issue2_3/ch_123/index.html
- [8] Y.-H. Hu, "Some thought on Agent Trust and Delegation," In *Proc. AGENTS'01*, ACM Press, pp. 489-496, 2001.
- [9] Kerr, "Providing for autonomous electronic devices in the Uniform Electronic commerce Act," In *Proc. Uniform Law Conference of Canada*, 2001, Toronto, Canada, <http://www.law.ualberta.ca/alri/ulc/current/ekerr.htm>
- [10] H. Kim, J. Baek, B. Lee, and K. Kim. "Secret Computation with Secrets for Mobile Agent Using One-time Proxy Signature," In *Proceedings of the 2001 Symposium on Cryptography and Information Security*, (2001) 845--850.
- [11] B. Lee, H. Kim, and K. Kim, "Secure Mobile Agent using Strong Non-designated Proxy Signature. In *Proceeding of the Sixth Australasian Conference on Information Security and Privacy*," LNCS, Vol. 2119, Springer-Verlag (2001) 474--486.
- [12] Jean-Francois Lerouge, "UCITA: The use of electronic agents questioned under contractual law: suggested solutions on a European and American level," *18 J. Marshall J. Computer & Info. L.*403, 1999.
- [13] I. Kafeza, E. Kafeza and D.K.W. Chiu. "Legal Issues in Agents for Electronic Contracting," *HICSS38*, Big Island, Hawaii, IEEE press, CDROM, 10 pages, 2005.
- [14] Y.-B. Lin and I. Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley & Sons, 2000.
- [15] P. Maes, R. H. Guttman, A. G. Moukas, "Agents that buy and sell," *CACM*, 42(3):81-83, March 1999.
- [16] Stephen T. Middlebrook, John Muller, "Thoughts on Bots: The emerging law of electronic agents," *Business Lawyer*, 2000.
- [17] Object Management Group, *Foreword UML specification 1.4*, Sept. 2001.
- [18] T. Sander, C.F. Tschudin. "Protecting Mobile Agents against Malicious Hosts. Mobile Agent Security," LNCS Vol. 1419, Springer-Verlag, NewYork (1998) 44--60.
- [19] E. Tsang, *Foundations of Constraint Satisfaction*, Academic Press, 1993.
- [20] UETA, *Legislative Fact Sheet*, <http://www.nccusl.org>, 1999.
- [21] Web-Ontology (WebOnt) Working Group. <http://www.w3.org/2001/sw/WebOnt>