Negotiated Revealing of Trader Credentials in e-Marketplaces mediated by Trusted and Privacy-aware Admittance Controllers

Marco Casassa Mont, Mike Yearworth
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2001-216
September 12th , 2001*

E-mail: marco_casassa-mont@hp.com, mike_yearworth@hp.com

negotiation, admittance, B2B, e-marketplace, trust, privacy, trust service, credentials

The rise of e-marketplaces on the Internet is going to bring a broad new set of business opportunities to enterprises and customers at a fraction of the physical-world costs. However, to be really successful, these e-marketplaces must be open, trusted, fair and transparent. They must be able to convey on-line the same feeling of trust, security and privacy that traditional marketplaces do. This has implication on three critical aspects: the decisions to be made about membership of traders; their admissibility to negotiations; the controls over the negotiation processes. In this paper we discuss a novel method for automating the admittance to negotiation within marketplaces consistently with traders' privacy requirements.

* Internal Accession Date Only
Approved for External Publication

1. Introduction

In the last years there has been a proliferation of digital marketplaces on the Internet [1] supplying e-services like auctions and exchanges to a potentially huge set of customers and enterprises.

The advent of these services introduces many advantages [2], [3]: the on-line markets operate at a fraction of the physical-world costs; services are accessible to a potentially broader set of participants; the low cost of getting connected enables fragmented buyers and sellers to find each other, independently from their geographical locations; new price setting mechanisms can improve pricing efficiency; automated trading can eliminate many market inefficiencies; electronic marketplaces generate trading and pricing information that did non exist before.

However, providing open, trusted [4], fair and transparent e-marketplaces for all the traders is the key element to enhance the ability of market makers to attract business [5]. This has implication on three critical aspects: the decisions to be done about membership of traders; their admissibility to a negotiation phase; the controls to be put in place during negotiation processes.

To address the *membership* issue, a market maker can define admission policies to vet market participants. These policies define whether the participant is fit and proper, introduce constraints on participant creditworthiness and define regulatory controls.

To decide on the *admissibility* to a specific negotiation, the initiator of a negotiation should be able to verify the trustworthiness and credibility of the other potential traders and at the same time preserve the privacy of the disclosed information. Equally, market participants should have tools to verify the credibility and reliability of proposals made by other traders *during a negotiation* [6].

In order to take full advantage of the on-line aspect of e-marketplaces all the above controls and decisions should to be done as much as possible on-line, in a automated and digital way, without compromising the level of security, privacy and trust that are already available within traditional marketplaces. A broad set of e-trust services need to be implemented and deployed in the e-marketplace ecosystem to underpin trust. These e-trust services include certification authorities, trusted third parties, rating services, recommendation services, notaries and long–term storage of sensible digital documents.

We concentrate this paper on the problem of admittance to negotiation. The objective is to describe a novel model for automating the *admittance process to negotiation* within marketplaces by using trusted third parties.

Different negotiation models are possible in a marketplace: *1:1*, *1:many* and *many:many*. In a 1:1 negotiation a first trader initiates a negotiation with a second trader, for instance for a sale of goods. Generally the initiator has control of the negotiation process. In a *1: many* negotiation, a first trader initiates the negotiation and communicates with a plurality of other traders. For instance this may be an auction hosted by a marketplace. In a *many:many* negotiation a plurality of traders

negotiate with each other through the auspices of a communication medium which could be a marketplace controlled by a market maker.

In each of the above models, it is important that only those participants satisfying the required criteria are admitted to negotiation. This phase is separate from and prior to the negotiation phase: admittance criteria might change and be customized to the specific negotiation. For buyers the admittance criteria usually include credit information, identification information, address information, credit and payment credentials, etc. For sellers this might include evidence of title to the goods/services being sold, etc. Presently out of bounds communications such as FAX, letters, phone, etc. are used to solve the problem, in a non-automated way.

In the example of a marketplace, admittance criteria are usually imposed in a non-negotiable way by the market maker. The market maker may require a given set of parameters to be revealed and only permit admittance to the marketplace (and the negotiation phases) if all the parameters are supplied and they are satisfactory. Not always traders can or are willing to satisfy such requirements. Some parameters may not be available to a trader seeking admittance to a marketplace or, for privacy reasons, it may choose to withhold them.

2. Model for automating the admittance to negotiation

In this section we describe a novel model that specifically address the problems of automating the admittance to negotiation in a consistent way to privacy constraints and requirements dictated by traders.

Our model consists of:

1. A method to allow the definition of admittance requests from a superset of parameters within a trusted third party, referred in this paper as *admittance controller*;

2. An admission service, run by the admittance controller, to determine whether the received admittance request satisfies the admittance criteria;

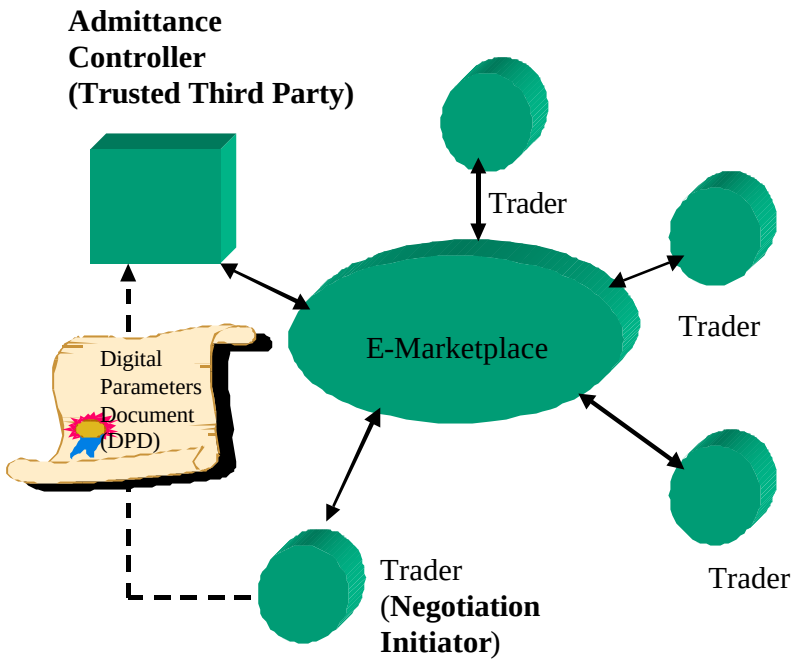
3. A digital communication method to allow a potential participant to make an admittance request to the admittance controller.

2.1 Admittance Controller

The admittance controller is a trusted third party that makes admittance decisions. Its decisions are driven by the content of a *Digital Parameters Document* (DPD). The DPD document is provided by the initiator of a negotiation or a market maker (running a marketplace) or it is defined by the admittance controller itself (figure 1).

To simplify our exposition, in the remaining part of this section we make the assumption that the DPD provider is a market maker. We concentrate on the 1:many model although all the following concepts apply also to the other models.

Figure 1: Diagram of involved entities



The DPD document is composed of two parts: a public part *A* and a private part *B*. The part *A* is accessible in read-only mode to the admittance controller and the market participants while the part *B* is accessible only to the admittance controller. Only the market maker (DPD provider) has the ability to amend any part of the DPD definition though this might be delegated to the admittance controller.

The part *A* of the DPD sets out the superset of admissible parameters the market maker is willing to consider in making an assessment of whether to admit a trader to the negotiation in a marketplace. A simple list of parameters includes: personal/company identification information, credit information, address information, third party references information, payment instrument type and details, billing address, shipping address, historical information, rating information, proof of conformity to standards, etc.

The part *A* of the DPD may also specify the extent of disclosure options available for each parameter. For instance there may be a self-consistent combination of the following constraints: only reveal to the admittance controller, reveal to market maker, reveal a non-repudiable proof of the parameter (such as its digest) to the market maker, reveal parameter specifics before negotiation for admittance starts, reveal parameter specifics when admittance parameters agreed, reveal on trade, etc.

The part *B* of the DPD allows the admittance controller to determine, without reference to the market maker, whether admittance is permitted. A large number of criteria can be expressed ranging from simple parameter-based constraints to more complex logical constraints.

For instance, simple examples of admittance criteria are shown in figure 2.

Figure 2: Examples of admittance criteria

Example 1

Admit if: *identification is provided to the admittance controller (AC) or market maker (MM) prior to admittance*
AND
Trader credit > $50000 revealed to AC prior to admittance

Example 2

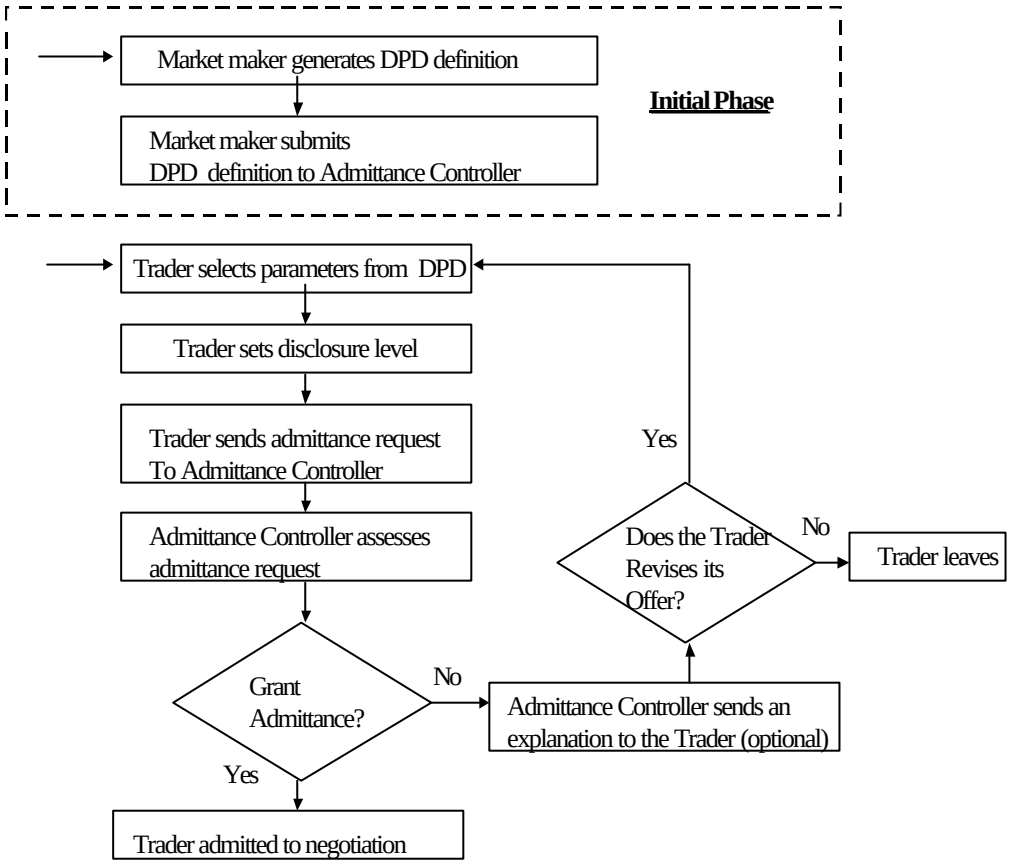
Admit if: *identification is provided to AC prior to admittance*
AND
Trader credit > $20000 provided to AC prior to admittance
OR
Third party reference provided to MM prior to admittance

The DPD document plays a key role in the admittance process as it contains all the information and the policies necessary to the admittance controller to make admittance decisions.

2.2 Admittance Service

Traders interact with the admittance controller to gain access to the negotiation. The overall admittance negotiation process is shown in figure 3.

Figure 3: High level algorithm for admittance to negotiation



As a precursor to the admittance negotiation, the market maker generates a DPD definition and provides it to the admittance controller.

A trader, as a potential negotiation participant, reviews the public part of the DPD definition at the admittance controller site and selects those parameters it is willing to provide for admittance to the negotiation.

The trader sets the disclosure level. It characterizes each parameter by stating in an *extent of disclosure statement* the level of disclosure it is willing to offer. Different parameters may be defined by different characteristics and attributes. The extent of disclosure will usually include the party or parties to which disclosure is made and the timing thereof. These parties can be the market maker, the admittance controller or the other parties seeking admittance. More generally disclosure may be possible to regulatory authorities, banks, tax offices, trading associations, government, public record offices, etc.

The trader sends an admittance request to the admittance controller containing the parameters it is willing to disclose. These parameters are generally a subset of the parameters specified by the DPD.

The admittance controller analyses the parameters and the associated characteristics and determines whether they satisfy the admittance criteria, by evaluating the admittance constraints specified in the part *B* of the DPD. Part of the parameters could be available as digital credentials [15] issued by trusted third parties to the trader: the admittance controller can verify their integrity and validity by interacting with their issuers (if trusted) and other e-trust services [16].

It communicates to the trader whether the admittance has been granted or refused. In case of refusal, the answer can (optionally) be accompanied by a statement describing the grounds on which the request has not been accepted.

The trader can then revise and resubmit its offer for admittance or leave the negotiation.

2.3 Digital Communication Method

The communication between traders and the admittance controller needs to be secured and private. Communication protocols like SSL [13] can be used to securely exchange messages and information on the Internet. If required, the involved parties can make use of digital identity certificates [14] for authentication and non-repudiation purposes.

3. Related Work

The problem of trust, privacy and security in negotiation has been widely researched in the context of cooperative and competitive agents, interacting together to achieve a particular goal. An overview of pioneering work in this area is provided by [7].

A number of models and architectures for electronic marketplaces (e.g. *COPS* [8], *MAGNET* [9]) apply mechanisms to enforce trust, privacy and control during the negotiation phase by prescribing that the market maker itself acts as a trusted third party to enforce market rules, deadlines, penalties and disclosure of identities. In our model we explicitly target the problem of *admission* to a negotiation phase. Not necessarily the market maker is the trusted third party to make this decision and definitely it is not the only entity that can define the admission criteria for a specific negotiation. Specification of admission criteria and their control is devolved. The admittance controller can be an entity external to the marketplace. The negotiation initiator can define its own admission criteria and the participants seeking for admission have control over the disclosure and privacy of their admission parameters.

The usage of digital information, as digital credentials and digital documents has already been explored in the past, both in the context of negotiation and fulfillment.
The *SEMPER* open architecture [10] comprehends the usage of digital credentials in an e-marketplace context. The *Netbill* system [11] supports a digital credential mechanism that is used to obtain discounts when negotiating over information goods on the Internet. Their usage of digital credentials is to enhance trust during the

execution or negotiation phase, whereas we make use of digital credentials during the admission to a negotiation phase. In addition in our model the participants can explicitly define metadata describing their requirements in term of disclosure levels and privacy of their digital credentials.

Relevant work has been described in [12] about digital certificate showing protocol techniques that enable the selective disclosure of personal (and other) data, and analyzes their privacy and security properties. A particular effort is made to describe how to design generic digital certificates that preserve privacy without sacrificing security. In our model we describe specific mechanisms and algorithms to deal with the negotiated disclosure of credentials. Security is not the major concern while trust, privacy and enforcement of admission criteria are.

4. Conclusions

The admittance to negotiation is a very important phase as decisions are made about which traders can negotiate. This decisional process has to be tailored to each specific negotiation in order to satisfy the requirements of the negotiation initiator.

Today, out of bounds communications such as FAX, letters, phone, etc. are used to solve the problem, in a non-automated way. In addition, admittance criteria are usually imposed in a non-negotiable way by market makers.

We believe that to be really successful, e-marketplaces need to take full advantage of their on-line aspect and introduce automation as much as possible. Additionally, e-marketplaces need to be more flexible to satisfy traders' needs, in term of negotiation requirements and privacy.

We described a novel method to address these issues. This method automates the admittance to negotiation by making use of a trusted third party playing the role of an admittance controller. Our method allows negotiation initiators to customize the admittance criteria depending on their needs: they define which parameters and which conditions need to be satisfied to be admitted to the negotiation and delegate their enforcement to the admittance controller. This method is aware of traders' privacy requirements: traders can decide which credentials are willing to provide and define the associated level of disclosure and privacy.

5. References

[1] Net Market Makers - *Digital Marketplaces: Enabling the Internet Economy.* Net Market Makers - 1999

[2] Timmers, T. - *Electronic Commerce: Strategies and Models for Business-to-Business Trading.* John Wiley & Sons, Inc. - 2000

[3] Aldrich, D. - *Mastering the Digital Marketplace.* John Wiley & Sons, Inc. - 1999

[4] Raish, W - *The e-Marketplace Strategies for Success in B2B e-Commerce.* McGraw-Hill - 2001

[5] Sculley, A. – Woods, W. *B2B Exchanges (Chapter 5: Membership and Ownership Models).* ISI publication - 1999

[6] Bartolini, C. - Casassa Mont, M. - *Digital Credentials and Authorization to Enhance Trust in Negotiation within E-Services Marketplaces*. HPL-2000-75 - 2000

[7] Laasri, A. – Laasri, S. – Lander, S. – Lesser, V. - *A generic Model for Intelligent Negotiating Agents.* International Journal of Intelligent and Cooperative Information Systems, pages 291-317 - 1992

[8] Pernul, G. – Rohm, A. - *Modeling Secure and Fair Electronic Commerce*. Proc. Of Annual Computer Security Applications Conference. ACSAC'98 - 1998

[9] Collins, J. – Youngdahl, B. – Jamison, S. – Mobasher, B – Gini, M - *A Market Architecture for multi-agent contracting*. Proc. Of the Second International Conference on Autonomous Agents, pages 285-292 - 1998

[10] Waidner, M. - *Development of a Secure Electronic Marketplace in Europe*. IBM Zurich Research Laboratory. Proceedings of ESORICS'96 - 1996

[11] Sirbu, M. - Tigar, D. – *NetBill: An Internet Commerce System Optimised for Network Delivered Services*. IEEE Personal Communication, pages 6-11, - 1995

[12] Brands, S. - *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. The MIT Press - 2000

[13] Frier, A. O. - Karlton, P. and Kocher, P. C. - *The SSL protocol - IETF* - 1996

[14] Housley, R. - Ford, W. - Polk, W. – Solo, D. - *RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL profile*, IETF – 1999

[15] Casassa Mont, M. - Brown, R. - *PASTELS project: Trust Management, Monitoring and Policy-driven Authorization Framework for E-Services in an Internet based B2B environment.* HPL-2001-28 - 2001 [HP Restricted]

[16] Baldwin, A. – Beres, Y. – Casassa Mont, M. – Shiu, S. – *Trust Services: A Trust Infrastructure for E-Commerce.* HPL-2001-198 - 2001