# Digital Credentials and Authorization to Enhance Trust in Negotiation within E-Services Marketplaces

Claudio Bartolini (claudio_bartolini@hp.com)
Marco Casassa Mont (marco_casassa-mont@hp.com)

Trusted E-Services Laboratory
Hewlett Packard Laboratories – Bristol, UK

Abstract

In the present economy, business-to-business (B2B) relationships are usually long-termed and characterised by a high degree of mutual pre-existing trust. With the advent of the Internet economy, E-Services marketplaces will provide an infrastructure where B2B relationships will be set up in a highly dynamic fashion.

The increased dynamism of the marketplace introduces issues of lack of trust among the market participants, due to the shorter time span of business relationships. The marketplace responds to it by defining admission policy to vet the market participants. Still, the market participants will want to base their negotiation decisions on subjective aspects of trust with regard to other participants. Our model of E-Services marketplaces addresses these issues by means of authorization and digital credentials.

This paper presents scenarios that highlight trust issues during negotiation within our model. We then produce a first list of requirements that an architecture should satisfy to enhance trust in negotiation within E-Services marketplaces.

# 1. Introduction

Electronic commerce can be defined loosely [PTIM99] as 'doing business electronically'. Electronic commerce includes electronic trading of physical goods and of intangibles such as services and information. One of the problems of the initial forms of business-to-business (B2B) electronic commerce such as Electronic Data Interchange (EDI) was the lock-in in the relationship. Both suppliers and purchasers had to invest significantly up-front in the relationship, so were not easily able to move their business elsewhere. The technological relationship between the parties was a friction factor, preventing free competition in the longer term [CSHA99].

A new phase of electronic commerce is just beginning. It aims to address these issues, allowing automated business interactions to take place in a fluid environment. The emergence of electronic marketplaces [NMM99] makes technology no longer a friction factor to change supplier or customer. Long-term relationships will still play an important role, but they will persist because of the choice of both parties rather than technological lock-in. The key building blocks of this new paradigm, E-Services [PSEY99], will be able to interact dynamically with each other to create short-term or long-term trusted trading relationships to satisfy the needs of different business partners.

The increased dynamism of the marketplace introduces issues of lack of trust among the market participants, due to the shorter time span of business relationships. The marketplace responds to it by defining admission policy to vet the market participants. Still, the market participants will want to base their negotiation decisions on subjective aspects of trust with regard to other participants. This is independent of the fact that market participants have been pre-screened as "trusted" by the marketplace. The model of E-Services marketplaces that we adopt responds to it by making the assumption that market participants will base their decisions on digital credentials that are exchanged during the negotiation process in the marketplace.

Moreover, our model introduces a separation between the trader who negotiates in the marketplace and the enterprise that is its main stakeholder. This entails trust issues of a different nature between the enterprise and the trader that negotiates on its behalf. Precisely, the trader may need to obtain authorization from the enterprise during its decisional process. [1]

Our research addresses the two points above, i.e. usage of digital credentials and authorization to enhance trust in negotiation within E-Services marketplaces.

This paper presents scenarios that highlight trust issues among the participants to negotiation in our model of E-Services Marketplaces. From the scenarios, we sketch a first list of requirements that an architecture should satisfy from the point of view of

[1] This may appear to be in contradiction to the trend that sees traders gaining more and more intelligence and autonomy. In fact it is not. Our separation of responsibilities between negotiation and authorization is purely functional. This does not advocate an architectural separation. "Intelligent" trader agents will implement functionality that our model relates to both the trader and the enterprise role.

negotiation only. The requirements that we derive are far from being an exhaustive list of what is needed to address the whole complexity of the trust issues in E-Services marketplaces. Our research addresses this topic as well, but it has to be considered beyond the scope of this paper.

The remainder of this paper is structured as follows: in section 2 we will introduce our model of E-Services Marketplaces. In section 3 we will briefly discuss the relationship between authorization, digital credentials and trust. In section 4 we explore the trust issues in our model and describe how they are addressed by means of authorization and digital credentials. In section 5 we present the scenarios and in section 6 we sketch the requirements. In section 7, we present related work, to conclude in section 8.

In appendix we outline some previous work about relationships between trust, digital credentials and authorization carried out in Hewlett-Packard Laboratories Bristol [RBRO00].

## 2. E-Services Marketplaces

E-Services [PSEY99] are Internet-based applications that communicate with one another, fulfilling requests and/or triggering other E-Services that, in turn, carry out their parts of some complex workflow or transaction. E-Services are self-contained, modular, mix-and-match applications. E-Services are self-describing applications. Each E-Service knows what functions it is capable of performing, what inputs it requires, what outputs it produces, and what its attributes are (e.g., security, location, cost, etc.). Moreover, E-Services can be brokered and auctioned. Once an E-Services broker or directory service receives a request, different E-Services applications may vie for the opportunity to perform the requested functions, based on their attributes and their current state.
E-Services can be the building boxes for the new digital marketplaces models such as Procurement Marketplaces (buyer-hosted), Vertical Marketplaces (single industry), and e-business Portals or Horizontal Marketplaces [NMM99].

We briefly sketch a model of the E-Services marketplace. In the rest of the paper, we will illustrate trust issues among the actors in the model.

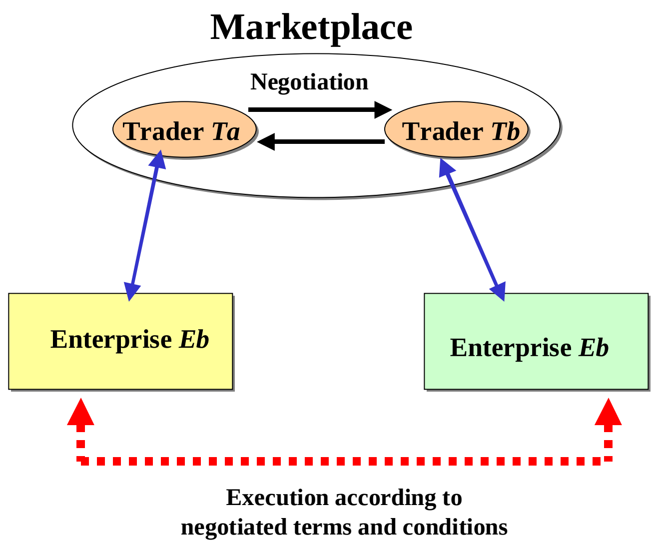



Figure 1

A marketplace is a virtual place where one or more buyers and one or more sellers (*traders*) meet to trade goods or services. The traders are seeking to strike the best deal for their stakeholders (*enterprises*), who are the organizations that have an economic interest in the exchange of the good or the provision of the services being traded. Traders incrementally get to agree on the terms and conditions that will regulate the exchange of goods or the provision of the services through the process of *negotiation*. Traders negotiate by exchanging offers and bids. The enterprises will then have to perform according to the rights and obligations agreed among traders in the marketplace. We refer to the aggregation of the trader and enterprise role as *market participant*.

In the following sections, we will discuss trust issues that arise among the actors in the E-Services marketplaces. Our model introduces a separation of responsibilities between the trader - who is responsible for negotiating - and the enterprise that will have to execute according to terms and conditions that the trader has agreed to on its behalf. As a logical consequence, the last word on trust matters is left to the enterprise. It is up to the enterprise to define the trust policy and authorize the trader's decisions accordingly.

We consider two categories of trust issues: the first is among market participants; the second is between an enterprise and a trader who negotiates on its behalf. The two categories of trust issues are addressed in our model by using *authorization* and *digital credentials*. In the next section we analyze in more detail how these concepts relate to trust.

## 3. Authorization, Digital Credentials and Trust

Authorization is the act of determining whether an entity has the right or the authority to perform a certain action on another entity.

An entity might be granted *authorization privileges* depending on their attributes or their roles. Authorization mechanisms verify whether the entity can exercise their privileges by checking whether they satisfy authorization conditions [MCAS99]. These conditions can be expressed by high-level policies [ELUP95] based not only on user and role privileges but also on service dependent information and external data.

When someone receives information and has no guarantee of the validity of the information that is presented to them, trust issues arise. *Digital credentials* [RHOU99], [SFAR99], [CELL99] can be used to cope with aspects of trust; authorization has to deal with them [MBLA99], [GUST97].

Digital credentials are a powerful way to describe both identity and attributes associated to people and services. They can be used programmatically by authorization mechanisms to make decisions involving trust issues. Certificate authorities underwriting digital credentials must manage their life cycle (credential issuing, verification and revocation) and provide ways to measure and judge trust. Nevertheless the ultimate decision on trusting digital credentials and their contents has to be taken through definition of proper trust policy [MBLA96]. Authorization mechanisms can deal with trust issues by making decisions according to this policy.

In appendix we provide more detail about the above concepts by briefly describing the work done at Hewlett Packard Laboratories, Bristol [RBRO00].

## 4. Digital Credentials and Authorization to enhance Trust in Negotiation

As we anticipated in section 2, we consider two categories of trust issues: the first is among market participants; the second is between an enterprise and a trader who negotiates on its behalf.

A trust issue arises from that the marketplace brings together market participants that do not necessarily trust each other. The marketplace enforces a certain degree of trust among the participants by defining a vetting policy. Still, the market participants will want to base their negotiation decisions on subjective aspects of trust with regard to other participants. Digital credentials are exchanged during negotiation to cope with this aspect of trust. Credentials may relate to the trader who is negotiating, the enterprise that it negotiates on behalf of, or the service itself that is being negotiated over.

A trust issue of a different nature exists between an enterprise and the trader who negotiates on its behalf. The partition of the market participant role into trader and enterprise follows from the idea of isolating the responsibility of negotiating an agreement from execution of terms and conditions expressed in the agreement. Therefore, we associate to the enterprise the responsibilities that are not directly related to negotiation. The enterprise retains the right to define trust policies and direct the trader accordingly. Also, the enterprise retains the right of authorization over any offer or bid that the trader can make during the negotiation process.[2]

## 5. Scenarios

This section describes scenarios that highlight the trust issues we discussed. From the scenarios, we sketch a rough list of requirements than an architecture should satisfy from the point of view of negotiation only.

The context of the scenarios is a one-to-many negotiation happening among three enterprises, *Ea*, *Eb* and *Ec*. A trader *Ta* is selling an E-Service *S* on behalf of *Ea* while traders *Tb* and *Tc* are competing to buy this E-Service on behalf of *Eb* and *Ec* respectively.

The underlying assumption is that all the involved parties share a *common ontology* about *service description* and *digital credentials*. Each market participant involved in the process has its own definitions of what the trusted entities are and implements its own procedures for verifying digital credentials.

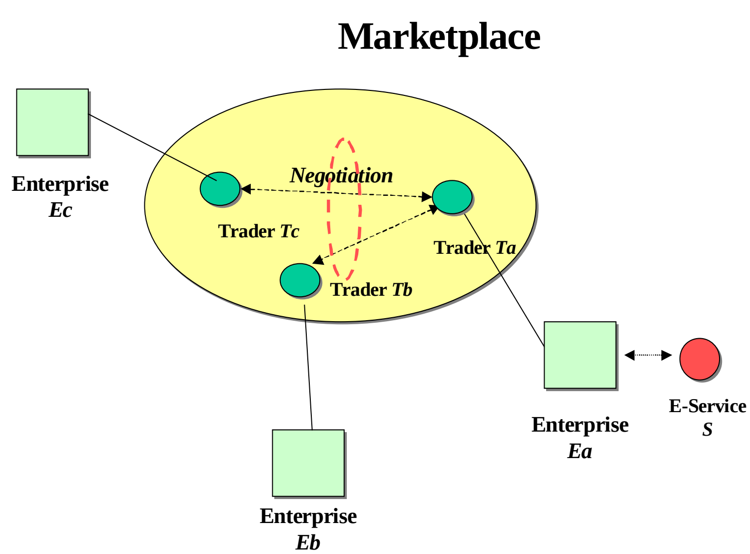



Figure 2

[2] Same as note 1.

As we highlighted in the previous section, we identify two categories of trust issues among the actors. The first is about trust issues among market participants and is addressed through the usage of digital credentials as part of the negotiation process. The second has to do with trust issues between the enterprise and the trader that negotiates on its behalf and it is addressed by the enterprise retaining the right of authorization over the trader's decisions.

**Case 1: Digital Credentials**

This case is about the exchange of digital credentials during the negotiation process to support decision making on trust issues. Market participants do not necessarily trust each other; in any case they may want to base their negotiation decisions on aspects of trust. Digital credentials may relate to the trader who is negotiating, the enterprise that it negotiates on behalf of, or the service itself that is being negotiated over.

A few sub-cases have been considered:

- During the negotiation process, the trader *Ta* receives a bid from *Tb* involving digital credentials (credit card details or digital bank statement) issued by third parties to *Eb*. *Ea* has to make decisions on the acceptability of the bid based on its trust policy. These conditions for example define which certificate issuers and which kind of digital credentials can be trusted.

- During the negotiation process, the trader *Ta* needs authorization from *Ea* to expose to foreign traders adequate digital credentials as part of an offer that it is placing.

- During the negotiation process, the trader *Ta* receives two competing bids, along with digital credentials. Other conditions being even, discriminating over digital credentials will decide on the choice to make. *Ta* prompts *Ea* to make a decision on which bid has to be accepted. *Ea* has policies defining priorities based on credentials issuers and credential contents. For example if the two bidders provide digital credentials defining who guarantees for the payment, an authorization rule could say that VISA is preferable to other guarantors if the involved amount of money is greater then $5000 while for lower amount of money whatever trusted bank is acceptable.

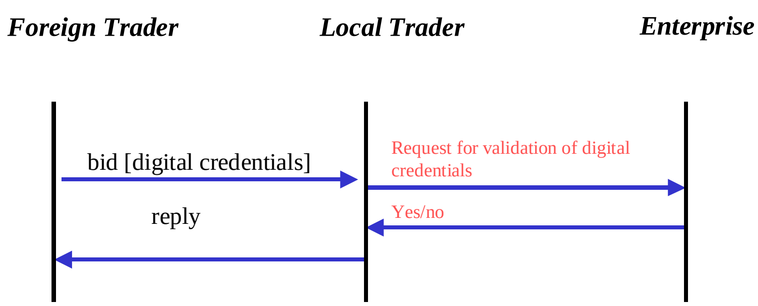
**Case 2: Authorization**

The enterprise will be accountable for acting according to the terms and conditions that the trader negotiates. Therefore it retains the right of authorization over any offer or bid that the trader can make during the negotiation process:

- The trader *Tb* has been instructed by the enterprise *Eb* to buy an E-Service S. The trader *Tb* receives an offer and then it interacts with *Eb* to be authorized to accept this offer.

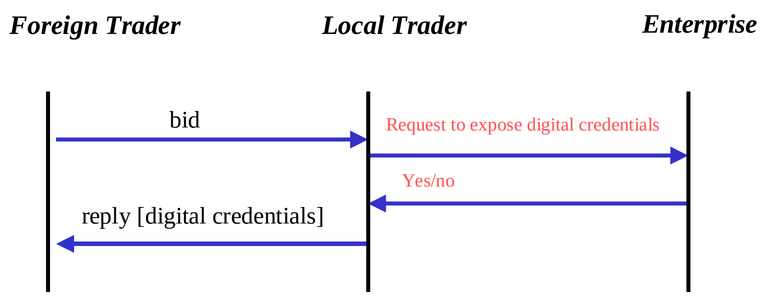
*We cannot stress enough the point that this is purely a separation of functionality in the model. It does not imply any architectural decision.*

The following interaction diagrams describe some scenarios. Scenario 1, 2 and 3 fall in the digital credentials case. Scenario 4 is about authorization.



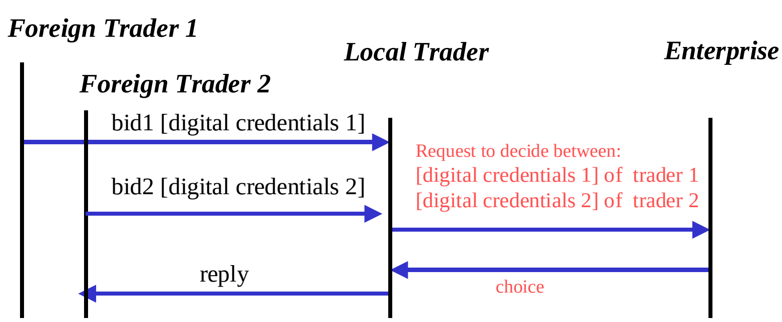

- Digital credentials are sent within a bid by a foreign trader.
- The local trader analyses the bid and, before making any offer, it asks the enterprise to validate the credentials.
- The enterprise can accept or reject the credentials.
- The local trader will act accordingly.

Scenario 1



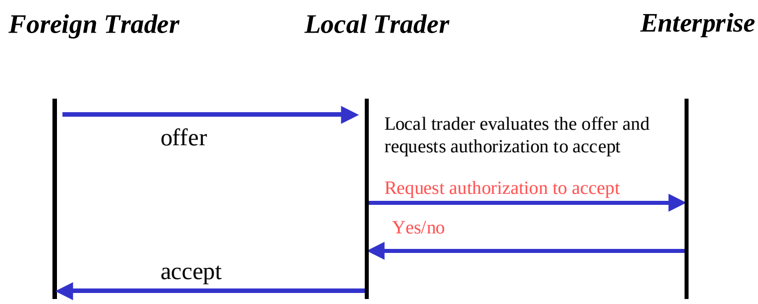

- A bid is received from a foreign trader.
- The local trader needs to expose digital credentials belonging to the enterprise within an offer.
- The local trader asks the enterprise if it can expose these credentials to the foreign trader.
- The local trader replies accordingly to the foreign trader.

Scenario 2




- Two bids are received from two foreign traders.
- The local trader needs to choose between the two traders. Being other conditions even, a choice will be based on their credentials
- The local trader asks the enterprise to make a decision based on these credentials.
- The local trader replies accordingly to the foreign trader.

Scenario 3




- A foreign trader sends an offer to the local trader.
- The local trader evaluates the offer, and decides to accept it based on its utility function.
- The local trader requests authorization to accept the offer to the enterprise.
- The enterprise decides to authorize the trader to accept the offer.
- The trader acts accordingly.

Scenario 4

## 6. Requirements to Enhance Trust in Negotiation by means of Authorization

From a first analysis of the above scenarios, we derive the following rough list of requirements that an architecture should satisfy to enhance trust in negotiation within E-Services marketplaces. As we pointed out in the introduction, the requirements that we derive are far from being an exhaustive list of what is needed to address the whole complexity of the trust issues in E-Services Marketplaces.

- There is a need for an *information model* - based on a common ontology - to express digital credentials together with the messages that traders exchange during negotiation. Digital credentials are associated to and used by all the entities involved: local traders, remote traders, enterprises and other third parties.

- In order to control the negotiation process, the enterprise needs to base their authorization decisions on policy.

- The previous requirement entails the need for a notation to describe authorization constraints, rules and conditions based on trust information and knowledge internal and external to the enterprise.

## 7. Related Work

The problem of *trust in negotiation* has been widely explored in the contest of cooperative or competitive agents, interacting together to achieve a particular purpose. Initially, research on automated negotiation, focused primarily on collaborative problem solving, as a means towards improving coordination of multiple agents working together on a common task. Laasri, Lassri, Lander and Lesser [BLAA92] provide an overview of the pioneering work in this area. As electronic commerce became increasingly important, the work expanded to encompass situations with agents representing individuals or businesses with potentially conflicting interests. The contract net [RSMI80] provides an early architecture for negotiation among competing agents.

In our model, however, we explicitly make two important points. First, we introduce the use of *digital credentials* during negotiation to enhance trust among market participants. Second, we make the point of separating the responsibility of negotiating (associated to the *trader*) from the responsibility of executing according to terms and conditions agreed at negotiation time (*enterprise*). This leads us to associate the power of authorization with the part (again the enterprise) that has the responsibility for executing. From here, it follows that the enterprise also retains the power of defining trust policy referring to digital credentials and enforce them.

A number of models and architectures for electronic marketplaces (e.g. *COPS* [GPER98], *MAGNET* [JCOL98]) apply mechanisms to enforce trust in the negotiation phase by prescribing that the marketplace itself act as trusted third party to enforce market rules, deadlines, penalties, and disclosure of identity. However, in our model the negotiating parties can make their own decision on trust matters, based on their own trust policy and the digital credentials that are exchanged.

The *SEMPER* (Secure Electronic Marketplace for Europe) open architecture [MWAI96], comprehends the usage of digital credentials in an Electronic Marketplace context. Still, their usage of digital credentials is addressed to enhance trust during the execution phase, whereas, we make an explicit suggestion that digital credentials be used during the *negotiation* phase in making decisions involving aspects of trust.

The *Netbill* system [MSIR95] supports a *digital credential* mechanism that is used to obtain discounts when negotiating over information goods on the Internet. Its focus is on micro-payment for information goods on the Internet. In contrast, our model places emphasis on the trust aspect of negotiation.

## 8. Conclusion

Our model of E-Services marketplaces introduces a separation of responsibilities between the trader - who is responsible for negotiating - and the enterprise that will have to act according to terms and conditions that the trader has negotiated on its behalf. We made the point that the separation is purely functional and does not suggest any architectural choices.

We then explored the trust issues among the actors in the marketplace. We explored two categories of trust issues: the first is among market participants; the second is between an enterprise and a trader who negotiates on its behalf. The two categories of trust issues are addressed in our model by using *authorization* and *digital credentials*. Digital credentials are used during negotiation to support decision making on trust matters. The final decision is left to the enterprise. It is up to the enterprise to define the trust policy and authorize the trader's decisions accordingly. Moreover, the enterprise retains the right of authorization over any offer or bid that the trader can make during the negotiation process.

We presented few scenarios that highlight these trust issues among the participants to negotiation in our model of E-Services marketplaces. From these we moved onto deriving a list of requirements than an architecture should satisfy to enhance trust in negotiation within E-Services marketplaces.

The requirements are about: the need for an information model – based on a shared ontology – to express digital credentials along with the messages that traders exchange during negotiation; the need for the enterprise to base their authorization decisions on policies; and the need for a notation to describe authorization constraints.

The requirements that we derive are far from being an exhaustive list of what is needed to address the whole complexity of the trust issues in E-Services marketplaces. Still they are essential to enhance trust in negotiation within E-Services marketplaces.

## Acknowledgment

We would like to thank Giacomo Piccinelli (HP Labs–Bristol) for his feedback and Brian Monahan (HP Labs–Bristol) for his comments during the early stage of this paper.

## Bibliography

[PTIM99] P. Timmers - Electronic commerce - Strategies and models for business-to-business trading - Addison Wesley - 1999

[CSHA99] C. Shapiro, H. Varian Information Rules – A Strategic Guide to the Network Economy - Harvard business school press - 1999

[NMM99] Net Market Makers – Digital Marketplaces: Enabling the Internet Economy – Net Market Makers - 1999

[PSEY99] P. B. Seybold – Preparing for the E-Services Revolution – Seybold group, - 1999

[RBRO00] R. Brown, M. Casassa Mont – PASTELS, a PK based Authorization Service for E-Services, Trusted E-Services Laboratories, Hewlett Packard Laboratories, Bristol, UK - 2000 [HP Restricted]

[MCAS99] M. Casassa Mont, R. Brown, A. Baldwin – ACSIS, an Access Control and Authorization System for Internet Services in a B2B environment, Trusted E-Services Laboratories, Hewlett Packard Laboratories, Bristol, UK – 1999 [HP Restricted]

[ELUP95] E. Lupu, D. Marriott, M. Sloman, N. Yialelis - A Policy Based Role Framework For Access Control, First Acm/Nist Role Based Access Control Workshop, Gaithersburg, USA - Dec. 1995

[RHOU99] R. Housley, W. Ford, W. Polk, D. Solo – Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, IETF - 1999

[SFAR99] S. Farrell, R. Housley – An Internet Attribute Certificate Profile for Authorization – IETF - 1999

[CELL99] C. Ellison – SPKI Requirments, RFC 2692, IETF - 1999

[MBLA99] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis – The KeyNote Trust Management System, RFC 2704, IETF - 1999

[GUST97] Gustaf Neumann, Stefan Nusser – A Framework for Prototyping Environment for a W3 Security Architecture - 1997

[MBLA96] M. Blaze, J. Feigenbaum, J. Lacy - The PolicyMaker Approach to Trust Management, DIMACS Workshop on Trust Management in NetworksSouth Plainfield, New Jersey - September 30-October 2, 1996

[BLAA92] B. Laasri, H. Laasri, S. Lander V. Lesser - A Generic Model for Intelligent Negotiating Agents - International Journal of Intelligent and Cooperative Information Systems, 1(2) 1992 pp291-317 – 1992

[RSMI80] R. G. Smith - The contract net protocol: high-level communication and control in a distributed problem solver - IEEE Trans. Comput. 29, 1104-1113 - 1980.

[GPER98] G. Pernul; A. W.Röhm - Modelling Secure and Fair Electronic Commerce - Proc. of Annual Computer Security Applications Conference; ACSAC'98 - 1998

[JCOL98] J. Collins, B. Youngdahl, S. Jamison, B. Mobasher, and M. Gini - A market architecture for multi-agent contracting - In Proc. of the Second Int'l Conf. on Autonomous Agents, pages 285-292 - 1998

[MWAI96] M. Waidner - Development of a Secure Electronic Marketplace for Europe – IBM Zurich Research Laboratory – Proceedings of ESORICS 96 - 1996

[MSIR95] M. Sirbu, J. D. Tigar – NetBill: An Internet Commerce System Optimized for Network Delivered Services – In IEEE Personal Communication, Pages 6-11 – 1995

## Appendix

## PASTELS: a Public Key based Authorization Service for E-Services

PASTELS is a project [RBRO00] in the Trusted E-Services Laboratory, Hewlett Packard Laboratories, Bristol, UK. The research activities of the project involve the investigation of the relationships between trust, digital credentials and authorization services among others.

PASTELS addresses a B2B scenario where employees working for different enterprises want to interact together and need to access services provided by other enterprises (service providers). In particular PASTELS focuses on the case where enterprises have no previous business relationships and they are not member of any EDI VAN or common Extranet. In such a case very important issues are trust and trust management.

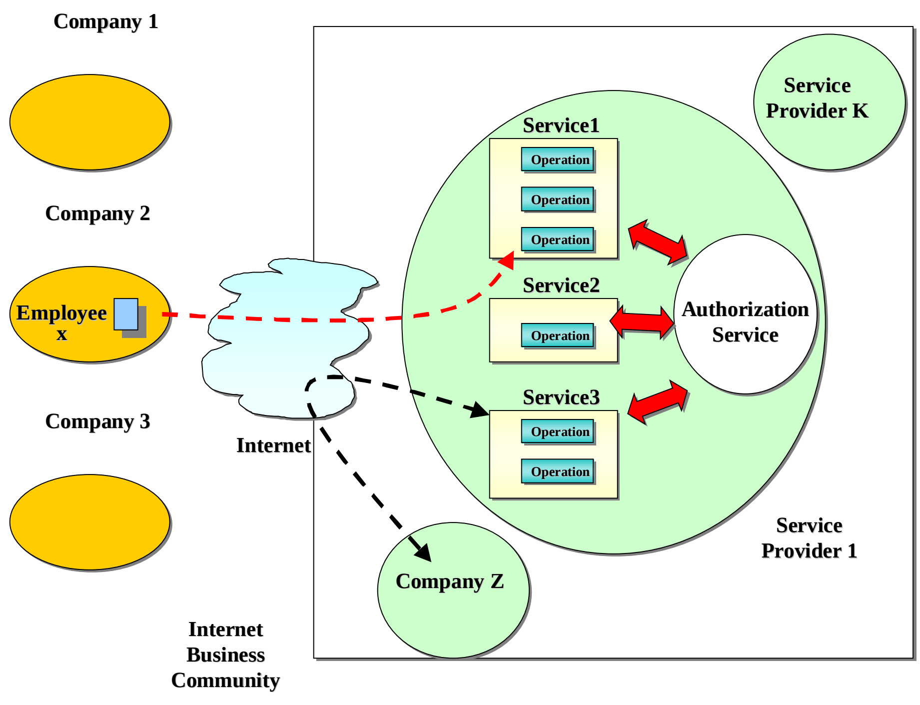



Figure A1

In the PASTELS approach, enterprises are asked to explicitly define the set of third parties and digital credential issuers they are going to trust. Enterprises also need to specify which attributes are going to be trusted that appear in a digital credential.

In PASTELS, enterprises can define their local validation and authorization policies by using a hybrid mechanism. This approach involves the usage of high-level rules (conditions) to express constraints both on trust issues (validation of credentials and their contents) and a more traditional access control issues (check for privileges defined in user profiles, roles, etc.). A rule can contain both trust constraints and authorization constraints.

Digital credentials are used both for authentication and authorization purposes. Users can identify themselves by using identity certificates and they can give their digital credentials to the system in order to get authorizations.

The PASTELS prototype, currently under an advanced stage of development, shows how digital credentials can be used by a rule-based authorization service to grant or deny the access to services and their functionalities, under a well defined set of trust constraints. The high level architecture of PASTELS is:

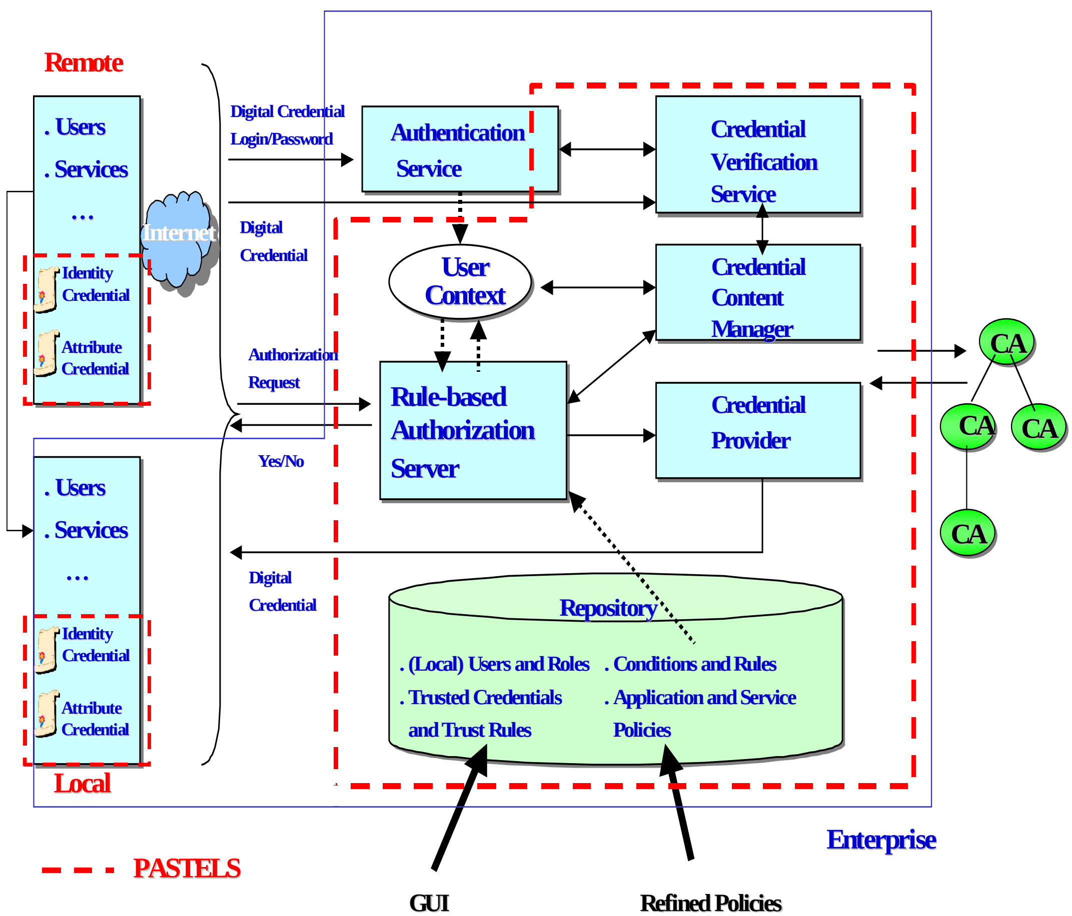



Figure A2

Within the enterprise, a repository contains trust rules to deal with the verification and management of digital credentials. It also contains fine-grained authorization rules associated to services and service functionalities along with attributes and capabilities associated to user profiles and roles. Authorization rules are logical expressions made of basic constraints on user capabilities, service parameters, time information, trust information (list of trusted third parties, trusted capabilities within digital credentials, etc.) and other external information.

Remote and local users (and services) pass their own digital credentials to the system. The system aggregates user's credentials in a user context, after validating them. A user context abstracts both local privileges (user profile information, roles) and digital capabilities (defined within digital credentials) in such a way they can be accessed and used by the authorization server, independently by their low level representation (data format).

A Credential Verification Service verifies the "validity" of digital credentials based on traditional certificate verification mechanisms, trust information and constraints defined in the repository. This service interacts with the authorization server for the interpretation of the trust constraints.

A Credential Content Manager is in charge of extracting and managing digital attributes defined within trusted digital credentials. An ontology on digital credentials is shared between the system and all the credential issuers trusted by the enterprise. The meaning of acceptable attributes (defined within digital credentials) is described by a common vocabulary.

A Rule-based Authorization Server is in charge of authorizing a user to access a service or a service function. In order to grant or deny the access to the user, the authorization server retrieves the set of relevant authorization conditions for the service or service function and interprets them against the current user's credentials and other source of information like time, service parameters and constraints on trust.