Proc. 14th Annual Computer Security Applications Conference, Phoenix, Arizona, Dec. 7-11, 1998. IEEE Computer Society Press.

Modelling Secure and Fair Electronic Commerce

Alexander W. Röhm, Günther Pernul, Gaby Herrmann
Department of Information Systems
University of Essen, Germany

{roehm | pernul | herrmann}@wi-inf.uni-essen.de

Abstract

Security and fairness in business transactions are basic requirements demanded by any participant in electronic markets. In this paper we propose COPS as an infrastructure for building adaptable electronic markets with main focus on security and fairness and MOSS as a methodology for analysing and modelling the security semantics of business transactions. Both are necessary to control the risks involved in dealing (trading) with untrusted parties in an open electronic commerce environment. We address the phases information, negotiation and execution of a business transaction and discuss security requirements which in the past were recognised as being very important for electronic market participants but had only received limited or little attention in the electronic commerce research community.

1 Introduction

Some very fundamental requirements inhibit, or at least slow down the success and growth of Electronic Commerce (EC). The most important requirements, among others, are the lack of

1. a generic and user-friendly infrastructure supporting EC,
2. security and fairness as integral parts of the infrastructure,
3. methodologies for analysing and modelling the security semantics of business transactions.

The *generic and user friendly infrastructure* is mainly necessary for the demander in an electronic market. The demander usually is the driving force in a business transaction and thus the infrastructure must enable him easy access to an electronic market. Otherwise, many potential demanders will not participate in the electronic market which could endanger all the benefits of EC. *Security and fairness* is necessary for all market participants. A supplier will not offer his goods if, for example, secure payment is not guaranteed. The same is true for a demander. He will not participate if, for example, delivery is not guaranteed after payment. Both may not participate in the market if they are not treated by the market infrastructure in a fair way and if privacy and confidentiality is not guaranteed in a business transaction. For secure and fair EC it is essential to know about all security risks of a business transaction. This requires a careful analysis of all security relevant knowledge involved in processing the transaction. We call this knowledge the *security semantics* of the business transaction.

While the first two requirements are enabling services for EC the third requirement is necessary because EC forces rapid changes in the business behaviour of trading partners. The changes will lead to a reorganisation of well-established procedures and thus may make corrections of existing systems necessary and may also have effects on their security. In this paper we deal with all three issues. We develop an infrastructure for secure and fair EC, evaluate the infrastructure by means of an example in a direct search market and outline a technique used for modelling the security semantics of the involved business transactions.

The paper is structured as follows: In section 2 we discuss examples of security requirements in the different phases of a business transaction on an electronic market. Each of the phases has its own security requirements. In section 3 we introduce the COPS project. COPS has the goal to develop and implement a prototype of a generic market infrastructure for EC with its main focus on security and fairness for market participants. Each market participant in each phase of the business transaction is defined (1) by a set of services offered by

the infrastructure, (2) by its communication relationships to other market participants, and (3) by a set of actions, conditions and events which are characteristic for this part of the business transaction. In section 4 we introduce MOSS, a methodology for carefully analysing the security semantics involved in (2) and (3). In section 5 the paper is concluded by giving a status report about the COPS and MOSS projects and by discussing our future planned work.

2 Security and Electronic Commerce

2.1Basic Definitions

Some words on the term “security” are in order. There is no general agreement about the term and its semantics may also have changed over time. This paper uses a very broad definition of security in EC. In this paper we subsume under security

- the general definition: confidentiality, integrity, availability
- intellectual property involved in digital goods: authorship, ownership, copyright, right to use, originality,
- bindings: legal binding, mutual dependencies, non-repudiation
- privacy, anonymity, fairness, trust.

These are not exhaustive lists and may be extended by further relevant issues for EC. A well accepted definition of EC is that it "... is the sharing of business information, maintaining business relationships and conducting business transactions by the means of telecommunication networks." [12]. An important part of EC according to this definition are business transactions, that may take place in electronic hierarchies or electronic markets.

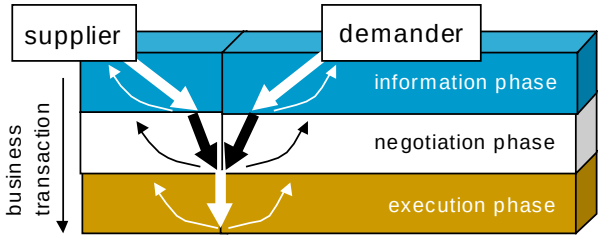


Figure 1: Business transaction phases

Any business transaction usually includes three phases (see fig. 1): the information phase, the negotiation phase and the execution phase (or settlement phase). In the *information phase* the demander (in few cases also the supplier) is searching for a matching business partner. For this purpose a demander asks potential suppliers for their offers. After he has collected these offers he chooses the one he prefers. After matching business partners are found the information phase terminates. During the *negotiation phase* the supplier and the demander have to find an agreement. Many details of the contract have to be fixed like the method of payment, the method of shipping and many others. All obligations for the supplier as well as the demander have to be mentioned in this contract. In the case all contract partners agree the negotiation phase terminates. During the *execution phase*, both the demander and the supplier have to meet the obligations described and fixed in the contract that they have made in the negotiation phase. The execution phase usually consists of two sub-phases: the payment and the delivery of goods phases. Both strongly depend on the type of the good and on the type of the market where the good is offered.

The different phases of a business transaction are processed in an interactive and iterative way. For example, if two matching partners cannot agree about signing a contract the negotiation phase terminates and the information process starts again. A market in which the three phases are supported by information and communication technology is called an *electronic market*. There also exists a broader definition which says that at least one of the three phases has to be supported by information and communication technology for a market to be an electronic market.

Each business transaction on an electronic market involves special risks that depend on the type of (electronic) media, the good and its value, the type of market and of course on the type of attacks that might occur. As a consequence for each phase of a market transaction certain security considerations are necessary. In an infrastructure for a secure electronic markets we have to cover a whole variety of security risks in all three phases by offering appropriate security services.

2.2Examples of security requirements

During the *information phase* the market participants do have different security demands. When browsing through the Internet a demander has to be sure that an offer he is considering is still valid. Additionally, he must even be sure that the supplier is still in operation under the network address he found the offer. In the case both pre-conditions are valid and in order to reduce the trading risk the demander wants to accept only authenticated offers. But there are also security requirements for the supplier: For example, the supplier may want his offers to be confidential because otherwise the competitors may gain advantages.

The need for security services in the *negotiation phase* is obvious. Most important is the legal binding of contract partners. The contract and its security services must include enough information to find out who is in the right when demander and supplier later disagree. During this phase the probably most important security demands are integrity, authenticity and the legal binding of the contract partners on the content of the contract.

In the case that the *execution phase* is conducted electronically both the electronic payment and the transfer of goods have to be secure. For secure payments several proposals have been made by academics as well as industries. They offer different levels of security and privacy. Secure delivery of digital goods can have many different security demands depending on the type of good that has to be exchanged. For example digital represented shares have to be original but an additional (and often conflicting) requirement is that they have to be anonymous (they do not contain the name or even a pseudonym of their owner) for economic reasons. But there are also security demands in the execution phase that do neither depend on the good nor on the method of payment. For example the fairness problem is evident and not solved by simply making a contract. As an example consider a protocol which assumes delivery of the goods after payment. This is an unfair situation for the demander. The same is true for the supplier if delivery proceeds payment. Additionally the supplier needs a confirmation when he delivers the goods in order to prove that he has met his obligations. The same problem exists with the demander vice versa.

The security of EC is influenced by the different phases of a business transaction, the market participants, the type and value of the digital good, the type of the market (market structure). Because of the diversity of the different security requirements it is necessary to have a clear understanding about all these key factors influencing security and fairness in EC.

3 COPS - An Infrastructure for Secure and Fair EC

In figure 2 we give a graphical model of the underlying market infrastructure of the project COPS (Commercial Protocols and Services). The three levels (I,N,E) show the three phases of the business transactions, while the corner elements are representing the different participants of open markets in an open network. In the following we will discuss the role of each participant in the COPS market model and will show by means of an example how an open electronic market for free trade with original and anonymous emission permits may be realised in COPS.

Within each phase of the business transaction the required *services* for each participant to take part in the market and *protocols* to handle the co-operation between participants are supported.

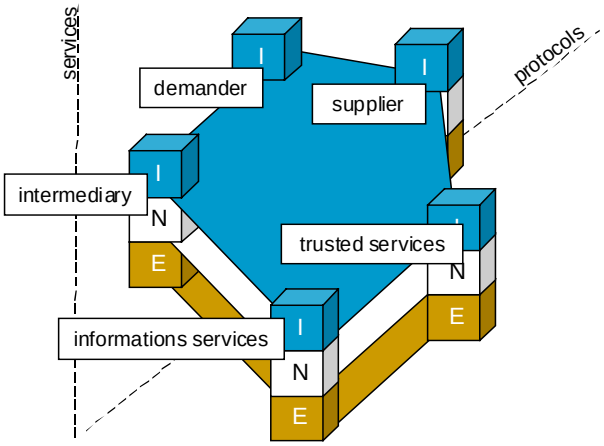


Figure 2: COPS Market Model

Market-based co-ordination can be classified into four categories: direct-search markets (where the future partners directly seek out one another), brokered markets (with the brokers assuming the search function), dealer markets (with the dealers holding inventories against which they buy and sell), and the auction markets [12, 3]. From this classification we derive four electronic market player roles: demander, supplier, electronic intermediary (cybermediary) and trusted third party. Together with the information services five roles of participants are considered in the COPS market model:

- The *demander* is the driving force of a transaction. Only in the information phase it is possible that a supplier offers products. All other phases are initiated by the demander. It is on the demander's side, where an infrastructure has to preserve the open character of an open market. In particular no or less technical or organisational preconditions for a demander to participate should exist. This openness generally includes, that there is no trust relationship between the business partners, which leads to additional security threads [1].
- The *supplier* has the choice to offer her/his goods either on a direct search market, through cybermediaries or on an electronic auction market. The choice will depend on the suppliers preferences, on the type of the good offered and on other strategic considerations.
- An electronic *intermediary* is trading information about products like their prices or quality. He offers product evaluation, quality assurance, or special combinations of products (e.g. travel agency). There are quite different

understandings of electronic intermediaries. All agree, that intermediaries will survive (despite the fact that direct producer buyer relationships are easier) in electronic markets, because they are able to produce an added value to electronic goods [2, 11].

- *Trusted third parties* play an important role in security infrastructures, because they are used for public-key certification. Public-key certification is a necessary requirement to support legal binding of contract partners to the contract. This is practically important for contracting but also for digital goods which often need authenticity, originality and similar properties. For future electronic markets we expect a lot of new tasks for trusted third parties. For example, we believe that the mass of communication can result in an increasing amount of lawsuits, so that traditional courts can not cope with it. Fortunately they don't need to, because in most cases an automatic court of arbitration will be able to judge. This „cyberjudge" is a new role of a trusted authority in the Internet and a legal system has to provide possibilities to appeal against decisions of the cyberjudge. We also propose the use of trusted third parties to realise fair electronic auction markets. In some cases the difference between cybermediary and trusted third party seems to disappear. In our understanding there is a distinguishing mark, that is based on the personal interests and the goals of the party. Consider as an example an anonymous mediated market: To simplify the example we take two parties, S who wants to sell a certain quantity of a good at the price of 100 Euro and D who ordered the same amount and is willing to pay 125 Euro. The intermediary would take the chance to earn 25 Euro. Intermediaries have own interests on the market but trusted third parties are supposed to do something transparent to A and B. For example, simply report the offers or in an exchange market meet all matching demands. Trusted third parties
- *Information services* provide technical information about the market infrastructure and the network. Examples are certificate directories or a special host which processes inquiries like: "What is the network address of a trusted third party issuing secure time stamps?".

Electronic markets reduce the trading immanent transaction costs, which can solve existing allocation problems for example in environmental policy. An example for this is the model of tradable emission permits which is supposed to efficiently and effectively reach given environmental goals. Each permit in this model allows its owner emission of a certain amount of toxins. Permits can be traded freely. When the permit is traded on an electronic market it has to be digitally represented, it must not be possible to forge or to copy it and finally the market should be anonymous.

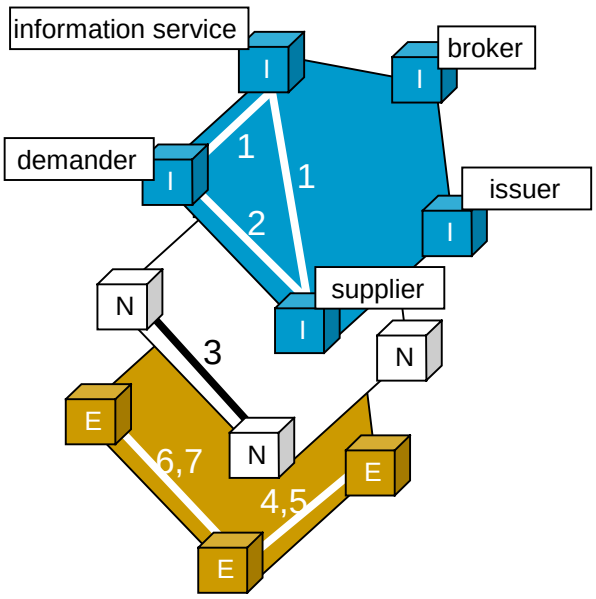


Figure 3: Business Transaction in COPS

In figure 3 we give an example of an open electronic market for free trade with original and anonymous emission permits. The example shows how the market may be realised in COPS and additionally how trusted authorities (in this example the issuer) can be used for guaranteeing originality and anonymity of digital goods. The example is from [9].

The business transaction is carried out in different steps. During the steps marked with 1 the demander and supplier search for each other. In step 2 the demander gets a binding offer from the supplier. This concludes the information phase of the transaction. In step 3, the contract terms are discussed, the contract is completed, and the demander sends a session key which is encrypted by using the public key of the issuer to the supplier. This is necessary for establishing the connection to the emission certificate and for preparing anonymity. The negotiation phase ends and the execution phase starts. During step 4 the supplier sends his original permit together with the encrypted session key to the issuer of the emission certificate. The issuer (trusted authority), deletes the old emission permit, generates a new original and encrypts it with the session key. Then the issuer sends it to the supplier in step 5, who gives it to the demander in step 6, who pays electronically in step 7.

It is important to note that it is only possible to guarantee a certain level of security if special care is given to the communication processes being part of the business transaction. In addition, it is necessary to carefully analyse all application dependent security

semantics that are part of the business transaction. This is where the MOSS project comes into the picture.

4 MOSS: Modelling security semantics of business transactions

Business transactions usually are described by using business process models. A business process is modelled by an executive of the organisation and usually contains the following components: information about organisational units involved in processing the business process (e.g. departments, agents, roles, and machinery), tasks to be performed and their co-operation, informational units and their usage and structure, and behaviour of all the objects involved. The executive responsible for specifying the business process usually is not a security specialist. At a very high level only he has knowledge about requirements like "sensitivity", "legal binding", "high integrity", "copyright", and similar, and will assign the requirements to business process components.

In figure 4 we show by using the MOSS terminology the most important parts of the business transaction of the example introduced above from the viewpoint of the demander. We will not explain the details of the MOSS syntax and semantics because they are self explaining in the example. Additional information may be found in [6].

At the demander different departments and employees acting in different roles are involved in processing the business transaction. The business transaction is initiated in the purchase department and passes each of the three phases of a market transaction. In the graphic representation the following notation is used: The first row represents the departments which are responsible for execution of tasks and the left column represents the agents (roles responsible for) carrying out the tasks. In the information phase, companies are determined which could act as possible suppliers. They are invited to submit offers (task 2). Offers need to be

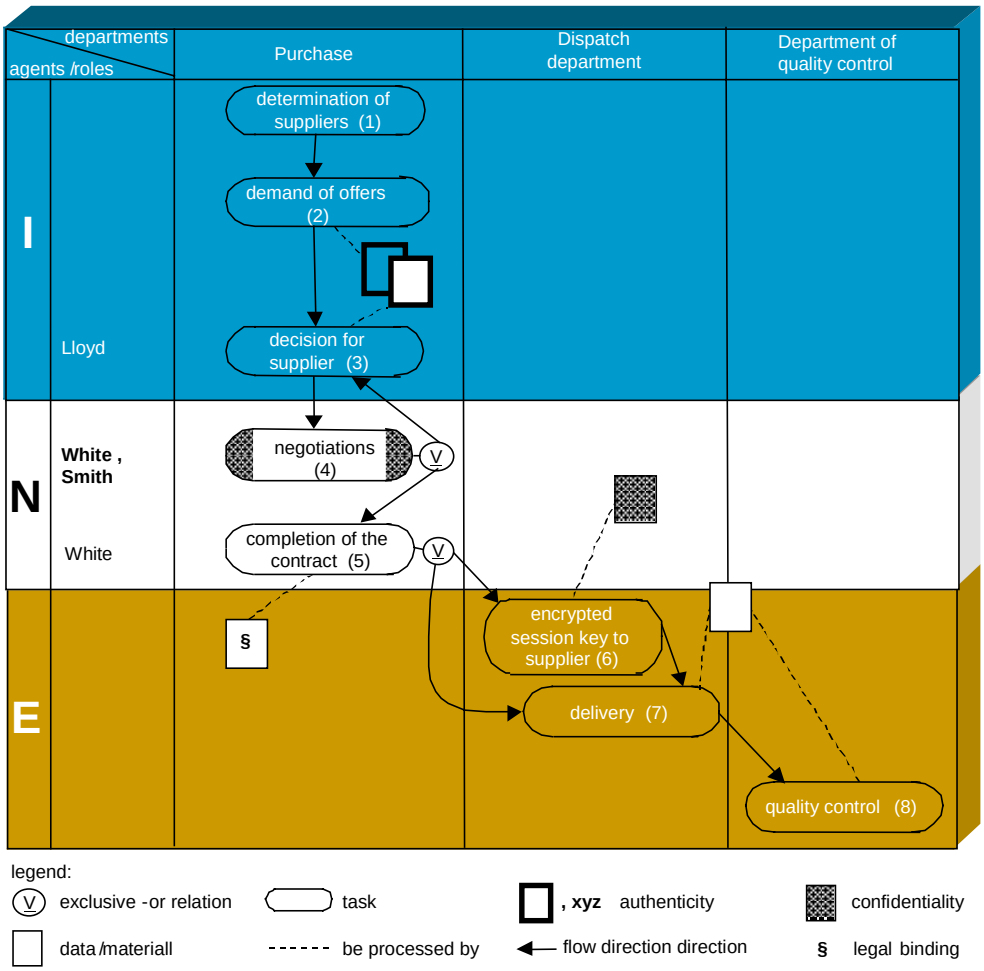


Figure 4: Business process extended by security semantics

valid for a specific period of time and must be *authentic*. Otherwise the decision about who will be chosen as supplier (task 3) is based on uncertain information. During the negotiation phase (task 4) negotiations with the chosen supplier take place which may lead to a completion of the contract (task 5) or to choosing another supplier (task 3). Negotiations may have several security requirements: First, the communication partners must be *authentic*. Second, negotiations are requested to be *confidential*. A completion of contract requires *legal binding* of both contract partners on the contract. During the execution phase the session key encrypted by using the public key of the issuer must be delivered to the supplier (task 6). To avoid competition disadvantages in the case of leaking out information, *secrecy* is demanded here. After the emission permits are delivered (task 7, waiting for delivery) a quality control (task 8) takes place. In this simple example of a market situation the demander at least has the following security requirements: authenticity, legal binding, and confidentiality (secrecy).

To realise a business transaction and its security requirements a more detailed analysis is recommended in MOSS. A detailed analysis is necessary because of two reasons: First, the executive responsible for specifying the business process usually is not a security expert. His understanding of the security semantics may be very vague and on an abstract level only. Second, a business process is not an isolated activity within an enterprise and there are interferences with databases, processing units, people involved, and others. Typically, for these components already models exist (i.e. data model). A security requirement in the business transaction must be supported by corresponding security constraints in related systems. Otherwise, these systems may be used by an attacker in order to gain information about the business transaction and a security hole exists.

5 Perspectives of business processes

In order to arrive at a complete understanding of the security requirements the MOSS business process model suggests to view a business transaction from at least five different perspectives (see figure 5).

- The *informational perspective* represents the information entities, their structuring and relationships between them. A common methodology for analysing and modelling the informational perspective is to use the Entity-Relationship approach [4].
- The *functional perspective* shows what activities (processes) are performed and which data flow occurs between activities. The functional perspective only represents the flow of data within the system. It may be modelled by using data flow diagrams [5].
- The *dynamical perspective* represents for each information entity all possible states and state transitions which may occur within the life cycle of the information entity. There are many different techniques available to model system dynamics. A common technique are state transition diagrams as used in OMT [8] and its successor UML.
- The *organisational perspective* shows where and by whom activities are performed. This perspective corresponds to the organigram of an organisation and to role models.
- The *business process perspective* represents the flow of work in terms of activities and information flow from the viewpoint of the whole business process. It consists of an integration of the functional and dynamic perspectives and references the informational and organisational perspectives. In MOSS it is modelled by using the method shown in the example given in figure 4.

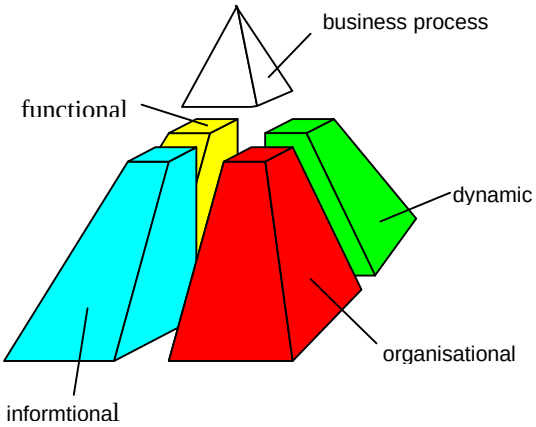


Figure 5: MOSS business process perspectives

In general, any requirement on business processes is represented in different perspectives with varying consequences. Consider a requirement "time dependency" of task execution (for example, task *a* should always be carried out before task *b*) which strongly influences functional and dynamic perspectives, does less influence the organisational perspective but does not influence the informational perspective of a business process at all. This is in contrast to requirements referring to security of business processes. They are more complicate to handle because they influence all perspectives of a business process at the same level of importance. In the case we have a security hole in one perspective the security of the whole business transaction

is in danger.

In the following we focus on our example again and analyse the different perspectives of contract completion and the security requirement “legal binding” of the contract partners (task 4 in fig. 5). In the examples we use the following notation: Components of existing models or attributes which are not effected by security requirements are written using standard characters. The attributes with relevance to legal binding are given in bold face.

To guarantee legal binding of contract partners on a contract different regulations are required according to corresponding law. In many countries a document is legal binding if the agreement between the contract partners is provable. For provability a common method is the usage of signatures. If the contract is a traditional document (by paper) a way to realise legal binding of the contract is to have it signed by the contract partners. In business transactions on electronic markets a (electronic) document should be signed digitally. The following is based on the IuKDG [7], the German bill for digital signatures. This bill requests the following for legal binding of a digital signature: A digital signature is a seal based on the signed data. The seal is realised by asymmetric cryptography and is created by using the private key of the signatory. It is possible to ascertain the correctness of signed data and the identity of the signatory by using its public key which must be certified by a certification authority. Each certificate is assigned with a period of validity. Which cryptographic algorithms and which certification infrastructure should be used is not included in the bill because of possible future developments which could influence security of digital signatures.

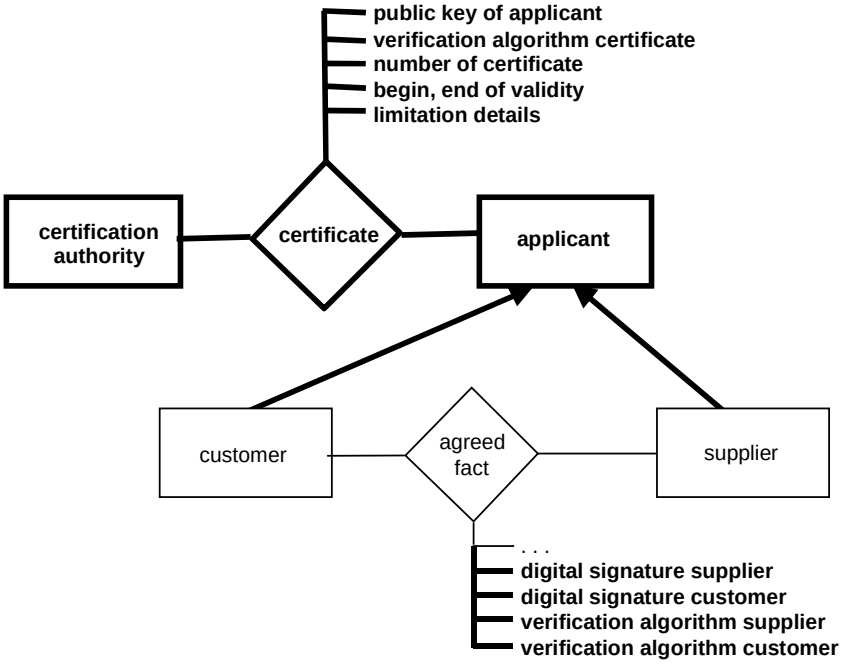


Figure 6: Informational perspective extended by security semantics.

5.1 Legal binding - informational perspective

In order to study what effects a digital signature has, we will first refer to the informational perspective of the business process of our example. As contracting information is usually stored in a database we assume the existence of a data model at the demander covering the demander-supplier relationship. According to IuKDG to sign an electronic document, the seal of each signatory and the corresponding certificates are necessary. In order to process the business transaction on an electronic market and to establish legal binding, the informational perspective of the business process must be extended by information about the signatories, the certificates used, and the (trusted) parties responsible for issuing the certificates. In figure 6 we have extended the customer-supplier-relationship of our example by appropriate data structures necessary for supporting legal binding. In particular these are: a new relationship type CERTIFICATE and modification of the existing relationship type representing the contract. The agreed fact is represented by a document which should be signed

and the relationship type between customer and supplier must be extended by one field for the seal (digital signature) of each signatory and by information about what algorithm was used for signing. In addition, are necessary to guarantee the provability of digital signed contracts. These actions lead e. g. to extensions of the functional perspective of a process responsible for archiving. Again, in figure 7 necessary extensions due to

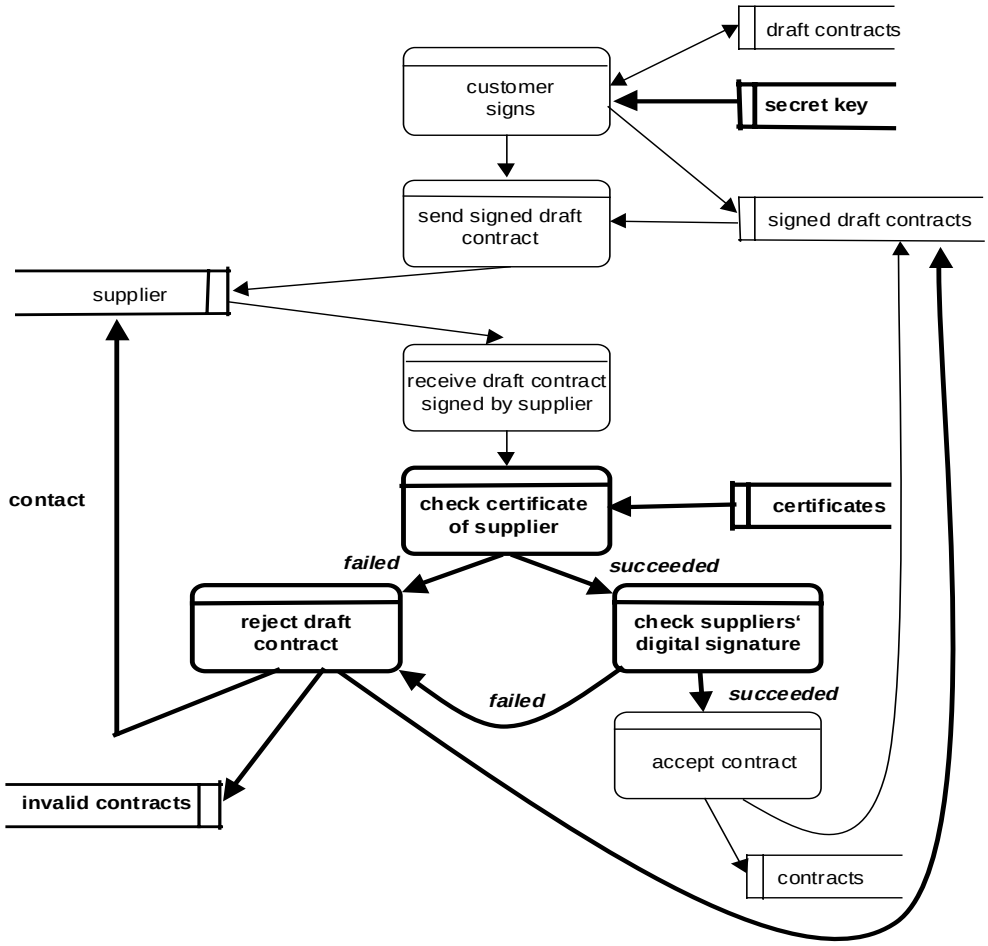


Figure 7: Functional perspective extended by security semantics

customer and supplier are specializations of a generic type applicant which must have a certificate relating the applicant to a certification authority.

5.2 Legal binding - functional perspective

During the process of completing a contract certain information flow takes place. The flow involved in the business transaction can be analysed in the functional perspective of the business process. To guarantee legal binding of the contract the functional perspective of the business process must be modified as follows (see figure 7): The document must be signed digitally by each contract partner and the signatures must be verified. Because a certificate of a public key may be expired (by time or by declaration of invalidity) additional actions security requirements in a functional model are given in bold face.

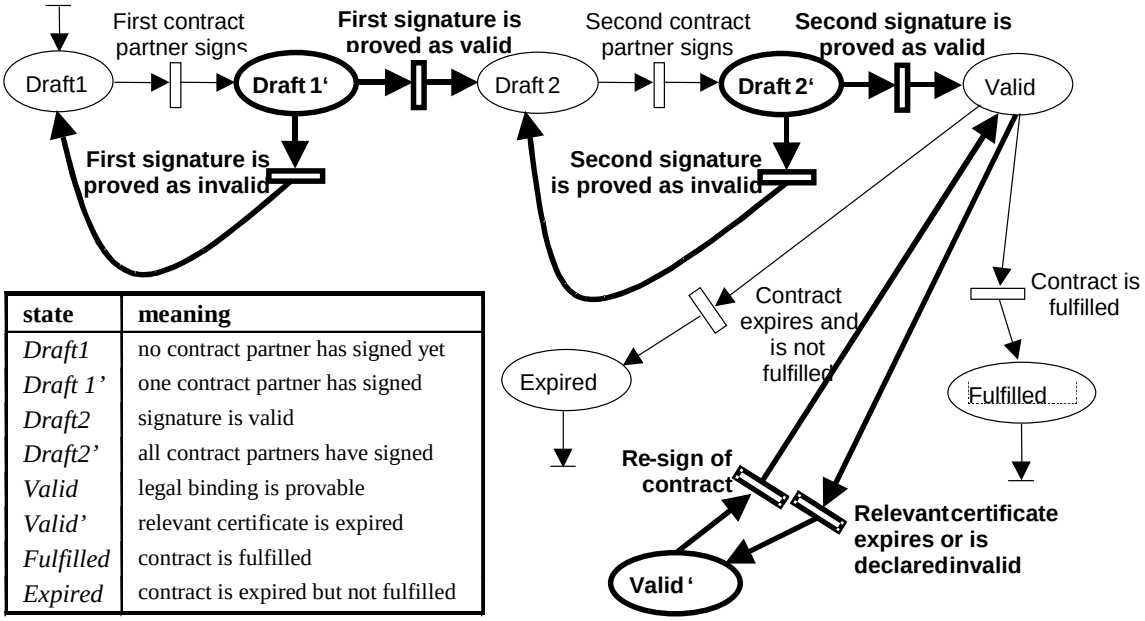
5.3 Legal binding - organizational perspective

Introducing legal binding to the business process has impacts to the organisational perspective, too. To check the validity of digital signatures and to initiate further actions, a new role in the organisation is necessary and leads to an extension of the organisational perspective. The additional role may be called SIG-MGR and is responsible for re-signing documents in case of certificates are no longer valid and for the verification of signatures. Additional roles may be necessary for key management. The role SIG-MGR may need the following authorisations: access to relevant certificates,

right to re-sign contracts when the corresponding certificate of the own enterprise is expired or is declared invalid, right to ask a contract partner for re-signing a contract in the case contract partner's relevant certificate is expired or declared invalid. A role responsible for signing contracts may already exist in organisations having the authority of signing contracts in the traditional way. Such a role is necessary when introducing digital signatures too but needs to be extended by a new privileges to access relevant certificates.

One reason may be the following: If signatory party A signs and gives the document to contract partner B (which has no time restriction for the signing process) B will be able to look for a more favourable offer while delaying the signing process but A already feels bounded by his/her signature. These time restrictions may be one variation of the semantic meaning of a digital signature. To cover this aspect the business process model of our example must be extended.

Unfortunately, security requirements of a business



state	meaning
Draft1	no contract partner has signed yet
Draft 1'	one contract partner has signed
Draft2	signature is valid
Draft2'	all contract partners have signed
Valid	legal binding is provable
Valid'	relevant certificate is expired
Fulfilled	contract is fulfilled
Expired	contract is expired but not fulfilled

Figure 8: Dynamic perspective extended by security semantics

5.4 Legal binding - dynamic perspective

Similar to the other perspectives the legal binding on a contract has impacts on the dynamic perspective as well. In figure 8 we show the life cycle of entity type CONTRACT in terms of its different states. From a security point of view the state Valid' is important to note. It represents an object of type contract which is valid (i.e. signed) but the certificate of the signature is expired. This means we have the situation that a contract is valid but no longer provable. Each contract in this state must be re-signed.

It is important to note that the different semantics of digital signatures are not always clear and as discussed above the signing process is not always fair. In our example a signatory party (the demander) may demand the signing of the corresponding document by the contract partner (the supplier) within a specific period of time. For this requirement different reasons may exist. transaction have effects on different perspectives of a business process. The example showed that legal binding as needed on electronic markets influences all perspectives of the business process. In MOSS we propose extensions to existing models which seem to be quite complex for the non security expert. However, the outlined extensions are identical for legal binding of a document in any business process requiring this functionality in identical legal environments. Therefore, these extensions may be reused.

6 Conclusion

Building secure and fair relationships in open electronic commerce requires the combination of several elements to address commercial, legal, and security concerns. In this paper we investigated this issue by firstly introducing COPS, an electronic commerce infrastructure, and secondly MOSS, a modelling

environment for analyzing security semantics of business transactions.

COPS has its main focus on security and fairness, includes five different roles of market participants, supports all phases of a market transaction, and can be used to build markets with different structures. MOSS can be used to analyse the security semantics of business transactions. It supports different views on a business transaction in order to arrive at a comprehensive picture of the security requirement. Both projects are currently implemented as academic prototypes. COPS is based on a layered architecture [10]. So far we have extended a commercially available cryptographic library by a security abstraction layer, have implemented a public key directory for market participants, and are working on the implementation of a certification server. For MOSS we are currently building a graphical editor which supports the specification of the business process perspective and some syntactical and semantical parsing of the security constraints specified.

7 References

[1] Bons, R. W. H.: Designing Trustworthy Trade Procedures for Open Electronic Commerce. PhD-Series in General Management 27; Rotterdam School of Management; (1997).

[2] Buxmann, P; König, W.; Rose, F.: An Electronic Market for Java SoftwareElements. Proceedings of ECIS 97; (1997). http://java.wiwi.uni-frankfurt.de/papers/jr_ecis97.html (last accessed 8/1997

[3] Clemons, E.K.; Croson, D.C.; and Weber, B.W.: Reengineering money: the Mondex stored value card and beyond. International Journal of Electronic Commerce (1997). http://www.cba.bgsu.edu/ijec/ (last accessed 8/1997)

[4] Chen, P. P.: The Entity Relationship Model: Towards a Unified View of Data. ACM Trans. On Database Systems (TODS), Vol. 1, No. 1, 1976.

[5] Gane, C. P.; Sarson, T.: Structured System Analysis: Tools and Techniques. Prentice Hall, Englewood Cliffs, NJ, 1979.

[6] Herrmann, G.; Pernul, G.: Viewing business process security from different perspectives. Proceedings of 11th International Bled Electronic Commerce Conference, 1998.

[7] Informations- und Kommunikationsdienste-Gesetz - IuKDG (version from 7/13/1997).

[8] Rumbaugh, J.; Blaha, M.; Premerlani, W.; Eddy, F.; Lorensen, W.: Object-Oriented Modeling and Design. Prentice Hall, Englewood Cliffs, NJ, 1991.

[9] Röhm, A. W., Gerhard, M.: A Secure Electronic Market for Anonymous Transferable Emission Permits. In: Proceedings of Thirty-First Hawaii International Conference on System Sciences HICSS-31; (1998). http://www.wi-inf.uni-essen.de/~ifs/publ_97.html (last accessed 9/1997)

[10] Pernul, G., Röhm, A. W.: COPS: A Model and Infrastructure for Secure and Fair Electronic Markets. To appear: Proc. of Thirty-Second Hawaii International Conference on System Sciences HICSS-32; (1999).

[11] Sarkar, M.B.; Butler, B.; and Steinfield, C.: Intermediaries and cybermediaries: a continuing role for mediating players in the electronic marketplace. Journal of Computer-Mediated Communication, 1, 3, (1995). http://www.usc.edu/dept/annenberg/vol1 /issue3/vol1no3.html (last accessed 8/1997)

[12] Zwass, V.: Electronic Commerce: Structures and Issues. International Journal of Electronic Commerce; Vol. 1; No. 1; M.E. Sharp; 1996.