2000

Supporting Market Transaction through XML Contracting Containers

Markus Greunz
University of St. Gallen, markus.greunz@unisg.ch

Bernd Schopp
University of St. Gallen, bernd.schopp@unisg.ch

Katarina Stanoevska-Slabeva
University of St. Gallen, katarina.stanoevska@unisg.ch

Supporting Market Transaction through XML Contracting Containers

Markus Greunz
Media and Communications Management Institute, University of St. Gallen, markus.greunz@unisg.ch

Bernd Schopp
Media and Communications Management Institute, University of St. Gallen, bernd.schopp@unisg.ch

Katarina Stanoevska-Slabeva
Media and Communications Management Institute, University of St. Gallen, katarina.stanoevska@unisg.ch

Abstract

Based on a Business Media Framework (BMF), this paper proposes an architecture for secure electronic contracts, which adhere to legal requirements and can be applied for an integrated management of market transactions. We propose the use of XML, digital signatures, and Java technology for secure electronic contracting. The resulting contract container can be applied for the support of an integrated information flow through the different services of an electronic market. In addition the container holds a control logic, that supports the management of the contract negotiation and the contract settlement. The concept provided in this paper was developed in the Secure Electronic Contracts (SeCo) project of the =mcm*institute of the University of St. Gallen and the University of Zurich, Switzerland, in cooperation with several business partners.*

1 Introduction

The utilization of electronic media, their ubiquity and their virtuality enable totally new and innovative forms of doing business. Electronic Commerce allows the design of new products and services, supports the evolution of new forms of organizations, brings up unprecedented coordination mechanisms, reorganizes value chains, and facilitates the emergence of value webs. Although a lot of research has been done in the field of Electronic Product Catalogs (Schmid and Linke, 1998), Payment-Systems (Abad-Peiro et al., 1998), Logistics Services, or systems to provide a better security infrastructure (Lacoste, 1997; Herrmann and Günther, 1998), the contracting phase of a business transaction is still lacking a common understanding for the problem and the way an optimal solution should look like.

Development of solutions for the contracting phase calls for an integrated approach considering legal requirements on contracts, the negotiation and contracting process as well as the contract fulfillment processes. But, aside from the legal issues (Pushkar et al., 1997) most of the research is dedicated to single aspects of online contracting. It focuses either on the negotiation (O.N., 2000) process or on the contract fulfillment process (Lee, 1998). The only existing project with a broad perspective (Boger et al., 1999; Boger et al., 1999) misses the contract fulfillment aspect

Based on a *Business Media Framework (BMF*) this paper suggests: 1) an architecture for a container for secure electronic contracts considering all relevant aspects of contracting and 2) a contracting framework that gives an overview over the services and roles that have to be fulfilled in order to provide legal validity of the contract. Finally, the implementation of a container architecture for a secure electronic contract will be presented.

The concept provided in this paper was developed in the Secure Electronic Contracts (SeCo) project of the =mcm*institute* of the University of St. Gallen and the University of Zurich, Switzerland, in cooperation with several business partners (Gisler et al., 1999).

2 Contracting in Electronic Markets

In this chapter, we provide the framework for the research methodology in the project and the basic assumptions that lead us to the container architecture of electronic contracts.

2.1 The Business Media Reference Model

We define media as information and communication spaces, which based on innovative information and communication technology (ICT) support content creation, management and exchange within a community consisting of human and artificial agents (Schmid and Lechner, 2000). We are particularly interested in business media as one specific type of media. Business media are defined as information spaces that provide services necessary for online exchange of goods and values among members of a business community of agents.

The components of business media as well as their implementation are structured by the business media reference model. The Business Media Framework distinguishes according to (Schmid, 1999) four layers or views and four action types or basic services. The layers denote different stages in the design and implementation of a medium and the basic services refer to generic modes of interaction. Following the views and services will be described briefly. For a more detailed description, refer to

(Lindemann and Schmid, 1998; Lechner and Schmid, 2000).

(1) *Community View*. On this layer, the potentially interested business community is described and structured. Therefore, in a first step the relevant business community and its organizational structure has to be identified.

(2) *Implementation View*. On this layer, the roles, protocols, and processes which have been identified in the Community View above are implemented based on the underlying generic services of the Transaction View.

(3) *Transaction View*. This layer contains the generic market services that can be seen as independent from the higher layers. Generic market services are services that are necessary to complete a Customer Buying Cycle (CBC).

(4) *Infrastructure View*. This layer contains communication, transaction, and transportation infrastructure and interfaces that provide access to this infrastructure. It basically serves as the facilitator for the implementation of the generic market services.

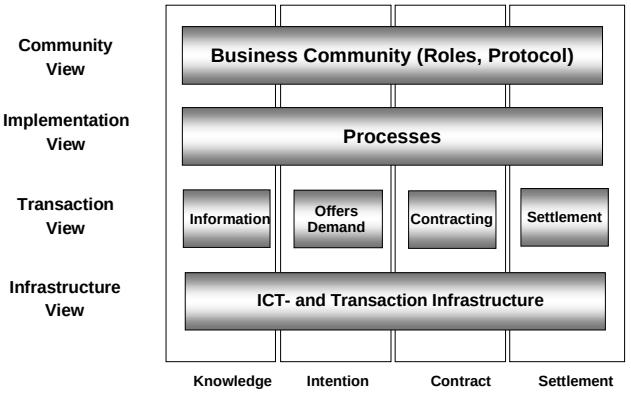

Figure 1. The Business Media Framework (Schmid, 1999)

The basic services have to provide generic modes of interaction for the fulfillment of the different stages of a Customer Buying Cycle. The following phases can be identified:

(1) In the *Knowledge Phase* information about the offered products, the supplier and selling conditions is provided. Access to the information is enabled by information and product catalogs and different search engines.

(2) In the *Intention Phase*, agents signal their intentions, derived from the knowledge in the knowledge phase, and from their desires and goals. Offer, counter offer and demand are the prevailing form of expressed intentions in business media. Services like electronic product catalogs (EPC) support this transaction phase. They provide an initial offer from the supplier and can be applied by the buyer for the formulation of counteroffers.

(3) In the *Contracting Phase*, the agents negotiate contracts starting from the initial offers presented in the EPC. In case of business media selling contracts are negotiated. The result of this phase is a legally binding contract which documents the agreed upon obligations of supplier and buyer in terms of traded products, prices, delivery and payment conditions

(4) In the *Settlement Phase*, agents act according to the negotiated contract, using services offered for this purpose. In commerce this means, e.g. logistics and payment services.

2.2 Implications for Electronic Contracts

The Business Media Reference Model as a design framework for business media reveals the position of contracting and its interfaces to other services. Contracting is the bridge between non-obligatory intentions and legally binding obligations and their fulfillment. Thus, it has to consider legal aspects in order to assure validity and to provide interfaces to the other market phases. The resulting contracts draw from the information provided in the knowledge and intention phase by EPCs, document the negotiation process and provide information for contract fulfillment activities.

Therefore, the information represented in EPCs could be used as a structured input for the negotiation process and contracts (Gisler et al., 1999). *Logistics Services can* use parts of the contract information as input parameters for the processes they provide. *Payment Services* can similar to logistic services use the information provided by contracts.

Contracts can therefore provide on the one hand legally binding agreements between seller and buyer and on the other hand serve as a file middleware integrating the market services. In order to achieve such contracts, the architecture of the contracting services has to provide the following components:

- the support of an integrated information flow (workflow components);
- the collection of all legally relevant information (document management components);
- the interfaces towards the market services to exchange the contracting information (communication components);
- secure communication between all agents involved in a market transaction (security components).

In the next section we will present the concept of a contract container and contracting services, which meet the above requirements.

3 The Contracting Container and Contracting Services

3.1 The SeCo Container Architecture

The above requirements and implications for electronic contracts lead us to a container architecture

with the components logic, information, and communication layer.

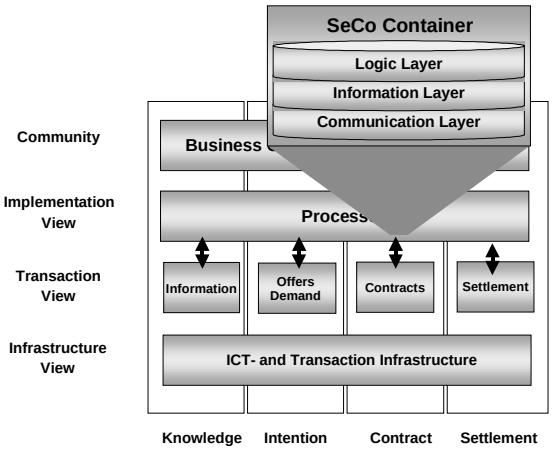

Figure 2. The Contracting Container Architecture

3.1.1 The Logic Layer

On the logic layer, the workflow logic of the business transaction is designed, managed, and performed. E.g.: The logic layer can manage the monitoring of the contracting process through checking critical dates and values, and through performing actions like reminding the outstanding signing of the contract or the non-performing of the delivery. The logic layer can be implemented either as mobile code that runs on the client side or as a market service that runs on the server side. Important is logic layer's secure access to the information structured on the information layer.

If the process logic is provided by the generic market services, the internal state of the container is changed with every communication act. If there is a more sophisticated process logic represented within the contracting container, each internal operation invokes a change of the internal state.

3.1.2 The Information Layer

The information layer provides data storage and contains the contract information. The data of the information layer contains a structured and an unstructured part. In the structured part, all the information is stored that is subject to further processing in the contracting or settlement phase. The structured part itself is divided into the following four blocks:

(1) *Who* Block: Who is involved in the business transaction. In this Block the involved parties are described.

(2) *What* Block: What product or service is the object of the contract. This information is usually imported from the product catalog.

(3) *Condition* Block: What are the settlement conditions of the transactions. This includes usually the payment and delivery conditions, which are again available in the EPC.

(4) *Legal* Block: Under what legal circumstances came the parties to a mutual agreement. This covers e.g. the legal terms of the agreement as well as the arbitration code.

In the unstructured part of the information layer, documents could be added that are collected throughout a market transaction. This will allow the parties to insert all the information that is legally relevant but not provided in a special format. E.g.: Delivery receipts are usually provided as regular e-mails. These documents will be attached to the contracting container and treated like a regular part of the information layer.

In a negotiation process, data will be changed until the state of the container indicates a legally binding contract. For the information layer of the contracting container we use a set of documents with changeable and non-changeable sections. In order to have a document history we propose to generate a new document for each step of the contracting process. This new document inherits certain attributes either from the container settings or from already existing documents.

3.1.3 The Communication Layer

The communication layer includes all protocols necessary for the communication with the generic market services and the contracting parties. Assuming established standard communication protocols for all generic market services, the contracting parties and the contracting container have to apply these protocols in order to initiate communication with the services.

The communication layer also includes the communication security for the message passing. Using this design, data of the information layer cannot be changed without having the proper authentication, which is checked by the communication layer. This authentication check requires to archive information on contracting parties, such as their individual access rights and their identification. The identification of contracting parties can be accomplished through the use of Public Key Infrastructure (PKI).

3.2 Contracting Services

Within a *Contracting Domain* all agents interact in a legally enforceable contracting environment in order to achieve an agreement, to enforce the performance, and, in case of non-compliance, to arbitrate contract disputes. By Contracting Domain we refer to the legal environment (e.g. Schweizer Obligationen Recht, OR; Handels-

gesetzbuch , HGB) in which contracting processes take part.

Milosevic (Milosevic, 1995) suggests a number of services necessary to enable two parties to come to a mandatory agreement and to settle the obligations.

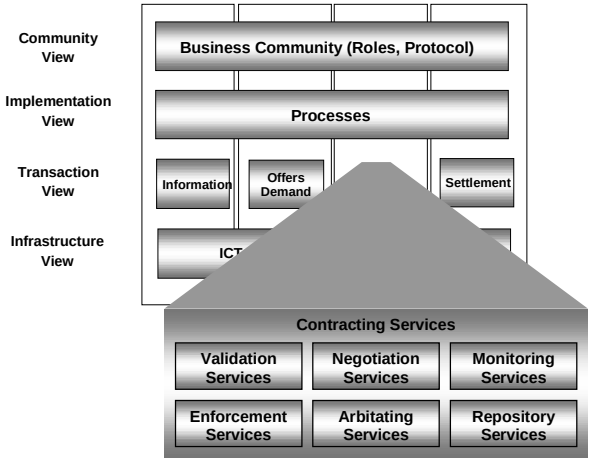

Figure 3. Generic Market Services within the contracting phase of the Business Media Framework

The *Validation Service (VS)* supports the process of ensuring that a contract satisfies certain contract validity rules of the nominated contract domain. E.g.: It has to be checked whether there are items in the contract which are not in accordance with existing export laws or which would not be accepted by the contracting parties.

Negotiation Service (NS) supports a multi-step process in which parties with conflicting interests come to a mutual assent regarding the terms and conditions of the contract. Based on predefined contract templates, negotiation can be regarded as the refinement of a contract template into a mutually agreed contract.

The *Monitoring Service (MS)* deals with the process of observing activities and furthermore measures the performance of parties that are determined by a contract, with the aim of ensuring that those activities correspond to the contract. In the case of non-performance, the Monitoring Service will have to inform the enforcement service to initiate an enforcement activity.

The *Enforcement Service (ES)* supports the process of indicating that the contract has not been honored by another party and performs the resulting corrective action. The ES can be divided into two sorts of actions:

- *Proactive enforcement* including all actions that can be enforced within the current market transaction;
- *Reactive enforcement* including all actions that protect market members from future non-performance (e.g. black lists, ranking).

The *Arbitrating Service (AS)* helps in settling a dispute between the contracting partners within the electronic business medium. The AS requires the specification of the arbitrating court in the arbitration clause of the contract.

The *Repository Service (RS)* provides contracting domain wide information that is mainly used by the Validation Service but also contributes information services to all contracting parties.

All these services must have well-defined interfaces on which the actual processes could be implemented. A requirement to support an entire market transaction in an open environment is the access to all generic services of different market phases through standardized interfaces.

4 The SeCo Container Implementation

As has been mentioned above, the SeCo Container can be seen as an information object that contains all information that is important to describe the workflow logic necessary for contract fulfillment (logic layer), all data that describes the terms that have been agreed upon between the contracting parties (information layer) as well as all information about needed communication protocols (communication layer). In order to make this data accessible to the various services within the contracting phase as well as in other phases of a market transaction, it is necessary to structure it in a way that allows to codify the semantics of the data in the same document.

4.1 The Container Structure

For structuring the data of the SeCo Container XML (Bray et al., 1999) was chosen as a suitable format. This allows the individual contracting services (i.e. contract monitoring) to easily access data in the container, and, at the same time, supports the openness to services other than contracting. A Data Type Definition (DTD) defines a document template for the container which specifies not only the data structure but can also be used to express the semantics of the SeCo Container elements. Figure 4 shows the basic structure of the SeCo Container.

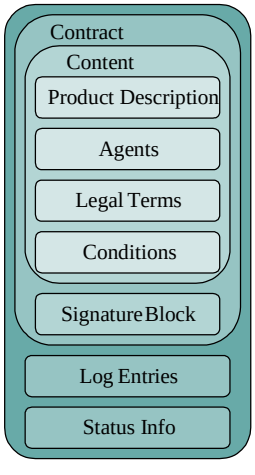

Figure 4. Basic Structure of the SeCo Container

For each market transaction that covers all transaction phases from the first offer until the fulfillment of the agreed upon liabilities, a new SeCo Container is created according to the structure defined by the DTD. A SeCo Container contains at least one *contract section* that, in turn, can be divided into a content section and a signature block.

The *content section* contains all data that is relevant for the contract and that the contracting parties have to agree on. Therefore, this section represents the structured part of the information layer. It includes

- the product or service descriptions with agreed upon quality or specifications of all products and services the customer intends to purchase;
- the identification and address data of the contracting parties (mandatory), as well as other involved market agents such as an arbitrator, a recipient other than the customer, or a notary (optional);
- the delivery and payment conditions together with the communication protocols applied in the integration of payment and logistics services (i.e. SET);
- the legal terms of the contract as well as the arbitration code.

This data is represented at a very fine grained level in XML. In order to facilitate the interoperation with other transaction services (E.g.:. payment services), parts of the contracting container DTD comply with the Internet Open Trading Protocol (IOTP) (Burdett, 1999). DTD.

Since the information stored in a SeCo Container describes the rights and obligations of the contracting parties, it is desirable that the contract is protected against unauthorized manipulation. Therefore each contract section has a *signature block* which holds the digital signatures signing the content section. Furthermore, the signature block contains the corresponding X509 certificates (Solo et al., 2000) that hold the public keys of the signers. Thus, the contract section of a SeCo Container includes all data that is necessary to authenticate the contracting parties and to guarantee the non-repudiation of origin of the content. Authentication is provided by a certification authority which therefore implements part of the Repository Service RS.

Supporting the contract negotiation, each container can hold more than one contract section, which allows tracking of the historical evolution of the contract. However, at any given time, there is only one valid contract section, that can be distinguished by a time stamp. The most recent contract section represents the current state of the contracting process.

In order to support the contracting process, a SeCo Container holds two more sections:

A *log section* logs the events that occur during the contracting process, as well as any relevant information that arises during the fulfillment of the contract. The information of the log section primarily supports the monitoring service. It allows to trigger events according to the current state of the contract. These events could start services in the contracting phase or of services in other phases of the market transaction, e.g.. the start of the payment process after the shipment. In addition, a log entry may also contain related documents (e.g. a receipt) that can be integrated into the SeCo Container either by reference or by directly embedding the data into the container by means of BASE64 encoding (Borenstein and Freed, 1993). Such entries represent the unstructured part of the information layer as it is mentioned in Sect. 3.1.2.

Finally, there is a *status section* that holds information about the current state of the SeCo Container. It can be used as a quick reference for queries for the status of a contract and may also answer queries for the payment and the delivery status if the applied payment and delivery protocols support exchange of status information. The log and the status section contain data representing the logic layer, and, therefore, support horizontal integration by providing process information needed for contract monitoring.

The above described document structure for the SeCo Container implements all parts of the SeCo Architecture as it is proposed in chapter 3 of this paper. In order to validate the applicability of the XML SeCo Container, a prototype has been built that implements a subset of the contracting services.

4.2 Implementation Status

The prototypical implementation fully implements the proposed SeCo DTD. The software architecture is based on a classical three-tier architecture using a Java applet as client, servlets to implement the contracting services and an XML-Server back-end. Contracting services implemented so far include the Validation Service that enables the verification of the content section of the container. The verification is based on the digital signatures as well as on the authentication of the contracting parties who signed the content by means of embedded X509 certificates. Furthermore the Negotiation Service is fully implemented allowing any number of negotiation steps during which parts of the content section can be altered by the contracting parties. The Monitoring Service currently only supports the monitoring of the negotiation process by a simple merchant interface that provides information about the current negotiation status of the single customer. In addition a simple e-mail notification service supports asynchronous negotiation. The Enforcement Service and the Arbitrating Service (AS) are currently not implemented, although the PKI applied in the prototype can be seen as proactive enforcement in a sense that offers made cannot be repudiated by any party. This may also aid the AS. The Repository Service is not implemented, though part of this service is provided by Certification Authorities (CA) that can be used by the prototype for the authentication of contracting parties.

In order to provide horizontal integration between the contracting phase and other phases of the market transaction, Java interfaces have been specified that enable the integration of Electronic Product Catalogs (EPC). This allows the Contracting Service to offer its service to any existing EPC. Interoperability with the payment and logistics services of the settlement phase is not implemented by the prototype and should be part of future research efforts.

5 Summary and Outlook

In this paper, we have developed a container architecture for electronic contracting, which meets the requirements identified in the analysis of open electronic markets. These requirements are the integrated information flow, the document collection function, the generic interfaces for market services, and the secure communication between the agents. The container is implemented in XML. All layers of the container architecture discussed in this paper are represented in the XML structure.

Future research focuses on the following issues:

(1) Implementing the services not covered by the current prototype;

(2) Defining generic open interfaces for the market services in order to facilitate the horizontal integration;

(3) Enhancing the container structure towards a recursive contract structure that allows to build hierarchies of contracts.

Acknowledgements

The authors would like to thank the partner institute and companies of the Secure Electronic Contracts Project for supporting the underlying research of this paper. The project was funded by the Swiss National Fund (SNF).

Literature

Abad-Peiro, J.L., Asokan, N., Steiner, M. and Waidner, M. (1998) Designing a Generic Payment Service. IBM Systems Journal [ISY] 37 (1), 1998.

Asokan, N., Schunter, M., and Waidner, M. (1997): Optimistic Protocols for Fair Exchange. 4th ACM Conference on Computer and Communications Security , 1997.

Boger, M.; Giffel, Frank; Merz, Michael; Lamersdorf, Winfried; Weinreich, H. (1999): Electronic Contracting im Internet. In: Kommunikation in Verteilten Systemen (KiVS), Berlin, Heidelberg, New York: Springer-Verlag, p. 314 - 325, 1999.

Borenstein, N., and Freed, N., "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Bellcore, Innosoft, September, 1993.

Bray, T., Paoli, J., Sperberg-McQueen, C. M. (Eds.): Extensible Markup Language (XML) 1.0; http://www.w3.org/TR/REC-xml, visited: Dec. 1999.

Burdett, D., Commerce One: Internet Open Trading Protocol – IOTP, Version 1.0; Internet Engineering Task Force (IETF) Internet Draft, [URL: http://www.ietf.org/internet-drafts/draft-ietf-trade-iotp-v1.0-protocol-07.txt], visited: Jan. 2000.

Gisler, M., Häuschen, H., Jöhri, Y., Meier, A., Müller, O. and Stanoevska, K., Schopp, B. (1999) Requirements on Secure Electronic Contracts. Work Report mcm-institute-1999-01, 1999.

Herrmann, Gaby; Pernul, Günther (1998): Viewing Business Process Security from Different Perspectives. In: International Bled Electronic Commerce Conference, Bled, Slovenia: p. 74 - 89, 1998.

Hoffmann, C.P. and Lindemann, M.A. (1998) Logistik und Electronic Commerce - LogEC. St. Gallen: MCM Institute - University of St. Gallen.

Lacoste, G. (1997) SEMPER: A Security Framework for the Global Electronic Marketplace. IIR London.

Lechner, Ulrike; Schmid, Beat F. (2000): Communities and Media - Towards a Reconstruction of Communities on Media. In: Sprague, E.: Hawaiian Int. Conf. on System Sciences (HICSS 2000), IEEE Computer Society Press, 2000.

Lee, Ronald M. (1998): Towards Open Electronic Contracting. In: Schmid; Beat F.; Selz; Dorian: International Journal of Electronic Markets, St. Gallen: vdf Hochschulverlag, p. 3 - 8, 1998.

Milosevic, Zoran; Berry, Andrew; Bond, Andy; Raymond, Kerry (1995): An Architecture for Supporting Business Contracts in Open Distributed Systems. In: International Workshop on Services in Distributed and Networked Environments, Whistler, Canada: 1995.

O.N. (2000): Multi-Agent Market Architecture for Automated Contracting and Electronic Commerce. In: Internet, 2000. [URL: http://maya.cs.depaul.edu/~mobasher/Research-03.html], visited: Jan. 2000.

Pushkar, Raymond S.E.; Graham, Ian T.; Closser, Arleigh V. (1997): Electronic Commerce & Contracting: The Legal Implications. In: Contract Management, Highway: p. 12 - 20, 1997.

Schmid, B.F. and Lincke, D.-M. (1998) Mediating Electronic Product Catalogs. Communications of the ACM 41 (7), 1998.

Schmid, B. F. (1997): The Concept of Media; In: Workshop on Electronic Markets, ed. R. W. H. Bons, 1997.

Schmid, B. (1999): Elektronische Maerkte – Merkmale, Organisation und Potentiale, In: A. Hermanns, M. Sauter (Eds.): Management-Handbuch Electronic Commerce: Grundlagen, Strategien, Praxisbeispiele, Munich: Vahlen, 1999, pp. 491.

Schopp, Bernd; Stanoevska-Slabeva, Katarina ; Runge, Alexander (1999): The Management of Business Transactions through Electronic Contracts. In: A. Camell; A. Min Tjoa; R.R. Wagner: Proceedings for the of the 10th International Workshop on Database and Expert Systems Applications, Florence, Italy: IEEE Computer Society Press, p. 824 - 831, 1999.

Solo, D., Housley, R., Ford, W., Polk, T.: Internet Public Key Infrastructure X.509 Certificate and CRL Profile; http://security.di.unito.it/crispo/pki/standards/ipki-part1-07.txt, 04/06/1998, (Current: 10.01.2000).