24 A LAWFUL FRAMEWORK FOR DISTRIBUTED ELECTRONIC MARKETS

Michael Conrad
conrad@tm.uka.de, Institut für Telematik, Universität Karlsruhe
Christian Funk
cfunk@ira.uka.de, Institut für Informationsrecht, Universität Karlsruhe
Oliver Raabe
raabe@ira.uka.de, Institut für Informationsrecht, Universität Karlsruhe
Oliver Waldhorst
waldhorst@tm.uka.de, Institut für Telematik, Universität Karlsruhe
GERMANY

While decentralized peer-to-peer market platforms are more suited for trading short-lived or non-material goods (e.g., electrical power, bandwidth-on-demand) due to reduced transaction cost, robustness and scalability, they lack the legal certainty provided by centralized electronic market places operated by a trusted third party. This paper presents a technical framework that, conforming to European regulations, provides legal certainty for distributed market platforms. The framework includes a market-consistent data model representing the facts for the legal subsumption process, maps the European framework for electronic signatures to a distributed system, and comprises solutions for both adducing the reception of electronic documents and their distributed long-time storage. Moreover, it includes an electronic legal adviser for an automatic verification of contracts.

1 INTRODUCTION

In the near future there is a need for markets trading short-lived or non-material goods like, e.g., electrical power (Eßer et al., 2006) or bandwidth-on-demand (Dinger et al., 2006). In addition to a high number of consumers, such markets comprise an equally high number of sellers, each selling only a few items at a marginal price. Centralized electronic market places are not well suited for such scenarios, since, compared to the price of the traded items, the transaction costs are too high. At the same time centralized markets limit the available options of individual contract negotiations.

Decentralized market platforms based on the peer-to-peer (P2P) paradigm reduce transaction costs by eliminating the intermediary. Additionally, P2P systems inherently provide higher robustness and scalability as centralized approaches. While an intermediary is missing, a distributed market place can provide higher flexibility for contract negotiations between individual market participants. However, while centralized electronic market places are operated by a trusted third party and, thus, provide a certain level of legal certainty to both consumers and sellers, distributed market platforms lack such certainty since they are operated by a multitude of individuals, which generally cannot establish trust easy to each other and are often legal laities. As a consequence, providing legal certainty is crucial for the acceptance of distributed market platforms.

Conrad, M., Funk, C., Raabe, O., Waldhorst, O., 2007, in IFIP International Federation for Information Processing, Volume 243, Establishing the Foundation of Collaborative Networks; eds. Camarinha-Matos, L., Afsarmanesh, H., Novais, P., Analide, C.; (Boston: Springer), pp. 233–240.

In this paper, we present a lawful framework for distributed market platforms, i.e., a technical framework for providing trust and legal certainty conforming to the appropriate European regulations. The framework is based on three building blocks: First, it includes both a market-consistent data model representing the facts for the legal subsumption process and model of juristic expertise as a formal workflow. Second, it provides provableness and verifiability. For this purpose, it maps the European framework for electronic signatures to a distributed system. Furthermore, it includes solutions for both adducing the reception of electronic documents in a distributed system and a distributed long-time storage for such documents. Third, it includes an electronic legal adviser for an automatic verification of the validity of contracts. Consequently selected legal norms are transferred to technical rules and the appropriate state of facts is modeled in a legal ontology.

The proposed framework has been developed in the project "Self-Organization and Spontaneity in Liberalized and Harmonized Markets" (SESAM) (Conrad et al., 2005), which is founded within the priority research program "Internet Economy" by the German Ministry of Education and Research (BMBF). As major application scenario, SESAM considers a virtual power plant with a multitude of participants equipped with small, decentralized facilities for electricity production, e.g., fuel cells, solar panels, and wind power plants. Participants buy required energy or sell surplus energy on a distributed market place implemented by the SESAM platform. For demonstration purpose, SESAM has developed a software prototype, which is currently evaluated in a large distributed setting.

The remainder of this paper is organized as follows. Section 2.1 introduces the data model employed in the proposed framework. In Section 2.2, we show how legal norms are mapped on a contract negotiation process represented by a basic workflow. Section 2.3 shows how provableness and verifiability are provided. As last building block of the framework, the electronic legal adviser is presented in Section 2.4. Finally, concluding remarks are given.

2 LAYOUT FOR A LAWFUL FRAMEWORK

2.1 A Market-Consistent Data Model

As a building block of the lawful framework, a consistent data model is required, which defines a standardized description for electronic document exchange on the distributed market. Besides general technical aspects, also legal and economic requirements have to be considered. For our lawful framework, we propose a data model, which is able to map all required technical, economical and legal aspects into a single object model. The base structure of our data model is shown as UML diagram in Figure 1 in a simplified manner.

The root element of the data model is the class *Object*, almost all other classes inherit from this root element. From economic side, the data model includes the classes *Intention* and *Product*, where each product is described by a set of attributes. The class *Intention* maps the intention of a market participant, where the two attributes outgoing and incoming define which product a participant wants to sell and which one he wants to buy. To reach legal conformity an intention is embedded into the class *Declaration* and *Invitatio*. While the class *Invitatio* only represents an announcement, the class *Declaration* stands for legal binding statement in the contract negotiation process. In addition to the economic attributes, the class *Declaration* includes several legal relevant attributes, for example, person related data, time ranges and consumer protection information as prescribed by the regulation of the Directive 97/7 EC. An even more complicated issue were the requisites for Information Society Services regulated in the Directive 2000/31 EC. The national regulatory implementation is orientated on the classic client-server paradigm. Therefore we mapped this to the specific requirements of the P2P architecture using concepts in the data model.

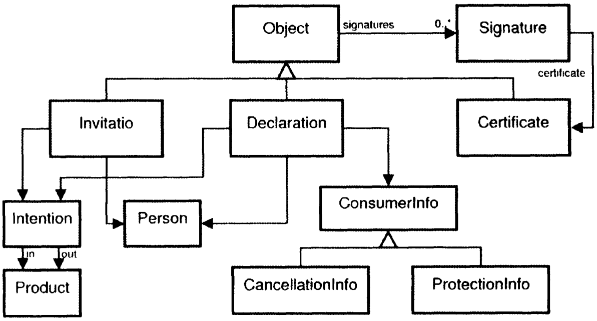

Figure 1: Data Model UML Diagram

Most objects represented by the data model require a guarantee of integrity. Thus the root element includes an attribute signatures of type Signature. Using this attribute, each instance can be secured against modification by applying a digital signature. To prove the identity of the issuer of a signature, the class Certificate is used. This class represents an identity certificate, which binds an identity to a public key. Although certificates typically require a trusted third party, they are issued in a distributed manner as shown in Section 2.3.1.

2.2 Judicial Expertise as Formal Workflow

Electronic Market places that allow negotiation are complex compared to Internet shops offering one click buying. To obtain legal certainty for such market places, it is necessary to embed the negotiation properly into a continental European[1] legal framework. Therefore judicial expertise has been transferred into formal workflow concepts so that automation of formation of contracts can be implemented. We present an easy to understand example of a short negotiation shown in Figure 2 as a UML sequence diagram.

The process starts with an offer[2], which could be based on an *invitatio ad offerendum* (invitation to bargain) previously published. Before being sent, the offer is checked for legal compliance by an electronic legal advisor (see Section 2.4). Optionally, the offer is delivered with a reception confirmation (see Section 2.3.3). A received document is passed automatically to the electronic legal advisor of the offeree. After evaluation the advisor informs the recipient that the document he

[1] We analyzed Austrian, French, German and Swiss law. There might be a different outcome for common law systems since the analyzed laws do not recognize concepts such as consideration.

[2] In Austrian, German and Swiss law binding and not revocable after reception or notice, in French law revocable.

received constitutes an offer. The offeree may now generate an acceptance, do not react at all, or (as in our example) create an acceptance conditioned on revisions or supplementary details. In the latter case, the acceptance legally counts for a rejection3 and new offer (sec. 150 German Civil Code, sec. 869 Austrian General Civil Code). The original offeror will be informed about this fact if he checks the incoming document. He now has the same choices as the original offeree, following the description above. In our example he accepts the counter offer. After successful negotiation both can use the distributed archive for long time storage of contracting documents (see Section 2.3.4).

Generally, the workflow will be more complex and dynamic, e.g., due to longer negotiations or auction mechanisms.

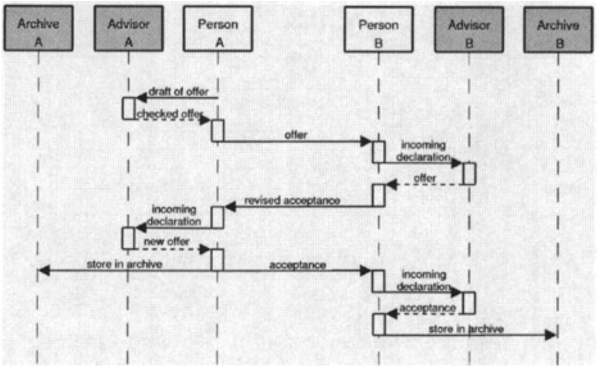

Figure 2: Contract negotiation UML Workflow

2.3 Provableness and Verifiability

Pacta sunt servanda is the root of all contract law. However in case of breach of contract remedies are provided by law and awarded by court. Usually the plaintiff bears the onus of proof for several facts as far as not challenged. Those are:

- identity of contracting parties (usually plaintiff and respondent)
- assignment of declarations, formal requirements (writing, electronic signature)
- reception of declarations (but see article 10 Swiss law of obligations)
- verifiability of declarations

The respondent on the other hand might be interested in being capable to prove the reception of termination notice and the reception time.

Some requirements of the preceding list are subject to the European framework for electronic signatures (as laid out in directive 1999/93/EC), but they are intentionally focused on a trust model with a single trust anchor. This constraint collides with one of the key principles of the P2P paradigm, the independence of centralized instances. After comprehensive analysis of the legal requirements, our framework provides essential functions without central instance in a distributed manner.

[3] Upon rejection the offer expires, i. e. it no longer exists (sec. 146 German Civil Code). Consequently it cannot be accepted any more.

2.3.1 Authenticity of Parties

In contrast to contract negotiations in the real world, on an electronic market it is difficult to prove the identities of the parties, since they are not standing vis-a-vis. Undoubtedly, the identities of the parties are important evidence. A common approach for establishing the required authenticity of an identity inside the digital world is to use public key infrastructures based on identity certificates. Identity certificates establish a binding between a unique identity and a given public key of an asymmetric cryptosystem (e.g. RSA). This binding is usually created by a trusted third party (denoted as trust anchor) after a successful verification of the participant's identity. To provide trust relationships among participants, all participants have to trust this dedicated authentication instance and the certificates it issues.

The existence of a single dedicated instance conflicts with the key paradigm of distributed system. On one hand, the whole system can be brought down by attacking this single instance. On the other hand not all participants may trust this dedicated instance. Therefore we propose a distribution of trust anchors across the distributed system. This enables participants to choose a trust anchor out of the available set of trust anchors. The selection of a trust anchor depends highly on the trust relationship and the provided authentication schemes. These authentication schemes are used to prove the participant's identity before a certificate is issued by the trust anchor. All trust anchors issue a certificate of type *Certificate*, described in Section 2.1. Each certificate can be signed by more than one authentication instance, avoiding a high amount of certificates by certifying a participant by multiple trust anchors. To establish a trust relationship between two participants, a subset of identical trust anchors has to be find out by merging the available sets of trust relationships of each participant.

2.3.2 Authentic Legal Declarations

Another important requirement for being able to verify a contract is a provable binding between declarations made by a participant and his identity. Without such binding, a participant can deny the entering into a contract, so that the opposite party is unable to verify the existence of the contract.

To meet this requirement we propose the application of digital signatures for relevant contracting information, building upon the certificates issued by the distributed approach described in the previous section. Using the associated private key of the corresponding public key of the participant's certificate, only the owner of the certificate is able to compute a valid signature. The opposite party is able to verify the validity of the signature using the public key from the certificate. In case of disputes about contract details, each party is able to evidence declarations made by the opposite party.

2.3.3 Reception of Declarations

In most cases contract law requires for receipt of both offer and acceptance; a mailbox rule is not recognized in German law, nor would be an "electronic mailbox rule", if there exists one at all. On an electronic market, one of the contracting parties can easily deny the reception of declaration. If one party denies a reception it can not be proved easily whether it happened in an action of fraud or bona fide.

So far, this problem has been solved by using a third trusted party supporting the reception of relevant documents and creating a reception confirmation signed by the recipient. However, since on a distributed electronic market such single trusted instance does not exist. Thus, alternative methods are required. Instead of using a dedicated instance, we propose the involvement of other market participants as witnesses, as described in (Conrad, 2006). Key idea of the proposed protocol is a selection of independent witnesses out of the mass of all participants, which support the delivery of contracting documents. The selection is performed by a deterministic function that depends on the chosen document and random information from sender and receiver, preventing a manipulation of the selected witnesses. In addition to the selection process, the protocol contains several features to avoid fraud by sender or receiver. As long as at least a single witness is not corrupted, the reception of a document can be delivered and the delivery can be confirmed by a reception confirmation signed by the witness. We believe that, at least when applying German law, the reception confirmation is sufficient to prove reception. From the point of judicial method this could either be based on an analogy to sec. 175 German Civil Procedure Code or on a prima facie evidence for reception. Here, the German concept of prima facie evidence allows concluding from certain given facts to such ones which usually were to be proven if experience of life states that the one normally leads to the other.

2.3.4 Archiving Contracts

The long term storage of contract documents is an important challenge. Without a backup all documents can be lost in case of a hard disk failure, resulting in a potential lack of evidence before court.

To provide long term storage, our lawful framework includes a distributed user archive, which provides a reliable distributed storage. All documents are secured against modification and unrestricted access by encryption and digital signatures. Due to the distributed storage of documents a breakdown of individual nodes does not infect the storage system at all. At the same time, the user archive acts as electronic mailbox receiving declarations, if the user is off line.

2.4 Legal Evaluation by Electronic Legal Advisors

While sellers and consumers on distributed markets are often legal laities, there is a need for legal assistance while inspecting the contract or negotiating for specific conditions. Thus, our lawful framework includes electronic legal advisors. Recall that the workflow shown in Figure 2 illustrated how automated legal advice is incorporated into an exemplary negotiation process. Due to regulation of legal profession the authorization to give legal advice is restricted. Our framework does not collide with this regulation thus we do not intend to substitute professional legal advice.

2.4.1 Methodology

Legal reasoning is a process that is influenced by numerous factors such as the legal framework, within one operates, or vagueness of a norm. Consequently, we have to begin by deciding on the framework – in our case, it is the Continental European norm-based system of positive law –, on the specificity of the norms, and a few specific legal consequences. This in turn determines a limited set of primary norms from which to start. For automated reasoning we need an abstract model of the legal norms and their classification.

Building a Graph of Norms

Hence, before beginning with legal reasoning it is necessary to find out the norms whose general domain covers the situation, starting from a primary set of norms. Decisions are made by inspecting the norms. Typically, norms determine a legal consequence resulting of one or more states of facts. Other norms may refer to related norms that show alternative routes or exceptions. Based on this set of routes a graph of norms can be built that allows a decision of whether the originally intended legal consequence can be reached or not. Each of these norms must now be inspected in order to determine whether the given real world situation, represented by object instances of the data model (see Section 2.1), matches the state of facts demanded by the norm. This may require to find statutory definitions (norms) or to build own definitions. In other words, we have to see if the individual facts match the states of facts or the (statutory) definitions. This process is called subsumption.

Formalizing the Subsumption Process

There are a number of legal philosophies that try to explain this subsumption process. Our approach is based on the work of Larenz (Larenz, 1991).

We assume that norms in the positive law mostly do not address singular cases but rather cover general classes of real-world situations. On the other hand, the relevant case is a specific real-world situation. Subsumption is an interpretative process. Consequently, to mechanize subsumption the semantics must be considered (Bohrer, 2003), and these should go beyond thesauri. Ontologies constitute a promising approach, because they reflect semantic relationships between terms. These relationships can particularly be defined so that they directly support the subsumption process. Our contribution is to explain the reasoning behind the match in an ontology, which incorporates judicial methodic knowledge. This knowledge summarizes in several steps by textual, historical, systematic and teleological interpretation, and by comparing concrete facts with legal terms that have no direct counterpart in the data model and may thus be subject to judicial opinion.

Ontologies are even more versatile. For example, one could translate some of the statutory definitions into the ontology and thus prune the norm graphs even further. Some related work can be found in (Senn et al., 2006).

2.4.2 Technical Architecture

Under the conditions mentioned before legal reasoning can be modeled as logical inference realized by classical logical rule processing. Therefore, our prototype includes a rule engine where the legal norms and summarized norm graphs are expressed as logical rules in the format required by the rule engine.

For the present implementation, a specific set of legal norms is transformed in logical rules. Those rules have the form *result* **if** *condition*. The states of facts within the condition are fed from user input or declaration instances. The legal reasoning starts from the legal consequence and then works its way backwards to construct a norm graph. Therefore, the rule engine must run a backward chaining strategy, except in some cases where legal obligations must be derived by forward chaining based on given facts. Furthermore, according to legal reasons or to minimize user interaction, the order in which rules are applied is important.

The prototypical implementation of our framework inside the SESAM project depends on the KAON framework (Maedche et al., 2003). The ontology is used to represent our data model and to perform decomposition of indefinite legal terms using the included description logic reasoner.

3 CONCLUSION

In this paper we present essential components to build a lawful framework for distributed electronic markets. Building upon a consistent data model, we proposed a flexible contract negotiation workflow. To provide provableness and verifiability we propose the use of a distributed public key infrastructure. In contrast to classical market scenarios we provide court-proof non-repudiation by digital signatures and a verifiable reception of documents. In addition, our lawful framework includes a distributed long-term storage of contracting documents. Finally, our framework supports legal laities by providing an electronic legal advisor component, which is able to perform an automatic verification of legal statements.

The proposed framework is implemented inside the software prototype of the SESAM project. For the legal subsumption process the rule engine JESS is used. Currently, we are working on a migration to KAON2, mobile phone-based authentication and signature generation.

4 REFERENCES

1. Bohrer, A.: Entwicklung eines internetgestützten Expertensystems zur Prüfung des Anwendungsbereiches urheberrechtlicher Abkommen, 2003
2. Conrad, M., Dinger, J., Hartenstein, H., Rolli, D., Schöller, M., Zitterbart, M.: A Peer-to-Peer Framework for Electronic Markets, in: R. Steinmetz, K. Wehrle (Ed.), Peer-to-Peer Systems and Applications, Lecture Notes in Computer Science 3485, p. 509-525, Springer, Sep 2005.
3. Conrad, M.: Non-repudiation mechanisms for Peer-to-Peer networks, in: CoNext 2006, 2nd Conference on Future Networking Technologies, 4 - 7 December 2006, Lisboa, Portugal, p. 249-250, Dec. 2006
4. Dinger, J., Raabe O., Hartenstein, H.: A Techno-Legal Perspective on Peer-to-Peer-Based Bandwidth on Demand Management, Proceedings of the 1st IEEE International Workshop on Bandwidth on Demand (BoD 2006) in conjunction with IEEE GLOBECOM 2006, p. 73-80, San Francisco, CA, USA, November 2006.
5. Eßer, A., Raabe, O., Rolli, D., Schöller, M.: Eine sichere verteilte Marktplattform für zukunftsfähige Energiesysteme. it- Information Technology, p. 187-192, Aug 2006
6. Larenz, K.: Methodenlehre der Rechtswissenschaft, Springer 1991
7. Maedche, A., Motik, B., Stojanovic, L.: Managing Multiple and Distributed Ontologies in the Semantic Web. The VLDB Journal 12:4 p. 286-302, 2003
8. Senn, A., Schweighofer, E., Liebwald, D., Geist, A., Drachsler, M.: LOIS: Erfahrungen und Herausforderungen bei die Weiterentwicklung mutilingualer Rechtsontologien. In: Schweighofer et al. (Hrsg.): e-Staat und e-Wirtschaft aus rechtlicher Sicht. Boorberg, p. 290-195, 2006