

Trust in Software Component Marketplaces

Thomas List and Jörg Köller
Informatik V – Information Systems, RWTH Aachen, Germany
{list|koeller}@informatik.rwth-aachen.de

Abstract

In electronic commerce trust building measures are one way to make a marketplace more attractive for suppliers and potential customers. Often trust on marketplaces is built up through external trusted third parties (TTPs). TTPs are organizations that deal with various trust-related problems and are themselves trusted by the customers. This paper describes the different trust problems that arose when designing a marketplace for (very specific) software components in the chemical engineering domain. To overcome these problems, different types of trust-building features will be included in the marketplace, each requiring different TTPs.

1 Introduction

Electronic marketplaces are portals to trade goods on the internet. They bring together several suppliers of goods and potential customers that are interested in these goods. While the first – and up to now most widely used – marketplaces are business-to-consumer (BtC) oriented, research focuses more and more on business-to-business (BtB) marketplaces. Differences between BtC and BtB marketplaces are large enough to require new and distinct approaches [12], especially as BtB solutions are often used for very domain-specific marketplaces.

One of the biggest problems for marketplaces is the acceptance by their customers who need to place some trust in the marketplace. In conventional commerce trust was mainly built up through personal contacts with the business partners. In electronic commerce, different trust building measures have been discussed [e.g.3,4,5,9]. Trust is not only (but partly) a question of (Internet) security but also addresses questions such as “Do I for sure get the product I paid for?” or “Is there no data about me on that marketplace that can be misused?”. Often trust on marketplaces is built up through external trusted third parties (TTPs) thereby providing an add-on value for potential customers or providers acting in the marketplace. TTPs are organizations that guarantee certain trust-related questions and themselves are trusted by the customers and providers.

This paper describes the different trust problems that arouse when designing a marketplace for (very specific) software components in the chemical engineering domain. To overcome

these problems different types of trust-building features will be included in the marketplace, each requiring different TTPs.

2 Software Components

Software component are executable, stand-alone pieces of software with a clearly defined interface and behaviour. They can be used as part of a new software under development or to extend the functionality of existing software. There are several component frameworks setting standards for all aspects of component based systems ranging from low-level network protocols to lifecycle issues or load balancing [10,11,13].

2.1 Trading Software Components

Because software components are stand-alone pieces of software with a well defined functionality they are a suitable good for electronic trade. Additionally, delivery of these products is rather easy because they can be downloaded via the web or remotely accessed through a link. However there are several specific problems and needs when trading software components [8] some of which we will present now:

2.1.1 Licensing

As software components are very flexible in the way they may be used an electronic marketplace should support licensing models that reach beyond simple buying of software. Usage and/or time based models should be supported as well for expensive components that are not used very often. Taking into account new business models such as application service providing (ASP) where the component resides on a provider's computer, even more complex models are needed [14].

These licenses cannot be implemented through license keys that are given to the user, as the real usage of the component is payed. The usage data on which payment is based has to be collected and processed. When dealing with small software providers this should be offered as a service of the marketplace.

2.1.2 Product Quality

When using and trading software components there are two major quality issues that have to be taken into account: stability and interoperability. The stability problem is the same as for normal software products like an office suite. The vendor has to make sure that the software does not crash and fulfils the functionality that it should. When using software components interoperability is also very important which means that such a piece of software must be easy to deploy and will co-operate with other components that are present in the customers environment.

2.1.3 Consulting

It is rather unlikely that a complex software component will be sold off the shelf from a component marketplace and be deployed in the buyers system without any customisation. In some cases this will be a very difficult task requiring special skills which require training sessions. This and other kinds of consulting can be offered on a marketplace as well as the component. Appropriate negotiation features for this have to be offered by the marketplace. Another important service with negotiable prices is the implementation of special tailored components not available in that form on the marketplace. Here a customer for software components is looking for a provider that is able to develop a new component or to tailor an existing component to fit the specific needs.

2.2 Cape Open: A Standard for Software Components

Because software components are well suited for web trade several concepts and technical architectures for web-based component marketplaces have been developed, e.g. [1,7]. However, all of these marketplaces follow a horizontal approach, i.e. the type of components that can be sold is not limited to specific domains. This raises the problem that most add-on and trust services have to remain on the horizontal level as well. As a consequence these services will be either very difficult to realize or be so simple and generic that they will not bring much add-on value to the customer.

Therefore, we will take a closer look at a horizontal marketplace in the chemical engineering domain. The narrow scope of this marketplace allows the design and implementation of specific services. Nevertheless, the problems arising in that context apply to other domains in a similar way. We will now start with brief introduction to the Global CAPE-OPEN project.

In the Global CAPE-OPEN project of the G7 Intelligent Manufacturing Systems (IMS) program, the worldwide chemical industries have defined an open standard for chemical engineering simulation software [2]. This opens up a market for simulation components of chemical plants provided by a number of large companies and many small specialised providers. For trading chemical engineering components this allows the creation of a vertical marketplace that is specialised for the domain and therefore allows to realise a multitude of add-on and trust services.

Additionally, the CAPE-OPEN consortium has set up a non-profit organization for maintaining and managing the standard called the CO-LaN [6]. The CO-LaN is independent from the companies involved CAPE-OPEN and can therefore be an instance for handling trust related issues in the marketplace.

2.2.1 The Cape Open Marketplace

The CAPE-OPEN marketplace which will be supported but not operated by the CO-LaN will implement a set of services addressing the problems in trading software components mentioned above. Additionally, it will offer several other component services which we will

not discuss here. All services have been designed on basis of user interviews and/or discussions within the CAPE-OPEN consortium so that the services implement real world requirements and take into account trust related problems that have been identified by the CAPE-OPEN and CO-LaN members. We will now present some of the services and the relevance of trust for them.

3 Trust-Problems within the Cape Open Marketplace

We will now describe three different areas where trust has been identified to be a crucial factor for the operation of the CAPE-OPEN marketplace. Similar to the requirements these trust problems have been identified by doing interviews and discussion among the CAPE-OPEN partners. What we will not discuss here are general security and trust aspects such as hardware reliability and availability and security related problems. These things can be treated by off the shelf solutions that are well known.

3.1 License Data Management

The existence of the CAPE-OPEN standard in combination with the Internet allows for creating more flexible license models. Especially useful are dynamic license models that enable the use of specific components on a per-use or per-time basis [8]. These models require a (direct or indirect) Internet connection from the engineer's workstation to a centralised license and billing server. All interviewed persons thought a local proxy billing server combined with https-tunnelling to resolve firewall problems are possible within their intranet. Most concerns here were about the company's data used in the calculations performed by the components. This data contains descriptions of chemical plants or novel chemical processes under development which therefore is considered highly confidential. Other vital information that must not be accessed by the marketplace owners are data about the user and data about the usage of certain components.

These issues are addressed by a standardized yet flexible way of handling licence and billing data in the CAPE-OPEN marketplace. Again these procedures have been designed on basis of user interviews to assure general agreement and trust to these procedures. As a consequence of the trade-off between the need of detailed information on the one hand and the protection of sensible data a two level licensing architecture with standardized licensing and billing protocols has been developed.

There are licence servers on the components users and on the providers networks. The licensing and billing data first passes through the local server (billing proxy) in the users network and is then transferred to the providers server. The users can define rules and filters to anonymize that data to an extend he needs. On the other hand all information that is really needed by the provider to make the billing will get through the billing proxy to the providers server. Otherwise, the billing proxy would not be give the necessary license information to the proxy which is needed for employing a component in the users network. With this mechanism the user can be sure that only the information that he wants to reach the supplier is transferred

there. On the other hand the supplier will receive all information he needs for billing will reach him so that he is paid for his services.

Another option which was not implemented in our system would be the installation of a TTP dedicated to handle the detailed usage and licence data. In this approach all data generated would be stored in the TTP's computers. The component user would always be able to access his data completely and only the data needed for billing would be passed by the TTP to the component owner. Only in case of a conflict between component user and provider this data would be revealed by the TTP. But due to the lack of a acceptable TTP in our scenario this option was not chosen. Theoretically the CO-LaN could act as such TTP but this could not be agreed upon by the various parties involved in Global CAPE-OPEN.

3.2 Guarantee of Product Quality

As the interfaces and behaviour of CAPE-OPEN standard compliant software components are very exactly specified CAPE-OPEN compliant components will interoperate in a plug-and-play manner. To ensure this plug-and-play interoperability standardised software compliance tests have been developed to define a certain level of product quality in terms of interoperability. On the CAPE-OPEN marketplace only those components will be sold that have successfully passed these tests. Therefore, a buyer can "trust" the marketplace to offer high quality software. This is not really a trust-issue itself as the quality is guaranteed: the customer knows that the product is compliant to the standard.

But the software quality involves another level of trust namely the trust in the label "CAPE-OPEN compliant" itself. The users must be sure that this label is granted only if a piece of software is really standard compliant (meaning that the label it cannot be bought) and the tests are really testing real world scenarios which have been agreed upon by the CAPE-OPEN and CO-LaN members. To handle these trust problems a combination of transparency and independent testing is used. These compliance tests are not performed by a marketplace owner because she cannot be considered independent. Therefore the CO-LaN as completely independent organization with lots of domain knowledge is responsible for defining and carrying out these compliance tests. It finally grants the label "CAPE-OPEN compliant" based on test suites which are available as open source. As the CO-LaN organization is independent and accepted by all current CAPE-OPEN members (which are also the first users of the standard) the trust in software quality and the trust in the quality assurance process itself is solved for the CAPE-OPEN context.

In the future the CO-LaN will not only function as a TTP for compliance checks but it will also grant other independent companies the right to act as a compliance TTP. This means that the CO-LaN will allow other companies to label a piece of software as CAPE-OPEN compliant. As a prerequisite this company will have to pass a CAPE-OPEN certification performed by the CO-LaN as some sort of master TTP.

3.3 Trust within Negotiations for Special Services

The software components traded on a CAPE-OPEN market place are in general no of-the-shelf products. Standard components that represent common units of a chemical plant are included with every simulation environment that is available. The special form of trading single components with highly specialised license models only applied to complex and specific components that are not used every day. The complexity here now results in two possible problems: First, for seldom used complex components, knowledge of how to deploy and use the component is missing in engineering companies. This knowledge is vital for the use of a component as discussed in section 2.1.3. Second, a suitable component that represents the chemical unit in question is often not available and has to be developed by domain experts.

For both problems external companies can offer solutions. They can offer consulting for the use of specialised components and they can develop or adapt components for the specific needs. An electronic marketplace for CAPE software components should offer the possibility to “buy” these services online. To define the precise service that is needed, negotiations between the engineering company (customer) and the software vendor (vendor) are needed in addition to facilities that allow the two parties to find each other. When dealing with software delivery and licensing of the product have to be a part of the market place. Trust related issues for the license handling are the same as with trading existing software components 3.1.

When dealing with these special services, we have noticed two trust problems. The customer has to trust the marketplace and the business partner – in different ways. Trust in the business partner means that the consulting is done in the way it was specified and that the software component is developed in the correct way and in the correct time. In general, all these information should be contained in the contract. But with the complex products in this scenario, the contract itself will not contain every small detail that was discussed during the negotiation. Such a detail for example could be a specific existing software component that has to cooperate with the new software in a specific parameter range. While for legal claims the contract alone is relevant, these information can be used to resolve problems that come up during the fulfilment phase. For example the software vendor might have problems solving certain specifications for the component. Reviewing the negotiation might reveal why this specification was made and can show is a change is possible. A solution for this problem is presented in [12]. A tracing and monitoring functionality is introduced that stores traces of negotiations and monitors these traces to find events that indicate possible problems (for example late delivery). This functionality allows a company to trust in the business partner’s ability to create exactly the software or deliver the service that is needed.

In the chemical engineering domain the data used in simulations are normally top secret and companies do not want that another party has access to these data in any way. When using an electronic market place to buy simulation components, especially when a tracing functionality as described above is involved, this becomes a problem. Normally only very few complex chemical units are used in one plant. Knowing these units is often enough to guess what the company is working on. The complex software components that are traded on a market place represent exactly these critical units as standard units are covered by standard software components. To avoid an accumulation of critical data on a market place the trace data should not be stored on the market place system itself but at a trusted third party that is

trusted to handle these data in a suitable way. This TTP can allow access to the data for the participant parties but can restrict the ability to analyse these data as a whole. As it is hard to find one TTP that is trusted by every company, the concept can be extended to involve several TTPs. Here the trace data is not stored at one TTP but distributed between several parties. Here a coordinator, another TTP, is responsible for data access. A technical solution for this concept is under development.

4 Conclusions

Within the single marketplace for CAPE-OPEN software components we have observed several trust-related problems that have to be addressed. Each problem can be solved through one or more approaches, often through the use of external trust services offered by TTPs. There is no single organisation within the CAPE-OPEN context that can serve as the only TTP but several different organisations are needed to services such as certification or monitoring. Some of the solutions, here the certification services, are highly dependant on the application domain. The domain standard CAPE-OPEN proved very useful to realise some solutions that are not possible in a horizontal marketplace.

Acknowledgements

This work was supported in part by the European Commission under BRITE-EURAM-IMS project Global CAPE-OPEN. Discussions with our colleagues from ESPRIT project MEMO concerning the structuring of e-commerce repositories are gratefully acknowledged.

References

- [1] A. Behle, An Internet-based Information System for Cooperative Software Reuse, In Proc. of 5th IEEE International Conference on Software Reuse, pp 236-245, 1998.
- [2] B. Braunschweig, M. Jarke, J. Köller, W. Marquardt and L. v. Wedel: CAPE-OPEN - experiences from a standardization effort in chemical industries. In Proc. Intl. Conf. Standardization and Innovation in Information Technology (SIIT99), Aachen 1999.
- [3] A.M. Chircu, G.B. Davis and R.J. Kauffman: Trust, Expertise, and E-Commerce Intermediary Adoptions. In Proceedings of the 2000 Americas Conference on Information Systems, Long Beach, CA, 2000.
- [4] T.H. Clark and H.G. Lee: Electronic Intermediaries: Trust Building and Market Differentiation. In Proceedings of the Thirty-Second Annual Hawaii International Conference on System Science, IEEE Computer Society, 1999.
- [5] R.C. Mayer, J.H. Davis and F.D. Schoorman: An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3):709-734, 1995.

- [6] CO-LaN web-site, www.colan.org, 2001
- [7] H.-A. Jacobsen, O. Günther and G. Riessen: Component Leasing on the World Wide Web, In Proc. of the 1st ACM Conf. Electronic Commerce, ACM Press, 1999.
- [8] J. Köller, T. List and M. Jarke: Designing a Component Store for Chemical Engineering Software Solutions, In Proc. 34th Hawaiian Intl. Conf. On System Sciences (HICSS-34), Maui, 2001.
- [9] M. Merz, W. Lamersdorf and K. Müller: Trusted Third-party Services in COSM. *Electronic Markets*, 4(2):7-8, 1994.
- [10] Microsoft COM web-site, www.Microsoft.com/com, 2001
- [11] OMG CORBA web-site, www.omg.org/corba, 2001.
- [12] M. Schoop and T. List: To Monitor or not to Monitor - The Role of Trusted Third Parties in Electronic Marketplaces, Proc. 5. Internationale Tagung Wirtschaftsinformatik (WI 2001), September, Augsburg, Germany.
- [13] Sun EJB web-site, java.sun.com/j2ee, 2001.
- [14] G.Tamm, O. Günther, On-Demand Application Integration: Business Concepts and Strategies for the ASP Market, Proc. 4th Workshop on Federated Databases, Shaker, 1999.