Web Service-based ERP Systems and an Open Security Model

Nico Brehm, Jorge Marx Gómez, Claus Rautenstrauch
Faculty of Computer Science
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2
391o6 Magdeburg, Germany
Tel: +49-5323-67-18386
Fax: +49-5323-67-11216
{brehm, gomez, rauten}@iti.cs.uni-magdeburg.de

Abstract

Modern enterprise resource planning (ERP) systems like SAP R/3 or Oracle Applications consist of many software components which provide specific functionality. However, these ERP systems are designed as an all-in-one solution, often implementing functionality not needed. Furthermore, such ERP systems depend on very large-scale infrastructures like servers and networking technology, which are very expensive to install and to maintain. The new idea is to develop a novel ERP system architecture which facilitates an overall reusability of individual business components (BC) through a shared and NON-monolithic architecture based on a peer-to-peer (P2P) network.

According to the common use of distributed applications, several security problems exist. This paper describes an open security model for a shared ERP system based on Web Service technology. The visualized approach underlines the security requirements of distributed ERP systems and gives a basic proposal for further research.

Keywords: ERP, Web Service, Web Service Security (WSS), SOAP, Peer-to-Peer (P2P)

1 Introduction

Modern ERP systems consist of many software components which are related to each other. Currently these components are administered on a central application server. In connection to the ERP system complexity several problems appear:

- Not all installed components are needed.
- High-end computer hardware is required.
- Customizing is expensive.

Due to the expensive proceedings of installation and maintenance only large enterprises can afford such complex ERP systems.

One solution to counter these problems is to develop a distributed ERP system where the system components are reachable over a network (e.g. internet). This component ensemble still appears as single ERP system to the user, however it consists of different independent elements which exist on different computers. Based on this construction it is possible for an enterprise to access on-demand functionality (components) of other network members over a P2P network.

This approach solves the mentioned problems as follows:

- Due to the separation of local and remote functions, no local resources are wasted for unnecessary components.
- Single components are executable on small computers.
- Due to decreasing complexity of the local system also installation and maintenance costs subside.

As a result of these (cost) advantages ERP systems of the specified kind would open up new vistas to small- and medium-sized enterprises, which require the same functionality and scalability as large enterprises [KuRa89, p. 477].

Enhancing this approach a lot of research and technique level problems accrue. If the goal is to connect different enterprises to one single ERP system, a characteristic issue is standardizing and disclosure of the underlying ERP system architecture. The application of extensible markup language (XML) standards offers an appropriate background to start up in this area, because XML, XML namespaces and XML schemas provide useful mechanisms to deal with structured extensibility in a distributed environment [W3C02]. Besides, in connection with the common use of distributed applications, several *security problems* exist. The most important security objectives in the case of distributed ERP systems are:

- *Resource protection*
- *Confidentiality* of transmitted data
- *Integrity* of transmitted data
- *Authenticity* of communication partners
- *Anonymity* of communication partners against unauthorized parties
- *Non-repudiation* of transactions
- *Reliability* (trustability) of communication partners

2 Technologies and standards

The main technological elements of the visualized design are a P2P system as fundamental network design schema and Web Service technology as approach to create a top level interconnection of business components. Particularly with regard to security aspects a lot of research is already done by the World Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS). The following collection of definitions and acronyms gives a brief survey of the theoretical and technical foundations.

- *P2P systems*
  The term ‚peer-to-peer' (P2P) refers to a class of systems and applications that employ distributed resources to perform a critical function in a decentralized manner [Mil+02, S. 1].

- *Web Services*
  Web Services are self-descriptive, encapsulated software-components, which are offering an interface for remotely calling their functionality and can be loosely coupled by the exchange of messages. For achieving universal interoperability, standard internet technology is used for communication [GI2003].

- *Web Service Security (WSS)*
  This term describes a collection of existing extensible markup language (XML) standards and security mechanisms and their combination to a standard for securing messages written in the Simple Object Access Protocol (SOAP) format. The appropriate OASIS technical committee (TC) deals with this standardization process and describes the most important of all existing specifications (SOAP Message Security) as follows:
  The specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies [OAS04].
  Further specifications in this context are *X.509 Certificate Token Profile* [OAS04b] and *UsernameToken Profile* [OAS04a] which were published by OASIS WSS TC, too.

XML Encryption [W3C03a], *XML Signature* [W3C03b], *XML Key Management Specification* (XKMS) [W3C03c], *Security Assertions Markup Language* (SAML) [OAS04c] and *Extended Access Control Markup Language* (XACML) [OAS04d] are the most important and model-independent XML standards that zoom in on security aspects.

3 A shared ERP architecture

As explained above, the distribution of the ERP system is based on a P2P architecture. Each peer can communicate with all the rest of the participating network nodes. Among other forms of P2P structuring, the

illustrations below use a pure P2P architecture whereas the integration of a centralized control is abandoned. The assets and drawbacks of this method shall receive no further consideration in this first instance.

The duties and responsibilities of every network node are divided into two sections. On one hand the service providing peers and on the other hand the ones which utilize theses services establish the basis for exchanging software components, whereas the over-all system-functionality will be available to the whole ERP network. SOAP messages which are described in Web Service Description Language (WSDL) build up the communicational basis of this scenario. In a Web Services registry ERP components can be searched out by using the Universal Description, Discovery and Integration (UDDI) standard. Because of the integration of these standards, new providers can be involved easier. New system functions are added by implementing new Web Services whereby high flexibility is warranted. Figure 1 shows the general set-up of the shared ERP system.

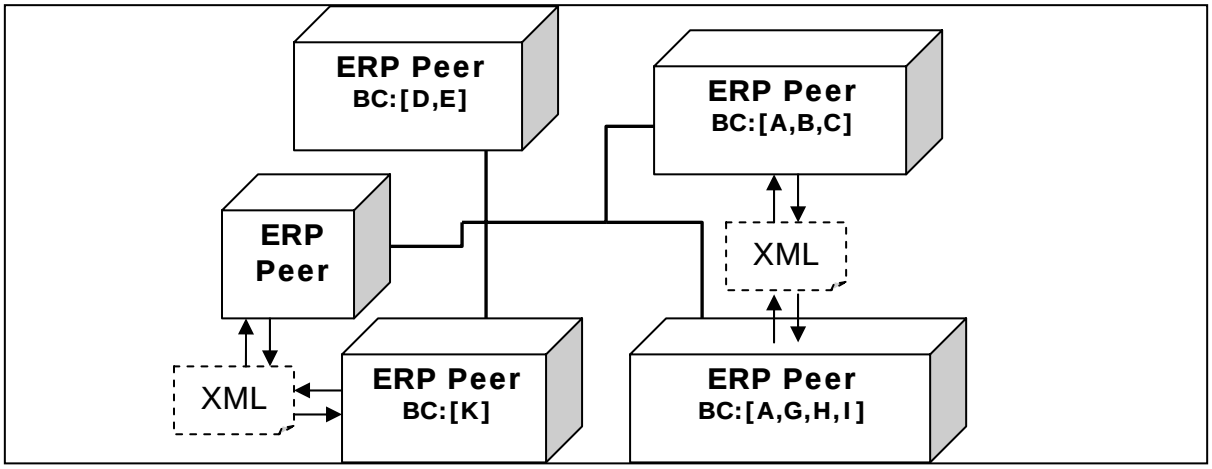

Figure 1: ERP peers provide various ERP components in a P2P network based on Web Services

Premise for a coherent communication between the peers is a standardized vocabulary, which enables them to express interface calls to remote business components (BC). This necessitates a schema of all language elements of all BC. According to other related „internet languages“, XML schema should be used for drafting such standards.

4 An ERP peer architecture

The communication between client and server (provider) is handled by exchanging Web Service requests and responses as SOAP messages. Requests include all necessary input parameters of the remote component interface. Responses represent an instance of the pre-described return object. Figure 2 shows this message interchange.

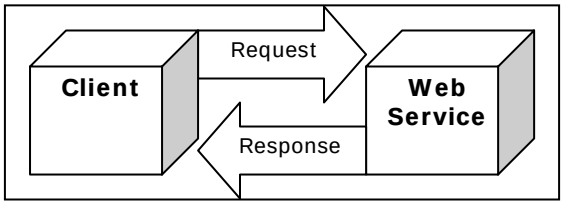

Figure 2: Communication by exchanging messages

All incoming and outgoing messages must pass the hierarchic back end architecture of each individual peer. Commensurate with the motivation to integrate standard techniques, an ERP peer back end consists of the following elements:

- *Webserver* when Hypertext Transfer Protocol (HTTP) is application layer basis
- *UDDI registry* for provision of public business component offering
- *Component repository* which administrates the local components
- *Central enterprise database management system* (DBMS)

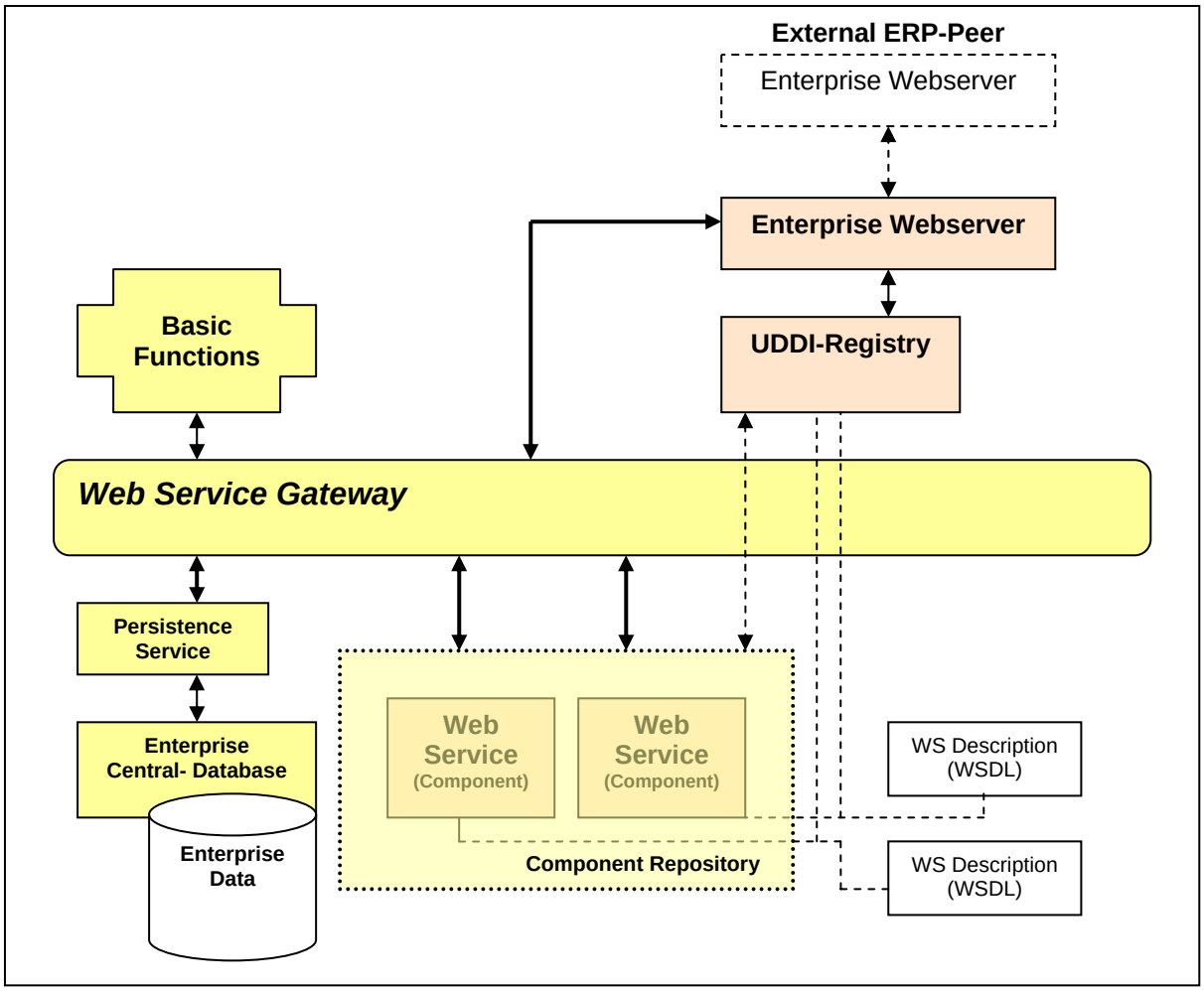

Figure 3: Internal ERP peer architecture

Figure 3 shows how the Web Service Gateway controls the whole internal and external access to all available Web Service components.

5 Security model

Constructing a security layer and involving it into the already existing architecture, attention should be paid to the different specifications of individual security requirements. Within the shown context of a shared ERP system those requirements commonly correspond to message integrity, authenticity and data confidentiality of all interface calls and responses and thus of the whole network traffic.

As these strategic security objectives differ from each ERP peer to another, it is essential that the security model is open for virtually all security mechanisms and standards, which allows the processing of generic definitions of security profiles. Referring to the existing security mechanisms a security profile describes the concrete security requirements of the appropriate network node including the respective configuration parameters.

A suitable profile processor is then able to audit all incoming messages for security conformance on the own security profile and to extend all outgoing messages according to the security policy of the remote peer. This process sequence can be seen in figure 4.

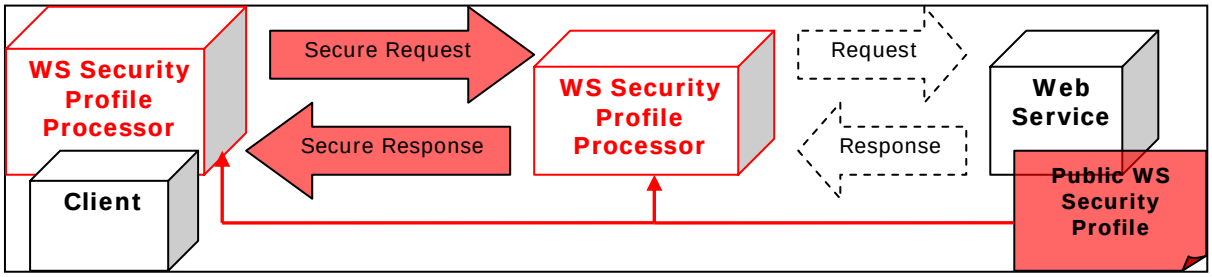

Figure 4: Processing of Web Service Security profiles

Similarly to the Web Service description (in WSDL) which is referenced by the „enterprise-own“ UDDI registry, it is possible to ask for the related security profile and then to decide whether the remote guidelines are in accord with the security requirements of the potential caller and as result to communicate or not. Example parts of those descriptions can be XML encryption-, XML signature- or SAML-configuration parameters. A Web Service Security profile does not only include the security policy of a Web Service, but also a list of all supported security mechanisms or standards and „interesting“ system characteristics are imaginable. Such properties that are related to the remote system security could for instance describe the existence of a trusted environment according to the Trusted Computing Group (TC) PC specification [TCG04] which in turn would offer more significant data confidentiality for non-public enterprise information.

As visualized in figure 5, the demands of the Web Service Security descriptions are processed and satisfied by a new security layer that we call security control gateway.

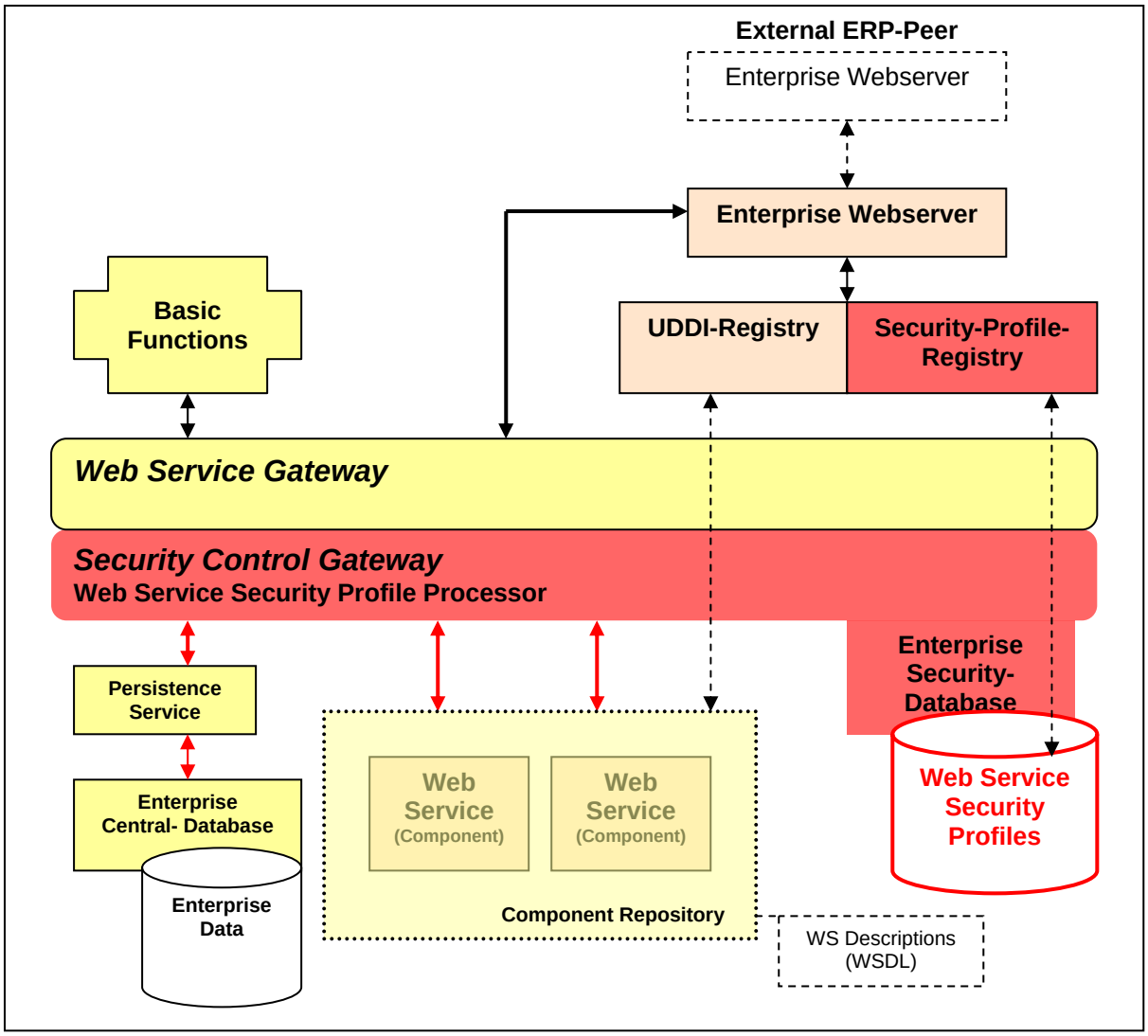

Figure 5: Secure ERP peer architecture

6 Conclusions and Outlook

Separation of transport data and content is the key-note of the introduced security model. Extended interface calls and responses encapsulate the respective information a network peer uses to serve or rather request ERP functionality.

The prefixed article constructs an open architecture which not only considers the integration of existing security standards like XML encryption, XML signature or SAML but also facilitates future developments like Trusted Platforms. Before such a secure shared ERP system can be switched on, further research into Web Service security profile schemas must be done.

References

[KuRa89] Kurbel, K.; Rautenstrauch, C.: Ein verteiltes PPS-System auf Arbeitsplatzbasis, München, GI-19.Jahrestagung II Computergestützter Arbeitsplatz, Springer-Verlag 1989

[Mil+02] Milojicic et. al.: Peer-to-Peer Computing. HP Labs (HPL-2002-57), Palo Alto. 2002

[OAS04] Organization for the Advancement of Structured Information Standards (OASIS): Web Services Security: SOAP Message Security 1.0, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf. 2004

[OAS04a] Organization for the Advancement of Structured Information Standards (OASIS): Web Services Security: Username Token Profile 1.0, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf

[OAS04b] Organization for the Advancement of Structured Information Standards (OASIS): Web Services Security: X509 Certificate Token Profile, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf

[OAS04c] Organization for the Advancement of Structured Information Standards (OASIS): Security Services TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[OAS04d] Organization for the Advancement of Structured Information Standards (OASIS): eXtensible Access Control Markup Language TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[TCG04] Trusted Computing Group: TCG PC Specification V1.0, www.trustedcomputing.org

[W3C02] World Wide Web Consortium (W3C): Web Services Activity Statement, Introduction, http://www.w3.org/2002/ws/Activity. 2002

[W3C03] World Wide Web Consortium (W3C): Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/SOAP/. 2003

[W3C03a] World Wide Web Consortium (W3C): XML Encryption WG, http://www.w3.org/Encryption/2001/. 2001

[W3C03b] World Wide Web Consortium (W3C): XML Signature WG, http://www.w3.org/Signature/

[W3C03c] World Wide Web Consortium (W3C): XML Key Management Specification (XKMS), http://www.w3.org/TR/xkms/. 2001