Miriam Hamel

Sicherheitsservices für Service Oriented Architecture (SOA) am Fallbeispiel Enterprise SOA

Diplomarbeit

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 2007 GRIN Verlag
ISBN: 9783656062202

Miriam Hamel

Sicherheitsservices für Service Oriented Architecture (SOA) am Fallbeispiel Enterprise SOA

GRIN Verlag

Sicherheitsservices für Service Oriented Architecture (SOA) am Fallbeispiel Enterprise SOA

DIPLOMARBEIT

für die Prüfung zum
Diplom-Ingenieur (BA)

der Fachrichtung Informationstechnik
an der Berufsakademie Mannheim

von
Miriam Hamel

September 2007

Bearbeitungszeitraum:	25.06.2007 – 21.09.2007
Kurs:	TIT 04 APE
Ausbildungsbetrieb:	Fraunhofer SIT, Darmstadt
Abteilung:	Secure Processes and Infrastructures (SPI)

Zusammenfassung

Sicherheitsservices für Service Oriented Architecture (SOA) am Fallbeispiel Enterprise SOA

Service Oriented Architecture – Durch sie ist es möglich, Geschäftsprozesse zu automatisieren und dabei völlig flexibel auf unternehmensspezifische Veränderungen einzugehen. Hierfür müssen Unternehmen jedoch ihre bisher im Einsatz befindlichen Sicherheitsmechanismen anpassen und für Geschäftspartner öffnen. So wird es möglich, durchgängige und automatisierte Geschäftsprozesse abzubilden und damit die Vorteile der globalen Märkte mit Hilfe des neuen Architekturgedankens zu nutzen. Dies birgt neben den Chancen aber auch Risiken.

Unternehmen müssen sich dieser Gefahren bewusst werden und sie bewerten, nur so können entsprechende Maßnahmen zur Reduzierung des Risikos ermittelt werden. Hierfür ist ein strukturiertes und prozessorientiertes Vorgehen notwendig. Im von der Autorin beschriebenen Verfahren wird zu diesem Zweck zunächst der Schutzbedarf für den zu analysierenden Geschäftsprozess ermittelt. Anschließend werden Risiken identifiziert und deren Risikohöhe mit Hilfe der Eintrittswahrscheinlichkeit und des Schadensausmaßes bestimmt. Mittels dieser Werte kann eine Aussage über die Notwendigkeit der Risikominimierung gemacht werden, um effektive Kontrollmaßnahmen zu ermitteln, beginnend beim kritischsten Risiko.

Grundlegender Gedanke und Nutzen einer SOA ist die Wiederverwendbarkeit. Dies trifft auch auf die Sicherheitsaspekte zu. Mithin demonstrierte die Autorin das zuvor beschriebene Verfahren an zwei Geschäftsprozessen, so dass auf Basis der erhaltenen Kontrollen Sicherheitsservices bestimmt werden konnten. Diese enthalten sinnvolle Kombinationen von technischen und nicht-technischen Maßnahmen zur ganzheitlichen Absicherung von Geschäftsprozessen und können immer wiederverwendet werden.

Schließlich wurden die Sicherheitsservices in die SAP-spezifische Lösung der SOA, die Enterprise SOA, übernommen. Zur sicheren Realisierung der Enterprise SOA beim Kunden müssen darüber hinaus weitere Aspekte berücksichtigt werden. Aus diesem Grund wurde beispielsweise aufgezeigt, wie interne Governance-Richtlinien einbezogen, gesetzliche Vorschriften eingehalten oder auch bisherige Sicherheitsmechanismen in die Enterprise SOA übertragen werden.

Abstract

Security services for Service Oriented Architecture (SOA) on the paradigm Enterprise SOA

Service Oriented Architecture enables automation of business processes. It is flexible and can be adapted to the specific requirements of organizations, thereby making the more responsive to occurring changes. In order to fully realize all benefits, it is required for companies to open their IT security infrastructure for direct communication with business partners. This would allow mapping and automation of business processes along the entire value chain and across global markets. The advantages do not come without risks, however.

Organizations need to know and understand these risks so that they can be properly managed and mitigated. Therefore, a structured, process-oriented approach is essential. In the technique described by the author, the first step is to identify the required security level for the business process being analyzed. Next, the security risks must be identified and categorized taking into account the parameters for likelihood and impact. According to the various categories it is then possible to assess the need for mitigation and institute appropriate security inspection measures, beginning with the most critical risk.

One of the major benefits of SOA is reusability. This applies to security as well. Using the process-oriented approach described above on two business process examples the author created so called security services derived from the obtained security measures. These involves suitable combinations of technical and non-technical procedures to safeguard the business processes and are completely reusable.

Finally, the security services are introduced into the Enterprise SOA, which is an SAP-specific implementation of SOA. However, there are additional security issues to be considered in implementing Enterprise SOA for a customer. The author discusses how to develop internal governance policies, how to comply with legal regulations, and how to maintain existing security mechanisms for Enterprise SOA.

Danksagung

An dieser Stelle möchte ich allen Personen danken, die wesentlich zum erfolgreichen Erstellen meiner Arbeit beigetragen haben. Ich danke

- *Prof. Dr. Heinz Jürgen Müller* für die Betreuung meiner Arbeit von BA-Seite aus und die vielen interessanten Gespräche,

- *Barbara Mayer (SAP)* für die zahlreichen inhaltlichen und fachlichen Tipps, die interessanten und anspruchsvollen Aufgaben, auch neben der Diplomarbeit, die ständige Sorge um mein Wohlbefinden und die sehr gute Zusammenarbeit, wodurch ich mich in den paar Monaten bei SAP sehr heimisch gefühlt habe,

- *Max Larsson und Dr. Markus Schumacher (Fraunhofer SIT)* für die inhaltlichen und rechtschreiblichen Anmerkungen, die sehr gute kollegiale Kommunikation und die unkomplizierte Zusammenarbeit.

Darüber hinaus gab es zahlreiche andere Personen, welche mich permanent unterstützten oder weitere Ideen für die Arbeit gaben. So danke ich

- *meinem Mann Marko Hamel (SAP)* für das permanente Korrektur-Lesen, die zahlreichen fachlichen Diskussionen, die vielen Momente zum Knetschen, damit ich Abstand zur Arbeit gewinnen und anschließend wieder voller Elan weiter arbeiten konnte, die hervorragende Hilfe im Haushalt und bei unseren Kindern, ohne welche mein Kopf nicht so frei für die Arbeit hätte sein können und die vielen anderen Dinge, die mir das gesamte Studium erst ermöglichten,

- *meinen Eltern Brigitte und Klaus Mäder* für das finale Korrektur-Lesen, so dass nun ziemlich alle Rechtschreib- und Tippfehler beseitigt sein müssten, und für all die Dinge, die sie mir in meinem Leben mitgaben und beibrachten, so dass mir dieses Studium und nun ein erfolgreicher Berufsstart möglich wurde,

- *Hubert und Christine Röder* für die unermüdliche Betreuung unserer Kinder, auch zu unmenschlichen Zeiten und den Auftrieb, den sie mir einfach durch ihr Dasein und ihre Freundlichkeit und Herzlichkeit gaben,

- *Stephan Raschke (SAP)* für die zahlreichen Interviews zum Thema der Enterprise SOA und Sicherheitsservices,

- *Matthias Händly (SAP)* für die Informationen zur Enterprise SOA,

- *Dr. Bernhard Drittler (SAP)* für die Auskünfte zum PIC-Prozess der SAP,

- *Björn Steinemann (Fraunhofer SIT)* für die vielen Antworten zur WS-Security,

- *Daniel Atzesdorfer (Microsoft)* für die reichlichen Informationsmaterialien und die Interviews,

- *Reiner Meiser (LSGV Saarland) und Marko Görg (Software AG)* für die interessanten Informationen über die Realisierung einer SOA beim Landesamt für Soziales, Gesundheit und Verbraucherschutz in Saarbrücken,

- *Petra Guse (IBM)* für die Hinweise zur Sicherheit bei SOA,

- *Anika Hamel (Commerzbank)* für die zahlreichen Auskünfte über den SEPA-Prozess,

- *Familie Yearwood* für das Korrektur-Lesen meines englischen Abstractes, für meine ersten positiven Erfahrungen mit der englischen Sprache und für die vielen motivierenden Erinnerungen an die wunderschöne karibische Insel Barbados und

- *Stefan Bock (MAN Roland Druckmaschinen)* für den vielen Spaß im Studium, vor allem in manch langweiliger Vorlesung, die äußerst gute Zusammenarbeit und das Korrekturlesen nicht nur dieser Arbeit.

Sicher gibt es noch einige weitere Personen, welche mir bewusst oder unbewusst zum Gelingen der Arbeit verhalfen. All diese sollen hier nicht vergessen bleiben, denn auch ihnen gilt mein Dank dafür.

SOA-Technologien sind wie Sportgeräte: Egal, wie gut diese sind, Sie werden durch sie nicht fit, solange Sie sie nicht benutzen.

Anne Thomas Manes [Thomas Manes 2007, S. ix]

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

ABKÜRZUNGSVERZEICHNIS

AG Aktiengesellschaft

API Application Programming Interface

A2A Application-to-Application

BAPI Business Application Programming Interface

BDB Bund Deutscher Banken

BPEL4PEOPLE WS-BPEL Extension for People

BI Business Intelligence

BIC Bank Identifier Code

BO Business Object

BPEL Business Process Execution Language

BPEL4WS BPEL For Web Services

BPM Business Process Management

BPML Business Process Modelling Language

BSI Bundesamt für Sicherheit in der Informationstechnologie

BSP Building as a Service Provider

B2B Business-to-Business

CAF Composite Application Framework

CE Composition Environment

CEO Chief Executive Officer

CFO Chief Financial Officer

CIA Central Intelligence Agency

CIO Chief Information Officer

CORBA Common Object Request Broker Architecture

CRM Customer Relationship Management

CSM Clearing & Settlement Mechanismus

DCOM Distributed Component Object Model

DoS Denial of Service

DTD Document Type Definition

EAI Enterprise Application Integration

EBICS Electronic Banking Internet Communication Standard

EC Electronic Cash

ECM Enterprise Content Management

EDIFACT Electronic Data Interchange For Administration, Commerce and Transport

EIPP Electronic Invoice Presentment and Payment

EJB Enterprise JavaBeans

EPC European Payments Council

ERM Enterprise Risk Management

ERP Enterprise Resource Planning

ES Enterprise Service

ESB Enterprise Service Bus

ESRRA Einzelsystem-Restrisiko-Analyse

EU Europäische Union

EU-Kommission Europäische Kommission

EVT Extrem Value Theory

EW Eintrittswahrscheinlichkeit

EZB Europäische Zentral-Bank

FMEA Failure Mode and Effects Analysis

FTP File Transfer Protocol

GUI Graphical User Interface

HR Human Ressources

HTML HyperText Markup Language

HTTP HyperText Transport Protocol

HTTPS HTTP Secure

IBAN International Bank Account Number

ICM Internet Connection Manager

ID IDentifier

IdAS Identity Attribute Service

IDE Integrated Development Environment

IDL Interface Description Language

IFX Interactive Financial Exchange

IIOP Internet Inter ORB Protocol

IM Identity Management

IP Internet Protocol

IT Information Technology

JCA Java Cryptogrphy Architecture

JCo Java Connector

JDBC Java DataBase Connector

JEMS JBoss Enterprise Middleware Suite

JSF JavaServer Faces

J(2)EE Java (2) Platform, Enterprise Edition

KonTraG Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

MARCO MAximized Risk COntrol

MDA Model Driven Architecture

MOM Message-Oriented Middleware

OASIS Organization for the Advancement of Structured Information Standards

PDF Portable Document Format

PE-ACH Pan European Automated Clearing House

PI Process Integration

PIC Process Integration Content Council

PKI Public Key Infrastructure

QoS Quality of Service

R Risikohöhe

RBAC Role Based Access Control

REST REpresentational State Transfer

RFC Remote Function Call

RMI Remote Method Invocation

RoI Return on Investment

RPC Remote Procedure Call

RR Rest-Risiko

SA Schadensausmaß