

**Miriam Hamel**

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

**Diplomarbeit**

# BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei [www.GRIN.com](http://www.GRIN.com) hochladen  
und kostenlos publizieren



### **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.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

### **Impressum:**

Copyright © 2007 GRIN Verlag  
ISBN: 9783656062202

### **Dieses Buch bei GRIN:**

<https://www.grin.com/document/182364>

**Miriam Hamel**

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

## **GRIN - Your knowledge has value**

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite [www.grin.com](http://www.grin.com) ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

### **Besuchen Sie uns im Internet:**

<http://www.grin.com/>

<http://www.facebook.com/grincom>

[http://www.twitter.com/grin\\_com](http://www.twitter.com/grin_com)

**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 . . . . .	VII
Tabellenverzeichnis . . . . .	IX
Listingverzeichnis . . . . .	XI
Abkürzungsverzeichnis . . . . .	XIII
<b>1 Einleitung</b>	<b>1</b>
1.1 Fragestellungen und Zielsetzung . . . . .	2
1.2 Aufbau der Arbeit . . . . .	3
1.3 Hinweise zur Arbeit . . . . .	6
<b>2 Forschungsgrundlagen</b>	<b>7</b>
2.1 Definitionen . . . . .	8
2.1.1 Schutzbedürfnisse . . . . .	8
2.1.2 Risiko . . . . .	11
2.1.3 Kontrolle . . . . .	12
2.1.4 Sicherheitsservices . . . . .	13
2.2 Von Web Services zur Service Orientierten Architektur . . . . .	14
2.2.1 Web Services . . . . .	14
2.2.2 Service Orientierte Architektur (SOA) . . . . .	16
2.3 Standards bei Web Services . . . . .	26
2.3.1 Grundstandards . . . . .	26
2.3.2 Sicherheitsstandards . . . . .	34
<b>3 Risikoanalyse und -klassifizierung</b>	<b>43</b>
3.1 Methoden zur Risikoanalyse und -klassifizierung . . . . .	44
3.1.1 Bekannte Verfahren . . . . .	45
3.1.2 Vorgehen im Kontext der Arbeit . . . . .	49
3.2 Erstellen eines Risikokataloges für die Service Orientierte Architektur . . . . .	51
3.2.1 Beispiel 1: Purchase to Pay . . . . .	51
3.2.2 Beispiel 2: SEPA-Überweisung . . . . .	69



<b>4 Implementierung von Kontrollmaßnahmen</b>	<b>89</b>
4.1 Methoden zur Bestimmung geeigneter Kontrollmaßnahmen . . .	90
4.1.1 Bekannte Verfahren . . . . .	90
4.1.2 Vorgehen im Kontext der Arbeit . . . . .	91
4.2 Erstellen eines Kontrollkataloges zur Absicherung der Service Orientierten Architektur . . . . .	97
4.2.1 Ermitteln von Kontrollmaßnahmen . . . . .	97
4.2.2 Ermitteln von Sicherheitsservices . . . . .	123
4.2.3 Bewerten der Sicherheitsservices . . . . .	138
<b>5 Paradigma: Enterprise SOA</b>	<b>161</b>
5.1 Aufbau und Funktionsweise . . . . .	162
5.1.1 Entwicklung . . . . .	162
5.1.2 SAP NetWeaver . . . . .	163
5.1.3 Enterprise SOA . . . . .	168
5.2 Sicherheitsbetrachtung . . . . .	174
5.3 Prozessorchestrierung mit Enterprise SOA . . . . .	176
5.3.1 SAP NetWeaver Composition Environment . . . . .	176
5.3.2 Prozess orchestrieren . . . . .	177
5.3.3 Zuweisung der Sicherheitsservices . . . . .	181
5.4 Enterprise SOA-Sicherheit in der Beratungspraxis . . . . .	182
5.4.1 Rechtliche Sicherheitsaspekte für die IT . . . . .	183
5.4.2 Vorgehensweise im Projekt . . . . .	185
<b>6 Fazit</b>	<b>191</b>
<b>A Listings zu Web Service-Standards</b>	<b>193</b>
<b>B Abbildungen zur Prozessorchestrierung mit Enterprise SOA</b>	<b>205</b>
<b>Glossar</b>	<b>215</b>
<b>Literaturverzeichnis</b>	<b>219</b>

# Abbildungsverzeichnis

1.1	Forschungsfragen und Aufbau der Arbeit . . . . .	4
2.1	Zusammenspiel von Web Services . . . . .	15
2.2	Web Services Architecture Stack . . . . .	16
2.3	Aufbau einer SOA . . . . .	19
2.4	Modell eines SOA-Stacks . . . . .	20
2.5	Das ESB-Konzept . . . . .	22
2.6	SL&I-Modell nach Offermann . . . . .	25
2.7	WSDL-Script . . . . .	29
2.8	UDDI-Registry der SAP AG . . . . .	30
2.9	Erweiterungen von WS-Security . . . . .	39
2.10	Beispiel-Szenario für die Verwendung von SPML . . . . .	41
3.1	Risikomanagement-Prozess . . . . .	44
3.2	Zusammenwirken der Analyse-Verfahren . . . . .	46
3.3	Kategorisierung der Analyse-Methoden . . . . .	48
3.4	Matrix zur Bestimmung der Risikohöhe . . . . .	50
3.5	Prozess „Zulieferer auswählen“ . . . . .	53
3.6	Prozess „SEPA-Überweisung“ . . . . .	72
4.1	Funktionsweise der Sicherheitsservices und des ESB . . . . .	130
5.1a	Monolithische Anwendungsstruktur . . . . .	163
5.1b	Zweischichtige Anwendungsstruktur . . . . .	163
5.1c	Dreischichtige Anwendungsstruktur . . . . .	164
5.1d	Derzeitige Unternehmensstruktur . . . . .	164
5.1e	Enterprise Services Architecture . . . . .	165
5.2	Kernbereiche des SAP NetWeaver . . . . .	166
5.3	SAP NetWeaver Process Integration als Basis für Enterprise SOA . . . . .	167
5.4	Enterprise SOA und SAP NetWeaver . . . . .	170
5.5	SAP NetWeaver Security . . . . .	175

B.1	SAP Developer Network . . . . .	206
B.2	Enterprise Service Workplace . . . . .	207
B.3	Enterprise Services Index nach Prozesskomponenten . . . . .	208
B.4	Prozesskomponente „Purchase Request Processing“ . . . . .	209
B.5	Enterprise Service „Manage Purchase Request In“ . . . . .	210
B.6	Enterprise Services Operation „Create Purchase Request“ . . . . .	211
B.7	Informationen zur ES Operation „Create Purchase Request“ . . . . .	212
B.8	Business Object „Purchase Request“ . . . . .	212
B.9	Link zur detaillierten Feldbeschreibung für die ES Operation „Create Purchase Request“ . . . . .	212
B.10	Detaillierte Feldbeschreibung für die ES Operation „Create Purchase Request“ . . . . .	213

# Tabellenverzeichnis

2.1	Bei XML-Signature verwendete Algorithmen . . . . .	38
3.1	Beispiel für Bewertung des Schutzbedarfs . . . . .	49
3.2	Beispiel zur Auflistung der identifizierten Risiken . . . . .	51
3.3	Beispiel für den Risikokatalog . . . . .	51
3.4	Schutzbedarf im Prozess „Zulieferer auswählen“ . . . . .	56
3.5	Risiken für den Prozess „Zulieferer auswählen“ . . . . .	59
3.6	Risikokatalog für den Prozess „Zulieferer auswählen“ . . . . .	69
3.7	Schutzbedarf im Prozess „SEPA-Überweisung“ . . . . .	74
3.8	Risiken für den Prozess „SEPA-Überweisung“ . . . . .	78
3.9	Risikokatalog für den Prozess „SEPA-Überweisung“ . . . . .	87
4.1	Beispiel zur Auflistung von Kontrollmaßnahmen . . . . .	92
4.2	Beispiel zur Klassifizierung der Risiken . . . . .	93
4.3	Beispiel zur Auflistung von Sicherheitsservices . . . . .	94
4.4	Beispiel zur Zuordnung von Kontrollmaßnahmen und Sicherheits- services . . . . .	95
4.5	Beispiel für den Kontrollkatalog . . . . .	96
4.6	Liste von Kontrollmaßnahmen . . . . .	106
4.7	Klassifizierung der Risiken für den Prozess „Zulieferer aus- wählen“ . . . . .	108
4.8	Klassifizierung der Risiken für den Prozess „SEPA-Überwei- sung“ . . . . .	117
4.9	Liste von Sicherheitsservices . . . . .	129
4.10	Kontrollmaßnahmen und Sicherheitsservices für den Prozess „Zulieferer auswählen“ . . . . .	133
4.11	Kontrollmaßnahmen und Sicherheitsservices für den Prozess „SEPA-Überweisung“ . . . . .	137
4.12	Kontrollkatalog für den Prozess „Zulieferer auswählen“ . . . . .	148
4.13	Kontrollkatalog für den Prozess „SEPA-Überweisung“ . . . . .	160

5.1	Prozess „Zulieferer auswählen“ mit benötigten Enterprise Services . . . . .	180
-----	---	-----

# Listings

A.1	XML-Script . . . . .	194
A.2	SOAP-Script . . . . .	195
A.2	SOAP-Script (Forts.) . . . . .	196
A.3	HTTP-Header . . . . .	196
A.4	WSDL-Script . . . . .	197
A.4	WSDL-Script (Forts.) . . . . .	198
A.4	WSDL-Script (Forts.) . . . . .	199
A.5	UDDI – Anmelden eines businessEntity-Elements bei der Registry . . . . .	199
A.6	Prozessformulierung mit BPEL . . . . .	200
A.7	GET-Request in REST-Architektur . . . . .	200
A.8	XML Encryption . . . . .	201
A.9	XML Signature . . . . .	202
A.10	Syntax einer SOAP Nachricht mit WS-Security . . . . .	202
A.11	Authentifizierung mit SAML . . . . .	203



# 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



<b>CFO</b>	Chief Financial Officer
<b>CIA</b>	Central Intelligence Agency
<b>CIO</b>	Chief Information Officer
<b>CORBA</b>	Common Object Request Broker Architecture
<b>CRM</b>	Customer Relationship Management
<b>CSM</b>	Clearing & Settlement Mechanismus
<b>DCOM</b>	Distributed Component Object Model
<b>DoS</b>	Denial of Service
<b>DTD</b>	Document Type Definition
<b>EAI</b>	Enterprise Application Integration
<b>EBICS</b>	Electronic Banking Internet Communication Standard
<b>EC</b>	Electronic Cash
<b>ECM</b>	Enterprise Content Management
<b>EDIFACT</b>	Electronic Data Interchange For Administration, Commerce and Transport
<b>EIPP</b>	Electronic Invoice Presentment and Payment
<b>EJB</b>	Enterprise JavaBeans
<b>EPC</b>	European Payments Council
<b>ERM</b>	Enterprise Risk Management
<b>ERP</b>	Enterprise Resource Planning
<b>ES</b>	Enterprise Service
<b>ESB</b>	Enterprise Service Bus
<b>ESRRA</b>	Einzelssystem-Restrisiko-Analyse
<b>EU</b>	Europäische Union
<b>EU-Kommission</b>	Europäische Kommission

## *ABKÜRZUNGSVERZEICHNIS*

---

**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 Cryptography 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