

# Contents

- Lists .....XVII
- Abbreviations and Acronyms ..... XIX
- 1 Introduction..... 1
  - 1.1 Aims and Objectives .....3
  - 1.2 Structure of this Book .....5
- 2 Cross-Organisational Deployment of Business Processes .....7
  - 2.1 Extended Use of Business Process Definition Languages  
in CBP Scenarios.....9
  - 2.2 Motivating Example of Cross-Organisational Business Process .....10
    - 2.2.1 Description of Business Process Example .....11
    - 2.2.2 Security Policy-Induced Restrictions in Cross-Organisational  
Business Process Execution .....12
  - 2.3 Security Issues Related to Cross-Organisational Deployment of CBP .....13
  - 2.4 Limitation of Scope to WS-BPEL without Loss of Generality.....15
  - 2.5 Summary .....18
- 3 Approaches to Specification and Enforcement of Security Policies ..... 19
  - 3.1 Specification of Security Aspects for Web Services.....20
    - 3.1.1 Web Service Security (WS-Security).....21
    - 3.1.2 WS-SecurityPolicy .....22
    - 3.1.3 WS-Trust .....22
    - 3.1.4 Web Services Policy Framework (WS-Policy).....22
    - 3.1.5 Security Assertion Markup Language (SAML) .....23
    - 3.1.6 eXtensible Access Control Markup Language (XACML).....23
  - 3.2 Role-Based Access Control for Web Services and Business Processes .....24
  - 3.3 Relation of Programs and Programming Languages  
with Security Policies.....27
  - 3.4 Verification of Consistency between Program Code  
and Security Policies .....30
  - 3.5 Security Policy Enforcement via Code Instrumentation  
and Runtime Monitoring .....32
  - 3.6 Classification of Approaches to Security Policy Enforcement.....34
  - 3.7 Summary .....36

4	Analysis of Security-Relevant Semantics of BPEL .....	39
4.1	Scope of Analysis.....	39
4.1.1	Search for Security-Relevant Building Blocks of BPEL Semantics ...	40
4.1.2	Trade-Off Between Policy Strictness and Functional Richness .....	41
4.1.3	Need for Information Flow Analysis in Policy Compliance Assessment.....	42
4.1.4	Approach to Dispensability of Security Classification System.....	43
4.1.5	Risks of Policy Violations of Remotely Defined Business Processes.....	44
4.2	Overview of BPEL Semantics .....	45
4.2.1	General Structure of BPEL Scripts .....	47
4.2.2	Primitive and Structured Activities in Normal Process Flow .....	48
4.2.3	Additional Flow Control and Structuring Elements.....	49
4.2.4	Special Activities for Fault Handling .....	50
4.2.5	Concept of Multiple Instantiation in BPEL.....	51
4.2.6	Extensibility of BPEL and Problems for Compliance Assessment Involved.....	51
4.3	Classification of Security Policy-Derived Restrictions for WS Invocation .	52
4.4	Analysis of Security-Relevant Semantic Patterns of BPEL .....	56
4.4.1	Definition of Security-Relevant Semantic Patterns of BPEL .....	56
4.4.2	Results of Security Analysis of Semantic Patterns.....	57
4.5	Considerations with Respect to Separation of Duty Constraints .....	63
4.6	Summary .....	64
5	Specification of Security Policy for Compliance Assessment of CBPs .....	67
5.1	Redefinition of Security Policy in Terms of Security-Relevant Semantic Patterns.....	69
5.2	Security Policy Statement.....	69
5.2.1	Security Policy Statement Template .....	70
5.2.2	Internal Web Service Restriction Statement .....	72
5.2.3	External Web Service Restriction Statement.....	74
5.3	Approach to Reduce Complexity of Security Policy Statements.....	76
5.4	Coping with Dynamic Aspects in Static Compliance Analysis .....	77
5.5	Summary .....	80
6	Security Policy Compliance Assessment for BPEL Scripts .....	81
6.1	Procedure of Compliance Assessment .....	81
6.1.1	Prerequisites for Compliance Assessment.....	81
6.1.2	Analysis of Declaration Part in BPEL Script.....	82
6.1.3	Checking BPEL Script for Security-Relevant Semantic Patterns .....	83

6.1.4	Example of Covert Channel Establishment in BPEL Script .....	83
6.1.5	Information Flow Analysis in Parallel Flows.....	84
6.2	Workflows in Distributed Definition and Execution of CBPs .....	86
6.3	Delegation of Security Policy Compliance Assessment.....	88
6.3.1	Domain-Internal Delegation of Compliance Assessment .....	89
6.3.2	Domain-External Delegation of Compliance Assessment .....	90
6.4	Summary .....	91
7	Proof of Concept by Prototypical Implementation.....	93
7.1	Scope of Prototypical Implementation.....	93
7.2	Machine-Readable Format of Security Policy Statement.....	98
7.2.1	Rationale for Definition of XML Schema in Current Form .....	99
7.2.2	Annotated SPS Schema in Condensed Notation .....	99
7.3	Architecture of Prototype .....	103
7.4	Functionality of Prototype at a Glance.....	105
7.4.1	Conversion of SPS into Internal Representation .....	105
7.4.2	Conversion of Variable Declarations into Internal Representation.....	106
7.4.3	Combined Forward/Backward Information Flow Analysis .....	106
7.4.4	Handling of Parallel Flows in Information Flow Analysis .....	108
7.4.5	Implementation of Covert Channel Prevention .....	108
7.5	Evaluation of Prototype .....	109
7.6	Summary .....	111
8	Extending Results to Grid and Cloud Computing .....	113
8.1	Motivation for Remote Definition of Grid Processes .....	114
8.2	Approaches to Specification of Grid Service Security.....	118
8.3	Security-Relevant Semantic Patterns in BPEL-Based Grid Processes .....	119
8.4	Rewriting Security Policies to Support Pre-Execution Security Policy Assessment .....	123
8.5	Delegation of Security Assessment.....	126
8.6	Security Policy Enforcement for BPEL Processes in Cloud Delivery Models .....	127
8.7	Summary .....	131
9	Conclusions and Directions of Further Research and Development .....	133
9.1	Which Contributions Have Been Achieved?.....	133
9.2	What is Still to be Done? .....	137
9.3	Directions of Further Research and Development .....	139

---

Appendix 1: XML Schema for Security Policy Statement.....	141
Appendix 2: Outline of Sophisticated Covert Channel Prevention for Activity validate.....	145
References.....	147
Index.....	159