Table of Contents

Foreword I

Acknowledgements III

Table of Contents V

List of Figures IX

List of Tables XI

List of Abbreviations XIII

1 Introduction 1

1.1 Motivation and Problem Statement 1

1.2 Versatile Perspectives on 'Security' 5

1.3 Research Objective 6

1.4 Research Design 10

1.5 Thesis Structure 14

2 Fundamentals of Supply Chain Security in Parcel Mail Services 17

2.1 Security-by-design 17

2.1.1 In Absence of a Definition: What is Security-by-Design? 18

2.1.2 Security-by-Design Principles 18

2.2 Systems Security Engineering 22

2.2.1 Terminology and Definitions 22

2.2.2 Systems Security Engineering Framework 23

2.2.3 Systems Security Life Cycle Process 25

2.3 Supply Chain Security Management 27

2.3.1 Terminology and Definitions 27

2.3.2 Supply Chain Security Management Framework 28

2.4 Security in Parcel Mail Services 32

2.4.1 Terminology and Definition 32

2.4.2 Parcel Mail Service Network 33

3 Adapting Enterprise Architecture Development for Security-by-Design 41

3.1 Enterprise Architecture Management 41

3.1.1 Terminology and Definitions 41

3.1.2 Enterprise Architecture Frameworks 43

3.2 Requirements for Secure-by-Design Architecture Development Methods 46

3.3 State of the Art in Architecture Frameworks and Security Architectures 48
3.3.1 Comparison of Enterprise Architecture Frameworks 48
3.3.2 TOGAF® Architecture Development Method 50
3.3.3 Enterprise Information Security Architectures Frameworks 53
3.4 Methodology for Adapting the Enterprise Architecture Development 56
3.5 Secure-by-Design Architecture Development Method 60
3.5.1 Security Preliminary Phase 64
3.5.2 Phase As: Architecture Security Vision 66
3.5.3 Phase Bs: Business Security Architecture 69
3.5.4 Phase Cs: Information Systems Security Architecture 72
3.5.5 Phase Ds: Technology Security Architecture 74
3.5.6 Phase Es: Security Evaluation 76
3.5.7 Architecture Implementation 78
3.6 Enterprise Security Architecture Artifacts 79
3.6.1 Security Concept Specifications 79
3.6.2 Security Architecture Components 81
3.7 Evaluation and Discussion of Impact on Security Management 82
3.7.1 Requirements-based Evaluation 82
3.7.2 Impact on Supply Chain Security and Security Architecture Management 86
4 Enhancing Business Process Modelling for Security-by-Design 89
4.1 Business Process Modelling 89
4.1.1 Terminology and Definitions 90
4.1.2 Business Processes in the Context of Enterprise Architecture Modelling 91
4.2 Requirements for the Security Modelling Notation 92
4.2.1 Domain-Specific and Context Requirements 92
4.2.2 Modelling Notation Requirements 94
4.3 State of the Art in Extending Business Processes for Security 97
4.3.1 Security Extensions for Business Process Modelling 98
4.3.2 BPMN Extension Mechanism 100
4.4 Methodology for Creating a Domain-Specific BPMN Extension 102
4.5 Security-enhanced Business Process Modelling Notation 106
4.5.1 Security Domain Analysis 106
4.5.2 Decision Modelling Language 106
4.5.3 Equivalence Check 107
4.5.4 Security Domain Modelling 111

4.5.5 Abstract Syntax of the BPMN Security Extension 113
4.5.6 Concrete Syntax of the BPMN Security Extension 116
4.6 Extensibility to Information Security Modelling 120
4.7 Evaluation and Discussion of Impact on Security Engineering 124
4.7.1 Requirements-based Evaluation 124
4.7.2 Impact on Supply Chain Security and Secure Process Modelling 129
5 Linking Architecture Requirements to Process Implementation 131
5.1 Architecture Requirements in Business Processes 131
5.1.1 Terminology and Definitions 132
5.1.2 Security Specification in Enterprise Architectures with ArchiMate 133
5.1.3 Business Process Analysis Techniques 136
5.2 Requirements for Analysing Security Requirements in Process Models 142
5.3 State of the Art in Linking Enterprise Architecture and Business Processes 144
5.3.1 Combination of Enterprise Architecture and Business Process Models 144
5.3.2 Security Engineering Framework by Haley et al. 146
5.4 Methodology for Analysing Security Requirements in Business Processes 148
5.5 Combined Architecture and Process Security Assessment 150
5.5.1 Mapping the Research Outcomes to the Systems Security Life Cycle 150
5.5.2 Identifying Connections between Architecture and Process Models. 152
5.5.3 Using Requirements to Connect Architecture and Process Models 154
5.5.4 Analysis Approach for Security Requirements in Business Processes 158
5.5.5 Security Measures and Analysis Techniques 161
5.6 SeBPMN Graph and Modelling Rules Verification 164
5.6.1 Alignment of SeBPMN Extension with Analysis Techniques 164
5.6.2 Specification of SeBPMN Modelling Rules as Constraints 167
5.7 Evaluation and Discussion 173
5.7.1 Requirements-based Evaluation 173
5.7.2 Impact on Supply Chain Security and Requirements Analysis 176
6 Case-based Evaluation in Parcel Mail Services 179
6.1 Case Study Background 181
6.2 Case Study Part I – Developing the Security Architecture 181
6.3 Case Study Part II – Modelling the Security Measures 194
6.4 Case Study Part III – Assessment of the Security Approach 200
6.5 Discussion 206

7 Conclusion 209
7.1 Summary 209
7.2 Limitations 212
7.3 Outlook 214
References 217
Appendix 235
A Comparison of Security Architecture Frameworks 236
B BPMN Extension Mechanism 238
C Security Engineering Framework Process Activity Diagram 239
D Case Study Baseline BPMN Parcel Import Process 240