Carl von Ossietzky Universität Oldenburg

Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften
Department für Informatik

A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility

Dissertation

Submitted in fulfillment of the requirements for the degree of

Doktors der Ingenieurwissenschaften (Dr.-Ing.)

Submitted by

M.Sc. Basel Hasan

Supervisors:

Prof. Dr.-Ing. Jorge Marx Gómez

Prof. Dr. Hermann Strack

Disputation Date: 15.05.2019

Oldenburg, Germany

Acknowledgements

This dissertation would not have been possible without the support I always received from my first supervisor Prof. Dr.-Ing. Jorge Marx Gómez, who always gave me invaluable comments, advices and suggestions regarding the content as well as regarding the formal structure of this thesis. I am also thankful for my second supervisor Prof. Dr. Hermann Strack. Through him, I received lot of comments that enriched the thesis. I would also like to thank Dr. Joachim Kurzhöfer for the interesting discussion sessions at LHIND. He was always available for me during the last years. My gratitude extends also to the PhD examination committee members Prof. Dr.-Ing. Jürgen Sauer and Dr.-Ing. Sven Rosinger. Thanks also go to my colleagues at the VLBA department. It has been a pleasure to work with them and to supervise students doing their bachelors' and masters' theses.

Special thanks go to Tishreen University for funding my study by a scholarship for master and PhD. Here, I would also like to thank Dr. Nasser Nasser for giving me the support I was highly needed.

I am grateful to my parents and to my sisters for their encouragement and support within whole my life. They always believed in me, which has helped me to get where I am now. I am waiting with highest patience to see you soon!

I am grateful to my beautiful family, my wife Ola and my children Zeinab and Karam. I will never forget your invaluable support and endless love you are giving to me. I am waiting with highest patience to see you soon!

To the strong persons who gave their souls to save my home, Syria. Without you, we would not have been able to protect our home. You made the history and I will be always telling about your heroic victories. My brother **Alaa**, I miss you in everything, you remain inside my heart and I will never forget you, Rest in Peace.

Thanks God for everything.

Basel Hasan

Oldenburg, May 2019

Zusammenfassung

Heutzutage fordern Unternehmen die Mobilität und Flexibilität ihrer Mitarbeiter als unerlässliche Erfolgsfaktoren ein. Die Integration von mobilen Endgeräten, wie Smartphones und Tablets, gibt den Mitarbeitern der Unternehmen die Möglichkeit, produktiver zu arbeiten. Diese Integration birgt allerdings auch neue Sicherheits-herausforderungen und Risiken. Trotz aller Vorteile dieser Mobilität scheuen viele Unternehmen diese Umsetzung, da sie ihre Sicherheitsrisiken nicht einschätzen können. Mobile Endgeräte sind einer Vielzahl von Bedrohungen ausgesetzt, denen begegnet werden muss. Eine einfache Portierung der Informationssicherheitsstandards von Workstations, Notebooks und Serverdomänen auf mobile Endgeräte ist jedoch nicht wirkungsvoll. Aus Unternehmenssicht sind die Schutzstufen auf mobilen Endgeräten daher nicht eindeutig. Einerseits kann eine hohe Schutzstufe auf mobilen Endgeräten durch ein hohes Maß an Einschränkungen erreicht werden. Andererseits kann dies die Akzeptanz und Zufriedenheit der Nutzer minimieren.

Um die oben genannten Probleme anzusprechen, wird ein konzeptionelles Framework vorgeschlagen, welches Unternehmen bei der Einführung von mobilen Unternehmens-applikationen unterstützt. Es wird eine Risikoanalyse mit Fokus auf mobile Endgeräte durchgeführt. Bei der Risikoanalyse werden potenzielle Sicherheitsbedrohungen sowie deren Eintrittswahrscheinlichkeit und Auswirkungen auf das Unternehmen ermittelt und in einer Liste zusammengefasst. Jede Sicherheitsbedrohung wird einer oder mehreren Sicherheitsmaßnahmen und deren Konsequenzen für mobile Benutzer zugeordnet. Darüber hinaus wird das vorgeschlagene Framework mit einer Sicherheitsüberprüfungs-methode unterstützt, die überprüft, ob das Sicherheitskonzept einer mobilen Unternehmensapplikation den Sicherheitsanforderungen entspricht, welche zum Erreichen einer vordefinierten Schutzstufe erforderlich sind.

Diese Forschung soll Unternehmen hauptsächlich bei der Entscheidungsfindung bei dem Design von mobilen Unternehmensapplikationen unterstützen und ihnen helfen, Problembereiche der mobilen Sicherheit zu verstehen. Somit bietet das vorgeschlagene Framework ein Konzept für den Wissenstransfer im Bereich der Sicherheit, um das Sicherheitswissen von Sicherheitsexperten auf Nicht-Sicherheitsexperten zu übertragen. Darüber hinaus fördert die durch das Framework geschaffene Sicherheitstransparenz die vertrauenswürdige Nutzung von mobilen Endgeräten im Geschäftsbereich. Das

Framework wird unter Berücksichtigung seinen Leitfäden entwickelt und mit einem Metamodell angereichert, welches seine Komponenten und ihre Beziehungen beschreibt. Schließlich wird das Framework (das Artefakt) deskriptiv durch detaillierte Szenarien evaluiert, um seine Nutzbarkeit zu demonstrieren.

Abstract

Nowadays enterprises demand mobility and flexibility of their employees as inevitable success factors. Integrating mobile devices, namely smartphones and tablets, into the enterprise gives the employees the ability to work more productively. However, this integration has also brought new security challenges and risks. Despite all the advantages of mobility, many enterprises continue to be doubtful about it due to security concerns. Mobile devices are exposed to wide range of threats that have to be countered. Simply porting information security standards from workstations, notebooks, and server domains to mobile devices is unlikely to be effective. Thus, from an enterprise point of view, security levels are unclear on mobile devices. Generally, a high level of security might be attained on mobile devices by setting a high level of restrictions. On the other hand, this might minimize user acceptance and satisfaction factors.

To address the issues mentioned above, a conceptual framework that supports enterprises in adopting Mobile Enterprise Applications (MEAs) is proposed. A risk analysis with focus on mobile devices is conducted. During risk analysis, potential security threats are determined and assembled in a list, along with their likelihood of occurrence and harm impact on business. Each security threat is mapped to one or more security measures along with their consequences for mobile users. Furthermore, the proposed framework is enriched with a security check method, which checks if the security concept of MEA meets the security requirements needed to achieve a predefined security level.

This research is mainly intended to support enterprises in a decision-making process when designing MEAs and will help them to understand mobile security issues and classify the MEAs into security levels. Thus, the proposed framework provides a security knowledge transfer concept to transfer security knowledge from security experts to non-security experts. Moreover, the security transparency provided by the proposed framework promotes trustworthy usage of mobile devices in the business sector. The framework is developed along with its guidelines and enhanced with a meta-model that describes its components and their relations. Finally, the framework (the artifact) is evaluated descriptively by constructing detailed scenarios around it to demonstrate its utility.

Table of Contents

List of Abbreviations IX
List of Figures XIII
List of Tables XV
1 Introduction 1
1.1 Motivation 2
1.2 Problem Definition 5
1.3 Thesis Objectives 8
1.4 Thesis Structure 9
2 Background and Related Concepts 11
2.1 Mobile Technologies 11
2.1.1 Mobile Devices 11
2.1.2 Mobile Infrastructure 13
2.1.3 Mobile Operating Systems 14
2.2 Enterprise Mobility 16
2.2.1 Mobile Business Applications 16
2.2.2 Strategic Management and Mobile Strategies 19
2.2.3 IT Security in Enterprises 21
2.2.4 Information Security Standards and Catalogues 22
2.2.5 Mobile Security 24
2.2.6 Enterprise Mobility Management 28
2.3 Knowledge Management 33
2.3.1 Knowledge Classifications 33
2.3.2 Knowledge Conversion Modes 34
2.3.3 Knowledge Transfer 35
2.4 Summary 36
3 Research Methodology 37
3.1 Information Systems Research Framework 37
3.2 Employing Design Science in Research 39
3.3 Employing Behavioral Science in Research 44
3.4 Literature Review 44
3.4.1 Guidelines for Literature Review 45
3.5 Summary 47
4 Conception of Framework for Adopting Secure Mobile Enterprise Applications 48
4.1 Methodology 48
4.2 Framework Structure 50
4.2.1 Framework Meta-Model 52
4.2.2 Framework Guidance Model 52
4.2.3 Framework Decision Model 54
4.3 Framework Workflow and Guidelines 54
4.4 Requirement Definition 59

4.4.1 General Requirements 59
4.4.2 Functional Requirements 60
4.4.3 Non-functional Requirements 63
4.5 Framework User: Role Definition 64
4.6 Concept of Security Knowledge Transfer 65
4.7 Summary 67
5 Framework Data Structure 69
5.1 Risk Catalogue for Mobile Enterprise Applications 69
5.1.1 Overview 69
5.1.2 Mobile Business Scenarios 70
5.1.2.1 Mobile Customer Relationship Management 71
5.1.2.2 Other Use Cases for Mobile Enterprise Applications 72
5.1.3 Assets in Relevance to Mobile Enterprise Applications 73
5.1.4 Risk Catalogue Structure 76
5.1.5 Risk Estimation 77
5.1.6 Threats Categorization and Overview 78
5.1.6.1 Mobile Device Category 78
5.1.6.2 Mobile Applications Category 80
5.1.6.3 Mobile Operating System Category 82
5.1.6.4 Wireless Networks Category 85
5.1.6.5 Mobile User Category 87
5.1.7 Summary 89
5.2 Mobile Security Measures 90
5.2.1 Mobile Security Measures and their Consequences for Mobile Users 90
5.2.1.1 Authentication 91
5.2.1.2 Encryption 93
5.2.1.3 Containerization 97
5.2.1.4 Protection Software 99
5.2.1.5 Other Security Measures 99
5.2.2 Proposed Model for User Acceptance of Mobile Security Measures 103
5.2.2.1 Overview 103
5.2.2.2 Methodology 105
5.2.2.3 Proposed User Acceptance Model 107
5.2.2.4 Discussion 108
5.2.3 Summary 108
5.3 Security Levels for Mobile Enterprise Applications 109
5.3.1 Mobile Security Requirements 109
5.3.2 Security Level Definition 113
5.3.3 Summary 122
6 Prototypical Implementation and Evaluation 123
6.1 General Overview of the Prototypical Implementation 123
6.1.1 UML Class Diagram of CFMS Meta-Model 125
6.1.2 Main CFMS Interactions 127

6.1.3 Database Model of CFMS 129
6.2 CFMS Demonstration 130
6.2.1 CFMS Guidance Model 133
6.2.2 CFMS Decision Model 136
6.3 Evaluation 137
6.3.1 Functional Testing and Conducted Workshops 137
6.3.2 Business Scenarios from Praxis 140
6.3.3 Utilization of CFMS in Smart Cities Applications 143
6.3.3.1 Privacy Concerns in Smart Cities Applications 144
6.3.3.2 Problem Definition 146
6.3.3.3 Possible Utilization of CFMS in Smart Cities 147
6.4 Summary 150
7 Conclusion and Outlook 151
7.1 Research Summary 151
7.2 Outlook and Future Work 153
References 155
Publications 175
Appendix A 176
Appendix B 182
Appendix C 184
Appendix D 186

List of Abbreviations

4G	Fourth Generation
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
API	Application Programming Interface
AWC	Application-Wrapping Container
B2C	Business-to-Customer
B2E	Business-to-Employee
BI	Business Intelligence
BSI	Bundesamts für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CC	Common Criteria
CEMIS	Corporate Environmental Management Information Systems
CFMS	Conceptual Framework for Mobile Security
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
COBO	Corporate Owned, Business Only
COPE	Company Owned, Personally Enabled
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSS	Cascading Style Sheets
CYOD	Choose Your Own Device
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
EDGE	Enhanced Data Rates for GSM Evolution
EED	Enterprise-Enabled Device
EFS	Enterprise File Sharing
EMM	Enterprise Mobility Management
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning

ESC	Encrypted Space Container
FAR	False Acceptance Rate
FDE	Full Disk Encryption
FIBS	Federal Information Processing Standards
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HR	Human Resource
HSDPA	High Speed Downlink Packet Access
HTML	Hypertext Markup Language
IDC	International Data Corporation
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standards Organization
IT	Information Technology
ITU	Intention to Use
KM	Knowledge Management
LTE	Long Term Evolution
MAM	Mobile Application Management
MANET	Mobile Adhoc Network
MCM	Mobile Content Management
MDM	Mobile Device Management

MEA	Mobile Enterprise Application
MitM	Man-in-the-Middle
MMS	Multimedia Messaging Service
MNOs	Mobile Network Operators
MSM	Mobile Security Management
MSP	Mobile Service Provider
MTM	Mobile Trusted Module
MVC	Model-View-Controller
MVP	Mobile Virtualization Platform
NFC	Near-Field Communication
NGOs	Non-Governmental Organizations
NIST	National Institute of Standards and Technology
OHA	Open Handset Alliance
ORM	Object-Relational Mapping
OS	Operating System
OWASP	Open Web Application Security Project
PC	Personal Computer
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PEOU	Perceived Ease of Use
PIM	Personal Information Manager
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
POP	Post Office Protocol
PR	Perceived Restriction
PU	Perceived Usefulness
QR	Quick Response
RAM	Random Access Memory
RIM	Research In Motion
SD	Secure Digital
SECI	Socialization, Externalization, Combination and Internalization
SIM	Subscriber Identity Module
SMS	Short Message Service

SOAD	Service-Oriented Architecture Decision Modeling
SPs	Special Publications
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAM	Technology Acceptance Model
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UI	User Interface
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USB	Universal Serial Bus
UX	User Experience
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

List of Figures

Figure 1. Security professionals' biggest sources of concern related to cyber attacks 4
Figure 2. User satisfaction and security.....6
Figure 3. Thesis structure 9
Figure 4. Main mobile technologies 11
Figure 5. Mobile device communication mechanisms 13
Figure 6. Classification of apps in business 17
Figure 7. Types of strategies.....19
Figure 8. Factors that affect the adoption of MEAs 26
Figure 9. EMM overview 29
Figure 10. SECI model 34
Figure 11. Information systems research framework 38
Figure 12. Design science research process model 42
Figure 13. Framework for literature review 45
Figure 14. Risk management process 49
Figure 15. CFMS structure 51
Figure 16. Workflow of the CFMS 56
Figure 17. UML use case diagram of the guidance model 62
Figure 18. UML use case diagram of the decision model 63
Figure 19. Concept of security knowledge transfer within CFMS 65
Figure 20. Mobile enterprise infrastructure 71
Figure 21. Android version market share distribution among smartphone owners as of September, 2016 84
Figure 22. Share of Apple devices by iOS version worldwide in 2016 84
Figure 23. Abstract encryption model 95
Figure 24. App sandboxing. 98
Figure 25. Original technology acceptance model 104
Figure 26. Mobile devices' usage for work 106
Figure 27. Proposed user acceptance model.....107
Figure 28. Multi-dimensional view of security levels 116
Figure 29. CFMS meta-model as UML class diagram 125
Figure 30. Main interactions to create a new project 128
Figure 31. Main interactions to refine the guidance model 129
Figure 32. Database relational model of the CFMS 130
Figure 33. CFMS home page.....131
Figure 34. CFMS login screen.....131

Figure 35. Main page after logging as security expert 132
Figure 36. Main page after logging as non-security expert 132
Figure 37. Main page after logging as security expert 133
Figure 38. CFMS versions administration.....134
Figure 39. Management of guidance model versions.....134
Figure 40. Screenshot of administrating the content of the guidance model 135
Figure 41. Project list in the decision model 136
Figure 42. CFMS decision model – create a new project.....141
Figure 43. CFMS decision model – choosing a security level 141
Figure 44. CFMS decision model – presenting the security requirements.....142
Figure 45. CFMS decision model – overview on the project being created 143
Figure 46. Need of communications between public and private sectors 147
Figure 47. CFMS as communication interface between public and private sectors.....148

List of Tables

Table 1. Worldwide smartphone OS market share (share in unit shipments) 15
Table 2. MEA examples 18
Table 3. Most work-related information security standards and publications 22
Table 4. Smartphone secure development guidelines 27
Table 5. MDM functions 30
Table 6. MAM functions 31
Table 7. MCM functions 31
Table 8. MSM functions 32
Table 9. Design-science research guidelines 39
Table 10. Outputs of design science research 43
Table 11. Taxonomy of literature reviews 46
Table 12. CFMS guidance model's version types 62
Table 13. CFMS roles definition 65
Table 14. Excerpt of the results of the Statista's survey 66
Table 15. Potential assets associated to the usage of MEAs 74
Table 16. Risk catalogue structure 76
Table 17. Risk levels estimation matrix 77
Table 18. Adverse impact estimation matrix 78
Table 19. Potential consequences of applying mobile security measures and restrictions 103
Table 20. Internal consistency for the investigated factors 106
Table 21. Correlations between the constructs 107
Table 22. Interviewed enterprises 109
Table 23. Security requirements related to mobile communications 110
Table 24. Security requirements related to mobile OS 112
Table 25. Security requirements related to mobile applications 113
Table 26. Potential impact definitions for security objectives 114
Table 27. Possible definition of security levels 117
Table 28. Examples of personal information with assigned protection level 118
Table 29. Access matrix of an MEA regarding the possible access of personal data 119
Table 30. Security levels considering the legal dimension – an example 119
Table 31. Mapping security levels to security requirements 122
Table 32. Used software products for CFMS prototype 124

1 Introduction

Mobile devices usage has grown at a very fast rate in the past few years. These devices have developed from being an instrument that just offers the ability for making calls and sending SMS to becoming handheld devices (e.g. smartphones and tablets) that can run numerous applications. The spread of mobile devices has increased significantly. For instance, according to a study conducted by Statista, the number of smartphone users[1] in Germany reached 43.65 million in 2015, and it is predicted that this number will rise by 50 percent by 2022. Due to the constant advances in mobile technologies, and the ubiquitous availability of information through mobile devices, enterprises' employees demand mobile applications to support general business activities (Stieglitz & Brockmann, 2012).

In recent decades, Information Systems (IS) have become an essential component of successful enterprises. Such systems are implemented within enterprises for the purpose of improving the effectiveness and efficiency of that enterprise (Hevner, March, Park, & Ram, 2004). Enterprises have been implementing mobile applications that actually connect to their backend systems, such as Enterprise Resource Planning (ERP) (Jankowska & Kurbel, 2005; Lee, 2016; Stieglitz & Brockmann, 2012). They have been adopting mobile technologies to increase their operational efficiency (by providing employees access to real-time information), to improve their responsiveness and competitiveness, and to meet new customer demands (Unhelkar & Murugesan, 2010).

However, the involvement of mobile technologies and applications has also brought new security challenges and risks, particularly when using mobile devices[2] like smartphones and tablets that roam out the enterprise into insecure environments. Therefore, it has become crucial to address security concerns associated with this involvement. Hence, this work is devoted to addressing problems related to mobile security in the context of Mobile Enterprise Applications (MEAs). It provides the enterprises with a tool that supports them in mobile security management and designing of the security concepts of MEAs. The following presents brief definitions that help to understand the most frequent related terms, namely mobile device, threat, risk and security measure.

[1] Individuals of any age who own at least one smartphone. https://www.statista.com/statistics/467170/forecast-of-smartphone-users-in-germany/

[2] Within this research, the term "mobile device" namely refers to smartphones and tablets. On the other hand, the term "traditional computer" to all other computers like laptops and desktop computers.

According to (Souppaya & Scarfone, 2013), a *mobile device* is a device that has the following hardware and software characteristics:

- A small form factor
- At least one wireless network interface for network access (data communications). Such as Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)
- One or more digital cameras/video recording devices
- Microphone

As defined by ISO/IEC 17799, a *threat* is *"a potential cause of an unwanted incident, which may result in harm to a system or organization"* (ISO/IEC 17799, 2005). Such potential threats present security risks. Stoneburner et al. defined *risk* as *"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."* (Stoneburner, Goguen, & Feringa, 2002). To mitigate potential risks, suitable *security measures* have to be applied. There are many definitions of a security measure, however in this research mobile security measures can be in form of security methods, functions, mechanisms, restrictions, and enforced policies that have to be applied when using mobile devices for work purposes. These measures can be technical or organizational.

The rest of this chapter presents the motivation behind this research. Thereafter, it presents the research problem, research objectives, and the structure of the dissertation.

1.1 Motivation

Over the past few years, the evolution of mobile technologies and applications has made ubiquitous communications a growing reality (Basole & Rouse, 2006; Jain, A. K. & Shanbhag, 2012). According to (Internet Society, 2014), mobile broadband connections are forecast to continue growing worldwide to 5.3 billion in 2018, and mobile users will steadily

increase to reach 1.37 billion in 2017. Moreover, the number of mobile devices such as smartphones and tablets is increasing every year (Murauer, 2013).

The increasing advance of mobile technology and its usages, not only in private but in business sectors as well, triggered the enterprises to consider mobility as inevitable success factors in their business and develop IT strategies to derive more revenue, enhance customer engagement, and be more competitive in the market. An enterprise mobility concept is crucial when the enterprise integrates mobile technologies into its existing IT infrastructure to give its employees better possibilities to work on the move effectively (Ranjan & Bhatnagar, 2009). Enterprise mobility represents the next logical transition in mobile technology evolution, and will continue to gain more prominence in enterprises not just to improve the return on investment, but also to improve operational efficiency of their employees (Maan, 2012).

The reasons for this include for example location flexibility, time saving, portability and ease of research. For example, salespersons can access their mobile Customer Relationship Management System (mobile CRM) that allows them to update their customer details while they are away from their offices. Mobility gives enterprises many advantages. It enables ubiquitous real-time access to critical business information which supports the managers when making strategic decisions in a shorter time to satisfy their customers' needs. Consequently, mobility increases employees' productivity and reduces business operation costs (Hurley, Lai, & Piquet, 2011). Due to these advantages, enterprises demand mobility and flexibility of their employees (Detken, Diederich, & Heuser, 2011).

Many enterprises nowadays provide mobile versions of their desktop applications allowing access to their services via mobile devices (Zhauniarovich, Russello, Conti, Crispo, & Fernandes, 2014). However, many enterprises continue to procrastinate on mobility due to fear of security issues (Hardy, 2015; Hurley et al., 2011; Kaneshige, 2015). This is due to the pervasive nature of mobile technologies that might introduce new and significant risks to business. Thus, enterprises that allow use of mobile devices for work purposes have to pay increasing attention to a huge amount of new risks that differ clearly from traditional computer risks. Mobile devices have low technical capabilities in comparison to traditional computers. This hinders mobile devices from porting traditional computer security technologies and standards (Park, Yi, & Jeong, 2014; Wright & Poellabauer, 2012). Mobile devices are small and portable and therefore can easily be stolen or lost. Furthermore, as mobile devices become ubiquitous, risk in using them is increasing. They increasingly deal

with personal and business data, and roam in public networks with limited security and cryptographic protocols to protect the data (Kizza, 2015).

In this research, the most relevant definition of information security is taken from the ISO/IEC 17799 standard that defined it as follows: *"Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities"* (ISO/IEC 17799, 2005). The proposed research provides a tool that helps enterprises to assess the potential risks they face when adopting MEAs and it will determine the needed security measures to mitigate these risks. The key concern in MEAs is mobile application security including information confidentiality, integrity, and availability. This is due to the fact that in communications via mobile networks security threats can be present anywhere, and vulnerability to attack is higher than wired networks (Unhelkar & Murugesan, 2010). Kelton Research has shown that 75 percent of 250 surveyed companies, with revenues up to $100M across the United States and United Kingdom, considered security the major factor that prevents companies from adopting mobile applications (Hurley et al., 2011). Moreover, as stated by Wang and Xu, *"Enterprises need to understand the security challenges of supporting both work and personal data on a single mobile device and find a solution that balances the two effortlessly without compromising security or employees' privacy"* (Wang, H. & Xu, 2012).

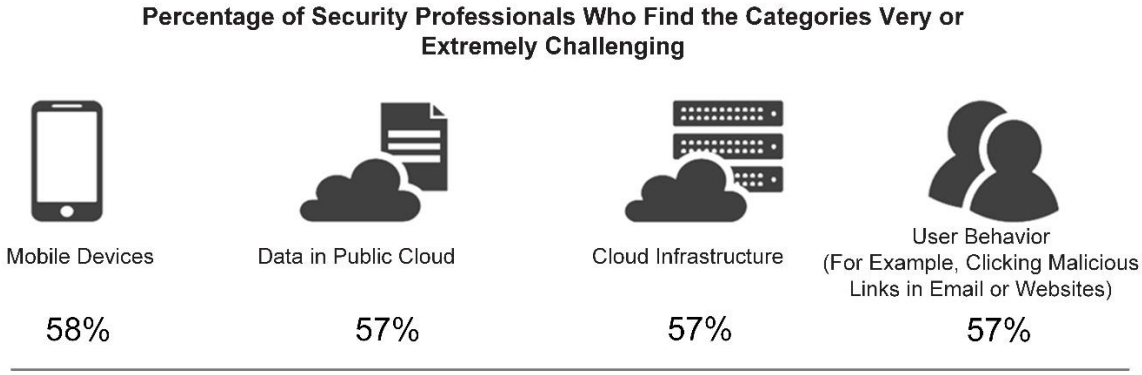

Figure 1. Security professionals' biggest sources of concern related to cyber attacks
Source: Cisco 2017 Security Capabilities Benchmark Study[3]

In addition, a security capabilities benchmark study conducted by Cisco in 2017 shows that security professionals who participated in this Study cited all the four elements depicted in

[3] https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

Figure 1 as top sources of concern when they think about their organization's risk of exposure to cyber attacks. Hence, the cloud is expanding the security perimeter, and users are a weak link in the security chain. Apparently, mobile devices are on the top of these sources of risk, since the proliferation of mobile devices creates more endpoints to protect. Although the number of mobile security threats is increasing almost exponentially, enterprises are not aware of the threats that mobile devices are exposed to, furthermore, mobile device security is still in its infancy and improvements have to be made to provide adequate protection (v Do, Lyche, Lytskjold, & van Thuan, 2015).

Security concerns as major factor that prevent enterprises from adopting MEAs form the motivation of this research to deliver a conceptual framework, which will help enterprises understand the mobile security issues, side by side with promoting trustworthy usage of mobile devices in business sectors.

1.2 Problem Definition

Mobile devices are exposed to a wide range of threats. Those devices usually have multiple interfaces, such as SD card, USB, Wi-Fi and Bluetooth for sharing data. This complexity of mobile devices places them at higher exposure to threats than traditional computing devices (Souppaya & Scarfone, 2013). Therefore, to overcome these potential threats and to mitigate potential risks, appropriate mobile security measures have to be applied. Due to the significant resource constraints of mobile devices, many security measures from traditional computing domains do not translate well to mobile devices. In other words, simply porting standard information security tools from stationary computers, notebooks, and server domains to mobile devices is unlikely to be effective (Landman, 2010; Wright & Poellabauer, 2012). Thus, from an enterprise point of view, security levels are unclear on mobile devices. Enterprises need to know which security level can be applied on mobile devices, and then they can decide which data can be transferred to mobile devices.

According to McKinsey & Company[4], 250 CIOs, who were surveyed on their mobility strategies, identified security as a major challenge and the primary barrier to broad mobile deployments within the enterprise (Akella, Brown, Gilbert, & Wong, 2012). Many

[4] McKinsey & Company is a global management consulting firm that serves leading businesses, governments, non-governmental organizations, and not-for-profits.

enterprises avoid adopting MEAs due to security fear, and are often unsure about the impacts on their business when using MEAs. Moreover, in order to achieve a certain level of security on any mobile device, the mobile user has to accept some restrictions on the features and functions supported by these devices. Examples for possible restrictions are: specifying exactly which applications are permitted to be installed, or restricting the types of connections that a third-party application can establish. The employee who wants to access very critical information using mobile devices, might accept a wide range of restrictions. However, these restrictions might be not acceptable in the case that the employee has no need to access such critical information. Generally, a high level of security can be reached on mobile devices by setting a high level of restrictions. But, on the other hand, this might minimize user acceptance and satisfaction factors.

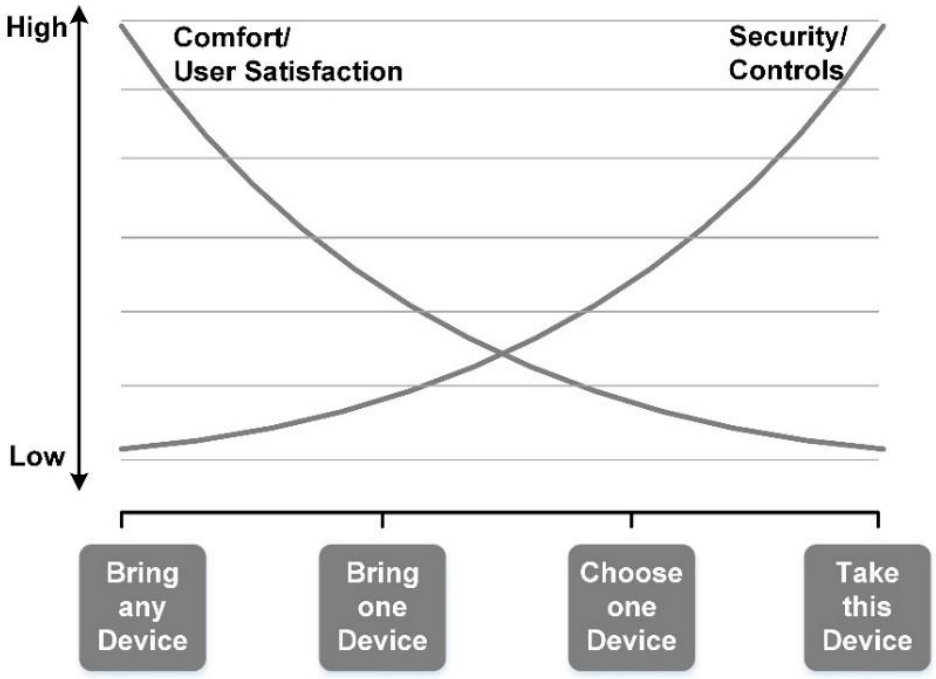

Figure 2. User satisfaction and security
Source: Adapted from (Disterer & Kleiner, 2014)

Figure 2 shows the opposition between user satisfaction and security controls. In the variant "take this Device", mobile devices are provided and set up by the enterprise. This variant is extended through "Choose one Device", where the employee can choose between a variety of mobile devices, which are provided and set up by the enterprise. These two variants can provide a high level of security, but low user acceptance. On the other hand, in the two variants, "Bring one Device" and "Bring any Device", the enterprise allows employees to use their private mobile devices at work. These later variants provide a high level of

usability, but low security. These variants are referred to as mobile strategies (see Section 2.2.2). Thus, a balance between usability (user view) and security (technical view) should be carefully taken into account when adopting MEAs. Achieving this balance is considered as a serious dilemma for CIOs and security professionals (Landman, 2010).

Applying high restrictive security measures on mobile devices would drive users away and/or encourage them to find other less secure alternatives that will eventually compromise enterprise data (Jaramillo, Furht, & Agarwal, 2014). An example is when the user forwards his business emails to his private email address that can be accessed on his private mobile device.

There are many existing standards, catalogues and guidelines, mostly targeting IT security professionals (see Sections 2.2.4, 2.2.5 and 5.1.1), and therefore they are too complex for business users or users who do not have specialized know-how in security. This research is devoted to supporting enterprises, when adopting MEAs, with a conceptual framework that can also be utilized by non-security specialists without requiring high levels of technical knowledge in mobile security.

Based on the afore-mentioned security issues concerning enterprise mobility, this research defined the following Research Questions (RQs):

- *RQ1*: How to support enterprises in improving their know-how in mobile security?
- *RQ2*: Which potential threats and risks may exist when using mobile devices for work purposes?
- *RQ3*: To what extent can MEAs be protected?
  - Which security level can be applied?
  - Which security measures can achieve the intended security levels?
  - What are the accompanying consequences for mobile users (employees)?
  - To what extent may these consequences be accepted by the mobile users?

To address the problem defined, and to answer the defined research questions, the following section defines the goals of this research.

1.3 Thesis Objectives

The main goal of this research is to develop a conceptual framework that supports the enterprises in the following aspects:

- Decision-making process when adopting MEAs
- Mobile security management
- Better understanding of mobile security
- Promoting the trustworthy use of mobile devices for work purposes
- Classifying MEAs into security levels

The proposed framework is role-based tool that enables the transfer of mobile security knowledge from security expert users to non-security expert users (users with little or no security expertise). Therefore, the content provided in this framework is administrated by security experts and made available to non-security experts in a simplified and structured way. This will significantly reduce the complexity of existing security catalogues and guidance for non-security experts. Moreover, sharing security knowledge within the enterprise will increase its employee's security awareness.

In addition, as complementary goals, this research analyzes potential risks related to the usage of MEAs, suggests suitable security measures together with their potential consequences and investigates how these consequences can affect employees' attitude towards using mobile devices for work purposes. Based on potential consequences, enterprises can survey their employees to get an insight about their acceptance rate, which will help the enterprises in selecting the security measures and keep a balance between security and usability. In this regard, an extension of Technology Acceptance Model (TAM) is presented.

Consequently, the framework provides a list of the potential mobile threats along with their likelihood of occurrence and their possible harm impact on business. Moreover, it also provides mobile security measures the enterprise can apply to mitigate the risks caused by potential mobile threats.

In addition, the framework enables the definition of security levels concerning MEAs based on three points of view, namely: business view (security requirements), technical view (security solutions) and user view (user acceptance). Each security level is mapped to a set

of mobile security requirements. Section 5.3 illustrates in detail how to define the required security level.

1.4 Thesis Structure

This thesis consists of seven chapters as depicted in Figure 3. Chapter one provides the introduction and includes the motivation behind this work, problem definition and research objectives.

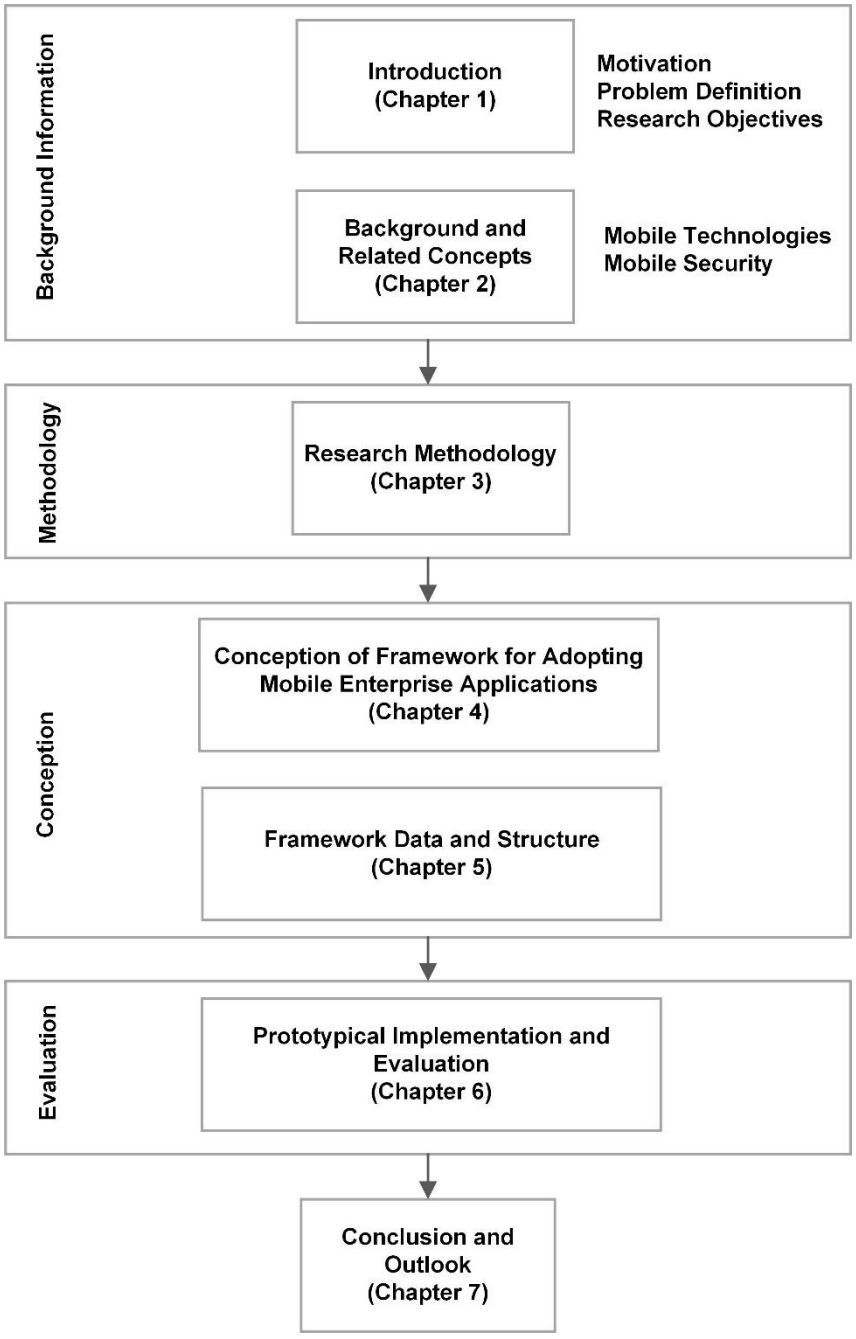

Figure 3. Thesis structure

An integrated overview on the main related concepts and technologies are placed in Chapter two, including mobile technologies (mobile devices, mobile infrastructure and mobile operating systems), mobile strategies and mobile security. That chapter also provides an overview of existing security standards, catalogues and guidance. It also illustrates the knowledge transfer concept.

Chapter three illustrates the research methods in design science research and presents the research methodology that has been followed to answer the identified research questions, and to achieve the main objectives of this research. The resulting artifact as a conceptual framework for mobile security is presented in Chapter four, including the framework structure, its workflow and its main requirements. Chapter five presents the framework content, including a risk catalogue for MEAs, mobile security measures and mobile security requirements.

Chapter six demonstrates the prototypical implementation of the resulting artifact as a web-based tool. It also presents the evaluation conducted, in which the prototype is an essential tool to demonstrate business scenarios within workshops in enterprises.

Finally, the main contributions of this research as well as directions for future work are summarized in Chapter seven.

2 Background and Related Concepts

This chapter provides background information and overview of mobile technologies, enterprise mobility and mobile security needed to understand the main work-related terms and to define the research landscape.

2.1 Mobile Technologies

Mobile technologies can be categorized into three main types, namely, mobile devices, mobile infrastructure and mobile software (Sathyan, Narayanan, Narayan, & K V, 2013) (Basole, 2007; Sahd & Rudman, 2016). Figure 4 summarizes the main mobile technologies and the principal components that form the core elements of mobile solutions.

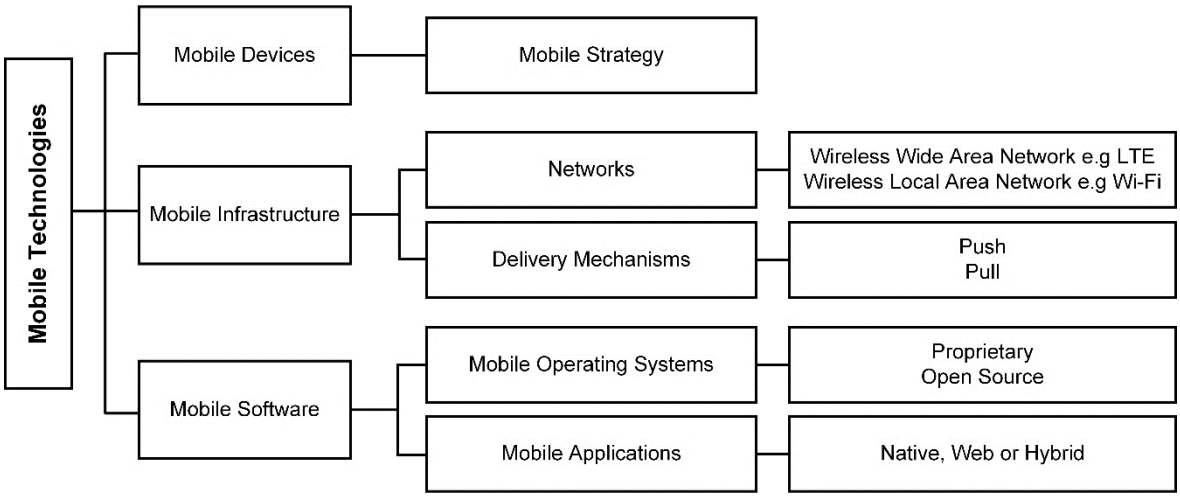

Figure 4. Main mobile technologies
Source: Adapted from (Sahd & Rudman, 2016)

The following section illustrates these mobile technologies in more details. Mobile applications are illustrated in Section 2.2.1.

2.1.1 Mobile Devices

The first mobile devices started to appear in the late 1970s, such as the early mobile phones that have very little in common with today's mobile devices, apart from the ability to make phone calls (Téllez & Zeadally, 2017). However, mobile devices are no longer only simple devices for voice communication. In 2005, Roth differentiated between five categories of mobile devices, namely, mobile Standard computer (like Notebook, Laptops, Tablets), on-

board computer (e.g. computers in vehicles) , Handhelds (e.g. Personal Digital Assistant (PDA) and Smartphones), Wearables (e.g. wristwatches) and Chipcards (e.g. Smart Card) (Roth, 2005). However, due to the further development of mobile devices, currently no clear distinction can be drawn between the afore-mentioned categories. Hence, in 2012, Kersten and Klett described new categories of mobile devices as follows (Kersten & Klett, 2012):

- Notebooks und Netbooks; as devices with powerful hardware. They are comparable to a classic desktop Personal Computer (PC) and use keyboard and mouse/touchpad as input peripherals. They run operating systems that are identical to that of a classic desktop PC (e.g. Windows or Linux).
- Tablet Computers; like notebooks, but have a touch display and can be operated with the fingers or touch pens.
- Smartphones; further development of classical mobile phones, usually operated via a touch display. These devices run smartphone-specific operating systems (e.g. Android or iOS) with numerous standard functions (calendar, e-mail client and media functions). Furthermore, the range of smartphone's functions can be considerably extended by its apps.
- Tablets; large smartphones in A5 format, but have more powerful hardware. They normally use the same apps as smartphones.

In recent years, the proliferation of mobile devices has increased significantly (Stieglitz & Brockmann, 2012). There are many definitions for the term "mobile device". For instance, as any handheld device, such as smartphones, tablets, e-reader, PDA, and portable music players with smart capabilities. However, the present work considers the definition presented in Chapter one, and therefore, focuses on smartphones and tablets as mobile devices. Mobile devices such as laptops are out of the scope of this work because the security controls available for laptops today are different to those available for smartphones, tablets, and other mobile device types (Souppaya & Scarfone, 2013), and they therefore provide a different experience. Moreover, this work also does not consider mobile devices with minimal computing capabilities such as featured phones because of the limited security options available for such devices and because of the limited threats they face.

Figure 5 explains the main communication mechanisms a mobile device might be equipped with, namely, Global Positioning System (GPS), Wi-Fi, Bluetooth, Subscriber Identity

Module (SIM), cellular, Near-Field Communication (NFC), Secure Digital (SD) card and power and synchronization cable.

Increasingly, mobile devices have become a usual part of everyday life. As reported by Gartner, global sales of smartphones to end users totaled 403 million units in the fourth quarter of 2015, a 9.7% increase over the same period in 2014 (Gartner, 2016). Gartner also reported that global mobile data traffic is predicted to reach 173 million terabytes (TB) through 2018, an increase of over 300% from 2014 (Gartner, 2015).

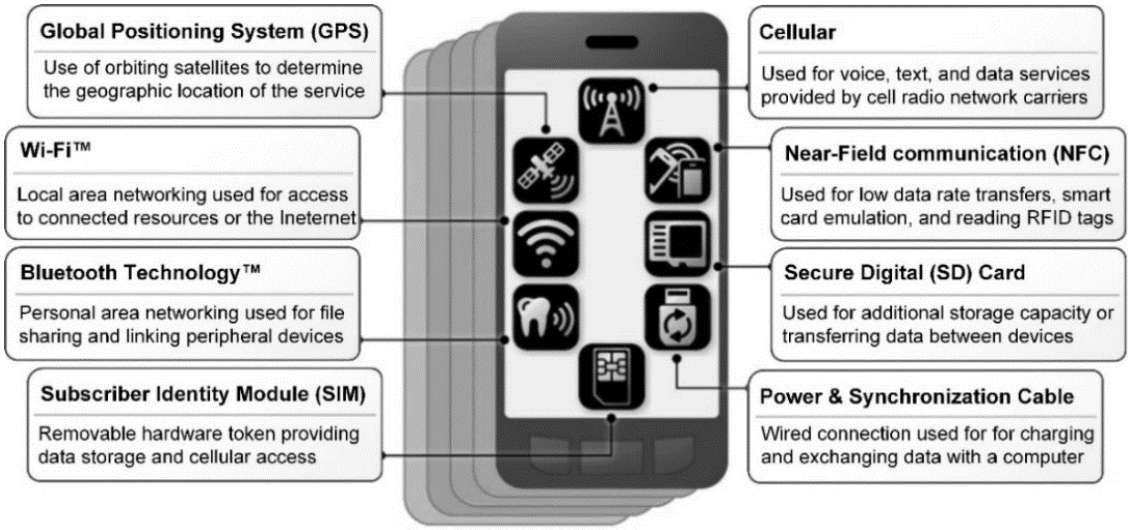

Figure 5. Mobile device communication mechanisms

Source: (Franklin et al., 2016)

In the rest of the thesis, the term "mobile devices" refers to smartphones or tablets. Nowadays, enterprises enable the usage of mobile devices for work purposes, and they apply different strategies for using mobile devices. These strategies are explained in Section 2.2.1.

2.1.2 Mobile Infrastructure

The core component of mobile infrastructure is wireless network as it facilitates location-independence and ubiquitous computing. One type, Wireless Local Area Network (WLAN), has achieved great popularity in enterprises. WLAN is described in the IEEE 802.11 standards that integrate a variety of security measures, including the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) protocols (Makki, Reiher, Makki, Pissinou, & Makki, 2007). Moreover, WLAN security standards include authentication of WLAN clients and data encryption and integrity within a WLAN network (Sauter, 2018).

However, despite these security measures, WLAN networks are considered to be significantly less secure than wired networks (Makki et al., 2007).

Mobile communications rely on wireless communication which has its roots in radio communication, and the first radio transmission, which was pioneered in 1895 (Pattnaik & Mall, 2015). However, the evolution towards mobile communication began in the 1980s with the introduction of the Global System for Mobile Communications (GSM). By extending the GSM standard, the General Packet Radio Service (GPRS) has created the basis for packet-based data transmission. Afterwards, the Enhanced Data Rates for GSM Evolution (EDGE) technology has increased data transmission rates and improved latency in data communications. GPRS and EDGE were followed by the Universal Mobile Telecommunication System (UMTS) and High Speed Downlink Packet Access (HSDPA) technologies, which brought further improvements in terms of possible data transmission rates and speeds. The current and latest technology today is Long Term Evolution (LTE), which represents a completely new transmission method compared to the other technologies and enables higher data transmission rates (Sauter, 2018).

To transmit data on wireless networks, delivery mechanisms are used. On the one hand, push mechanisms broadcast data to multiple users where the request for a given transaction is initiated by central server. On the other hand, pull mechanisms transmit data to the client when it initiates request for the transmission.

2.1.3 Mobile Operating Systems

A mobile Operating System (mobile OS) is an OS that is exclusively designed to run on a mobile device, such as smartphone and tablet. Thus, the mobile OS is the underlying technology that controls the mobile device and its capability directly impacts the device functionality (Ciaramitaro, 2012). The most common mobile OSes are Symbian from the Symbian foundation, Android from Google, iOS from Apple, RIM Blackberry OS, and Windows Mobile from Microsoft (Ciaramitaro, 2012).

However, the popularity of operating systems available for mobile devices has changed dramatically since their introduction. Suppliers who had high market shares in the early years are barely or no longer active today. According to a market study conducted by International Data Corporation (IDC), Android and iPhone Operating System (iOS) are the leading mobile operating systems. Table 1 shows the worldwide market share of smartphone operating

systems. The following briefly describes the most prominent mobile operating systems, Android and iOS:

Android[5]*:* Google's mobile OS. It is an open-source platform that runs on the Linux kernel and can be used and adapted by anyone. Android has also been adopted by the Open Handset Alliance (OHA) that includes large manufacturers such as Samsung, Sony and HTC (Rowles, 2014). Due to the open source platform and the cost-effective development of its apps, Android has become widely used. One of the fastest tools for building apps on every type of Android devices is Android Studio[6].

Period	Android	iOS	Windows Phone	Others
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%
2016Q4	81.4%	18.2%	0.2%	0.2%
2017Q1	85.0%	14.7%	0.1%	0.1%

Table 1. Worldwide smartphone OS market share (share in unit shipments)
Source: IDC, May 2017[7]

A challenge that comes with managing Android is the different versions available in the market. Since many manufacturers and mobile service providers make special adjustments to the operating system, it takes some time until the latest versions and patches for mobile devices are provided (Verclas & Linnhoff-Popien, 2012).

iOS[8]*:* The OS for the iPhone. It was designed by Apple and first released in version 1.0 with the first-generation iPhone in June 2008 (Morrissey, 2010). At the time of writing, the latest Version of iOS is version 11.4.1. iOS is structured on the Mac OS X operating system offering features that are pertinent to mobile devices such as iPhone and iPad (Silberschatz, Galvin, & Gagne, 2014). In contrast to Android, iOS is a closed-source platform that was designed exclusively for Apple-developed mobile devices. Thus, device selection is limited

[5] https://www.android.com/
[6] https://developer.android.com/studio/
[7] https://www.idc.com/promo/smartphone-market-share/os
[8] https://developer.apple.com/ios/

to Apple devices, and this in turn makes mobile device centralized management for enterprises easier than with Android mobile devices (Pierer, 2016).

2.2 Enterprise Mobility

This proliferation of mobile devices and the rapid development of mobile technologies are reinventing the way people interact and work. As more consumers invest in mobile devices, enterprises are being confronted and challenged by employees who want to use these devices for their work in addition to their personal life. So, the consumerization of IT does not only describe the process whereby information technology is developed primarily for corporate tasks and later passes into the consumer market, but also means that corporate IT today is confronted with the expectations of users from the consumer market (Kolbe & Ruch, 2014). Moreover, as predicted by the market research company IDC, the number of enterprise applications optimized for mobility will quadruple by year 2016 compared to year 2014, and IT organizations will dedicate at least 25% of their software budget to mobile applications by year 2017 (IDC, 2014). The consumerization of IT and the mobilization of business processes have been the main trends for the emergence of enterprise mobility.

The key enablers of enterprise mobility are mobile devices that run MEAs, which enable ubiquitous access to corporate data. The following subsections first present the types of mobile business applications and then the mobile strategies an enterprise can apply when adopting MEAs.

2.2.1 Mobile Business Applications

In general, mobile application software is typically known as mobile apps, most of these categorized into games, utilities, news, entertainment, social networking, and life style. In the mobile computing domain, there are three main development paradigms for mobile apps, namely, web apps, native apps, and hybrid apps (Budiu, 2013).

First, mobile web apps are web applications that have been customized and formatted for mobile devices to be accessed through the web browser of a mobile device. Such apps are developed by using web programming languages, such as Hypertext Markup Language (HTML5), Cascading Style Sheets (CSS3), and JavaScript APIs (Jobe, 2013). Since mobile web apps are browser-based, these types of apps are platform and device independent.

Second, mobile native apps are specifically designed and developed for a specific device platform, and can be installed manually from online AppStore of that platform. These apps are typically developed by Java for Android OS, Objective-C for iOS, or .NET framework for Windows Phone OS (Huy & van Thanh, 2012; Jobe, 2013). The third type, hybrid web apps, are neither truly mobile web apps nor native apps. They are basically written with the web technologies, HTML5, JavaScript APIs, and CSS, but they typically have access to the native device APIs and hardware. PhoneGap, Appcelerator, and Appspresso are examples of well-known hybrid mobile frameworks (Jobe, 2013). This work does not distinguish between these mobile app types; however, the required security measures must be applicable for each type the enterprise intends to use. Checking if the recommended security measures are applicable for an app type is out of scope of this work.

Nowadays, there are a huge variety of possible mobile applications, which can be used in every department or field of function in an enterprise, e.g. Customer Relationship Management (CRM), Business Intelligence (BI) or Human Resource (HR). Typically, mobile business applications are focused on the Business-to-Customer (B2C) and Business-to-Employee (B2E) domains. Three main types of mobile business applications are differentiated according to the target group of users (Gröger, Silcher, Westkämper, & Mitschang, 2013). These are depicted in Figure 6. The first type is mobile applications for customers, e.g. apps for booking flight tickets. The second type is mobile applications for employees, e.g. mobile CRM (see Section 5.1.2.1) and the third is mobile applications for business partners, which support inter-organizational interaction, e. g. in supply chains.

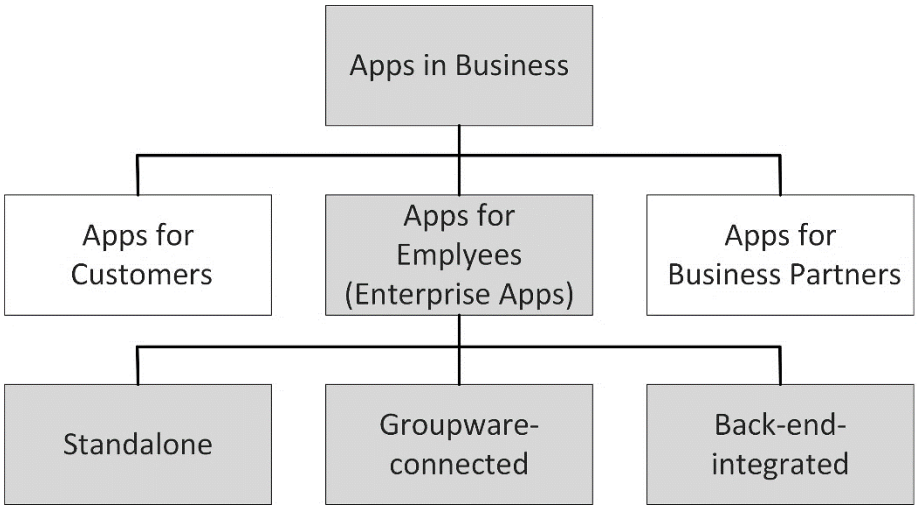

Figure 6. Classification of apps in business

Source: (Gröger et al., 2013)

Mobile applications for employees are further classified into three categories (Gröger et al., 2013): a) standalone mobile applications that are not integrated with a server-side and data storage, b) groupware-connected mobile applications that are linked with standard enterprise groupware systems, e. g., Microsoft Exchange, c) back-end-integrated mobile applications tightly integrated with the company's back-end, e.g. mobile ERP and mobile CRM.

This research focuses on mobile applications for employees, which are also called MEAs. Table 2 presents examples of MEAs.

MEA	Short Description
PIM Services (e.g. VMware Boxer[9])	Apps provide employees with e-mail, calendar and contacts functionalities.
Human Resource Apps (e.g. Sovanta iPeople[10])	Apps provide executives, managers and HR department the ability to quickly and easily access important personal information.
Sales Apps (e.g. Sovanta Sales Companion[11], SuperOffice Mobile CRM[12])	Apps support sales staff with important information about customers and current sales activities.
Apps for Approvals (e.g. SAP Fiori[13])	Apps offer employees and managers the functionality to approve orders or invoices.
Apps for Filesharing (e.g. Citrix ShareFile[14], Microsoft OneDrive for Business[15])	Apps provide employees with remote access to corporate data.
Apps for remote access (e.g. Citrix Workspace Receiver[16])	
Apps for top management (e.g. Sovanta Executive Cockpit[17])	Apps provide access to financial reports, key figures and committee documents for the top executives.

Table 2. MEA examples

[9] https://www.air-watch.com/capabilities/enterprise-email
[10] https://appadvice.com/app/sovanta-ipeople/410572272
[11] https://sovanta.com/index.php?p=reference-projects/sales-companion-2
[12] https://www.superoffice.com/features/mobile-crm/
[13] https://www.sap.com/products/fiori.html
[14] https://www.citrix.com/products/citrix-content-collaboration/
[15] https://onedrive.live.com/about/de-DE/business/
[16] https://www.citrix.com/products/workspace-app/
[17] https://sovanta.com/de/executive-cockpit

2.2.2 Strategic Management and Mobile Strategies

The term strategy can be understood as the orientation of an organization in order to achieve long-term goals (Johnson, G., Scholes, & Whittington, 2011). Strategic management deals with the planning and implementing of strategies and involves the understanding an organization's strategic position, including strategic choices for the future (Johnson, G. et al., 2011). According to Mintzberg, a distinction can be made between two types of strategies, namely, planned strategies and unplanned strategies (Mintzberg, 1978). The planned (or intended) strategy is deliberately developed by managers. On the other hand, strategies that emerge in an unplanned way are referred to as emergent strategies. Emergent strategies were never intended from the outset and arise by chance. An emergent strategy, once recognized, becomes a deliberate strategy. The phenomenon of employees bringing their private devices to work is a good example of emergent strategy (Brodin, 2016).

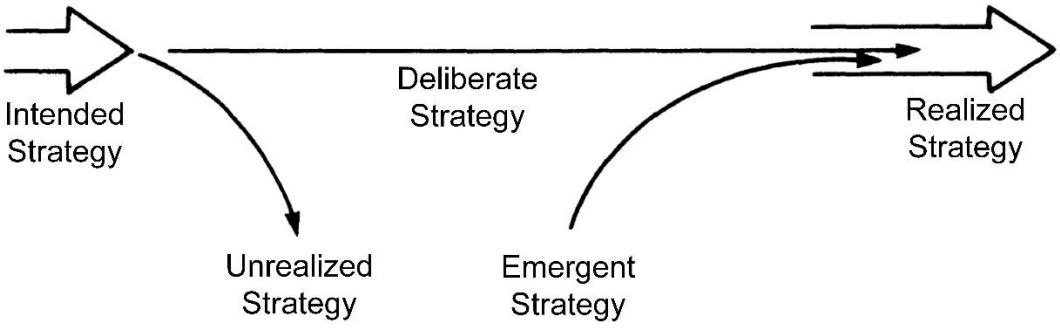

Figure 7. Types of strategies
Source: (Mintzberg, 1978)

Enterprise mobility enables employees to remotely access and update enterprise databases from any location at any time by using MEAs. However, this can not be achieved by merely equipping employees with mobile devices, but organizational strategies have to be developed to allow mobile access to relevant enterprise systems (Stieglitz & Brockmann, 2012).

Many enterprises have already started to make MEAs available to their employees applying different strategies. Basically, there are three main strategies enterprises can apply when using mobile devices for business purposes. In the first, enterprises provide their employees with corporate-owned mobile devices that can be used for business only. This strategy is called "Corporate Owned, Business Only" (COBO), in which, employees are only allowed to use the mobile device for business purposes. In addition, this strategy is usually accompanied by strong restrictions and limitations, so that employees, for example, are not

authorized to install third-party mobile applications on these devices. This strategy is mostly applied today to set strong security restrictions for highly sensitive business areas. To increase user acceptance, other strategies such as "Bring Your Own Device" (BYOD), "Choose Your Own Device" (CYOD) or "Company Owned, Personally Enabled" (COPE) can be applied (Disterer & Kleiner, 2014). On the one hand, the Bring Your Own Device (BYOD) strategy allows employees to access to corporate data from their private mobile devices, e.g. access to e-mails, calendars, databases (Kohne, Ringleb, & Yücel, 2015). On the other hand, in the Corporate Owned, Personally Enabled (COPE) strategy, enterprises provide their employee with corporate-owned mobile devices with an explicit permission for private usage of these mobile devices. The term Choose Your Own Device (CYOD) is often used as a synonym for the COPE strategy. CYOD offers the employee a choice from a portfolio of mobile devices (Disterer & Kleiner, 2014).

According to (Oluwatimi, Midi, & Bertino, 2017) these strategies are collectively considered as an Enterprise-Enabled Device (EED) scenario, where the same mobile device is used for personal and business purposes. This thesis considers the EED scenario when extracting the risk catalogue (see Section 5.1), mobile security requirements (see Section 5.3.1) and mobile security measures (see Section5.2).

Enterprises should enroll the mobile devices in an Enterprise Mobility Management (EMM) System (see Section 2.2.6). This provides the enterprise the ability to deploy, control, manage, and grant or deny privileges to secure containers (Oluwatimi et al., 2017). Some of these systems operate at the application level, whereas others are integrated into the mobile OS (Asokan et al., 2013). EMM systems can apply security measures in form of restrictions to the mobile device's usage, e.g. prohibition of the installation of certain mobile apps (e.g. for the use of social networks) or they might enforce a complex password for unlocking the mobile device. These measures usually lead to low user acceptance, which in turn can affect the user decision for using their mobile devices for business (Kolbe & Ruch, 2014). However, enterprises have to consider the usability factor when choosing their mobile strategy. In other words, security measures might have consequences that can affect both usability and security (see Section 5.2.1). These consequences should be considered when choosing a mobile strategy.

2.2.3 IT Security in Enterprises

IT systems process a huge amount of business information and make an important contribution to the business success of enterprises. The number and interconnection of these systems is constantly increasing. Furthermore, IT services and data can be accessed almost anytime and anywhere via mobile devices, and are often accessible via the Internet. The distributed storage of data and information is leading to an increasing importance of IT security, especially from the enterprise point of view (Grünendahl, Steinbacher, & Will, 2012). IT security is basically about security in information technology, taking into consideration business processes and legal compliance with data protection requirements (Kersten & Klett, 2012).

IT security aims to protect the availability, the confidentiality and the integrity of data and systems (Grünendahl et al., 2012). A loss of availability can happen when the required information is no longer available, because it has been deleted or the system is unavailable or partly unavailable. The loss of access rights to some information also lead to a loss of availability. Confidentiality means that the information is only accessible and available to authorized persons. A loss of confidentiality occurs when unauthorized persons have access to confidential information. Confidentiality is usually threatened by security gaps in IT systems, hacker attacks or poorly secured communication channels that allow data and information to be spied on. Integrity of data means the modification of data can be done by authorized persons only. To achieve data integrity is to guarantee that data can be added, modified or deleted by an authorized group of persons only. Integrity can be threatened by malfunctions in IT systems or by malicious software (malware).

In order to achieve the security goals of availability, confidentiality and integrity when enterprise enables access to its corporate data through mobile devices, it has to apply suitable security measures on mobile devices and their mobile applications (see Section 5.2). These security measures help enterprises to protect their data against potential threats in mobile environments (see Section 5.1).

Enterprises have also to comply with legal and regulatory requirements, such as the requirements of personal data protection in complying with General Data Protection Regulation (GDPR[18]) that harmonizes data privacy laws across Europe (see Section 5.3.2).

[18] https://gdpr-info.eu/

Furthermore, risk management is a prerequisite to consider in all the aspects of security in enterprises. There are standards for information security management which are intended to help enterprises keep information assets secure. The following section presents the main related standards.

2.2.4 Information Security Standards and Catalogues

There are an enormous number of information security standards that help as guidelines for IT security professionals when developing or implementing IT projects. This section presents the most relevant information security standards that can improve the information security of organizations, with a summarized overview in Table 3.

Standard	Title	Notes
ISO/IEC 27001[19]	Information technology — Security techniques —Information security management systems — Requirements	It defines the basics of building and controlling an ISMS, helps enterprises to identify appropriate security controls and use ISMS to mitigate business risks
BSI standard 100-1	BSI Standard 100-1 Information Security Management Systems (ISMS)	Defines general requirements for an information security management system (ISMS) and it is compatible with the ISO/IEC 27001
BSI standard 100-2	BSI-Standard 100-2: IT-Grundschutz Methodology	Provides methodology for effective management of information security, based on the BSI-Standard 200-1
NIST SP 800-53[20]	Security and Privacy Controls for Federal Information Systems and Organizations	Provides guidelines for selecting security controls for organizations and systems supporting the executive agencies of the Federal Government to meet the requirements of FIPS Publication 200[21].
FIPS PUB 199[22]	Standards for Security Categorization of Federal Information and Information Systems	Provides a standard for categorizing Federal information and information systems according to confidentiality, integrity, and availability and the potential impact on organizations in case of losing them.

Table 3. Most work-related information security standards and publications

[19] https://www.iso.org/isoiec-27001-information-security.html
[20] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
[21] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
[22] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

The most popular information security standard is ISO/IEC 27001, which is a part of the ISO/IEC 27000 standards family. ISO 27001 is an international standard published by the International Standardization Organization (ISO) and was first published in 2005. The standard is characterized by the principle of continuous improvement in the form of the Plan-Do-Check-Act model (PDCA model) (Kersten & Klett, 2016). It is more of a process-oriented model and does not describe concrete security measures, but merely formulates requirements for an Information Security Management System (ISMS). Its appendix contains a catalogue of security controls, however the selection of the appropriate measures is left to the enterprise (Kersten & Klett, 2016). ISO/IEC 27002 contains further notes and examples on these controls that can help in the selection of individual measures.

Further standards for information security are standards published by BSI, the German Federal Office for Information Security (German: Bundesamts für Sicherheit in der Informationstechnik, abbreviated as BSI). The BSI Standards[23] contain recommendations by the BSI on methods, processes, procedures, approaches and measures related to information security. BSI standard 100-1 defines the general requirements for an ISMS and it is completely compatible with ISO Standard 27001. Moreover, BSI has developed an IT-Grundschutz methodology that describes how information security solutions can be selected, developed and tested based on standard security measures (BSI, 2008). This methodology has been published as BSI standard 100-2.

When it comes to information security standards, the National Institute of Standards and Technology (NIST) publications are also often mentioned. These publications include a specific set of Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) that are related to information security and risk management. Table 3 briefly presents the most relevant standards in publications of NIST and FIPS to this work.

Beside the afore-mentioned standards, there are international frameworks for IT management and governance that have an extended view of information security perspectives. An example of such frameworks is the Control Objectives for Information and Related Technologies (COBIT) framework in version 5 - the latest version at the time of writing. COBIT[24] was introduced in 1996 by the Information Systems Audit and Control

[23] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/it_grundschutzstandards.html
[24] http://www.isaca.org/cobit/

Association (ISACA), which is a framework that helps organizations by developing a clear IT strategy and by implementing best practices and procedures for IT management (Krcmar, 2015). COBIT 5 for Information Security[25] is an extended overview of information security and aims to be an umbrella framework to connect to other information security standards such as NIST SP 800-53.

The above-mentioned standards and catalogues are general and can be applied to different enterprises in different situations. However, the problem here is that such standards are too general to easily be applied when dealing with a specific problem (Brodin, 2016; Doherty & Fulford, 2005). To provide more specificity, catalogues and guides that focus on mobile security are presented in the following section.

2.2.5 Mobile Security

In general, mobile security refers to the efforts needed to secure data on mobile devices. Enterprises must consider mobile security to retain control over their sensitive information when accessed via mobile devices. Due to the proliferation of such devices, security has increasingly become a crucial feature required when using mobile technologies. Since mobile devices might hold valuable, sensitive, and possibly classified information, they face the same or higher levels of attacks and threats which affect the desktop computing environment (Téllez & Zeadally, 2017).

Compared to traditional computing domains like PCs, mobile devices have different security principles. Thus, mobile security is distinguished from traditional computer security in the following main ways (Daojing He, Chan, & Guizani, 2015; La Polla, Martinelli, & Sgandurra, 2013; Téllez & Zeadally, 2017):

- Mobility: Mobile devices have high mobility, which increases, in comparison with stationary devices, the chances of loss, or physical tampering.
- Strong Personalization: Mobile devices are strongly personalized, and they are normally operated by a unique user and are usually not shared among multiple users, while computers often are.

[25] https://www.isaca.org/COBIT/Pages/info-sec.aspx

- Strong Connectivity: They have strong connectivity accessing various Internet services, connected to large number of interfaces (such as SD-cards, USB, Bluetooth), and using different types of communication (such as Wi-Fi, UMTS). Thus, their vulnerability to malware is increased through this variety of channels.
- Technology Convergence (a single device combines different technologies): Today mobile devices integrate numerous functional features (such as gaming, video and data sharing, and internet browsing). These features can be used by attackers to exploit various routes to execute their attacks.
- Limited Resources and Reduced Capabilities: Compared with stationary devices, mobile devices have four major inherent limitations, namely, limited battery life, limited computing power, very small display screen size, and very small keys for inputting. These limitations create challenges for mobile security solutions.

This is emphasized by Tupakula and Varadharajan, "*Today mobile devices are increasingly being used to access data services in addition to the voice communications. However such devices have limited resources to enforce strong security measures and hence they are easily vulnerable to attacks.*" (Tupakula & Varadharajan, 2013). Moreover, mobile devices are not necessarily trustworthy, since most current mobile devices lack the root of trust features (e.g., trusted platform modules, TPMs) that are increasingly built into laptops and other types of hosts (Souppaya & Scarfone, 2013). There is also frequent jailbreaking and rooting of mobile devices, which means that the built-in restrictions on security are bypassed. Enterprises should assume that all mobile devices are untrusted unless the enterprise has properly secured them and monitors their security continuously while in use with enterprise applications or data (Souppaya & Scarfone, 2013).

Researchers stated that security is one of the biggest barriers to introducing mobile technology in enterprises (Gröger et al., 2013; Hoos, Gröger, Kramer, & Mitschang, 2015). Moreover, the Mobile Helix survey identified several impediments to the deployment of enterprise applications on mobile devices. These impediments, including the cost of development, concerns over security, increased support and maintenance costs and performance challenges, can slowdown the adoption of MEAs (McLellan, 2014). Figure 8 shows that 63 percent of the Mobile Helix survey respondents consider that security concerns are second only to development costs when an enterprise wants to adopt mobility.

Important sources for the IT security professional to improve mobile security within enterprises are in form of standards, catalogues and guidelines. Most of these sources are not dedicated for mobile security, however the following sources, which focus on mobile security, were found in the literature.

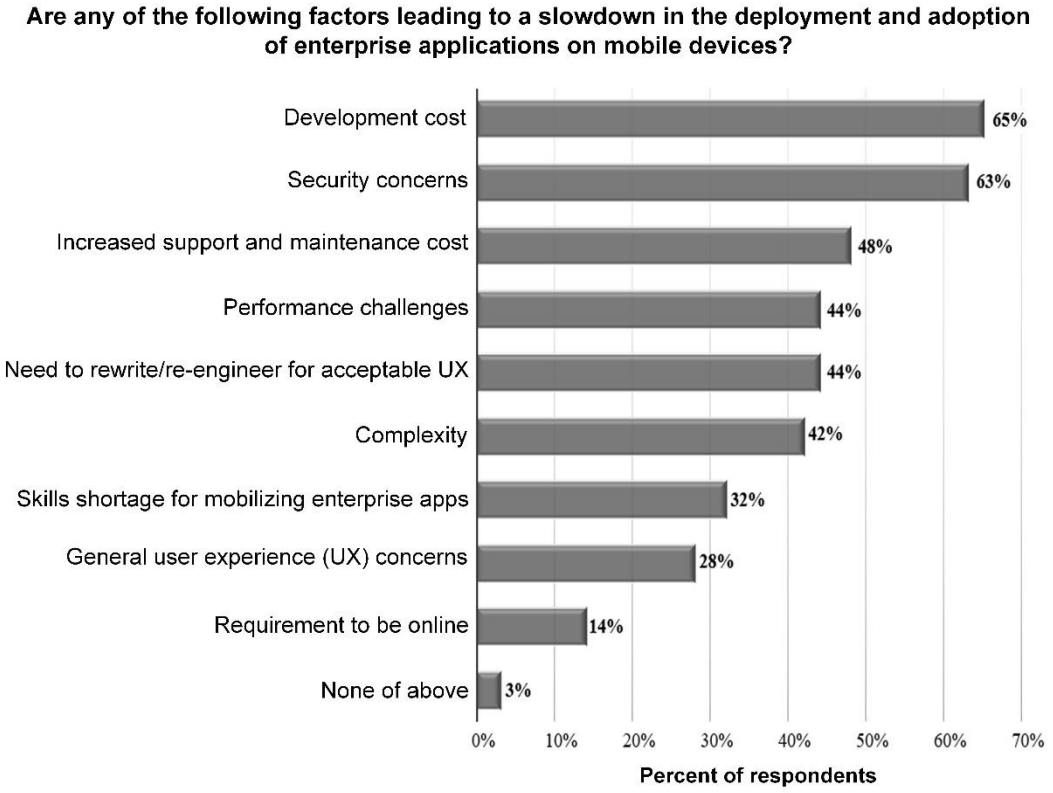

Figure 8. Factors that affect the adoption of MEAs

Source: (McLellan, 2014)

BSI Minimum Standard for MDM[26]: Security requirements for Mobile Device Management (MDM) systems are the focus of the minimum standard. Through its specification, the minimum standard sets a defined security level for the use of MDMs by the German Federal Government, where the MDMs providers and other interested parties may use this minimum standard to increase information security or to compare with what they offer. The use of an MDM is only one part of the overall concept of secure mobile work. Others are for example the selection of secure applications or the use of secure solutions for Personal Information Management (PIM) data processing.

Furthermore, the European Union Agency for Network and Information Security (ENISA[27]) report (Privacy and Data Protection in Mobile Applications) focuses on the concept of

[26] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/mindeststandards_node.html
[27] ENISA is a center of network and information security expertise for the EU. https://www.enisa.europa.eu/

privacy by design and it is especially centered around the mobile application developers and the secure development lifecycle (ENISA, 2017). ENISA also explored challenges specific to mobile application developers with regard to the processing of personal data. The report they published discussed the relevant key legal and regulatory issues arising from the use of mobile applications, these issues have been considered in this research in Section 5.3, where the significant effect of legal requirements on the selection of the security levels is discussed.

Another publication from ENISA that targets developers of mobile applications is "Smartphone Secure Development Guidelines", which provides a guide for developing secure mobile applications. It provides developers with 152 guidelines categorized in 13 categories as depicted in Table 4.The framework presented in the present research can be easily extended by including these guidelines and made available to mobile application developers only, so other user roles like business users will not be confused by these technical guidelines.

Category	**Number of Guidelines**
Identify and protect sensitive data on the mobile device	34
Implement user authentication, authorization and session management correctly	19
Handle authentication and authorization factors securely on the device	9
Ensure sensitive data is protected in transit	13
Secure the backend services and the platform server and APIs	8
Secure data integration with third party code	5
Consent and privacy protection	15
Protect paid resources	6
Secure software distribution	8
Handle runtime code interpretation correctly	6
Check device and application integrity	4
Protect the application from client-side injections	16
Ensure correct usage of biometric sensors and secure hardware	9

Table 4. Smartphone secure development guidelines

Source: Adapted from (ENISA, 2016)

Recent work that addresses the inherent threats of mobile devices has been presented by NIST in form of a mobile threat catalogue (Franklin et al., 2016). NIST has also published guidelines for managing the security of mobile devices in the enterprise (Souppaya

& Scarfone, 2013). Another guidance in mobile security is the OWASP Mobile Security Project[28] that intends to give developers and security teams the resources they need to build and maintain secure mobile applications. These guidelines and catalogues, from NIST and OWASP have been also considered in this research when extracting potential threats on MEAs and the needed security measures to overcome such threats. Whereas the catalogues and guidelines discussed above targets mobile security engineers, information system security professionals, mobile application developers or other technical staff like mobile OS developers and Mobile Network Operators (MNOs), the risk catalogue presented in this thesis mainly targets business users, who are mostly non-security experts.

Dealing with many security catalogues and guidelines, which are mostly technical, makes the administration of security knowledge within the enterprise hard and complex task. Such catalogues and guidelines form an important resource for security experts to extract security knowledge and administrate it within the framework presented in this thesis, in a structured and simplified way. This framework is intended to be a centralized tool to administrate and share mobile security knowledge within the enterprise.

2.2.6 Enterprise Mobility Management

The adoption of mobility is a critical success factor and is one of the central investment topics for many enterprises. It does not make sense to use mobile devices without a strategic foundation. Thus, a holistic approach, an Enterprise Mobility Management (EMM) system, is required to make business processes and data available via mobile devices (Wächter, 2016).

The management of mobile devices is distinguished from traditional device management, essentially in that the devices are not bound to a fixed location. EMM systems emphasize security and management of mobile devices, including their mobile applications and data (David, Singh Dikhit, Shrivastava, & Sawlani, 2017). It helps employees become more productive by helping them to perform work-related tasks and activities on their mobile devices. An EMM system involves four control areas, namely, Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM)

[28] OWASP stands for Open Web Application Security Project https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Home

and Mobile Security Management (MSM) (Pierer, 2016; Wächter, 2016). These areas are depicted in Figure 9.

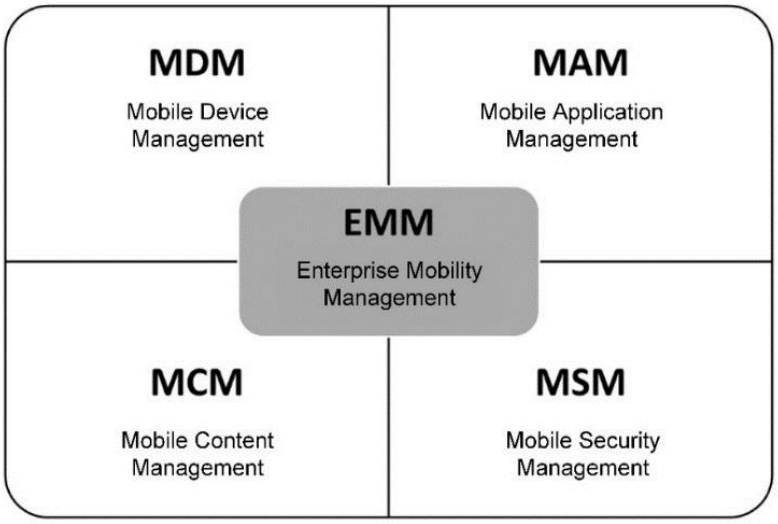

Figure 9. EMM overview

Source: (Pierer, 2016)

Mobile devices have an important feature so that they can be managed remotely via an MDM system. Furthermore, this system secures, monitors, manages and supports mobile devices deployed across an enterprise to optimize the functionality and security of a mobile communication network while minimizing cost and downtime. This applies to both corporate-owned and employee-owned devices across the enterprise (Johnson, M., 2011) (Pierer, 2016). Table 5 presents the main functions of MDM system.

MDM Function	Description
Mobile operating system support	MDM is typically a client/server architecture, where a mobile client is installed on mobile devices to communicate with the server and exchange relevant data. It indicates the supported operating systems for mobile device.
IMEI/IMSI status	Identifies the mobile device using International Mobile Equipment Identity (IMEI) – a unique serial number to determine which device is used by which user.
Roaming status	Controls the roaming status to determine which mobile network is used, e.g. mobile data transmission.
Battery status	Delivers information about battery consumption.
GPS localization	Global Positioning System (GPS) functionality to locate mobile devices, e.g. to find stolen or lost mobile devices.

Firmware information	Delivers information about the mobile OS, e.g. version number. This help to check if the OS is up to date.
Mobile device manufacturer/model	Deliver Information about the mobile device manufacturer.
Installed software and applications	Delivers detailed information about mobile applications installed on mobile device. This helps further to blacklist or whitelist mobile applications.
Service history	Shows the activities of the mobile device and the mobile user, e.g. which activities were done when and by whom.
Enrolment date	Indicates the date when a mobile device starts being controlled by an MDM.

Table 5. MDM functions

Sources: Adapted from (Pierer, 2016)

The second area of control is MAM, which applies management and policy control functionality to individual mobile applications that are then delivered via an enterprise app store and are managed locally on devices via the EMM console (Smith, Taylor, Bhat, Silva, & Cosgrove, 2017). Table 6 presents the main functions of MAM system.

MAM Function	Description
Application installation and background installation	The ability of installing mobile applications over MDM system. The installation can be done automatically in the background.
Corporate App Store	A store where MEAs can be provided to employees.
Application blacklist/whitelist	The installation of third-party apps can be prohibited or allowed.
Vendor AppStore deactivation	Public AppStore can be completely prohibited. The required apps can be provided in the corporate AppStore.
Mandatory applications	The deinstalling of mandatory applications is reported to the administrator.
Active sync/corporate exchange settings	When enterprise operates a Microsoft exchange server, parametrized settings can be rolled out to all employees automatically, to connect them to their mailboxes.
E-Mail management	The needed settings for IMAP or POP can be rolled out automatically to the employees.
Per App VPN	Per app VPN is used to grant mobile applications access to internal resources, where each mobile application connects itself to the internal infrastructure and receives and sends data over an encrypted tunnel.

Containerization/Sandboxing	Enforces the usage of special container application, e.g. Samsung KNOX to segregate the private from the business area.
App wrapping	Mobile applications can be wrapped with their own layer of security to control and monitor their usage.
Block copy/paste	Disallows copying and pasting files, folders or text between different mobile applications to avoid copying sensitive data from the business area to the private area.
App usage monitoring	Gathers information regarding usage, performance or availability of mobile applications.

Table 6. MAM functions

Source: Adapted from (Pierer, 2016)

The third area of control is MCM, which ensures that content (like data, media or documents) is made available on mobile devices, transmitted in encrypted form and synchronized. MCM also enables mechanisms for document exchange between employees and customers. In addition, MCM can use role-based authorization concepts to determine which employees can access which mobile applications in the corporate app store (Wächter, 2016). Table 7 presents the main functions of MCM system.

MCM Function	Description
Data management	Enterprises have to provide necessary content for the employee while they are on the move. For example, sales rep needs current sales material to provide customers with accurate offers.
PIM (Personal Information Management)	Administration of contacts, calendar, appointments and emails.
Document management software support	This function is important when an enterprise allows access to its document libraries and other relevant data via mobile devices.
Data synchronization	This function provides an automatic synchronization of data between mobile devices and enterprise backend system.
Data push	A mechanism to push important documents and files directly to a mobile device, in order to keep such data up-to-date.
Secure web browsing	As enterprises provide business relevant content to mobile users via internet, such content and especially the connection to internal resources need to be secured (e.g. encrypted).

Table 7. MCM functions

Source: Adapted from (Pierer, 2016)

Finally, the fourth area of control is MSM, which is a management approach for protecting and verifying mobile users through the enforcement of policies to registered mobile devices, in order to restrict or allow a defined level of settings (Pierer, 2016). The main functions of MSM are presented in Table 8.

MSM Function	Description
KIOSK mode	Mobile device can be used only under defined restrictions and functionalities.
Passcode/Password	This function defines the password policy that can be enforced. For example, enforce complex password with a certain number of alphanumeric letters, digits and special characters.
Mobile device reset	Administrator with privilege can reset the mobile device and wipe its data remotely.
Maintain mobile device lock	This function is important to lock the mobile device remotely to apply new configurations, e.g. to enforce an immediate passcode/password policy.
Prohibit application installation/uninstallation	Enterprises can prohibit the usage of certain applications, and prohibit the deinstalling of certain application, e.g. for mobile device monitoring purposes.
Maintaining certificates	The distribution of certificates that are used to establish a secure connection, and to identify users and provide them the needed privilege to use a certain application.
Mobile device encryption	The encryption of the on-device data. (see Section 5.2.1.2)
Device compromise detection (root/jailbreak)	Some users try to root their mobile device to get more privileges from the operating system. This function is important to detect rooted mobile devices and to define further security measures, e.g. data wipe or device reset.
Mobile VPN	A VPN profile has to be installed on the mobile device to enable secure connection to enterprise internal network.
Single-Sign On support	This function can enable the authorization of a mobile user on many applications with only one credential.

Table 8. MSM functions

Source: Adapted from (Pierer, 2016)

Although the above mentioned areas of management form the subsystems of the EMM system, almost all software vendors term their EMM products as MDM due to marketing aspects and the historical background (Pierer, 2016). Thus, within this thesis, both terms,

MDM and EMM, are used interchangeably. Examples of EMM vendors include Citrix[29], AirWatch[30], and MobileIron[31]. EMM solutions might be offered in two different variations, cloud based and in-house. Each variant has its own advantages and disadvantages regarding security and other factors, like costs and ease of integration to existing enterprise systems. Investigating the difference between both variants is out of the scope of this thesis. However, there is existing work that recommends requirements for MDM systems. For instance, BSI defined the minimum standard for the use of MDM systems (BSI, 2017). Through MDM and other subsystems of EMM, enterprises can apply security measures on mobile devices and enforce policies, and this is considered in this thesis in Section 5.2. Finally, the function scope provided by EMM can differ from one vendor to other. Thus, the framework presented in this thesis will help an enterprise with EMM selection by determining the necessary functions that fit its requirements.

2.3 Knowledge Management

As the framework presented in this research intends to manage and share mobile security knowledge within the enterprise, the present section provides the related definitions in the knowledge management domain. There are many definitions of the term Knowledge Management (KM), most of them are focusing on KM processes. KM is defined as the process of capturing, distributing, and effectively using of knowledge (Davenport & Prusak, 1998; Ponzi & Koenig, 2002). In other words, it is a collaborative and integrated approach to discover, capture, organize, access and reuse both tacit (in people's heads) and explicit (digital or paper based) knowledge as well as the cultural and technological means of enabling the KM process to be successful, to effectively use expertise (Bhatia & Mittal, 2009; Dalkir, 2005; Gasik, 2011).

2.3.1 Knowledge Classifications

Knowledge is often classified into two types, namely, tacit knowledge and explicit knowledge (Botha, Kourie, & Snyman, 2008; Nonaka & Konno, 1998). On the one hand, tacit knowledge is defined as personal know-how and it resides in the head of knower. It is

[29] https://www.citrix.com/
[30] https://www.air-watch.com/
[31] https://www.mobileiron.com/

the most valuable knowledge and represents expertise and know-how (Dalkir, 2005). On the other hand, explicit knowledge represents the knowledge that has been captured in a tangible form like words (Dalkir, 2005). This research focuses on these two types of knowledge, the tacit and explicit knowledge.

2.3.2 Knowledge Conversion Modes

To improve their knowledge, enterprises try to externalize or convert knowledge from tacit to explicit knowledge, after that they store this knowledge in their intranet or portal. Hence, efforts should be made to improve the sharing of this stored knowledge (Dalkir, 2005; Nonaka & Konno, 1998; Nonaka, Toyama, & Konno, 2000). Processes to transform between tacit and explicit knowledge have been presented by Nonaka et al. within a Socialization, Externalization, Combination and Internalization (SECI) model (Nonaka et al., 2000). This model is shown in Figure 10 showing four modes of knowledge conversion:

- *Socialization - Tacit to Tacit*. In this case, the knowledge is converted through shared experience such as spending time together or living in the same environment, or face-to-face meeting.
- *Externalization - Tacit to Explicit.* This is a process of articulating tacit knowledge into explicit knowledge by transforming the knowledge of people's minds into electronic forms like storing it in wikis, forums and collaborating systems.

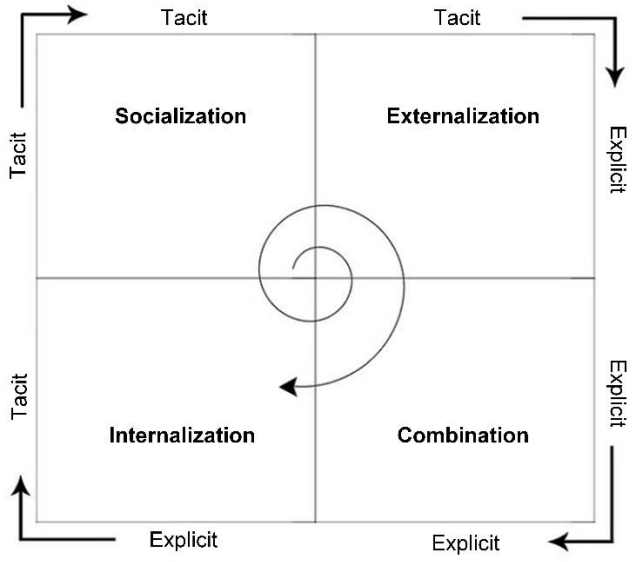

Figure 10. SECI model

Source: (Nonaka et al., 2000)

- *Combination - Explicit to Explicit.* The knowledge here is converted based on the desire of the user, e.g. from paper to electronic form.
- *Internalization – Explicit to Tacit.* The intranet of the enterprise allows the end users to access the information which is stored in the knowledge repository. In this mode, explicit knowledge is used and learned from by the user to extend her/his tacit knowledge.

2.3.3 Knowledge Transfer

Alavi and Leidner considered knowledge transfer as an act of communication between source (the sender of the knowledge) and receiver (where the knowledge is transferred to). Both sides of the communication channel can be represented by a single person, as well as a team of people (Alavi & Leidner, 2001; Gasik, 2011). Knowledge transfer is the conveyance of knowledge from one place, person or ownership to another, and then this process can be considered as successful when it has enabled a successful creation and application of the knowledge in the enterprise (Liyanage, Elhag, Ballal, & Li, 2009; Major & Cordey-Hayes, 2000). In the literature, the knowledge transfer process was described using models. Most of these models were focused on the idea of collaboration and communication between the source and receiver of the knowledge (Liyanage et al., 2009). Therefore, the basic knowledge transfer model consists of two main components namely: the source who shares the knowledge and the receiver who acquires the knowledge.

Normally, security knowledge transfer is practiced within enterprises by conducting security awareness training programs. Other approaches for security knowledge transfer focus on how to write secure code. For instance, OWASP developed a security knowledge framework[32] that provides checklists (e.g. for input validation, authentication and password management, session management, cryptographic practices, database security) for developers helping them in writing secure code. Furthermore, a knowledge transfer framework for secure coding practices with guidance for the development of secure software products has been proposed by (Sodanil, Quirchmayr, Porrawatpreyakorn, & Tjoa, 2015). However, such approaches are technical and can be very helpful for developers, but they are too complex for other users. The framework presented in this thesis applies the knowledge transfer model, to transfer the security knowledge from security expert users to non-security

[32] https://www.securityknowledgeframework.org/

expert users. The concept of the security knowledge transfer that is provided within this framework is illustrated in Section 4.6.

2.4 Summary

This chapter provided the background information to the related concepts and technologies for this thesis. Since the main output of this work is a framework for mobile security that will help enterprises when adopting mobility, this chapter provided the basic information about mobile technologies and how these technologies can be adopted by enterprises applying different strategies. Afterward, the existing and related information security standards, publications and catalogues were discussed. Then, different principles related to mobile security were illustrated and security publications and catalogues that focus on mobile security were discussed.

In addition, since the framework proposed in this thesis supports the security knowledge transfer from security experts to non-security experts, this chapter also provided the background information in the domain of knowledge management to understand the basics of that domain. This in turn will help to understand the idea behind the security knowledge transfer concept within the framework proposed here.

3 Research Methodology

This chapter explains the research methodology that has been employed to conduct this research, and follows the Information Systems Research Framework, based on seven guidelines provided by (Hevner et al., 2004).

Two foundational paradigms characterize much of the research in the Information Systems discipline: behavioral science and design science (Hevner et al., 2004). In the behavioral-science paradigm, human or organizational behavior are investigated and analyzed to develop theories that explain or predict human or organizational behavior. On the other hand, the design-science paradigm seeks to extend the boundaries of human and organizational capabilities by creating new and innovative IT artifacts, which are broadly defined as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems) (Hevner et al., 2004). In this thesis, both afore-mentioned paradigms have been employed; the design-science paradigm to develop an artifact in form of a conceptual framework for mobile security that will support enterprises when adopting MEAs (see Chapter 4) and the behavioral-science paradigm to investigate the user acceptance of restrictions that might be caused by mobile security measures (see Section 5.2.2).

3.1 Information Systems Research Framework

For understanding, executing, and evaluating IS research, combining both behavioral and design science, an Information Systems Research Framework was presented in (Hevner et al., 2004). This framework is depicted in Figure 11. The environment defines the problem domain (Simon, 1996) where the research interest resides. As shown in Figure 11, the environment includes people, business organizations and their technologies. The environment's problems, goals, tasks and opportunities define the business needs as perceived by people within the organizations (Hevner et al., 2004). The business needs are normally assessed and evaluated within organizational strategies, structure, culture and processes. They are positioned in regard to existing technology infrastructure, applications, communication architectures, and development capabilities. Together these define the business need (the problem) as perceived by the researcher (Hevner et al., 2004).

This research began by defining the problem business organizations face when adopting MEAs. Interviews and discussions with experts from business organizations revealed that they want to adopt MEAs under different categories/levels of security. Here, balancing the security and usability must be carefully considered. Lot of enterprises avoid adopting mobile applications due to security fears. Security knowledge should be a shared knowledge within the whole enterprise, especially when it allows the use of mobile devices for work purposes.

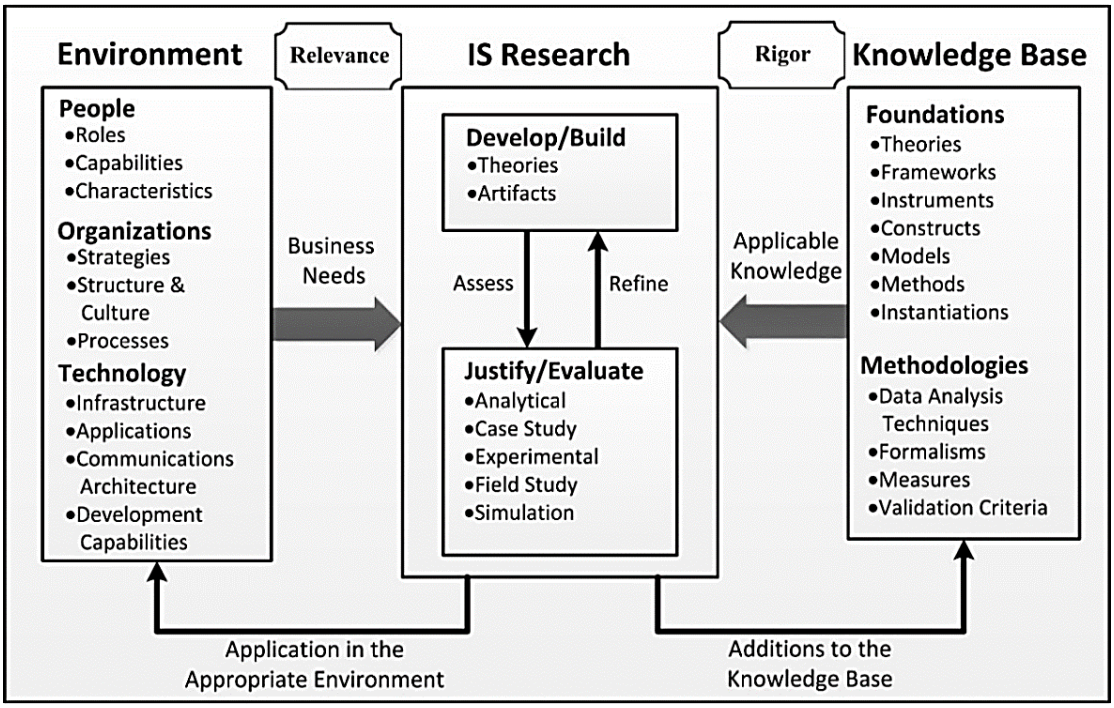

Figure 11. Information systems research framework

Source: (Hevner et al., 2004)

Enterprises face the problem that their business users mostly lack the know-how in security and that makes adoption of new mobile applications a difficult process. Beside business users, security expert users face a problem with unstructured information about the security knowledge and how this knowledge can be transferred and shared within the whole enterprise. This unstructured information also makes the designing of the security concept of MEAs a difficult task. Furthermore, enterprises need to know which data types can be transmitted to mobile devices, potential risks in a mobile environment and the extent that data can be protected on a mobile device. The present research is conducted through developing a Conceptual Framework for Mobile Security (CFMS). The CFMS together with its knowledge transfer concept aims to meet business needs (see Chapters 4 and 5).

A structured approach is conducted in this research to build and evaluate the CFMS to ensure that it has rigor and relevance. Based on (Hevner et al., 2004), IS research needs to be rigorous through providing "additions to the knowledge base", and relevance through "application in the appropriate environment".

3.2 Employing Design Science in Research

This thesis employs design science as a research approach to address the research problem. Hence, the seven guidelines provided by (Hevner et al., 2004) have been followed. These are summarized in Table 9. Following (Klein & Myers, 1999); the use of guidelines that assist researchers to understand the requirements for effective design-science research is considered mandatory (Hevner et al., 2004).

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 9. Design-science research guidelines

Source: (Hevner et al., 2004)

Following the first guideline (design as an artifact), the present work produces the CFMS that helps enterprises in adopting MEAs and forms the artifact of this research, as described in Chapters 4 and 5. Design-oriented IS research aims at the development of artifacts, of which the concrete manifestations include, but are not limited to, axioms, guidelines, frameworks, norms, patents, software (with open source code) (Österle et al., 2010). Furthermore, artifacts are innovations that define ideas, practices, technical capabilities, and products that make the analysis, design, implementation, and use of information systems effective and efficient (Denning, 1997; Hevner et al., 2004; Tsichritzis, 1997). The CFMS serves as a role-based tool that supports enterprises in designing security concepts of MEAs and in sharing mobile security knowledge within the whole enterprise (see Section 4.6).

Design science meets the second guideline (problem relevance) through the construction of innovative artifacts towards changing the phenomena that occur (Hevner et al., 2004). As a problem can be defined as the differences between the goal state and the current state, problem solving can be defined as a search process using actions to reduce or eliminate these differences (Hevner et al., 2004; Simon, 1996). Field studies and reports clearly indicate the increasing advance of mobile technology and its usages, not only in private but in business sectors as well (Gartner, 2016; IDC, 2014). However, from enterprise point of view, security levels are unclear when integrating mobile technologies into business processes. Thus, in spite of the advance in mobile technologies, security is still the primary barrier to the adoption of mobile applications within the enterprise (CISCO, 2016; Luenendonk, 2014). The CFMS will address this problem. Through its decision model, the CFMS will support business users in the decision-making process when adopting MEAs side by side with promoting the trustworthy usage of mobile devices in business sectors.

Following the third guideline (design evaluation), the utility, quality, and efficacy of the CFMS will be demonstrated via well-executed evaluation methods (see Chapter 6). In (Österle et al., 2010), “expert reviews” were represented as an artifact evaluation method. In this work, the CFMS has been implemented as a web-based tool (a prototype as proof-of-concept) that facilitated discussions with experts within enterprises. Another method to evaluate an artifact is descriptive by constructing detailed scenarios around the artifact to demonstrate its utility (Hevner et al., 2004). Furthermore, IT artifacts can be evaluated in terms of functionality, usability, fit with the organization, and other relevant quality attributes (Hevner et al., 2004). The evaluation conducted in this thesis will be explained in details in Chapter 6.

In the fourth guideline (research contributions), design-science research must provide clear contributions in form of the design artifact (the contribution is the artifact itself), foundations (extending and improve the existing foundations in the design-science knowledge base) and methodologies (measures and evaluation metrics) (Hevner et al., 2004). On the one hand, the thesis in hand contributes by applying existing knowledge about mobile security in an innovative way. It mainly targets business users providing them with an innovative tool (the resulting artifact) that helps for better understanding of mobile security. In addition, this tool is also interesting for expert users, since the information about security is managed in a structured way that facilitates the management and extension of the security knowledge. On the other hand, this thesis also contributes by adding the CFMS to the knowledge base for future work.

Following the fifth guideline (research rigor), design-science research must apply rigorous methods in both the construction and evaluation of the designed artifact (Hevner et al., 2004). In this thesis, by constructing the artifact (the CFMS), suitable knowledge in the mobile security domain has been applied and security standards, catalogues and guidelines have been considered. Furthermore, the evaluation of the CFMS has been conducted using rigorous methods (following the third guideline "design evaluation").

As stated in the sixth guideline (design as a search process), problem solving or creation of effective artifact requires utilizing available means to reach desired ends while satisfying laws existing in the environment (Hevner et al., 2004; Simon, 1996). The CFMS can be conceived as the result of an extensive search process. A literature review has been conducted to: A) extract the security requirements for MEAs (see Section 5.3.1), B) determine the potential security threats along with their likelihood of occurrence and their impact on Business (see Section 5.1), C) determine existing mobile security measures needed to counter the potential mobile threats and to mitigate the risks (see Section 5.2). Through its guidance model, the CFMS facilitates the managing and mapping of all three, security requirements, threats and measures, and makes these available through its decision model to business users. During the research, it was always kept in mind that the information provided within the CFMS should be understandable for users with low or medium know-how in mobile security. To sum up, this work has searched for the best ways to extract, administrate and share information about mobile security in enterprises, supporting them when they want to adopt MEAs.

The seventh guideline (communication of research) advises the communication of the research. Following this guideline, the CFMS is presented to the academic audience to add to the knowledge base. Furthermore, the research was communicated and presented to various technological and managerial communities within different scientific conferences and workshops.

A model for the general process conducted by design-science research has been developed by (Takeda, Veerkamp, Tomiyama, & Yoshikawa, 1990) and has been extended and applied specifically to design science research by (Vaishnavi, V. & Kuechler, 2007). The present work follows the model provided by (Hevner & Chatterjee, 2010), adapted from (Vaishnavi, V. & Kuechler, 2007), and is depicted in Figure 12.

The first phase is the awareness of problem. This phase considers guideline 2 "problem relevance". Discussions with peoples from industry revealed that enterprises need to adopt MEAs, but they still have security fears that slow down the adoption process. However, the problem has been identified and defined here based on these discussions and literature review. The output of this phase was a proposal for this research effort.

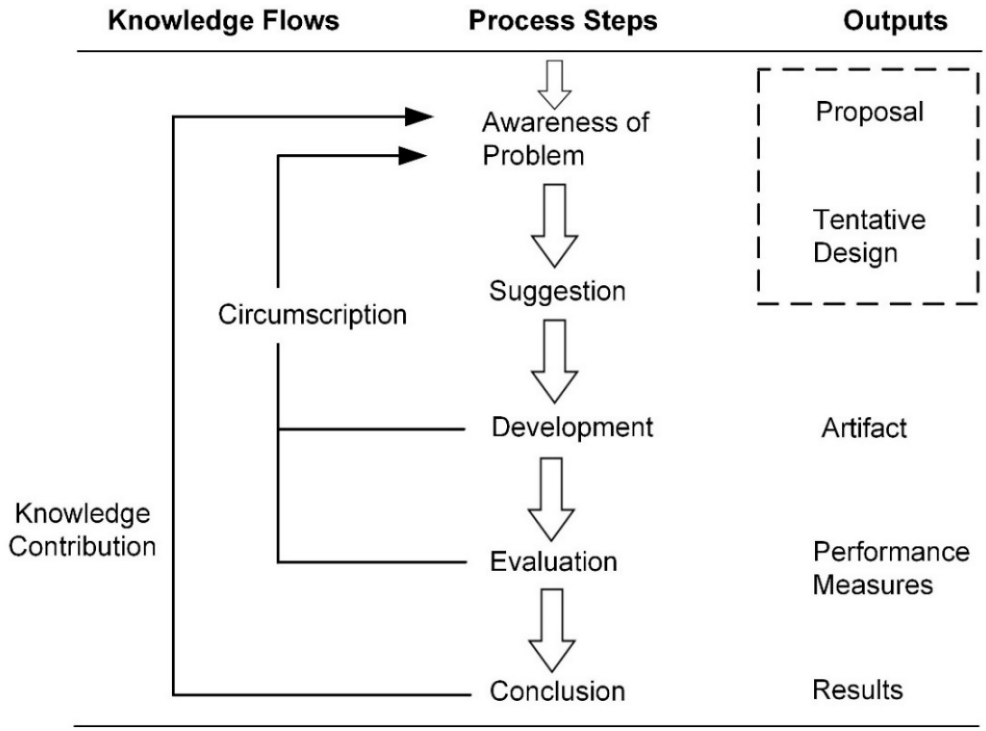

Figure 12. Design science research process model

Source: Adapted from (Hevner & Chatterjee, 2010; Vaishnavi, V. & Kuechler, 2007)

The next phase is a suggestion for a problem solution that is drawn from the existing knowledge or theory based on the problem area or developed using an appropriate research

methodology (Hevner & Chatterjee, 2010). This phase resulted in a tentative design, the concept of the CFMS. This phase considers the guideline 6 "design as a search process".

The tentative design is further developed and implemented in phase development. As stated by Vaishnavi and Kuechler, *"[…] the novelty is primarily in the design, not in the construction of the artifact*" (Vaishnavi, V. & Kuechler, 2004). This phase is creative and the design is further refined through many iterations (Hevner & Chatterjee, 2010). This phase follows the guideline 1 "design as an artifact" and the guideline 5 "research rigor", resulted in an artifact, the prototype or the proof-of-concept of the CFMS.

Once a prototype is ready, it is evaluated. The output of this phase determines how well an artifact works (Hevner et al., 2004). In the "development" and "evaluation" phases, there are iterations and feedback cited as circumscription (Hevner & Chatterjee, 2010). This phase followed the guideline 3 "design evaluation" and the guideline 5 "research rigor".

	Output	**Description**
1	Constructs	The conceptual vocabulary of a domain
2	Models	Sets of propositions or statements expressing relationships between constructs
3	Frameworks	Real or conceptual guides to serve as support or guide
4	Architectures	High level structures of systems
5	Design Principles	Core principles and concepts to guide design
6	Methods	Sets of steps used to perform tasks —how-to knowledge
7	Instantiations	Situated Implementations in certain environments that do or do not operationalize constructs, models, methods, and other abstract artifacts; in the latter case such knowledge remains tacit.
8	Design Theories	A prescriptive set of statements on how to do something to achieve a certain objective. A theory usually includes other abstract artifacts such as constructs, models, frameworks, architectures, design principles, and methods.

Table 10. Outputs of design science research[33]

Source: (Vaishnavi, V. & Kuechler, 2004)

The conclusion phase is the end of the research cycle or is a final specific research effort and should contribute further knowledge (Vaishnavi, V. & Kuechler, 2004). In this phase, research communication is very important (Hevner et al., 2004; Vaishnavi, V. & Kuechler,

[33] http://desrist.org/desrist/

2004). Hence, this phase followed the guideline 4 "research contribution" and the guideline 7 "communication of research". The output type of this phase can vary as described in Table 10; the output type "Frameworks" is highlighted as the output type of this research.

Beside the design science, a part of this this research also employed behavioral science as a research approach. The following section briefly presents this approach.

3.3 Employing Behavioral Science in Research

Software engineering is not only about technical solutions, but it is also concerned with organizational issues, project management and human behavior (Wohlin, Höst, & Henningsson, 2003). The behavioral science research paradigm seeks to develop and justify theories that explain or predict human or organizational behavior and human phenomena surrounding the analysis, design, implementation, management, and use of information systems (Hevner et al., 2004).

According to (Wohlin et al., 2000), there are two main types of research paradigms within empirical behavioral studies. The first type is qualitative research that is concerned with studying objects in their natural setting and it attempts to interpret a phenomenon based on explanations that people bring to them (Denzin & Lincoln, 1994). The second is quantitative research that mainly attempts to quantify a relationship or to compare two or more groups with the aim of identifying cause-effect relationships (Creswell, 1994; Wohlin et al., 2000). Depending on the conditions for the empirical investigation, there are four major different types of investigations (strategies), namely, experiment, case study, survey and post-mortem analysis (Wohlin et al., 2003). In this research, a survey has been conducted as an empirical method to investigate the user acceptance of the possible consequences on them when applying mobile security measures and restrictions (see Section 5.2.2).

3.4 Literature Review

Literature review creates a firm foundation for advancing knowledge and it is an essential feature of any academic research (Webster & Watson, 2002). Conducting a thorough literature review on a topic, where an accumulated body of research exists enables further analysis and synthesis. The following sections detail how the literature review was conducted in the present research.

3.4.1 Guidelines for Literature Review

A framework and guidelines for conducting literature review has been proposed by (vom Brocke et al., 2009). This framework is shown in Figure 13.

In Phase I, the scope of the research is defined. In order to clearly define the scope of a review, (vom Brocke et al., 2009) suggested drawing on an established taxonomy for literature reviews as presented by (Cooper, 1988). Cooper's taxonomy categorizes reviews into six categories according to a number of characteristics, namely, focus, goal, perspective, coverage, organization, and audience. Table 11 shows this taxonomy following Cooper.

First, most literature reviews focus on research outcomes, research methods, theories, and/or applications (Torraco, 2005; vom Brocke et al., 2009). The literature review conducted in this thesis focused on applications and research outcomes. Second, the goals of literature review concern what the author hopes the review will accomplish (Cooper, 1988). These include summarizing, criticizing, and/or integrating findings (Jackson, 1980; vom Brocke et al., 2009). The goal of the literature review conducted in this thesis was to integrate findings from other literatures.

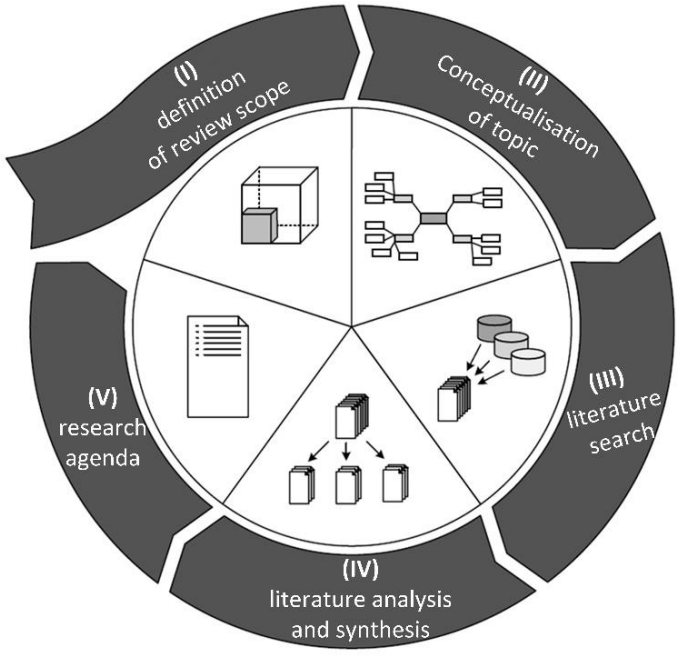

Figure 13. Framework for literature review

Source: (vom Brocke et al., 2009)

Third, the reviews were arranged conceptually, so that literature relating to the same abstract ideas appeared together (Cooper, 1988). In the fourth characteristic, "perspective" of a review concerns how the reviewer's point of view influences the discussion of the literature,

and the fifth characteristic "audience" determines the intended audiences of the reviews (Cooper, 1988). In the last characteristic, Cooper distinguished between four types of literature coverage, namely, exhaustive, exhaustive with selective citation, representative and central/pivotal (Cooper, 1988). This research targeted literatures that are pivotal to mobile security, especially from an MEA perspective. Table 11 shows in grey the categories that characterize the literature review conducted in this research.

Characteristic	**Categories**			
focus	research outcomes	research methods	theories	applications
goal	integration	criticism	central issues	
organization	historical	conceptual	methodological	
perspective	neutral representation		espousal of position	
audience	specialized scholars	general scholars	practitioners/ politicians	general public
coverage	exhaustive	exhaustive and selective	representative	central/pivotal

Table 11. Taxonomy of literature reviews

Based on (Cooper, 1988; vom Brocke et al., 2009)

Following Phase II, books and articles in domain mobile security and mobile enterprise applications were studied (BSI, 2013; Dwivedi, Clark, & Thiel, 2010; Eckert, 2009; Landman, 2010; Mylonas, Kastania, & Gritzalis, 2013; Souppaya & Scarfone, 2013; Unhelkar & Murugesan, 2010). These contain a summary and overview of the security issues an enterprise faces when adopting MEAs.

After completing this overview, the literature search was started (Phase III). Here, articles published in scholarly journals are often recommended, since they have typically been peer-reviewed before publication (Rowley & Slack, 2004). In addition, proceedings of reputable conferences are also recommended (vom Brocke et al., 2009; Webster & Watson, 2002).

In this research, the main targeted bibliographic databases include, but were not limited to, Web of Science[34], ACM Digital Library[35], SpringerLink[36], IEEE Computer Society Digital

[34] https://webofknowledge.com/
[35] http://dl.acm.org/
[36] http://link.springer.com/

Library[37] and Google Scholar[38]. Moreover, to get the praxis insight into the topic in hand, articles, reports, and white papers were also continually reviewed. This includes, among others, CISCO[39] Reports, Gartner[40], McAfee Labs[41]. Finally, the literatures selected in phase III were analyzed in Phase IV by arranging and discussing prior research focusing on outcomes, and in Phase V, the extracted information was structured and mapped in the CFMS along with an outlook of future research.

3.5 Summary

This chapter illustrated the research methods in information systems science that have been followed to manage the research behind this work. Design science has been employed as main research approach in this work and the seven guidelines provided by Hevner et al. have been followed. However, behavioral science has been also employed in the research concerning the investigation of user acceptance. Furthermore, Design Science Research Process Model, together with mapping its phases to the seven guidelines provided by Hevner et al., has been followed as the core research method in this work. A further research method followed in this work is the information systems research framework in which the research conducted reflects the relevance to the business environment and adds to the knowledge base in information systems science.

Last, but not least, this chapter illustrated the literature review method that has been conducted within this research. This method is very important within all research phases, especially when building the risk catalogue as well as when determining the mobile security measures needed to mitigate the potential risks when using MEAs.

Based on the design considerations derived from the methods and approaches in this chapter, the following chapter presents the conception phase of this work and defines all its requirements in detail.

[37] http://www2.computer.org/portal/web/csdl
[38] https://scholar.google.com/
[39] http://www.cisco.com/
[40] http://www.gartner.com/
[41] http://www.mcafee.com/us/mcafee-labs.aspx

4 Conception of Framework for Adopting Secure Mobile Enterprise Applications

Supporting business users with the needed know-how in mobile security when enterprises adopt MEAs is the major requirement behind this work. The main question in this regard is to find a means of enabling enterprises to better deal with information about mobile security. Hence, information about mobile security has to be stored in a structured way, to maintain, extend and share it easily.

This work defines the mobile security requirements and classifies them into security levels. Then, the potential threats to an enterprise when adopting MEAs is determined and mapped to the defined mobile security requirements. Finally, the mobile security measures that are needed to overcome the threats determined are suggested and mapped to the threats.

This chapter describes a Conceptual Framework for Mobile Security (CFMS). This organized as follows: Section 4.1 shows the methodology that considered when designing the framework and for identifying its contents. Then, Section 4.2 describes the framework structure and its models along with their components and the relations between the components within each model, as well as the relations between the models themselves. Section 4.3 presents the framework workflow and the utilization guidelines. After that, the requirements of the framework as well as its user roles are defined in Section 4.4 and Section 4.5 respectively. Section 4.6 describes the concept of security knowledge transfer behind this work, with a brief conclusion in Section 4.7.

4.1 Methodology

For designing the CFMS and for identifying its contents (e.g. threats and measures), ISO 31000:2009 risk management process (ISO 31000:2009, 2009) is considered. This process is shown in Figure 14. The standard ISO 31000:2009 has been developed on the basis of the world's first formal standard for managing risk, the Australian/New Zealand Standard AS/NZS 4360 that published in 1999 and revised in 2004.

As a first step, the context was established by defining business scenarios that show the typical usage of mobile applications for work purposes. These scenarios are described in Section 5.1.2. The main focus was to define the external parameters to be taken into account when managing the risks. These include the technological parameters, e.g. mobile networks.

Establishing the internal context was supported in the CFMS through its guidance model, which can be maintained by each enterprise based on its own culture, processes, structure, policies, objectives, and strategies. Such business scenarios define the scope of the risk management process, and the processes and assets related to MEAs. Moreover, this step includes defining the risk criteria that are used to evaluate the significance of risk.

A risk assessment then was conducted, including identifying, analyzing and evaluating the potential risks. After the assets and processes had been identified, a list of potential mobile threats was identified based on the defined scenarios and literature review. Then, these risks were analyzed and estimated based on two factors, the likelihood of threat occurrence and its potential impacts (see Section 5.1.5).

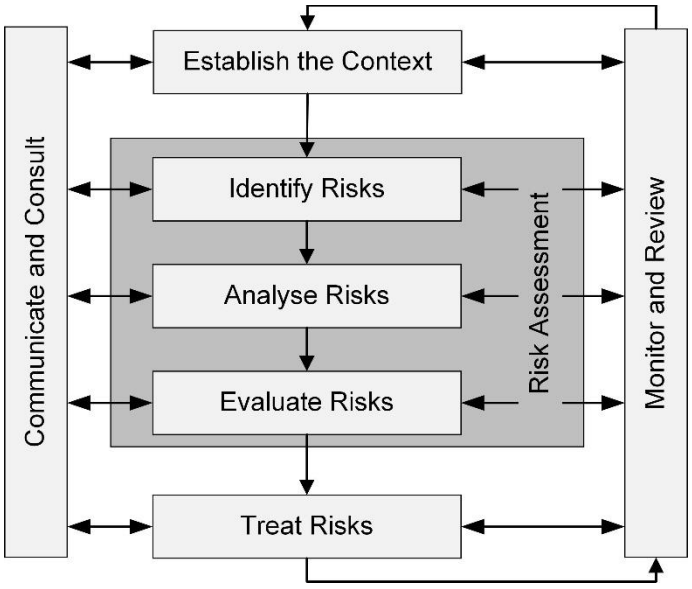

Figure 14. Risk management process

Source: (ISO 31000:2009, 2009)

Then, risk is evaluated to assist in making decisions, based on the outcomes of risk analysis to identify which risk needs treatment and the priority for treatment implementation (ISO 31000:2009, 2009). Based on a selected list of mobile security requirements, CFMS will show the related potential threats along with their accompanying risks classified in risk levels and will recommend the needed security measures to mitigate identified risks. However, classifying the risks in risk levels will not identify the priority for treatment implementation. This can be considered in future work.

During all the afore-mentioned stages, communication and consultation took place in form of: a) discussion with scientific community through conferences, b) discussions with experts

from the business domain and c) literature review. As stated in (ISO 31000:2009, 2009), the communication and consultation helped to:

- establish the context appropriately
- ensure that risks are adequately identified
- bring different areas of expertise together for analyzing the risks
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks
- ensure that the interests of stakeholders are understood and considered.

Finally, through its two models, guidance model and decision model, CFMS supports enterprises by monitoring and review processes, where the maintenance of the content that is related to the requirements, risks and measures is facilitated by adding, deleting, modifying and mapping functions. The monitoring and review processes includes, but is not limited to:

- Detecting changes in the context, including changes in risk criteria and the risk itself which can require new measures
- Analyzing and learning lessons from events, trends, successes and failures
- Ensuring that the measures are effective and efficient

The following section represents the CFMS structure and describe its models.

4.2 Framework Structure

The functional specifications of the CFMS are presented in (Hasan, Marx Gómez, & Kurzhöfer, 2013) and (Hasan, Dmitriyev, Marx Gómez, & Kurzhöfer, 2014), and the CFMS is further refined and implemented as a web-based tool, supporting different roles (Eilts, 2016; Hasan & Marx Gómez, 2017).

The initial idea of the concept of this framework was taken from the Service-Oriented Architecture Decision Modeling (SOAD) framework (Zimmermann, 2011), which aims at enhancing the SOA architectural style. In order to reuse the structure of SOAD framework in security and enterprise mobility domains, major adaptations were made to come up with a new structure for the CFMS.

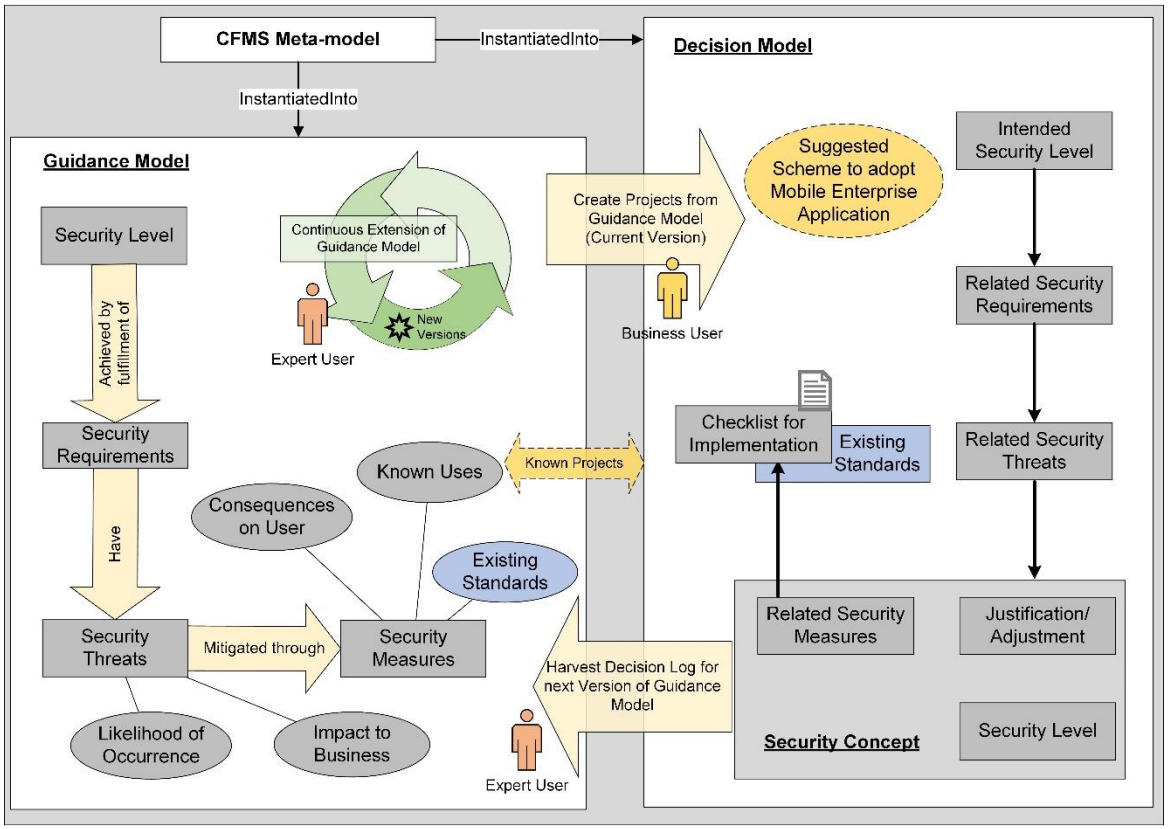

Figure 15. CFMS structure

Source: (Hasan & Marx Gómez, 2017)

Essentially, the CFMS is enhanced with a meta-model instantiated into two models, namely, a guidance model and a decision model. Figure 15 shows the structure of the CFMS. This framework serves as a role-based tool which provides recommendations that help users to create security concepts for MEAs. Two main roles[42] are provided within CFMS, namely, business user and expert user.

- A business user is the essential user in the CFMS. She/he lacks the know-how in mobile security. A business user might be managing director, project manager, sales representative, HR or any employee who is not a security expert. For instance, a project manager can create security concepts for individual projects in the context of MEAs.
- A security expert user is a privileged user in the CFMS. She/he has specialized know-how in the context of the mobile security. Such a user might be Chief Information Security Officer (CISO), administrator, information security manager, IT security

[42] Further roles are defined in Section 4.5.

designer, IT security architect or any employee who is responsible for planning, implementing, and maintaining the security of mobile devices and mobile applications.

The guidance model can be instantiated into a decision model in form of projects, which in turn can feed back information to the guidance model refining it into its next version (see Section 4.3). The versioning and the refinement process of the guidance model enables the CFMS's continual improvement. According to (ISO/IEC 27001, 2005), it is important to consider the continual changes of technology, identified threats, effectiveness of the implemented controls and external events (like changed contractual obligations).

The following subsections describe the CFMS models in more detail, where the components of each model and the relations between these components are described.

4.2.1 Framework Meta-Model

In order to define the components of the CFMS and the relations between them, the CFMS is enhanced with a meta-model that can be instantiated into guidance model and decision model. The CFMS meta-model is presented as a UML class diagram and is depicted in Figure 29 (see Section 6.1.1). It consists of nine classes, namely, SecurityLevel, SecurityRequirement, Threat, ThreatGroup, SecurityMeasure, UserImpact, Standard and Solution. The whole description of the framework meta-model is presented in Section 6.1.1.

4.2.2 Framework Guidance Model

This model includes four main components (profiles), namely, security levels, security requirements, security threats and security measures. These four profiles are mapped to each other. A security level of an MEA is achieved by the fulfillment of a set of security requirements, which are in turn mapped to potential mobile security threats. Each threat in the CFMS is described along with its likelihood of occurrence and its possible impact on business. Furthermore, the CFMS maps these threats to security measures to mitigate the potential risks caused by the associated threats.

The maintenance of the content and the mapping of these four profiles are administrated by those in the role "security expert user". In addition, security expert users can also manage the versioning of the guidance model. The guidance model versions are defined in Section 4.4.2 and versioning process is described in Section 6.2.1.

The following four profiles are now described with more details:

- Security levels;
- Mobile security requirements;
- Mobile threats;
- Mobile security measures

Security Levels: The CFMS guidance model enables the definition of three security levels, namely, high, medium and low (see Section 5.3.2). However, this model can be easily extended to include additional security levels. Each security level is achieved by the fulfillment of a set of security requirements, so that each security level in the guidance model is mapped to a set of security requirements. This mapping is based on current literature and discussions with experts within enterprises. However, enterprises can define their own security levels and requirements and administrate these in the CFMS.

Mobile Security Requirements: In this work a list of security requirements for MEAs were first extracted from the existing literature on guidelines and standards, especially publications from BSI (BSI, 2013), NIST (NIST, 2013) and Common Criteria (Common Criteria, 2012). Then, the extracted list was refined through expert interviews. This refinement of the extracted requirements included: a) deleting the irrelevant requirements (in the context of MEAs), b) refining the extracted requirements, and c) adding new requirements arising through the interviews. The resulting security requirements have been included in the security requirements catalogue and split into three categories, namely, mobile communications, mobile OSes, and mobile applications. The whole description including the list of mobile security requirements is presented in Section 5.3.1.

Mobile Threats: Section 5.1 shows how mobile threats are determined and included in a risk catalogue along with their likelihood of occurrence and their potential impact on business. The guidance model maps the catalogues of security requirements, and threats, where each security requirement is mapped to a set of threats. The content administration and the mapping are taken over by security expert users via the guidance model. Security expert users also have privileges to map each threat to a security solution, which consists of a set of mobile security measures that are needed to fulfill the related security requirements and to mitigate the risks that can be caused by potential threats.

Mobile Security Measures: A balance between security and usability become of crucial importance when applying mobile security measures, due to usability barriers of mobile devices (e.g., screen size, keypad size). Beside security measures, restrictions can also be applied on mobile devices, like restricting user and mobile application access to hardware (such as digital camera), GPS, and removable storage. Moreover, mobile security measures and restrictions can have consequences on the end user (e.g. high chance of error when entering a complex alphanumeric password). Security expert users have the privilege to map each threat from the risk catalogue to one or more security solutions (A security solution is a combination of one or more mobile security measures, e.g. authentication through password and fingerprint). Hence, the CFMS suggests security measures along with their possible consequences on the end user and their known uses in previous MEA projects. Showing the possible consequences on users is an important criterion for balancing usability and security when choosing between security solution alternatives. Mobile security measures along with their consequences on the end user are presented in Section 5.2.1.

4.2.3 Framework Decision Model

The decision model represents an instantiation of the guidance model in form of projects, which in turn represent security concepts of MEAs. This model is available for business users and expert users as well. However, expert users are responsible for the content administration of the guidance model. The content of CFMS guidance model is made available to the business users through the decision model, where the business users can administrate (create and edit) the MEA's projects. They can select appropriate security solutions based on the potential consequences on the end users. The outcome of the decision model (the security concept along with the related security measures) can be used as a checklist for MEA implementation.

The use cases of the decision model as well as its possible utilizations are described in Section 4.4.2 and Section 6.2.2 respectively.

4.3 Framework Workflow and Guidelines

Before going on to consider the CFMS guidelines, the following definitions should be taken into consideration:

- $SR = \{sr_1, .. , sr_k\}$ is the set of k security requirements
- $SL = \{sl_1, sl_2, sl_3\}$ = {Normal, Medium, High} is the set of three security levels
- Each security level $sl_i \in SL$; $i \in [1, 3]$ requires a fulfillment of a subset of security requirements $SR' \subset SR$
- $T = \{t_1, .. , t_n\}$ is the set of n threats
- $M= \{m_1, .. , m_p\}$ is the set of p measures
- Each threat $t_i \in T$ is countered by one or more alternative (security solution). The set of alternatives is represented as $A= \{a_1, a_2 \dots a_j\}$; $a_i \in P(M)$, where $1 \leq i \leq j$ and j is equal to size of the power set of M.

The CFMS is enhanced with guidelines that show how this framework works and serve as a general guide for enterprises when using this framework. For better understanding of these guidelines, a workflow is presented in Figure 16. These Guidelines are:

- Predefined security level as a starting point;
- Selecting threats and alternative measures;
- Decision making process;
- Decision log and refinement process

Guideline 1: Predefined security level as a starting point: Firstly, as prerequisite for use of the CFMS, the enterprise should analyze the importance and sensitivity of its own data and classify them into security levels.

Standards and guidelines for this classification already exist. Managers or information owners are responsible for classifying information into categories or levels. For instance, ISO 27001 provides an information classification matrix[43], in which, information is classified in terms of confidentiality into three levels, namely: 1) PUBLIC or open: "*Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders*"; 2) INTERNAL or proprietary: "*Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient.*"; and 3) CONFIDENTIAL or restricted: "*Highly sensitive or valuable information, both proprietary*

[43] iso27001security.com/ISO27k_Information_classification_matrix.xlsx

and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager."

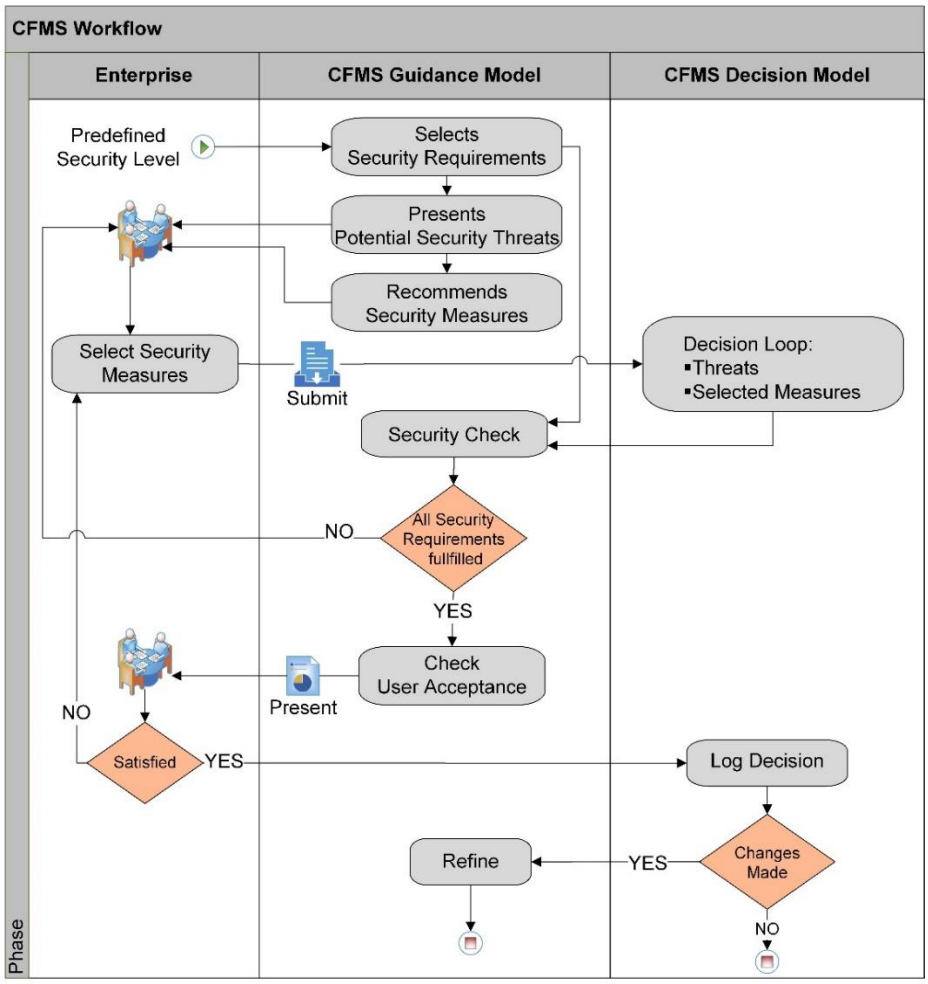

Figure 16. Workflow of the CFMS

Source: (Hasan et al., 2014)

The second example is FIBS PUB199, which defined standards and guidelines for security categorization of Federal information and information systems (NIST, 2004). In this standard, each security category is defined based on the potential harm impact of losing security objectives confidentiality, integrity, and availability. For each security objective, three impacts are defined, low, moderate, and high. Thus, the enterprise firstly determines the intended security level, which has to be maintained for the corporate data on mobile devices. The workflow[44] presented on Figure 16 shows that the starting point in the CFMS begins with a predefined security level as an input to the guidance model. The CFMS guidance model defines three security levels, namely, high, medium and low (see Section

[44] In order to simplify the guidelines, this workflow is presented independently of its user roles.

5.3.2 that also presents how to determine a security level needed by the enterprise for an MEA), with the flexibility of adding further security levels if required. In the CFMS, each security level is mapped to a set of security requirements needed, this is described as follows:

$$\text{For each } sl_i \text{ in } SL$$

$$\exists! \, SR'[n] \in SR \; (SR'[n] \mapsto Sl_i)$$

Guideline 2: Selecting threats and alternative measures: After the enterprise defines the intended security level (e.g. sl_i), the CFMS maps the security level sl_i to a subset of security requirements SR´, which should be fulfilled to achieve the security level sl_i. Then, in the next step, the CFMS determines and presents the potential security threats ($T' \subset T$), which should be countered, and recommends all the possible alternative security solutions {a_1, a_2 …}; $a_i \in P(M)$, which should be implemented to counter the threats T´. This is described as follows:

$$\text{For each } t_j \text{ in } T'$$

$$\exists \, a_i \in P(M) \; (a_i \mapsto t_j)$$

One alternative might include one or more security measures. As an example, to counter a threat $t_1 \in T$, the following two alternatives, a_1 and a_2 might be needed:

$a_1 = \{m_1, m_2\}$; and $a_2 = \{m_1, m_5, m_7\}$

There are also dependencies between the individual measures. For example, to achieve the alternative a_1, the security measure m_1 cannot be selected and implemented without the security measure m_2. The guidance model incorporates such dependencies between security measures. So, the framework recommends the possible alternatives by presenting them to the enterprise to start the next step.

Guideline 3: Decision making process: The enterprise now has the potential threats, and the possible alternatives, so one alternative for each threat can be selected and both the threats and the selected alternative submitted to a security check method through a decision loop. The selection is done through instantiating the guidance model in the decision model, which might involve adding adjustments (see Section 4.4.2). Two important actions take place at this step:

1) *Security Check:* The security check method takes the security requirements, threats and the selected alternative as input. This method checks if all the measures needed

have been selected by the enterprise. If the security check finds that not all the requirements needed are selected, or if not all the security measures needed are selected, then the enterprise should select another alternative. When all the security requirements are fulfilled, the workflow will proceed to the next step to check the user acceptance. The mathematical pseudocode for the security check method is described as follows:

```
Method SecurityCheck is
     input: sl_i, SR[m], T[k], A[p]
     output: checkResult
     if SR[m] ⊆ SR´[n] and
          for each t_j in T[k]
               ∃ a_i∈A[p](a_i ↦ t_j)
          set checkResult to true
     else set checkResult to false
     return checkResult
```

2) *User Acceptance:* It is very important that the possible consequences on users be considered when applying security measures on mobile devices, because some security measures are applied as restrictions that may affect the employee's intention to use their mobile device for work. In its guidance model, the CFMS maps each security measure to a set of possible consequences (see Section 5.2). Thus, the CFMS will show the possible consequences that are associated with the selected alternatives, more specifically the selected security measures. Based on these possible consequences, the enterprise may design a questionnaire asking its employees about their acceptance. If the user acceptance rate does not satisfy the enterprise, another alternative that includes other security measures can be selected for a next decision loop.

Guideline 4: Decision Log and Refinement Process: Through the CFMS decision model, the enterprise can create projects. Each project can have its own attributes; security level, threats and measures. This is important because the enterprise can then adopt different MEAs that have different security levels. Through a decision log process, a history can be kept for

decisions that have been previously made. This will be stored in form of known-uses as in Figure 15. If some changes (adjustments) have been made in the previous step (decision making process), the decision model sends these adjustments back the guidance model, where they can be reviewed by security expert users, who can accept or reject these adjustments. If accepted they will be considered in the next refined version of the guidance model. For example, the new threats or new security measures, which were not considered in the guidance model, will be harvested and integrated back to the guidance model in form of suggestions for change to an expert user who can review the suggested changes.

The CFMS was intentionally developed to be a generic framework, so each enterprise can adapt its own version of it. Its requirements are explained in the following section.

4.4 Requirement Definition

This section describes the requirements for the CFMS. This includes both general requirements and the functional requirements (the scope of functions) the framework should fulfill. Furthermore, other requirements, for example, scalability and usability (non-functional requirements) are also described.

4.4.1 General Requirements

The CFMS should serve as a web-based tool that supports enterprises by designing the security concept of MEAs. Furthermore, this tool should also serve as a guide for enterprises to improve their overall mobile security posture. Thus, the CFMS should fulfill the following general requirements:

- Provide a list of classified potential threats in mobile environment
- Provide a list of the available mobile security measures together with their possible consequences on users
- Map both lists to mitigate the risks to business
- Define security levels and classifying mobile enterprise applications into these levels
- Provide a mechanism of transferring and sharing knowledge about mobile security within the enterprise

In addition, CFMS has to support enterprises in both, security by design and security management:

Security by design: The CFMS will help by designing the security concept of the MEA the enterprise wants to adopt, and it will provide a checklist[45] for mobile applications developers and project managers. This checklist includes the security measures needed, which have to be applied when using MEAs.

Security management: The CFMS will support by documenting the information about mobile security (such as the needed security measures) in a structured way, so that this information can be easily reused when adopting new MEAs. This documented information will govern the implementation and ongoing management of an organization's mobile security. Furthermore, the CFMS will also support enterprises in justifying the applied security measures to their employees using MEAs.

4.4.2 Functional Requirements

The functional requirements help by directing the development of the CFMS prototype, and they describe the basic functionalities and the desired behavior of the CFMS. The following main functional requirements are supposed to be accomplished by CFMS:

Roles administration: CFMS should be a role-based tool, where different roles can be defined and user accounts can be created and associated to specific roles. Thus, after the login, users can access and perform actions according to the associated roles. For instance, access to the guidance model should be available to security expert users only.

Administration of content in the guidance model: The CFMS contents, such as mobile security requirements, threats and measures, can be added, edited or deleted. CFMS should also provide functions to perform the mapping of contents, e.g. mapping threats to the needed security measures to mitigate the potential risks to business.

Administration of versions of the guidance model: Table 12 (Page 56) defines three different types of the CFMS guidance model. Security expert users should be able to create new versions of the guidance model (see Section 6.2.1).

[45] The checklist will only serve as a high-abstract description of the security measures that need to be applied, and it does not provide information about how to implement these measures. So, in the context of this thesis, the "security by design" refers to the design of security concepts of MEAs.

Administration of projects in the decision model: The CFMS should provide the following functionalities within its decision model:

- *Create new projects:* CFMS users should have the possibility to create new projects, which are an instantiation of the guidance model and are always based on the current version of the guidance model, however, a project should still represent the security concept of an MEA.
- *Selecting an intended security level:* CFMS users, who have the right to create new projects, should be able to select the intended security level for the MEA the enterprise adopts. Moreover, those users should be supported in the selection of a security level. After selecting a security level, the CFMS should display the security requirements mapped to the selected security level. The users should be able to select additional security requirements or to exclude some requirements, however CFMS should check if the selected security level is still fulfilled and the results should be displayed accordingly.
- *Displaying the related threats:* After selecting the security level and security requirements, the CFMS should display the related threats. Further information on security threats such as likelihood of occurrence and impact on business can be also displayed. Moreover, the assets that might be affected by those threats can also be displayed. The users should also be given the possibility to include adjustments in the project being created, such as including additional threats to be considered. The adjustments should be sent back to the guidance model, where they can be reviewed by security expert users.
- *Suggesting security solutions:* The CFMS, based on the selected security level and security requirements, should suggest security solutions including the security measures along with the related possible consequences on MEAs users. Furthermore, the non-security expert users should be able to select the appropriate alternatives of security solution according to those consequences.
- *Exporting project(s) as a PDF:* After creating a project, the CFMS should enable its users to export the project as a PDF document, which includes the intended security level, the related security requirements, the related threats and the security measures. The PDF document can be used as a checklist for the implementation of security measures needed for an MEA.

Administration of the adjustments: Through its guidance model, the CFMS should provide security expert users with the possibility to check added adjustments. Security expert users should be able to reject or accept these adjustments. Accepted adjustment should be available in the next version of the guidance model.

Version Type	Description
Draft Version	The guidance model version that is being edited and prepared by security expert users. The content included in this version will be available to non-security expert users once a security expert user releases a new version of guidance model.
Current Version	The guidance model version that is available for non-security experts. Once a new version of the guidance model is released, the content of the current version cannot be manipulated anymore. However, if changes become necessary, then the security expert user should create new version of the guidance model.
Old Versions	Old versions of the guidance model are archived to keep a documented history of the guidance model versions. Old versions can still be viewed by expert users.

Table 12. CFMS guidance model's version types

To understand the requirements from a user perspective, UML use case diagrams are employed to represent these requirements. Figure 17 and Figure 18 describe the main use cases of the guidance model and decision model respectively.

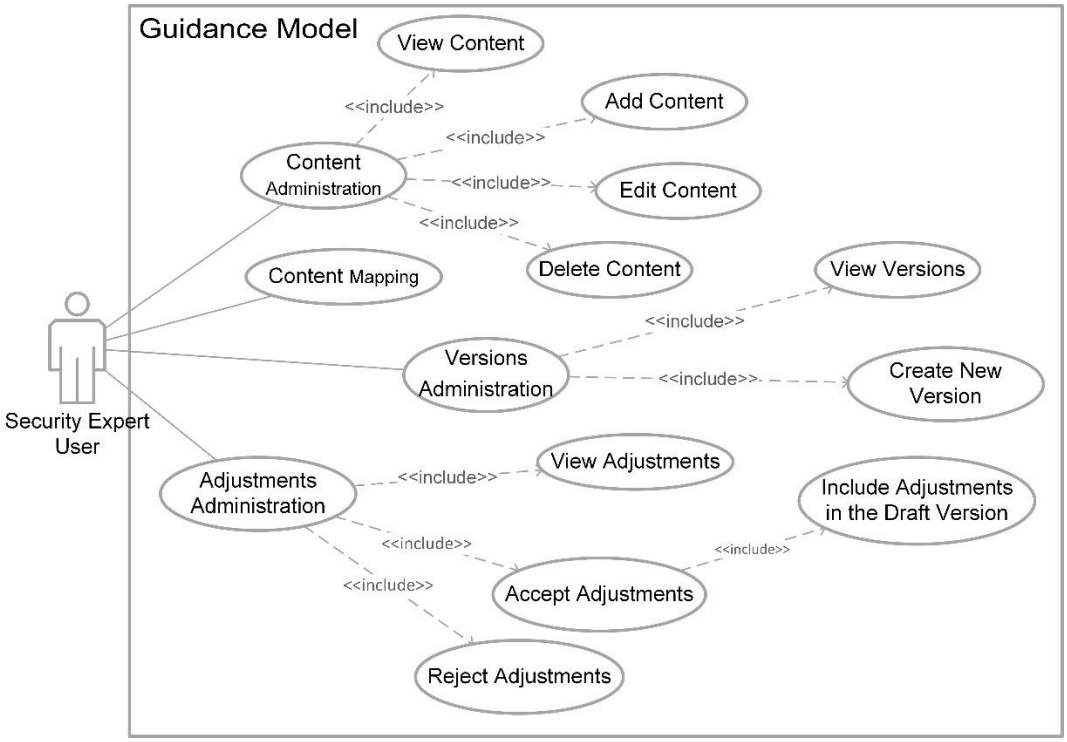

Figure 17. UML use case diagram of the guidance model

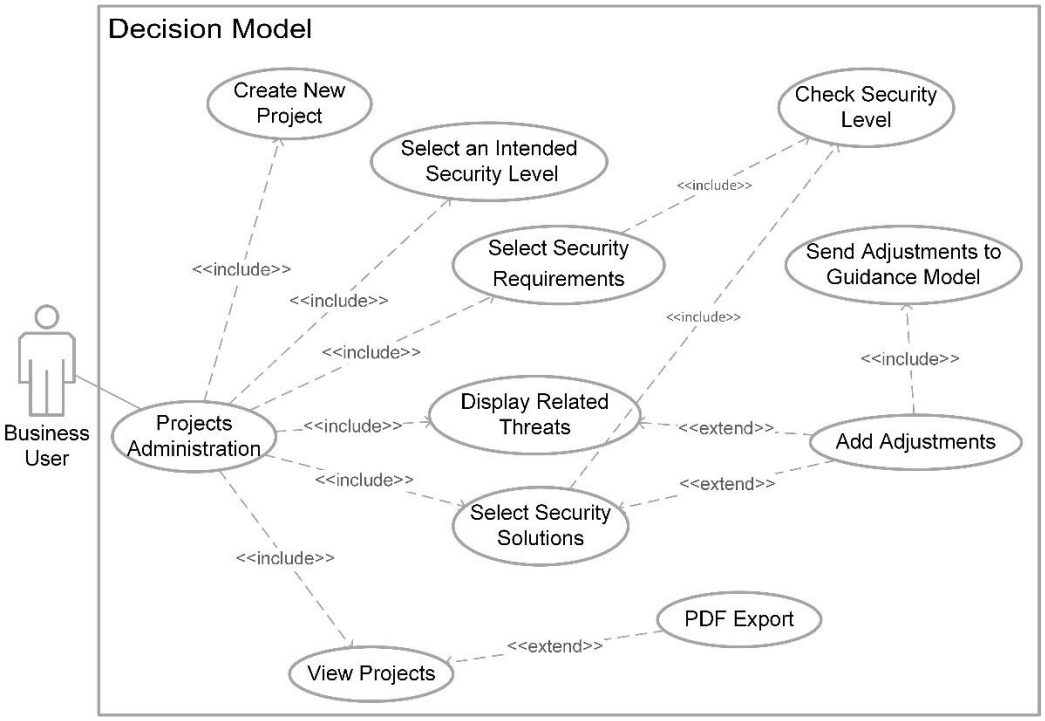

Figure 18. UML use case diagram of the decision model

4.4.3 Non-functional Requirements

The CFMS must take into account a set of non-functional requirements to be defined and met accordingly. The following list is the non-functional requirements that have been taken into account in this work:

Usability: The User Interface (UI) of the implemented CFMS must be user-friendly and intuitive. The users must have clearly identifiable data structures and the stored information must be presented in a well-structured manner. The users may not be overloaded with too much detailed information, but they must be able to retrieve it if necessary. Web browsers, such as Google Chrome and Mozilla Firefox, are supported.

Scalability: CFMS components should be easily replicable or even replaceable and the entire framework able to cope with the changes that might accompany any change in the security requirements. Hence, scalability is to be considered as a mandatory requirement. Furthermore, the framework should be also applicable to other domains than mobile security for MEAs.

Reliability: The implemented functions of the resulting prototype must work reliably and error-free. Errors are to be adequately intercepted and treated. User input errors caused by

users must be intercepted and checked immediately so that any invalid input is handled, and a meaningful warning message sent back to the user who caused it.

Correctness: The delivered data values and results must be correct, adequate and conform in quality with defined business scenarios.

Internationalization and localization: The designed UI and the prototype are initially implemented using the English language. Multilingual interfaces with the possibility to switch between different languages might be provided in future.

Legal and licensing aspects: The final implemented prototype will be open source and can be published after implementation.

4.5 Framework User: Role Definition

The CFMS supports two main roles, namely, security expert user and business user. The implementation of the CFMS considers these two roles to demonstrate its core functionalities, such as administrating and versioning of the guidance model, creating and editing projects. However, CFMS was so designed that further roles (e.g. restricted business user and technical user) can be easily included and administrated. Table 13 describes four possible roles together with their responsibilities and rights.

Role	Description	Responsibilities/Rights
Security Expert User	A security expert user might be CISO, Information Security Manager, IT Security Designer, IT Security Architect or any employee who is responsible for planning, implementing, and maintaining the security of mobile devices.	– Administrate the content of the guidance model – Guidance model versioning – Review information suggested by other roles – Create new projects – Edit existing projects that are not closed – Open and review a closed project
Business User	A business user might be Managing Director, project managers or any employee who is non-security specialist. This Role may take over the adopting of MEA.	– Create new projects – Edit existing projects that are not closed – Open and review closed projects

Business User (Restricted)	Any employee who uses MEA for work.	– Open and review closed projects
Technical user	A Technical user might be App developer (security by design[46]), IT administrator or any IT employee who is non-security specialist.	– Edit existing projects that are not closed – Open and review closed projects

Table 13. CFMS roles definition

4.6 Concept of Security Knowledge Transfer

This section defines the concept behind CFMS to transfer the security knowledge from security experts to other users who do not have specialized know-how in mobile security. Figure 19 shows the concept of the security knowledge transfer the CFMS supports.

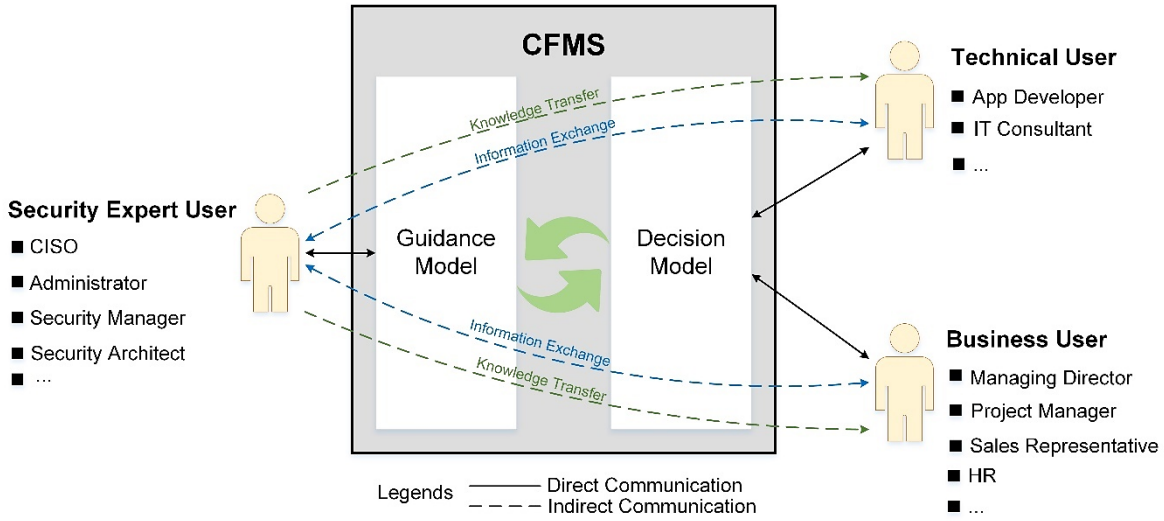

Figure 19. Concept of security knowledge transfer within CFMS

Source: (Hasan & Amin Rezaei, 2018)

On the left, security expert users administrate the guidance model. On the right, other users like technical users and business users can access decision model to create, edit or view projects (security concepts of MEAs). Thus, there is a direct communication between

[46] Developers can use the list of security measures the CFMS provides as a check list, which serves a high-abstract description of security measures that need to be applied. Information about how to implement these measures can be provided in future work by the integration of technical security catalogues (see Section 7.2).

security experts and the guidance model, and between other roles and the decision model. This direct communication means that user logs in to the CFMS with a defined role, and she/he can perform actions associated to that role. For instance, a security expert user can administrate security requirements (add, edit or delete) and map each of that requirements to security measures needed.

Security expert users, through their direct communication with the guidance module, prepare the security knowledge, documenting it in a structured way provided by the guidance model. At this step, the transformation mode "Externalization - Tacit to Explicit" takes place. The explicit security knowledge stored in the guidance model is made available to other user roles through the decision model. Through their direct communication with the decision model, other users have direct access to the security knowledge (as prepared by security experts). At this point, the transformation mode "Internalization – Explicit to Tacit" takes place. Consequently, the mobile security knowledge of security experts is transferred indirectly to other users.

In addition to security knowledge transfer, CFMS also supports information exchange between non-security experts and security experts. Since via the decision model, non-security experts can feed information back to the guidance model to be reviewed by security experts. This information is in form of justifications and adjustments.

Threats	1st Priority	2nd Priority	1rd Priority
Careless or unaware employees	37%	22%	15%
Cyber attacks to steal financial information	33%	23%	21%
Outdated information security controls or architecture	31%	16%	16%
Cyber attacks to disrupt or deface the organization	30%	22%	13%
Fraud	26%	27%	16%

Table 14. Excerpt of the results of the Statista's survey

Source: Statista[47]

A survey conducted by Statista shows that 37 percent of respondents identified unaware employees as their top priority when they were asked about the threats that have most

[47] The survey targeted 1,836 CIOs, CISOs, CFOs, CEOs and other information security executives from 64 countries and across all industry sectors. https://www.statista.com/statistics/258806/top-information-security-priorities/

increased their risk exposure over the 12 months. Table 14 shows an excerpt of the results of that survey. The security knowledge transfer mechanism provided in the CFMS will increase the employee's security awareness when using MEAs and consequently would increase the user acceptance rate.

Finally, the stakeholders of the CFMS are the enterprise and its employees. This would be the case of enterprises that have a good IT security department, where the security experts reside within the company. However, in case the enterprise outsources its IT, the CFMS can be used as a communication interface between the enterprise and the service provider. Furthermore, Section 6.3.3 presents also a possible utilization of CFMS as a communication interface between public and private sectors.

4.7 Summary

This chapter has explained the concept of the CFMS, including its structure and its models, guidance model and decision model. Guidelines that explain how the CFMS works in general have been presented together with the framework workflow. Moreover, the main requirements of CFMS have been also defined to show the core functions of this framework. Use cases for guidance model and decision model have been also presented. As this CFMS serves as role-based tools, examples of possible roles have also been defined. An important concept behind this framework -the transferring of security knowledge from security expert users to non-security expert users- has been also illustrated.

To conclude, whereas existing approaches such as MDM are mobile-device based approaches, the CFMS presented in this section is mobile-application based approach. It focuses on MEAs, however, it can also be extended for other application types. Whereas enterprises may use the existing approaches to enable mobile devices and integrate them into their existing IT infrastructure, they may use CFMS to specify which enterprise applications and resources can be accessed over mobile devices. A mobile-application based approach attains importance, since the mobile security requirements differ from one MEA to another, based on the importance of the data the MEA can access and consequently on the required security level. Thus, the needed mobile security measures can also differ from one mobile application to another. This, in turn, might cause different consequences when using MEA. The user acceptance of these consequences is also considered and investigated within this work (see Section 5.2.2).

A further contribution of the CFMS is that it mainly targets non-security specialists (e.g. Business Users) providing them with the needed knowledge for mobile security. This has been done through the concept behind this framework – the concept of mobile security knowledge transfer.

The following chapter presents the main content that has been included in the CFMS. This content has been administrated within the framework prototype, which has been demonstrated within enterprises to show its functions and possible utilizations (see Chapter 6).

5 Framework Data Structure

This chapter represents the content of the CFMS separated into three sections. Firstly, Section 5.1 explicates potential mobile threats as well as their potential consequences and the estimated risk on enterprise when adopting MEAs. Secondly, to overcome the potential mobile threats and to mitigate that estimated risks, Section 5.2 presents and suggests the needed security measures the enterprise should apply. Moreover, it proposes a model for user acceptance of that security measures. Finally, Section 5.3 presents a list of mobile security requirements classified into three security levels and it illustrates how to determine a security level for MEA taking into consideration multiple dimensions.

5.1 Risk Catalogue for Mobile Enterprise Applications

5.1.1 Overview

The risk catalogue provided within the CFMS includes the potential threats enterprises might face when using MEAs. Each threat is described along with its likelihood of occurrence and its possible impact on business. To mitigate the risks arising from these threats, CFMS, via its guidance model, enables security experts to map these threats to the needed security measures that have to be applied when using MEAs. These measures are presented in Section 5.2.

Security risk assessment methods and standards come with catalogues of threats and security measures. According to (Gramatica, Labunets, Massacci, Paci, & Tedeschi, 2015), these catalogues can be divided by size and specialization into two main types: Domain-general Catalogues, like BSI IT-Grundschutz Catalogues[48], ISO/IEC 27002[49], NIST SP 800-53[50], and domain-specific catalogues like Payment Card Industry Data Security Standards[51] (PCI DSS) for banking domain. An interesting empirical study was conducted to investigate whether existing threat catalogues facilitate the risk assessment process (Gramatica et al., 2015). The qualitative analysis in that study revealed that non-security experts are mostly worried about the difficulty of navigating through the catalogue (the larger and less specific

[48] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
[49] https://www.iso.org/standard/54533.html
[50] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
[51] http://www.pcisecuritystandards.org

the worse this task was). To avoid this, the risk catalogue provided within CFMS will support non-security experts since it is specific for MEAs. Moreover, (Gramatica et al., 2015) have outlined the key features that effective catalogues must have, namely, catalogue structure, catalogue size and coverage (for non-security experts, the size of the catalogue must kept low with focused content), catalogue as common language (the catalogue by itself provides a common terminology for all users) and security knowledge (non-security experts concern about the usability and navigability of the catalogues). Beside catalogues, STRIDE was provided by Microsoft as a threat modelling approach that defines six different categories of threats depending on the kind of attack that might be performed (Howard & Lipner, 2006). Those categories are: spoofing identities, tampering with data, repudiation, information disclosure, denial of services and elevation of privileges. Such an approach is basically a general classification scheme and can be used to classify threats when conducting risk analysis, however it does not provide a detailed listing of potential threats.

The existing risk catalogues as found in the literatures need a technical background in security. However, the risk catalogue provided within CFMS provide a simplified presentation of potential threats related to MEAs along with estimation of the risks to business. Through its guidance model, CFMS maps each threat in the risk catalogue to the needed security measures. Thus, the simplified presentation of the risks and mapping them to the security measures will help enterprises to justify the need for these measures to their employees (especially to those who do not have security technical knowledge). This in turn would increase the employee's security awareness when using MEAs and consequently would increase the user acceptance rate.

5.1.2 Mobile Business Scenarios

Mobile business scenarios are described to show the typical usage of mobile applications for work purposes. These scenarios help later to determine the potential threats to MEAs. They have been derived from practice through discussion with business users from different enterprises who use mobile devices for work purposes. Then, a set of possible assets related to MEAs have been derived (see Section 5.1.3), these assets help to estimate the possible impact on business when using MEAs.

5.1.2.1 Mobile Customer Relationship Management

Figure 20 shows a general infrastructure of a mobile enterprise. Enterprises have business applications like CRM and Microsoft SharePoint, and also have PIM services like email, contacts and calendar, which are mostly starting points and key requirements for mobile enterprise (Euler, Hacke, Hartherz, Steiner, & Verclas, 2012). On the left side of Figure 20, are mobile devices with different mobile OSes, like iPhone OS (iOS) and Android. For MEAs, the communications between these devices and the application server take place over internet and mobile communications (such as Wi-Fi, cellular networks, GPS) through mobile middleware, which encapsulate the access to different backend systems and prepare and send data to different mobile platforms per push or synchronization mechanisms. In addition, mobile devices can be enrolled and managed by Mobile Device Management (MDM) systems, like Sybase Afaria.

In this thesis, when analyzing the potential threats to MEAs, possible threats in company's server-side (mobile security layer and intranet) are out of scope. The remainder of this section describes an excerpt from a scenario on mobile CRM.

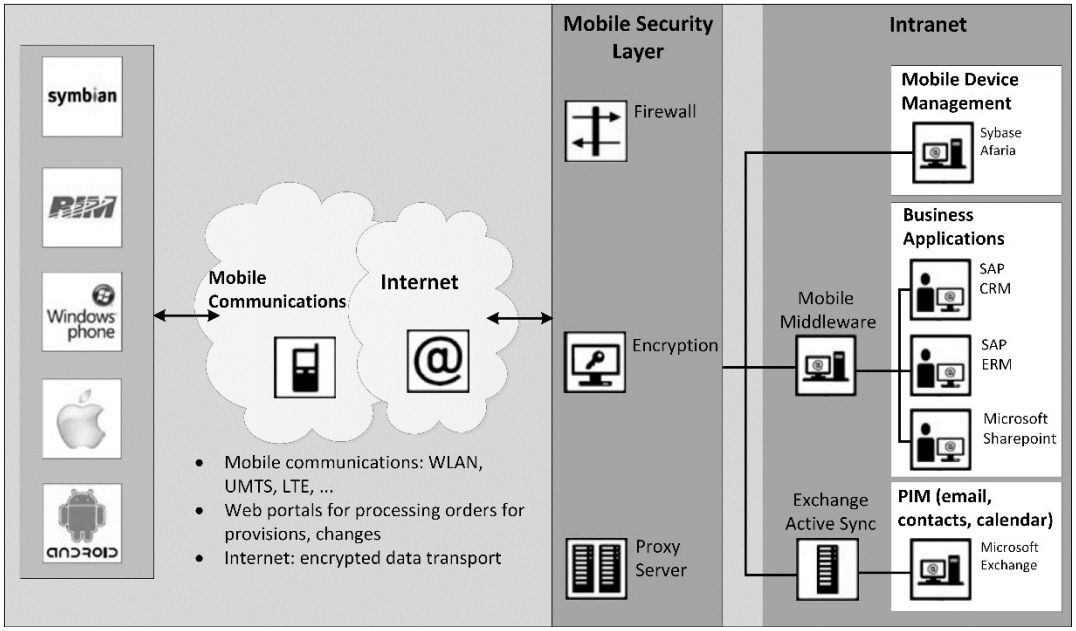

Figure 20. Mobile enterprise infrastructure

Source: Adapted from (Euler et al., 2012)

A sales representative (sales rep) is on a duty visit to a customer and uses a mobile CRM application on his mobile device to access important financial information about the customer. The sales rep is also able to gain insight into present and past sales and returns belonging to the customer, and can access the needed sales data from his enterprise database

server through the Internet. There are two options: a) WLAN connection, which is available in the customer's company, or b) mobile internet, which is provided by the Mobile Service Provider (MSP) of the sales rep's company.

The sales rep is also able to present new products and marketing campaigns to the customer. The information about products and marketing campaigns can be stored locally on the sales rep's tablet, so access to it does not need an internet connection, but such data should be synchronized from time to time.

During the duty visit, the sales rep connects his tablet with his enterprise's Virtual Private Network (VPN). Now he can use a reporting tool to get some personal information about his customer. Here, personal data are seen as information that the customer gives about himself, his family, his coworkers or his business that are not directly related to some kind of monetary or service-related transactions. Such data are stored on an enterprise database server and can be accessed via mobile devices. During the sales negotiations with the customer some difficulties appear. The customer did a supplier evaluation and concluded that there is a cheaper supplier than the sales rep's company. The sales rep now has to act quickly to retain the customer. He uses his tablet to get access to a reporting tool in order to get some information about the customer's possible frequency of orders, and the customer's willingness to pay. Such information helps the sales rep to estimate the customer's value to give him some kind of discount on the offered transaction conditions. After this meeting, the sales rep heads home. Once there, he uses his smartphone to connect to the internet via his own WLAN in order to create a report about his working time, and to give feedback about extra hours and travelling distances using a mobile application adopted by his HR department.

5.1.2.2 Other Use Cases for Mobile Enterprise Applications

To support and improve business decisions, a Business Intelligence (BI) system is used to collect and process business data. BI is defined as a broad category of technologies, applications, and processes for gathering, storing, accessing, and analyzing data to help its users make better decisions (Wixom & Watson, 2010). Due to the advance in mobile technologies, the use of BI systems is now extended for mobile devices. Thus, mobile BI is defined as "*a system comprising both technical and organizational elements that present historical and/or real-time information to its users for analysis on mobile devices such as*

smartphones and tablets (not laptops), to enable effective decision-making and management support, for the overall purpose of increasing firm performance" (Peters, Işık, Tona, & Popovič, 2016). In the context of MEAs, mobile BI has the potential to significantly support decision-making outside the office by enabling employees with the real-time access to critical business information (Brockmann, Stieglitz, Kmieciak, & Diederich, 2012). However, in contrast to these advantages, adoption of mobile BI faces security challenges. According to BI-Survey[52], security and privacy are major concerns of companies when they want to adopt mobile BI solutions, as the usage of mobile BI may put sensitive or confidential information at greater risk of being breached.

The second use case of MEA is in the ERP domain. The traditional core modules for ERP systems are accounting management, financial management, manufacturing management, production management, transportation management, sales & distribution management, human resources management, supply chain management, customer relationship management and e-business. (Rashid, Hossain, & Patrick, 2002). Albashrawi and Motiwalla defined mobile ERP as following: *"Mobile ERP refers to the use of mobile device (e.g. a smartphone or tablet) to perform different business functions such as sales, customer relationship management and supply chain management through a single integrated system. In other words, it is a tool used to carry out business functions on-the-go"* (Albashrawi & Motiwalla, 2016). Security has been considered as one of the major challenges when adopting mobile ERP (Omar & Marx Gómez, 2017; Omar, Rapp, & Marx Gómez, 2016).

5.1.3 Assets in Relevance to Mobile Enterprise Applications

After mobile business scenarios are defined, a set of assets is extracted from those scenarios. The relevant assets to MEAs play an important role in estimating the possible impact of a potential threat on business. Assets are defined as abstract or concrete resources that an enterprise must protect from misuse by an adversary; they can be tangible, such as processes and data, or more abstract concepts such as data consistency (Myagmar, Lee, & Yurcik, 2005). Thus, an asset does not only represent a physical object and data, but also business processes. For example, if an MEA uses customer data to analyze the buying behavior of the customers and the process of this analysis is threatened, the company gets distorted results,

[52] https://bi-survey.com/mobile-bi

which can lead to an adverse impact on the business. Rhee et al. have identified a set of possible assets that relate to MDM (Rhee, Won, Jang, Chae, & Park, 2013). Assets can be general or related to a use case (Stango, Prasad, & Kyriazanos, 2009). However, the assets that are extracted in this thesis focus on assets relevant to MEA from a mobile device perspective. Assets related to the backend side like MDM server and MDM management console, or those related to other mobile technologies such wireless networks are not in scope of this work.

*C: Confidentiality; I: Integrity; A: Availability

Category	Asset	Value*
Business Data (B) (Corporate Context)	Customer Business Data (B1)	C, I
	Customer Personal Data (B2)	C, I
	Potential Customer Business Data (B3)	C, I
	Product Data (B4)	C, I
	Contacts (B5)	C
	Messages (B6)	C, I
	Campaign Data (B7)	I
	Company Infobox (B8)	I
	Business Processes and their Data (B9)	C, I, A
	Authentication Data (B10)	C
	Documents (B11)	C
Personal Data (P) (Private Context)	Media (P1)	C
	Contacts (P2)	C
	Documents (P3)	C
	Messages (P4)	C
	Authentication Data (P5)	C
Technical-related (T) (Private and Corporate Context)	Mobile Device (T1)	A
	Battery (T2)	A
	Configuration Data (T3)	I
	Hardware (T4)	A
	Mobile OS (T5)	I
	Mobile Services (T6)	A

Table 15. Potential assets associated to the usage of MEAs

Source: (Hasan & Marx Gómez, 2017)

Based on the derived scenarios, literature review and discussion with experts from business domains, a set of assets that are relevant to MEAs have been extracted in the present work. These assets are depicted in Table 15 and classified into three categories.

The first category is business data (B) that contains all corporate-context data that can be stored locally on mobile device or accessed via MEAs. This category contains customer business data (e.g. customer's order history, list of current services the customer is using), customer personal data (e.g., gender, address, phone, date of birth, notes about customers' behavior, like notes about hobbies from personal conversations), data about new products (product data), text messages, calls and business contacts. This category may also include campaign data (e.g. marketing campaign) and information about the company (company's infobox). It is clear that business processes and their data, which should only be accessed by employees, can possibly be threatened. If these kinds of data are altered, deleted, or tracked by an attacker, it can cause severe damage to the business (e.g. misplaced or forgotten orders, deleted customer profiles). Therefore, an attack on these data can cause an enormous direct or indirect negative financial impact on the company. In addition, MEAs may store credentials (like username/password or a hash) on a mobile device to avoid requesting the users continuously for the authentication. These credentials are represented here as authentication data.

The second category, personal data (P), contains all the private-context data that can be stored or accessed via the mobile device and its mobile applications. This category may contain different types of media like videos, pictures and social networking. Some assets from a corporate context may also be used in a private context, these can be authentication data, text messages, contacts and documents. These data are typically stored on every smartphone or tablet.

The third category includes the technical-related (T) assets, which are shared for use in private and corporate context, such as battery, hardware (like SD card camera, microphone), mobile OS and the mobile device. The configuration data of the mobile device and services used are classified under this category.

The value of an asset can be estimated in terms of money, but also as impact in terms of CIA (Confidentiality, Integrity and Availability) (Lederm & Clarke, 2011). In this thesis, the value of an asset is estimated as impact in terms of CIA. For example, confidentiality and

integrity should be maintained for business customer data. Confidentiality is not relevant for Campaign Data, but integrity is.

5.1.4 Risk Catalogue Structure

The potential mobile threats are summarized in a risk catalogue, which enables a rapid and simplified overview of the threats included. Table 16 shows the structure of this catalogue and an excerpt of it is shown in Appendix A categorized into five categories.

Threats	**Description & Risk Estimation**	
Threat ID	Threat short description	
Threat Name	**Likelihood of Occurrence**	Low, Medium or High
	Short argumentation about the likelihood of occurrence	
	Possible Impact	Low, Medium or High
	Short argumentation about the possible adverse impact on business Potential affected assets: List of possible affected assets (see Section 5.1.3)	
	Risk Level	Low, Medium or High

Table 16. Risk catalogue structure

Source: (Hasan & Marx Gómez, 2017)

This structure presents the attributes of the risk catalogue. Each threat has the following attributes:

- *Threat ID* is used for purposes of navigating through the catalogue, this ID has the following format Category-T_n, e.g. MD-T_1 indicates the first threat in Mobile Device Category (MD).
- *Threat Name* briefly defines a threat.
- *Threat Short Description* provides a short description of the threat. This description should be understandable for users without the need of technical knowledge in mobile security.
- *Likelihood of Occurrence* provides an estimated value of probability that a threat occurs. In the risk catalogue, this value is shown as low, medium or high along with a short argumentation of this value.

- *Possible Impact* includes an estimated value of the adverse impact on the enterprise if the threat occurs. In the risk catalogue, this value is shown as low, medium or high along with a short argumentation about the assigned value. In addition, potential assets that can be affected is listed.
- *Risk Level* ranges again from low to high as it is a combination of the likelihood of occurrence and the adverse impact.

The following Section illustrates how the likelihood of occurrence, possible impact and risk level are estimated.

5.1.5 Risk Estimation

Stoneburner et al. define the risk as follows: „*Risk is a function of the **likelihood** of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that **adverse** event on the organization.*" (Stoneburner et al., 2002).

Two factors are taken into consideration when estimating the risk level of a threat, namely likelihood of occurrence and adverse impact on business. The estimation of the risk levels is shown in Table 17.

Threat		**Adverse Impact**		
		Low	Medium	High
Likelihood of Occurrence	High	Medium Risk	High Risk	High Risk
	Medium	Medium Risk	Medium Risk	High Risk
	Low	Low Risk	Medium Risk	Medium Risk

Table 17. Risk levels estimation matrix
Source: (Hasan & Marx Gómez, 2017)

The first factor "likelihood of occurrence" has been estimated based on literature review and available reports taking into consideration two criteria: a) the estimated frequency of threat appearance and b) motivation and capability of attacker.

The second factor "adverse impact" on business is rated based on the potential assets (see Section 5.1.3) that can be affected by a threat. For instance, the impact is considered high if the threat may enable access to personal customer data; publishing this information can damage the reputation of the enterprise severely, and lead to a huge loss of monetary resources. On the other hand, the potential impact is considered medium if an employee

cannot carry out a business process for a short time because the service needed is unavailable. Table 18 shows the estimation matrix of the adverse impact. In addition, further examples for potential business impact include financial impact (money lost, lost opportunities), reputation damage, additional costs for corrective actions or repairs, and violation of legal compliance.

Loss of CIA	**Potential Impact**		
	Business Data (B)	Technical-related (T)	Personal Data (P)
C – Confidentiality	High	n.a.	High
I - Integrity	High	High	Medium
A – Availability	Medium	Medium	Low

Table 18. Adverse impact estimation matrix

5.1.6 Threats Categorization and Overview

This section provides a threats overview categorized into five categories according to the threat source. These categories enable a simplified overview for users who do not have technical knowledge in mobile security.

5.1.6.1 Mobile Device Category

This category covers the physical threats that are related to the mobile device itself. Due to their small size and high mobility, physical security of mobile devices is an important consideration (Au & Choo, 2017). Mobile devices can be attacked in several ways. They can be harmed physically, but also the data stored locally on them and business processes can be threatened as well.

The first threat in this category is the *loss of mobile devices*. Back to the business scenario; the sales rep may lose his mobile device, while in a hurry on the way to the customer. Consequently, he would not be able to perform business processes such as placing orders for the customer. In addition, if business data are stored locally on the mobile device, the impact on business can be high, since corporate or customer data can be exposed and sold to competitors or other potential buyers. On the other hand, if the business data are not directly stored on the mobile device, the confidentiality and integrity of these data are not affected. However, the mobile device could still be used to access business data or perform business processes through MEAs installed on it, which may be not secure enough, or whose login

data is stored on the mobile device. This leads to loss of authenticity of certain performed actions and processes.

According to the Kaspersky survey in 2013, one in every six users has experienced loss, theft or catastrophic damage to a mobile device (such as laptop, smartphone or tablet) in the last 12 months (Kaspersky, 2013b). According to the same survey, 32% of smartphones and 28% of tablets had work emails, 20% of smartphones and 29% of tablets had business documents. In addition, a survey conducted by IDG Research on behalf of Lookout revealed that one in ten smartphone owners were victims of smartphone theft (Lookout, 2014). Moreover, Srinivasan and Wu differentiated between device theft and data theft (Srinivasan & Wu, 2012); according to them, the theft of a mobile device is random in nature and the adversary is not interested in the data stored on the device, but motivated by the financial gains from reselling of a stolen mobile device, however the third party who buys the device may be interested in the data on the device. Lost or stolen mobile devices could be used to gain access to user data stored on the mobile device or they could be used as an entry point into the user's corporate network (Au & Choo, 2017; Imgraben, Engelbrecht, & Choo, 2014). To sum up, the potential impact on business through lost or stolen mobile devices is rated as high.

The second threat in this this category is *unattended mobile devices*, which are left temporarily unlocked and unsupervised (Hasan, Schäfer, Marx Gómez, & Kurzhöfer, 2016). In the business scenario for example the sales rep leaves his tablet unattended in order to make a call with his smartphone. An unattended device for a short time is not such a great threat, because of the limited time and probable lack of intention of an unauthorized user to cause severe damage to the business. Therefore, the associated risk to business from unattended mobile devices is estimated as medium.

USB connection can be used to synchronize the mobile device with a PC, because most mobile platforms allow a mobile device to be connected as a USB storage device. In the case of loss of a mobile device or an unattended mobile device, an attacker can try to compromise the software used to synchronize the mobile device to access locally stored information or install malicious applications on the mobile device (Téllez & Zeadally, 2017). Even locked mobile devices, they can be fully compromised when they are connected via the USB to a PC (Wang, Z. & Stavrou, 2010). Thus, sensitive information like authentication credentials, business information, activity logs (e.g. mobile device usage), and private information (e.g. pictures or videos) can be threatened via the mobile device USB as an attack vector.

Finally, the *physical damage* of mobile devices is considered as a threat (Hasan, Schäfer et al., 2016). Every piece of the hardware (e.g. battery, network adapter, flash memory) can break at any time, because of defects in the production process or mishandling through the user; the sales rep can unintentionally drop his mobile device due to its small size. The direct financial loss is the mobile device itself, however, the sales rep cannot look up or place a customer's order because of a broken mobile device. This can result in an indirect financial loss, and the productivity of the sales representative can consequently decrease. Moreover, if the mobile device's data storage is broken, important business data that stored locally can be lost. However, most business data are not only stored on the device, but they are synchronized with the company system. The impact on business is therefore low. Physical damage of mobile devices is unintentional and the motivation and capability to threaten the business is low, so that the likelihood of occurrence of such threats is estimated as low, and consequently the associated risk is also estimated as low.

5.1.6.2 Mobile Applications Category

MEAs can be threatened through third party mobile applications that unintentionally exploit errors or use access rights not needed to perform their tasks. Moreover, malicious software or so-called malware can threaten MEAs.

The first malware aimed at smartphones hit in 2004 and the first virus for mobile phones was written by a group known as 29A in June 2004 (Ramu, 2012). Viruses contain every type of malicious code, mostly unintentionally downloaded by the mobile device's user. This can happen, for example, through drive-by downloads. There are many different forms of malware, e.g. trojans, worms, spyware, ransomware and grayware. These malwares can be can be distributed through different channels like peer-to-peer networks or through mobile applications stores from the operating system vendor. For instance, although the submission of mobile applications for Apple App Store are subject to approval by Apple's App Review team[53], mobile security company Lookout has reported a malware called XcodeGhost[54], which uses a tampered version of Apple's Xcode to steal data from iOS devices, was

[53] https://developer.apple.com/app-store/review/
[54] https://blog.lookout.com/xcodeghost

distributed through the Apple App store, so that hundreds of millions of iOS devices were potentially affected.

Furthermore, as stated by (Mulvehill, 2016), "*The risk from mobile malware is real and Growing*". According to the same author, the proliferation of mobile applications that conduct real business using access-sensitive and confidential information is one of the key contributors to the threat from mobile malware. Moreover, as typical users may have banking, credit card, hotel, airline and corporate applications installed on their mobile devices (Mulvehill, 2016), attackers will be highly motivated to target mobile devices and their applications. In addition, Kaspersky found over one hundred thousand mobile malware in 2013 and "*the trend is highly visible and continuing*" (Kaspersky, 2013a).

In comparison to normal malware on PCs, there are several additional attack vectors inherent to mobile devices using SMS, MMS, USB or different device sensors (Ramu, 2012). Moreover, consumer awareness of mobile security threats is still not mature, so users who would never install software from an unverified source on their PC readily click on links in SMS messages and unintentionally download files from unknown sources on their mobile devices (Chatterjee, Paul, Roy, & Nath, 2016). Malware can perform very different malicious actions depending on its type. It ranges from the collecting of user patterns, through denial of certain services, to the theft and leakage of critical business information like customer or production data. Therefore, the impact on business is estimated as high.

Trojans typically come with applications that look useful, and then deliberately perform harmful actions once installed, their real intention is a malicious action targeting a mobile device and its data (v Do et al., 2015). Example of mobile Trojans is "Trojan-Banker.AndroidOS.Svpeng", which obtains administrator rights on an infected mobile device in a hidden way and, using these rights, intercepts requests when the user tries to access paid online services and online banks and asks the user to enter his or her banking information (AO Kaspersky Lab, 2015). Another example of mobile Trojans is ZitMo, which is a mobile version of the Trojan Zeus that works in conjunction with the Zeus banking Trojan to steal login information or money from user's bank account (Pu, Chen, Huang, Liu, & Zen, 2014). According to (Bach, 2015), approximately 30% of Trojans targeted at stealing financial information, and the remainder are capable of performing malicious actions such as stealing personal information, sending SMS to premium numbers, keylogging and deploying cryptographic ransomware on the device, effectively hijacking images and files stored on it.

Worms can typically self-reproduce and propagate themselves to mobile devices via mobile technologies like SMS, MMS or Bluetooth. For instance, a Symbian OS worm that targets mobile phones through Bluetooth, so that the infected mobile becomes a portal for further propagation of this malware to all its Bluetooth neighbors. This can result in massive consequences such as increased network throughput, battery depletion and mobile failure by corruption of system binaries (Adeel & Tokarchuk, 2011).

Another type of malware is spyware, which typically focuses on collecting data from the user's mobile device without the user's knowledge or approval and sending it to an attacking entity (Lookout, 2011). The collected data can range from personal data like locations, contacts and messages to critical business data used by MEAs. A further type of malware is grayware, often downloaded and installed with free software or applications, for example adware. What makes adware dangerous is that the proposed advertisements can lead to scamming websites or websites with more downloadable malware, which can carry out many unintended activities without the user being even aware of them (Rao & Nayak, 2014).

There is also a type of malware known as ransomware that prevents the user from accessing some functionalities or files, requiring a payment in order to unblock the access to them (Lacerda, Queiroz, & Barbosa, 2015). For instance, Lockdroid.E is a Trojan for Android devices and functions as a typical ransomware that locks the victim's screen; the victim may then be asked to pay a ransom to unlock their mobile device (Venkatesan, 2016).

In mobile devices, *SMS Abuse* is considered as a threat, so malware can also abuse the SMS on mobile device silently by unauthorized sending of forged SMS messages to the recipients causing charges like premium-rate text service (Tu, Li, Peng, Li, & Lu, 2016). Another kind of SMS abuse is SMS spoofing, where the attacker can replace the originator's phone number and then send out SMS messages to a recipient on behalf of another mobile user without his/her awareness or involvement (Tu et al., 2016). Beside the victim's monetary loss, SMS abuse can also result in account hijacking, unauthorized donation, and unauthorized subscription (Tu et al., 2016).

5.1.6.3 Mobile Operating System Category

A mobile OS can serve as a source for possible threats to MEAs. Two main mis-configurations are considered as threat sources under this category. The first one is the *rooting of mobile OS*. Rooting itself is not a threat. However, it compromises the integrity

of the mobile OS and can make security technologies that depend on the operating system, such as containers, vulnerable to attack (Lookout, 2015). Rooting describes an action from the user to gain root permissions of the respective device and operating system. This process is generally referred to as rooting on Android OS and jailbreak on iPhone OS (iOS) (Damopoulos, Kambourakis, Anagnostopoulos, Gritzalis, & Park, 2013). Rooting of a mobile OS is usually used to remove preinstalled, unwanted applications, customize the theme and functions of the mobile OS or so that the user can access unofficial app markets and install unofficial mobile applications. Consequently, this not only bypasses their mobile device's built-in security, but also considerably increases the risk of downloading malicious apps; recent reports reveal that up to 32% of apps on unofficial markets contain malicious content (Bach, 2015).

By rooting of mobile devices, not only the user is able to use the permissions gained, but also malware or attackers can use them to perform severely adverse actions. This increases the vulnerability of the mobile OS. Gartner predicted that by 2017, 75% of mobile security breaches will be the result of mobile application misconfigurations like jailbreaking or rooting (Gartner, 2014). According to the same report, Gartner recommends that IT security leaders enforce "no jailbreaking/no rooting" rule, and devices in violation should be disconnected from sources of business data, and potentially wiped, depending on policy choices. If an attacker gains root access to the mobile OS, this may give access to the MEAs, intercepting data streams to prohibit remote IT commands, or give access to data stored locally on a mobile device (Michaelis, 2012).

The second misconfiguration possible in this category is *missing updates* of the mobile OS. Missing updates can cause risk because they often include patches and security updates. However, the impact depends on how critical the missing updates are. On the one hand, a mobile OS like Android has a wide range of versions, where each version supports only a specific model of mobile device, so that the mobile OS has to be optimized accordingly. Figure 21 shows the distribution of Android versions among smartphone owners as of September 2016.

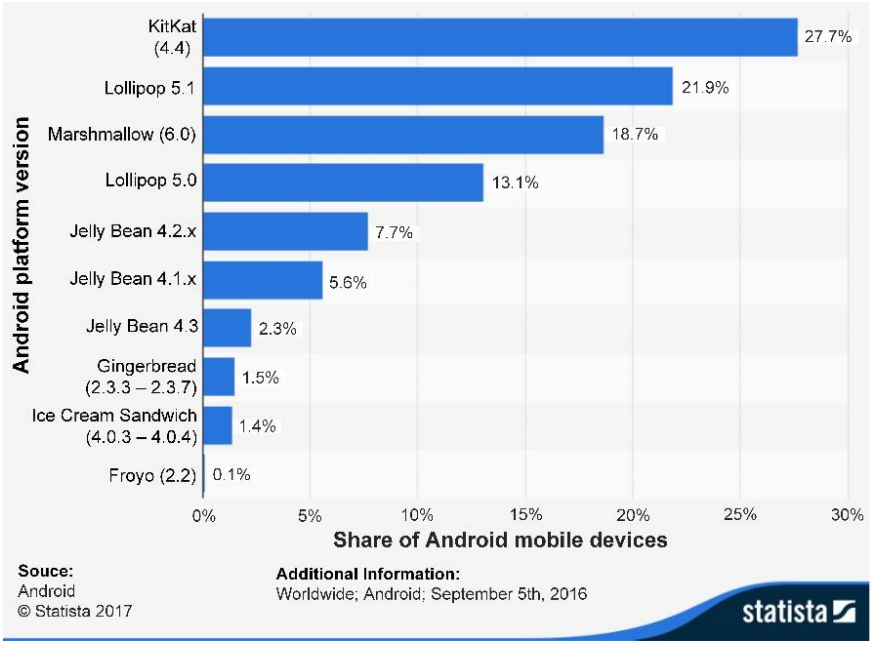

Figure 21. Android version market share distribution among smartphone owners as of September, 2016[55]

On the other hand, mobile OS like iOS does not have a multiplicity of versions like Android, but in spite of that, it also takes a significant time to get a new version installed on all Apple devices, a reason behind this could be that the newly released version of iOS does not support earlier models of Apple devices. Figure 22 shows the distribution of Apple devices by iOS version worldwide in 2016.

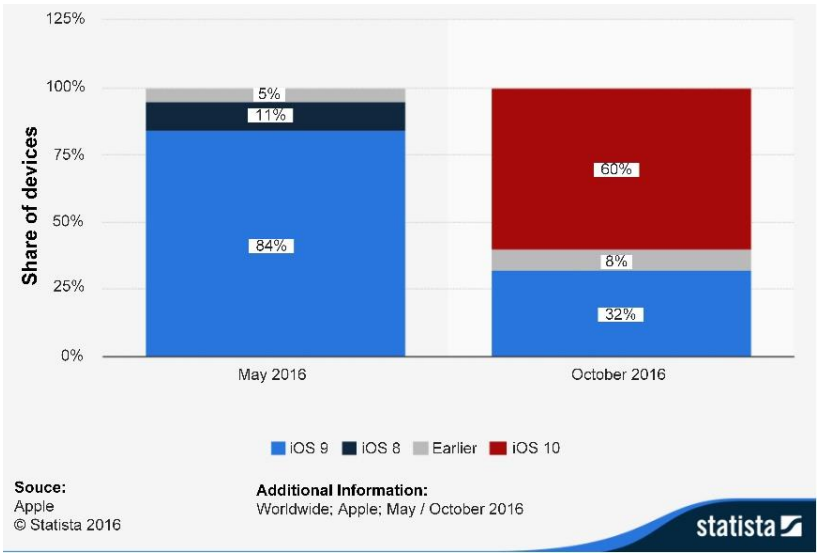

Figure 22. Share of Apple devices by iOS version worldwide in 2016[56]

[55] https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/
[56] https://www.statista.com/statistics/565270/apple-devices-ios-version-share-worldwide/

In addition, as reported by Skycure, 71% of mobile devices still run on security patches that are more than two months old, because the carriers are slow to make them available to users (Seals, 2017). Malware and other kind of mobile threats mostly depend on unpatched vulnerabilities to be successful.

5.1.6.4 Wireless Networks Category

The widespread usage of broadband mobile Internet also brings threats such as the Denial of Service (DoS) attacks and botnets (Oğul & Baktır, 2013). Different wireless networks can be used to launch attacks against mobile devices. Two main types of threats are discussed under this category, namely, Denial of Service (DoS) and Man-in-the-Middle (MitM).

The first type, the DoS attack, denies performing a certain service or running a certain software or application. DoS attacks do not only focus on the denial of services, they can reduce the ability of valid users to access resources (Myagmar et al., 2005) or they can induce incorrect operation (Rhee et al., 2013). For instance, DoS can be performed against mobile devices by sending thousands of silent SMS (or stealth SMS), which are indicated neither on the display nor by an acoustic signal (Croft & Olivier, 2007). Moreover, the intended victims will not be aware of such an attack, but will recognize an abnormal decline in battery charge capacity and the inability to perform other mobile services. Furthermore, DoS-attacks can also target Mobile Adhoc Networks (MANETs) like direct Peer-to-Peer Wi-Fi or Bluetooth-connections. As stated by (Padgette, Chen, & Scarfone, 2012), Bluetooth is susceptible to DoS and impacts include making a device's Bluetooth interface unusable and draining the device's battery. However, these types of attacks are not significant due to the required close range, and therefore they can easily be avoided by simply moving out of range (Padgette et al., 2012).

Another kind of DoS is sleep deprivation or battery exhaustion, which particularly targets a mobile devices battery. Such threat can drain the battery of a mobile device by preventing the device from saving battery in sleep modes or similar through constant service requests (Buennemeyer, Gora, Marchany, & Tront, 2007; Martin, Hsiao, Ha, & Krishnaswami, 2004). In addition, sleep deprivation can also be applied in form of a flooding attack in MANETs where either a specific node or a group of nodes are targeted by forcing them to use their vital resources (e.g. Battery) (Jain, S., 2014). The impact level of this type of DoS is estimated as low.

The most commonly known case of DoS is the Distributed Denial of Service (DDoS) attacks, in which, a huge number of malware-infected mobile devices and PCs are involved in the generation of attack traffic to disrupt the correct working of a server. DoS attacks can be launched through wired and wireless network connections like Wi-Fi or internet connections from a Mobile Service Provider (MSP). Typically, such networks can be attacked via DDoS attack, launched using botnets. A botnet is a network of internet connected devices, which were infected with malicious software without the knowledge of their users, and is capable of executing computationally demanding tasks in feasible time (v Do et al., 2015). DDoS attack is one of the adverse actions that can be performed by using botnets, with their users unaware of that. Clearly, an attack on the cellular internet of an MSP can have adverse consequences for businesses. If such an attack is launched, the use of services like Long Term Evolution (LTE) can be limited or completely denied (Jermyn, Salles-Loustau, & Zonouz, 2014). A look at the business scenario (see Section 5.1.2.1) reveals that MEAs often need a functioning Internet connection to company's server. If the sales rep wants to place an order, he needs an Internet connection to the server. If the server or the mobile internet connection of the MSP is attacked through a Denial of Service-attack, he cannot place this order. This might cause an indirect financial loss, because the loss of the availability of business services. Therefore, the impact level is estimated as medium.

The second type of mobile network threats is Man-in-the-Middle (MitM) attack, which intercepts communications in networks to eavesdrop, alter, or delete exchanged data. The attacker is placed in the middle between the client and the server. For instance, (Moonsamy & Batten, 2014) described three popular MitM attacks (SSL Hijacking, SSL Stripping, DNS Spoofing) targeted at smartphone applications. Two scenarios of MitM attacks were simulated by (Kennedy & Sulaiman, 2015). The first scenario used unencrypted Wi-Fi networks, that do not provide encryption of network traffic. A typical of such network attack is captive portals, that typically use encryption to secure user's credentials when authenticating to the network, but the network traffic is not encrypted and can be sniffed over the air (Godber & Dasgupta, 2002). In the second scenario, an active malicious actor can control the wireless access points and can launch attacks against mobile applications. For instance, the "evil twin" attack can be used to deceive users into connecting to a rogue access point (Nikbakhsh, Manaf, Zamani, & Janbeglou, 2012). Returning to the business scenario, the sales rep may use an available open Wireless Local Area Network (WLAN)

when meeting with customer, unaware that this network is unsecured. This open WLAN may be provided by an adverse entity, not the customer' company.

Mobile devices connected to unsecured Wi-Fi hotspots increase the threat of communication interception, such MitM attacks and password eavesdropping (Fitzgerald, Neville, & Foley, 2013; Landman, 2010). MitM attack can also take place on other mobile Internet networks that use cellular systems like the 2G (GSM) and 3G (UMTS) (Meyer & Wetzel, 2004). Moreover, 4G (LTE) networks might be vulnerable to MitM attack by impersonation of the user International Mobile Subscriber Identifier (IMSI) (Bhasker, 2013). Although LTE is widely used and it is considered to be more secure than UMTS and GSM against MitM attack, using a rogue base station broadcasting at a high-power level, an attacker can force a user to downgrade to either GSM or UMTS (Cichonski, Franklin, & Bartock, 2016). Consequently, this can potentially enable a MitM attack. If a MitM attack is successful, the attacker can capture and manipulate sensitive business information. So this leads to loss the integrity and confidentiality of business data. Consequently, the possible impact of MitM attack is estimated as high.

5.1.6.5 Mobile User Category

When talking about mobile security, the users are as important as the security technology that is put in place. This category deals with potential threats that can be caused by the user as a potential threat source, through unintentional actions while unaware of the security risks while using the mobile device. One of the main issues in this regard is the use of, or access to, untrusted websites content, accessed by users.

The first example in this category is *phishing*. Typically, business users are unaware of such risks and threats, to which they are exposed by simply browsing the internet and looking up things like shops, online travel agencies and others (Marble et al., 2015). Through phishing the attacker tries to steal login and personal data from the user, e.g. using mails, SMS, or advertisements as channels. These are used to trick the user into entering private information and login data in replicas of commonly known websites or through offering of free downloads or low price shopping. Phishing is a serious threat for business in areas like auction sites, payment services, retail and social networking sites (Symantec, 2014). In addition to the direct costs of phishing, a company can also lose the trust of customers if their data is compromised. Furthermore, if the attacker succeeds in obtaining login

credentials (username, password and PIN), then the attacker can perform all actions authorized to the mobile device's owner. Thus, the attacker may be able to access all assets related to MEAs installed on the mobile device. Consequently, this leads to loss the integrity and confidentiality of business data. Therefore, the impact level is estimated as high.

McAfee Labs Threats Report in 2014 revealed that phishing continues to be an effective tactic for infiltrating enterprise networks (McAfee Labs, 2014). According to the same report, 80% of test takers in a McAfee phishing quiz have fallen for at least one in seven phishing emails. Furthermore, results showed that finance and HR departments, those holding the most sensitive corporate data, performed the worst at detecting fraud, falling behind other departments by a margin of 4% to 9%. Attackers are motivated to target mobile devices for several different reasons, one of which is the mobile device's display constraints that could be used to hide the URL bar (Abura'ed, Otrok, Mizouni, & Bentahar, 2014). To sum up, the risk level of phishing is estimated as high.

The second type of threats under this category is *downloading of untrusted mobile applications*, which is another type of threat that may take place because the user is unaware of the associated risks of such applications. The most known form of such threat is called drive-by download, which works by exploiting vulnerabilities in web browsers, plug-ins or other components that work within browsers (Levinson, 2012). These threats try to prompt users through advertisements or malign websites to take an action that downloads malware on their mobile devices. An area of concern for mobile devices are also the Quick Response (QR) codes that can be scanned with a mobile device camera as input into a QR reader app; malicious attackers can then use these codes to redirect users to malicious websites to download malicious apps (Marble et al., 2015). As the drive-by download can install and launch a malware, the impact to business is estimated as high.

Finally, *unaware privilege granting* to third party mobile applications can take place without the knowledge of the mobile user. For example, although Android and iOS inform the user about the access rights required while installing a mobile application, and users are warned or informed about that, they tend to overlook this information and just grant the access privileges to the mobile application. Potential risk to business can arise if the installed third-party application gets the privilege to access mobile device's contact list, including business contacts.

In general, iOS is considered to be a relatively a secure platform and users think that they are not susceptible to attacks, since Apple has one app store, performs heavy screening and applies app sandboxing. However, users can install configuration profiles that anyone can create and send them to any iOS device through email, SMS, website or app, where compared to normal apps, there are no store, no screening and no sandboxing. These configuration profiles are legitimately used by IT departments, MDM owner, apps, service providers, or cellular carriers to configure elements on the mobile device. Thus, these profiles can also be used for malicious purposes, so that, the iOS security model can be broken and iPhones can be attacked through installing malicious configuration profiles (Amit, 2014; Amit & Sharabani, 2014).

The aforementioned threats under this category are associated with social engineering, which is based on human behavior. For instance, phishing is solely based on social engineering by exploiting human vulnerability in order to trick the victim into providing sensitive credentials (Abura'ed et al., 2014).

5.1.7 Summary

In this section, a risk catalogue, which includes a list of potential mobile threats classified in the five categories previously presented. First, mobile business scenarios have been defined to get insight in the typical usage of MEAs. Then, a set of assets related to MEAs have been determined considering the scenarios defined. This catalogue gives a simplified overview of mobile threats. Generally, there are existing risk catalogues, but they show a generic and not business-context view, which makes them complex for business users or users who do not have technical knowledge in mobile security.

The resulting risk catalogue was evaluated through discussion with people from business domain within two companies, THOSA-IT GmbH[57] and Lufthansa Industry Solutions GmbH & Co. KG[58]. They found that the threats overview in the risk catalogue is detailed enough and would allow a reader to access important information quickly. The structure of the risk catalogue was perceived as useful and comprehensive, and the included argumentation would allow interested readers to gain even further insight in each threat and its associated

[57] https://www.thosa-it.de
[58] https://www.lufthansa-industry-solutions.com/de-en

risk. Moreover, they found that mapping the assets with potential threats is meaningful for business users especially for those who do not know which assets can be threatened when using mobile devices for work purposes.

The structure of this catalogue was included in the CFMS and the security expert users can add, edit and delete threats through the CFMS guidance model, its content being made available to other users through the CFMS decision model. To mitigate risks, each threat in the risk catalogue is mapped to one or more security solutions. This mapping is done by security experts via the CFMS guidance model. Each security solution consists of a combination of one or more security measures, which are presented in the following section.

5.2 Mobile Security Measures

In order to mitigate the potential risks when enterprises adopt MEAs, the enterprise need to apply suitable security measures. First, this section presents these security measures together with their possible consequences for the user. User acceptance of these consequences is a very important consideration especially for balancing security and usability when using MEAs. Thus, this section then presents a proposed model for the user acceptance of mobile security measures.

5.2.1 Mobile Security Measures and their Consequences for Mobile Users

Based on the literature review and best practices within enterprises, the following mobile security measures along with their consequences for mobile users is presented. In the CFMS, mobile security measures can be in form of security methods, functions, mechanisms, restrictions, and enforced policies that have to be applied when using MEAs. These measures can be organizational or technical. Here, the security measures are defined at a high level of abstraction, in order to ensure the security measures are also understandable by non-security specialists. Extending the CFMS to include more technical information about security measures is seen as future work, however such information can be made available for developers who are granted the rights assigned to the role “technical user”.

5.2.1.1 Authentication

Most of the authentication methods from the traditional computing domain (e.g. desktop computers) may be adopted for mobile devices. However, due to instantaneous access times expected by the mobile user, these authentication methods do not seem to work very well because they are used in less secure versions (Rogowski, Saeed, Rybnik, Tabedzki, & Adamski, 2013). Authentication generally refers to methods that are used for user identification and verification. Possible implementations for authentication on mobile devices are:

- Knowledge-based methods;
- Biometric authentication;
- Continuous authentication;
- Multi-factor authentication

Knowledge-based methods: These methods (like passwords, PIN – Personal Identification Number, pattern locks and graphical passwords) are based on exclusive user knowledge (Rogowski et al., 2013). Passwords are the most popular authentication method. There are some rules of good passwords (Burnett & Kleiman, 2006), a high level of security demands a complex password. However, complex passwords seem to be less convenient for mobile device users compared with traditional computers, because they expect an instant access to their devices and mobile applications. Moreover, a consequence of authentication can be a high chance of error, when entering a complex alphanumeric password. Depending on the security policy applied by an enterprise, the mobile device data can be erased after a number of unsuccessful attempts. However, usability can be supported here by using multi-level authentication, which allows the implementation of passwords with varying complexities depending on the required security level.

PIN and pattern locks are to be considered as special cases of password. A PIN consists normally of four digits, however, new smartphones support a PIN of more than 4-digits. For instance, Android provides a numeric PIN or alphanumeric password (both between 4 and 16 digits or characters in length) to screen lock. Pattern locks can also be used as a security measure, where the user is required to connect between dots in a predefined order. In spite of users often feeling comfortable with pattern locks, this measure shows serious deficiencies regarding security (Aviv, Gibson, Mossop, Blaze, & Smith, 2010). Pattern locks are not

allowed by enterprises when using MEAs, pattern authentication is usually easy to handle for users but it is also easily predictable, which decreases security.

Biometric authentication: This type of authentication uses biological features (usually voice, face or fingerprint) for the identification and verification of a user (Mayron, 2015) (Wójtowicz & Joachimiak, 2016). The most popular type of biometric authentication in enterprises is the fingerprint. Biometric authentication is problematic because the recognition may produce false negatives and stops the user from rightfully accessing content. The reverse can be true as well and an unauthorized user may gain access due to adequate similarity. Thus, there is a tradeoff between False Acceptance Rate (FAR) and False Rejection Rate (FRR). The top priority in this regard is to achieve zero or extremely low False Acceptance Rate (FAR), which can prevent the mobile device from being illegitimately accessed. This is more important than authenticating the genuine user at the first attempt, as a low FRR would imply (Sun, Wang, Qu, & Zhou, 2016). Minimizing FAR makes the mobile device more secure, but this will increase the FRR which in turn causes discomfort for mobile users. This authentication method is therefore mostly used in combination with knowledge-Based authentication methods.

Continuous authentication: This authentication mechanism is basically a behavioral monitoring that continuously compares the current user activities or specific actions with the usual behavior of the authorized user, rejecting users that deviate to a higher degree than is allowed (Kambourakis, Damopoulos, Papamartzivanos, & Pavlidakis, 2014). An example is finger-gestures authentication using touchscreen (Feng et al., 2012). Continuous authentication simplifies the authentication process to the end user through automatization, but it may increase the usage of device resources due to the need for continuous monitoring. However, there is no practical usage of this authentication type found within the business domain.

Multi-factor authentication: Multi-factor authentication is a security method that has also been used by enterprises to enforce entitlements when accessing sensitive corporate applications and data. This method provides an extra layer of security beyond username and password authentication mechanisms. It requires the user to have two out of three of the credentials mentioned above, namely, something the user know (e.g. password or PIN), something the user has (e.g. mobile device, security token) and something the user is (e.g. fingerprint, voice). However, multi-factor authentication on mobile devices cannot follow the physical security token model due to barriers in usability. Multi-factor authentication can

be applied on mobile devices by pairing employee with their mobile devices and enforcing PIN entry on the MEA level (not the mobile OS level PIN) (Newman, 2014). So, employees can access MEAs only if they enter the correct PIN for the MEA (something they know) and the use the approved device paired with them (something they own). This procedure will enhance both, usability and security at the same time, since users just have to open the MEA and enter the PIN (for the MEA). A further development in multi-factor authentication for mobile devices is contextual authentication, where the authentication is requested based on factors such as the location of the device. For instance, restrictions can be applied on accessing specific MEAs when the mobile device is trying connect to enterprise backend system from an unsecured location, such as a hotel Wi-Fi network, and require additional forms of authentication, such as the use of a one-time password (RSA, 2016). Regarding contextual security, a security framework that elicits users' context information and adapts this information with security enforcements policy decisions has been presented (Mowafi et al., 2014). This framework controls the communication between mobile applications and their sources, where mobile applications' access requests are analyzed based on user's context information collected from the mobile device sensors and security configurations of the mobile application (Mowafi et al., 2014).

Every factor included in the authentication process increases the level of protection of the MEA, so if one factor is compromised, the others are still in place. Possible consequences for an employee can be the need to manage and remember different PINs/passwords. This in turn can decrease the employee productivity and lead to frustration as this can become a burden especially when having to repeat multiple steps each time an MEA is accessed.

5.2.1.2 Encryption

Encryption is the main key to ensuring data confidentiality and to ensure that only the right users can read the information. To encrypt mobile data, there are two encryption techniques:

- Data encryption for on-device data;
- Data encryption for transmitted data

Data encryption for on-device data: This encryption technique has two main variants. The first variant is the disk encryption (also known as Full Disk Encryption (FDE) or Whole Disk Encryption), which encrypt the entire data storage. Disk encryption is especially important

for mobile devices that can be physically lost or stolen. For instance, Android 5.0 and above supports disk encryption, that is based on dm-crypt[59]. However, disk encryption is disabled by default in Android devices that support it. To enable disk encryption in Android, the user has to lock it with a PIN or passcode, which is necessary to create the encryption key. Unlike Android, key security features in iOS like disk encryption are not configurable, so users cannot disable them by mistake (Apple Inc., 2017).

The second variant of encryption is file-based, which allows different files to be encrypted with different keys that can be unlocked independently. For instance, Android 7.0[60] and above supports file-based encryption.

The CFMS will suggest on-device data encryption as a security measures to protect data confidentiality on mobile devices from threats, such as loss and theft of mobile devices. Such information should be enough for the "business user" role to make a decision about using it. However, this framework can be extended to include more technical information that would support the user, who has the role of "technical user", with the implementation of these encryption techniques by providing the guidelines to implement and configure each component in the encryption system used.

On-device data encryption represents a core feature for all major mobile OSes, like iOS and Android. However, mobile application developers may rely on an encryption functionality provided by the underlying mobile OS, or can implement their own encryption solutions. Implementing in-house encryption solutions carries the risk of making implementation errors that can compromise security, thus, relying on encryption provided by the underlying mobile OS can be advantageous in most cases. However, reliance on this requires detailed knowledge of its capabilities and limitations (Teufl, Zefferer, & Stromberger, 2013). Hence, Teufl et al. proposed an abstract and platform-independent model for the evaluation of encryption systems provided by mobile OS (Teufl et al., 2013). This model is shown in Figure 23.

As depicted on Figure 23, mobile devices often provide three different locations to store data, namely, local file system, credential store or external storage. To encrypt data on these locations, mobile OS supports encryption module. Depending on the mobile OS, the encryption module contains one or more submodules to encrypt an entire storage location,

[59] https://source.android.com/security/encryption/full-disk
[60] https://source.android.com/security/encryption/file-based

or to encrypt specific files and credentials residing at a certain storage location (Teufl et al., 2013). Encryption keys are needed for the encryption modules, such keys are provided by the key derivation module which implements a key derivation function that derives the required encryption keys from different inputs (such PINs or passcodes entered by the user). This abstract encryption model also includes external components such as backup and cloud components, which also need to be considered as data is potentially transferred to these external entities.

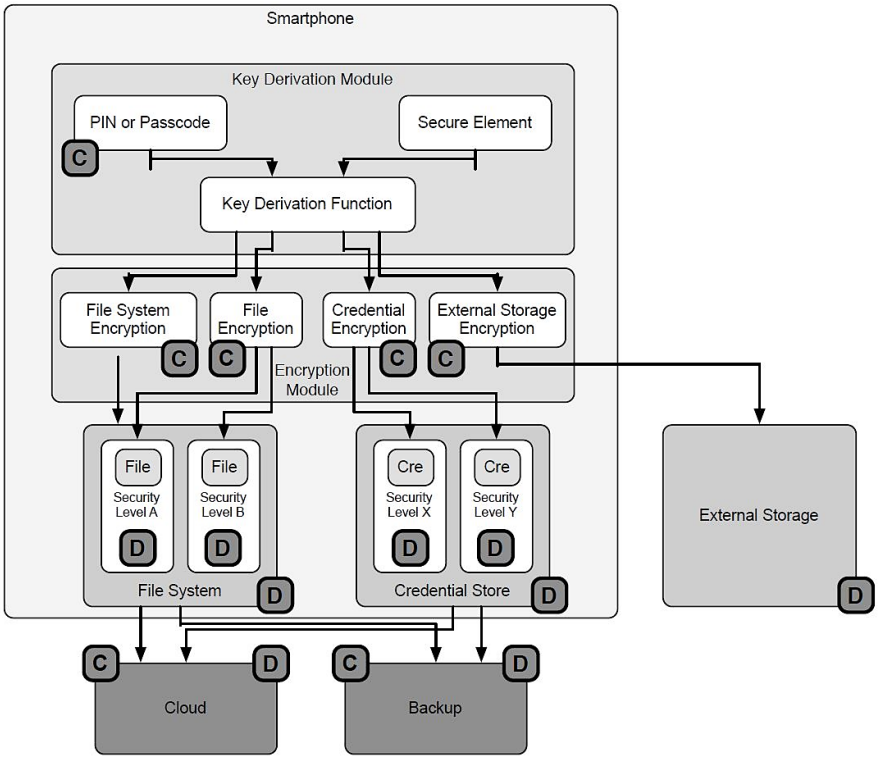

Figure 23. Abstract encryption model

Source: (Teufl et al., 2013)

However, the security of data and credentials stored on mobile devices does not solely depend on the components of the mobile device encryption system, but also on configuration options that can be defined by administrators or application developers, which can also influence the capabilities of encryption solutions and consequently the security and confidentiality of data stored on mobile devices (Teufl et al., 2013). Figure 23 marks the components that are subject to configuration options (C) and developer decisions (D). On the one hand, the administrators can manage the strength of the used PIN or passcode, and enable or disable file system encryption and encryption of external storages manually or via the EMM system. On the other hand, developers need to decide where to store data (file system, credential store, external storage). They can also choose to rely on a file-based

encryption of data, to select appropriate security levels for encrypted files and to decide whether data is transferred to external cloud or backup components (Teufl et al., 2013).

To protect sensitive information from malware attacks and device theft, the offline cache has also to be encrypted[61]. For instance, encryption standards like Advanced Encryption Standard (AES) (key length 256) and (Public Key Cryptography Standards) PKCS can be used to encrypt app-generated information on a device's storage, using random server-generated numbers for high security. An encrypted offline cache allows user authentication when servers are offline. The selection of the suitable encryption standards should be compliant with the policy the enterprise defines for the encryption, e.g. key generation, minimum length of the key used in the encryption.

Data encryption for transmitted data: This encryption technique is applied to protect corporate data from MitM attack by ensuring the integrity and the confidentiality of the data while transmitting them over mobile communications between mobile devices and the enterprise system. For instance, a mobile Virtual Private Network (mobile VPN) establishes an authenticated and encrypted tunnel to serve as a virtual leased line over a shared public wireless and cellular infrastructure (Liotta, Tyrode-Goilo, & Oredope, 2008; Uskov, 2012). Mobile VPN uses the encryption to keep transmitted data secure and also verifies the identity of anyone using network (Turban, King, Lee, Liang, & Turban, 2015).

There are two main variants of VPN on mobile devices, namely, full-device VPN and per-app VPN. In the first variant, the *full-device VPN*, VPN is configured for the entire mobile device so that, all traffic from all mobile applications comes back to the corporate network. However, this results in unwanted network bandwidth utilization. Moreover, users will have to open the VPN application each time and enter corporate credentials before accessing enterprise resources. For always-on mobile VPN, battery consumption is a major concern, because it requires continuous sending and receiving of control messages to keep the VPN tunnel alive (Alshalan, Pisharody, & Huang, 2016).

In the second variant, the *per-app VPN*, the enterprise can determine which mobile applications have to use a VPN for data transfer. Thus, a corporate network does not have to deal with unnecessary traffic from other personally used mobile applications on the mobile device, but MEAs that communicate over the Internet must use a secure encrypted

[61] https://www-01.ibm.com/software/mobile-solutions/worklight/features/security/

communication. Standard security protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS), an updated and more secure version of SSL, can be used to establish an encrypted communication between enterprise server and MEAs.

By encrypting the data on mobile device and also during transmission, security is enhanced and employees can work safely everywhere. However, users may experience longer loading and saving times when applying data encryption on mobile devices due to limited resources concerning CPU power and memory, and the encryption process can take time and consume battery. Encrypting all data on a mobile device reduces system performance, consumes already limited resources and increases the set up time of mobile devices (Olaleye, Ranjan, & Ojha, 2017).

5.2.1.3 Containerization

When mobile devices are used for both private and business purposes, and whether BYOD or COPE is used, MEAs and their data should be protected against third party applications. On the other hand, users' personal data might become easily accessible to enterprises (Oluwatimi et al., 2017). This consequently increases privacy risks or misuse of employee's private personal data by enterprises. Thus, both securing enterprise content and protecting employees' privacy are vital. This requirement can be addressed using the containerization approach (Oluwatimi et al., 2017). For instance, Airwatch[62] has developed mobile container solutions for corporate email, mobile applications, content and internet browser as a part of EMM platform. For the implementation of containerization, three approaches can be used:

Application level containerization: This approach enables the usage of both MEAs and third-party mobile applications operating side by side on the same mobile device, as MEAs can run within a container. This approach employs two main techniques, namely Encrypted Space Container (ESC) and Application-Wrapping Container (AWC). For instance, Figure 24 shows the iOS Sandboxing approach as an app level containerization. A mobile application within a sandbox can only access data and system resource within that sandbox.

[62] https://www.air-watch.com/downloads/resources/airWatch_container_brochure.pdf

Device level containerization: In this approach, the mobile device can be wrapped in a management layer, which lets a central administrator monitor and control the mobile device. This can be achieved via an EMM system.

OS level containerization: This approach enables two mobile OS instances to run on the same mobile device, with one mobile OS used for business and the other for private use. This approach is also called OS virtualization and it is yet to mature on mobile devices, however a virtualization of an Android OS has been demonstrated via an VMware's Mobile Virtualization Platform (MVP) (Barr et al., 2010).

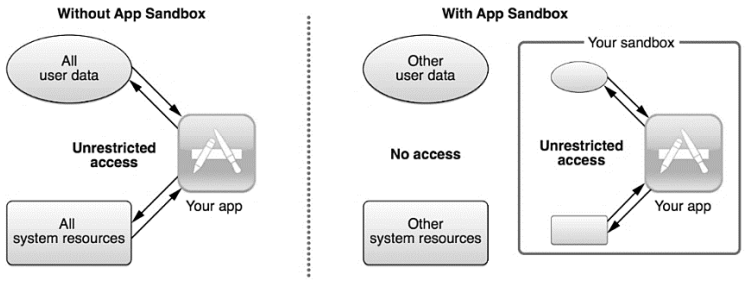

Figure 24. App sandboxing.

Source: Apple's App Sandbox Design Guide[63]

Containerization can be also supported natively by a mobile OS. For example, iOS sandboxes all its mobile applications so they are restricted from accessing data stored by other applications. This will thus protect mobile applications from malware that try to gather or modify information stored by other mobile applications. However, if a mobile application needs to access information other than its own, this can be enabled by using services explicitly provided by iOS (Apple Inc., 2017).

On the one hand, containerization improves data protection on mobile devices by limiting the access to these data and by providing IT administrators the ability to control everything from email to the camera in a container. Further, containerization can provide a second level of authentication to access the container regardless of the mobile OS login. On the other hand, applying containerization can cause consequences regarding usability. For example, the container can restrict some functionalities like caller ID due to limited or no integration with the native contact list, so that caller ID will not be available for corporate contacts. This in turn leads to that employees possibly having duplicated or non-managed contacts.

[63] App Sandbox Design Guide: https://developer.apple.com/library/content/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html

5.2.1.4 Protection Software

Protection software like Antivirus is also used to detect malware on mobile devices, protecting users whilst surfing the internet, primarily against phishing attacks, by defining blacklists or whitelists of specific websites (v Do et al., 2015). However, protection software can be also deployed on mobile devices as a supplemental security measure (Souppaya & Scarfone, 2013). For instance, to protect the users from the abuse of SMS (e.g. sending SMS messages to numbers that would cause monetary loss), antivirus applications monitor all the SMS activities from mobile applications, and then take actions when any malicious behaviors are detected (Tu et al., 2016). Furthermore, some actions can be taken by antivirus applications, such as stopping malicious SMS activities, bringing them to users' attention, or by mobile OS such as halting each malicious SMS activity until the user permits it through a pop-up dialog (Tu et al., 2016). Moreover, protection software is typically used to protect user from web-based threats, like drive-by download. Mobile devices can be monitored to detect intrusions by analyzing the mobile OS and user operations in search of undesirable and suspicious activity. This can be done by an Intrusion Detection System (IDS) based on two types of approach; prevention-based approach (IDS has to be running online and in real-time) and detection-based approach (IDS serves as a first line of defense by effectively identifying malicious activities) (Téllez & Zeadally, 2017).

Due to the need of continuous monitoring by protection software, consumption of device resources, like RAM and battery is high. Moreover, protection is dependent on the up-to-dateness of the malware signature stored in the protection software database as well as firewall rules.

5.2.1.5 Other Security Measures

- *Restrictions on mobile device:* Security measures can be also applied on mobile devices according to the enterprise security policies that can be enforced by an EMM in form of restrictions. Souppaya and Scarfone defined the following list of such possible restrictions (Souppaya & Scarfone, 2013):
  - Restrict user and mobile application access to hardware, like digital camera, GPS, Bluetooth interface, USB interface, and removable storage.

- Restrict user and mobile application access to native OS services, such as built-in web browsers, email client, contacts, etc.
- Restrict which mobile application stores may be used.
- Restrict which mobile applications may be installed through whitelisting or blacklisting.
- Restrict updating mobile applications or uninstalling them.
- Restrict the permissions (e.g., camera access, location access) assigned to each mobile application.
- Restrict the use of mobile operating system and application synchronization services.

- *Rooting detection:* To mitigate the risks caused by jailbroken or rooted mobile devices, compromised devices must be detected, the corporate data wiped and users be removed so their mobile devices are no longer managed by the EMM system. Applying a mandatory enterprise device management with jailbreak and rooting detection will decrease the opportunity of having a rooted mobile device enrolled into an enterprise device management (Michaelis, 2012). Most of today's EMM solutions (e.g. Citrix, AirWatch, MobileIron, Samsung Knox EMM) provide the functionality to detect jailbroken and rooted mobile devices.
- *Trusted mobile:* To ensure the mobile device integrity, the Trusted Computing Group (TCG) formed a working group[64] dedicated to mobile devices that released the Mobile Trusted Module (MTM) along with specifications to implement hardware-based security services, such as device authentication, integrity measurement, secure boot, and remote attestation measure (Téllez & Zeadally, 2017). However, according to Souppaya and Scarfone, *"Most current mobile devices lack the root of trust features (e.g., trusted platform modules, TPMs) that are increasingly built into laptops and other types of hosts"* (Souppaya & Scarfone, 2013). Enhancing mobile devices with all the specifications of MTM needs further technical adaptations that are not covered in this research. However, CFMS could be extended in future work to include an interface for the MTM specifications.

[64] https://trustedcomputinggroup.org/work-groups/mobile/

- Beside the above-mentioned technical measures that directly involve the IT system, enterprise should also consider the following organizational measures, that relate to the system environment and particularly to the people using it. Only a combination of technical and organizational measures can protect MEAs and their data. The following lists some organizational measures:
  - Ensuring timely installation of security updates for the mobile OS.
  - Regularly verifying mobile applications to identify potentially harmful applications.
  - Prohibiting the side-loading of mobile applications, which may bypass security checks.
  - Only requesting access to the minimal set of shared data stores (e.g., contacts, calendar), mobile OS services (e.g. location services), and device sensors (e.g. camera, microphone) necessary for the MEA's functionality.
  - Conducting security awareness programs for employees who use mobile devices for work. Applying technical security measures to mitigate risks can be insufficient if employees are unaware of potential security risks (Bulgurcu, Cavusoglu, & Benbasat, 2009). The risk catalogue provided in this thesis (see Section 5.1) will help to educate employees on potential threats and risks. Further security educational possibilities may include:
    - Educate employees so that, when using third-party mobile applications that require location services (e.g., map services), access to location services is revoked once the mobile application is no longer in use.
    - Educate employees when installing third-party mobile applications, to be suspicious of those requesting access to mobile OS services or sensors that do not appear related to the functionality of the mobile application.
    - Educate employees to revoke access to device sensors and OS-provided services for unneeded pre-installed mobile applications that cannot be uninstalled, or to disable those applications so they cannot be launched.
    - Educate employees on how to recognize phishing attempts and increase their awareness of techniques to browse safely from mobile devices, such as tap-and-hold on a hyperlink to examine its associated URL.

- Educate employees, to set Bluetooth configuration to non-discoverable when it is not in use.

– Prevent installation of third-party mobile applications from unknown sources (e.g., enforcing a policy, using the EMM system, to never permit the installation of mobile applications from unknown sources).

– Disabling the notification features for MEAs that may receive sensitive content, or configuring such notifications to be only displayed when the mobile device is unlocked.

– Enforcing policy by using the EMM system to limit the data or services available while the device screen is locked (e.g., notifications, camera).

– Applying penetration testing to detect MitM vulnerabilities, or ensuring that MEA does not store sensitive information in system logs or other unsecure storage locations.

– Monitoring the mobile device using the EMM system, for any unauthorized changes, or use of mobile remote wiping to remotely wipe data from lost or stolen mobile devices. However, monitoring of mobile devices can violate user privacy in the case that everything is monitored (like internet activities or private email). Such monitoring should thus only be applied to detect policy violations.

Further security measures that can be applied through the EMM system are included in Section 2.2.6.

Applying the security measures on mobile devices may have consequence on the usage of the mobile device for work purposes. Some of these consequences have been mentioned above in this section. Potential consequences along with their effects on security and usability are presented in summary form in Table 19.

+: positive; -: negative; 0: neutral

Potential Consequence	Security	Usability
User privacy violation when monitoring of mobile devices	+	-
Enforcing complex passwords will increase the chance of errors or failed logins. Depending on the security policy applied by enterprise, the mobile device data can be erased after a number of unsuccessful attempts	+	-
Employees need to manage and remember different PINs/passwords	+	-

The implemented measure can slow down the mobile device and services	+	-
Clear separation between private and business content. So, employees can use one mobile device for private and business	+	+
Implemented security measures can cause high rate of battery exhaustion	+	-
Multi-Level-Authentication: mobile device will not be entirely locked when authentication fails	+	+
Applying restrictions is based on context	+	+
Data encryption decreases battery lifetime on mobile device	+	-
Disallow the usage of mobile features and services	+	-
Limit the mobile applications that can be installed on mobile device	+	-
(Remote) Wipe of mobile device can lead to losing user personal information	+	-
User authentication is possible even when server is offline	0	+

Table 19. Potential consequences of applying mobile security measures and restrictions

Based on the mobile security measures determined and their potential consequences, a proposed model for user acceptance of mobile security measures is presented in the following section.

5.2.2 Proposed Model for User Acceptance of Mobile Security Measures

5.2.2.1 Overview

To understand the factors that affect the adoption and use of information technology, there are two models, namely, the Technology Acceptance Model (TAM) and User Experience (UX) models, which are central to human-computer interaction (Hornbæk & Hertzum, 2017). However, in user acceptance studies, the Technology Acceptance Model (TAM) is often applied. TAM was originally presented by (Davis, F. D., 1986) and was extended in TAM2 by incorporating additional constructs of social influence process and cognitive instrumental processes (Venkatesh & Davis, 2000). In this thesis, the original TAM was considered, since the additional constructs for the TAM2 are mostly irrelevant to the studied domain. This research applies TAM to address key factors that affect the adoption of MEAs in enterprises, taking security as its main focus. As depicted in Figure 25, TAM presents two

main constructs, perceived usefulness and perceived ease of use, that influence attitudes towards using technology, which in turn influence the actual use of systems.

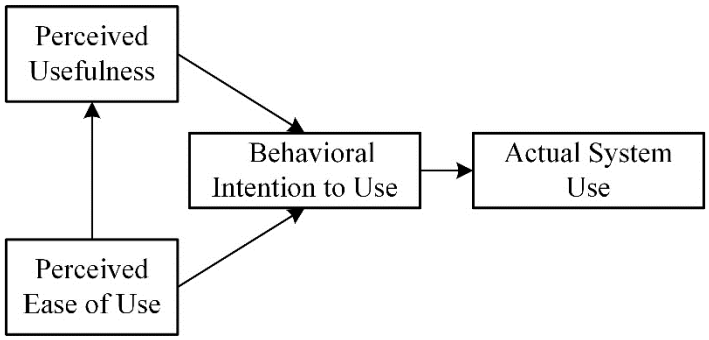

Figure 25. Original technology acceptance model

Source: (Davis, F. D., 1986)

The first construct; the perceived usefulness is defined as *"the degree to which a person believes that using a particular system would enhance his or her job performance"* (Davis, F. D., 1989). In the proposed model, this construct reflects the degree to which an employee believes that the applied security measures are important for secure usage of mobile devices in the business context. The second construct; the perceived ease of use is defined as *"the degree to which a person believes that using a particular system would be free of effort"* (Davis, F. D., 1989). In the proposed model, this construct reflects the degree to which an employee believes that using the applied security measures would be effort free.

User acceptance studies for security are rare. However, two works that correspond to the topic at hand have been found. Osman provided an extended model of the acceptance of mobile government systems (Osman, 2013). In that model, trust was included as a construct that directly affects the intention to use mobile government systems. Security was not included in that model. Arpaci et al. presented a study aimed at investigating the impact of perceived security on organizational adoption of mobile communication technologies, specifically smartphones (Arpaci, Yardimci Cetin, & Turetken, 2015). That work investigated how the perception of security, when using mobile technologies, can affect the organizational adoption of smartphones, since the perception of low levels of security can increase the technological risks of adopting these technologies in organizations (Arpaci et al., 2015). However, to achieve a reasonable level of security, proper security measures have to be applied. Applying security measures on mobile devices has consequences on mobile users. The perception of such consequences is the focus of the model proposed here. Some further works studied user acceptance, but their focus is different. Benenson et al. studied

the users' understanding, usage and acceptance of attribute-based credentials (Benenson et al., 2014). However, TAM extension for using mobile devices in business sectors concerning security and its consequences on the mobile users has not so far been studied.

5.2.2.2 Methodology

The main objective of the model proposed here is to investigate the factors that affect user acceptance of mobile devices for work purposes. A questionnaire was used to gather the required information. Its questions primarily concern the security measures and their possible consequences on users (see Section 5.2.1). Applying security measures on mobile devices has consequences, which can restrict the use of mobile devices. This research hypothesizes that perceived restrictions (the degree to which an employee believes that applied security measures can restrict the use of mobile device) would have a significant impact on perceived usefulness and perceived ease of use of security measures.

The Design of the Questionnaire. The basic design of this questionnaire consists of three primary sections. In the first, the employees were asked questions concerning their age, business and private usage of mobile devices and whether they use private or company-owned mobile devices. A second section included specific questions on security measures, the possible restrictions, perceived ease of use and perceived usefulness of security measures. In the final section, the participant is confronted with questions regarding personalized policies and intention to use the security measures introduced in the questionnaire. The questions are included in Appendix B. Apart from the general questions in the first section, which use question-specific options, respondents were asked to rate their acceptance using a 7-point scale ranging from 0 = no acceptance to 6 = very high acceptance. However, the questionnaire has some limitations. First, the majority of questions ask for the subjective perception of the participant regarding the consequences of certain security measures. Although subjectivity is usually discouraged, the topic at hand requires the participant's perception to assess future user acceptance and it is therefore allowed. A second limitation can be found in the different levels of understanding by the participants concerning the security measures introduced, the accompanying restrictions and their consequences. This may skew the participant's perception on the subject matter.

Sample and Data Collection. The questionnaire targets three German companies that make it possible for their employees to use mobile devices for work purposes. Hence, these

employees would be the most affected by implemented security measures on mobile devices. Furthermore, it is important to consider, whether the device is predominantly used for business or for private purposes, as it may influence the impact of the implemented measures on overall user acceptance as well. The questionnaire was designed online and distributed in three German companies. 88 participants took part in this questionnaire, with ages ranging from 24 to 63 years.

As depicted in Figure 26, about 86 percent of the participants use mobile devices (private device 28 percent, corporate devices 58 percent) in a business setting, with the majority of 55 percent are using smartphones and 27 percent using both smartphones and tablets. 71 percent of participants, who use their corporate devices for business, use these corporate devices privately as well.

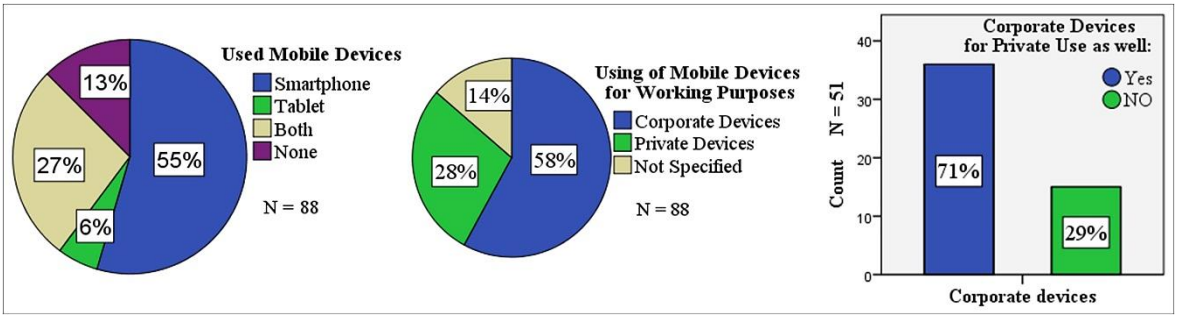

Figure 26. Mobile devices' usage for work

Source: (Hasan, Rajski et al., 2016)

After collecting the data, the internal consistency was assessed using the Cronbach's alpha coefficient (Cronbach, 1951). Cronbach's alpha was calculated for each of the factors of the proposed model, which is depicted in Figure 27, Page 94. The Cronbach's alpha values for the investigated factors are presented in Table 20. According to (Sekaran, 2003), internal consistencies less than 0.6 are considered to be poor, those in the 0.7 range, acceptable, and those over 0.8 good.

Factors	Cronbach α	Acceptable if in 0.7 range (Sekaran, 2003)
Perceived Ease of Use - PEOU	0.701	Yes
Perceived Usefulness - PU	0.782	Yes
Intention to Use - ITU	0.749	Yes
Perceived Restriction - PR	0.713	Yes

Table 20. Internal consistency for the investigated factors

Source: (Hasan, Rajski, Marx Gómez, & Kurzhöfer, 2016)

5.2.2.3 Proposed User Acceptance Model

The original Technology Acceptance Model (TAM) does not cover specific requirements concerning mobile security, such as the perceived restrictions when applying security measures on mobile devices when used in a business context. This in turn leads to distortion of the actual user acceptance of the technology studied. Additionally, the correlations between the standard factors may vary as well, due to different priorities in different application areas.

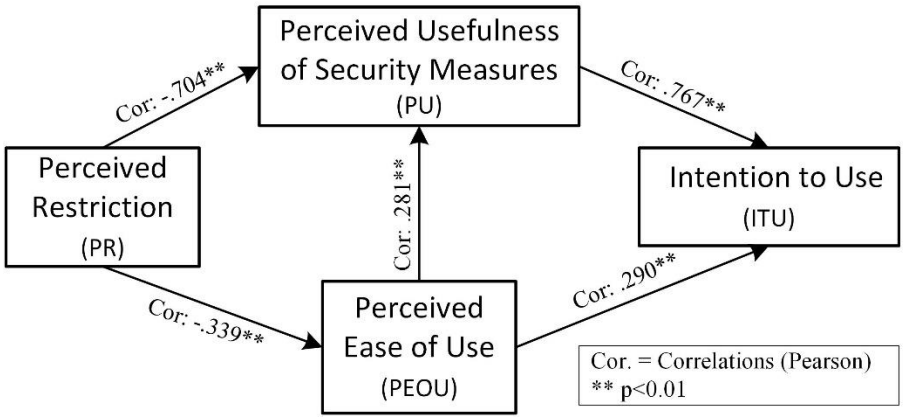

Figure 27. Proposed user acceptance model

Source: (Hasan, Rajski et al., 2016)

Figure 27 shows the proposed extension of TAM along with the correlations between its constructs. The construct "perceived restriction" was added to the original model. A statistical analysis using SPSS was conducted on the collected data in order to measure the Pearson correlation between the constructs of the proposed model. The resulting correlations are displayed in Table 21.

	PEOU	PU	ITU	PR
PEOU	1			
PU	.281**	1		
ITU	.290**	.767**	1	
PR	-.339**	-.704**	-.769**	1

**Correlation is significant at the 0.01 level (2-tailed).

Table 21. Correlations between the constructs

Source: (Hasan, Rajski et al., 2016)

Looking at the correlations displayed in Figure 27, it is evident that the perceived restriction has a significant impact on the perceived usefulness of security measures. As this correlation is negative, the higher perceived restriction level the lower the perceived usefulness of

mobile security measures. The perceived restrictions show also a negative correlation to ease of use. The ease of use shows a positive correlation to both usefulness and intention to use the security measures. These two correlations are relatively low. Furthermore, perceived usefulness is significantly correlated with the intention to use mobile security measures.

5.2.2.4 Discussion

Achieving a balance between security and usability is very important to encourage productive use of mobile devices for work purposes. Applying highly restrictive security measures lowers the overall user acceptance and may trigger the employee to circumvent those measures. The proposed model, implies that if security measures with a high restriction level are applied, the perceived usefulness of the applied security measures will decrease, which in turn minimizes the intention of using these measures, or in other words, minimizes the intention to use mobile devices for work purposes. Consequently, companies will lose advantages in employee flexibility and productivity when adopting MEAs with high level of restriction. Data analysis has also revealed that the users' acceptance of the perceived restrictions is relatively dependent on whether they use corporate or private devices, where users of corporate devices seem more accepting of higher level of restrictions than those who wish to use private devices for work purposes. However, it is difficult to generalize the results presented due to some limitations. Besides those mentioned in Section 5.2.2.2, further limitations can involve cultural aspects, since different countries and cultures may emphasize different aspects. Moreover, the relevancy to work and the area of application can limit the results of this work. Employees who deal with sensitive data can show a higher acceptance rate compared to those who deal with less sensitive data. With other user groups, especially high-tech or health sectors, the results on perceived usefulness and perceived restrictions could be also different.

5.2.3 Summary

Based on literature review and best practices, this section first presented mobile security measures along with their potential consequences on the users (the employees). It is important for an enterprise is to apply only the needed security measures and align them with its intended mobile strategy. Thus, the user acceptance of mobile security measures is a very important consideration to achieve a balance between security and usability. Therefore, this

section presented a model for user acceptance by adding the perceived restrictions as a construct to the TAM. This model provides an argument that user acceptance of mobile security measures has to be given a special attention when adopting MEAs.

Due to the limitations discussed, it is difficult to generalize the results. However, during the research, several interesting aspects presented themselves for further investigation, including the sensitivity of data and mobile security awareness as additional constructs that affect user acceptance.

5.3 Security Levels for Mobile Enterprise Applications

5.3.1 Mobile Security Requirements

In this section, a list of security requirements of MEAs has been determined in three steps. In the first step, a literature review has been conducted, where standards and publications from three main sources have been considered, (BSI, 2013), NIST (NIST, 2013) and Common Criteria (Common Criteria, 2012). The outcome here was an extracted list of mobile security requirements.

In the second step, interviews have been conducted within four enterprises in Germany, as shown in Table 22 along with the roles interviewed. Each interview lasted about two hours. The first 15 minutes were used for an introductory presentation that briefly introduced the work, then discussions took place based on a prepared list of questions that cover all the security requirements resulting from the first step.

Enterprise	**Role of Interviewee**
EWE AG[65]	IT Security Officer
BTC Business Technology Consulting AG[66]	Manager IT-Operation
CEWE Stiftung & Co. KGaA[67]	Manager IT-Operation
Lufthansa Industry Solutions GmbH & Co. KG [68]	Managing Director

Table 22. Interviewed enterprises

[65] https://www.ewe.com/en
[66] https://www.btc-ag.com
[67] https://company.cewe.de/en
[68] https://www.lufthansa-industry-solutions.com/de-en

The following questions were used as a guide for structured interviews:

- Which possibilities of using MEAs are already made available to your employees today?
- What obstacles do you see when adopting MEAs?
- What are your requirements to protect your company data?
- What requirements do you have regarding mobile (data) communications?
- What policies do you have regarding the usage of mobile devices?

Then, in the third step, based on the interviewees' feedback, the security requirements extracted in the first step were refined. The refinement process included, deletion of irrelevant items, refining and reformulation of items, addition of new items that are not included in the list extracted in the first step. Thus, the outcome in the third step was a refined list of mobile security requirements that were considered within the CFMS. The refined list of the security requirements for MEAs is presented in the following tables categorized into three categories:

- $mCom_x$: Security requirements related to mobile communications (see Table 23)
- mOS_x: Security requirements related to mobile OS (see Table 24)
- $mApp_x$: Security requirements related to mobile applications (see Table 25)

Prefix	Requirement
$mCom_1$	The integrity of mobile communication must be guaranteed.
$mCom_2$	The mobile communication must be encrypted in order to ensure the confidentiality of the transmitted data.
$mCom_3$	The information about sender, receiver must be recorded.
$mCom_4$	Mobile communication must not take place via unsecure communication channels, e.g. Open WLAN networks.
$mCom_5$	The communication of corporate data may only take place via secure and encrypted data connections (VPN).
$mCom_6$	Mobile communication may also take place in the private context of the user via unsecure communication channels, e.g. Open WLAN networks.
$mCom_7$	The integrity and authenticity of the communication content and data must be verifiable.

Table 23. Security requirements related to mobile communications

Prefix	Requirement
mOS_1	The mobile OS must support current encryption algorithms and cryptographic key management.
mOS_2	All local data must be stored encrypted. This means both the internal memory of the mobile device and the external memory on SD cards.
mOS_3	The access to the mobile OS may be protected by a simple authentication (e.g., PIN / passcode).
mOS_4	The access to the mobile OS must be protected by strong authentication (complex password or biometric features).
mOS_5	The mobile OS must automatically be locked after a certain number of failed attempts of authentication. A delay must be applied before allowing the user to make another attempt to authenticate.
mOS_6	After a certain number of failed attempts, the mobile OS must completely be reset to the factory state; sensitive local data must be permanently erased.
mOS_7	The mobile OS must be logged out automatically after a specified period of user inactivity (idle). The user must authenticate again.
mOS_8	Apps that are released and signed by the App Store may be installed on the mobile OS. The use of mobile device is allowed in private context.
mOS_9	Only apps provided and approved by the enterprise may be installed. The installation of the apps is checked by signatures. The use of mobile device is not allowed in a private context.
mOS_{10}	Enterprise must be able to control which apps are allowed to be installed, e.g. apps Blacklist. The use of a mobile device in private context is restricted.
mOS_{11}	Apps that are installed on the mobile OS must be updated regularly.
mOS_{12}	The distribution and updating of apps must be possible centrally by the enterprise.
mOS_{13}	The security policies and features of the mobile OS must be administered and managed centrally by the enterprise. This also includes device settings, configurations and certificates.
mOS_{14}	The validation and verification of the mobile OS for compliance with the defined security policies and attributes must be controlled by the enterprise. In the case of non-compliance, access to corporate resources must be denied.
mOS_{15}	The enterprise must be able to delete mobile device's local data remotely.
mOS_{16}	The enterprise must be able to lock the mobile device remotely and require a complex unlocking code or password. (Remote Lock)
mOS_{17}	The mobile device OS must be able to be tracked and localized remotely. (Remote Antitheft)

mOS_{18}	Synchronization of corporate information and data with cloud services not possible.
mOS_{19}	Synchronization of private information and data with cloud services restricted.
mOS_{20}	The transmission of diagnostic information (e.g., the manufacturer of mobile terminals) must be prohibited.
mOS_{21}	The configuration and installation of configuration profiles (policies) by the user must be disallowed.
mOS_{22}	Configuration profiles (policies) must not be removed by the user.
mOS_{23}	Modifications (Rooting and Jailbreak) on the mobile OS must be prevented.

Table 24. Security requirements related to mobile OS

Prefix	Requirement
$mApp_{1}$	The user can perform certain functions of the mobile app prior to authentication. But the user must authenticate to perform specific/privileged functions.
$mApp_{2}$	The user must authenticate to perform any function of the mobile app. All functions of the mobile app are completely unavailable without authentication.
$mApp_{3}$	Access to the mobile app must be protected at least by simple authentication (e.g. PIN/Passcode).
$mApp_{4}$	Access to the mobile app must be protected by strong authentication (e.g. complex password).
$mApp_{5}$	Access to the mobile app must be protected by one-time credential authentication (e.g. one-time token or TAN).
$mApp_{6}$	The user must authenticate using several different authentication features (e.g., 2-factor authentication)
$mApp_{7}$	The user must be prompted to re-authenticate before performing certain critical functions.
$mApp_{8}$	Successful and incorrect authentication attempts must be logged by the mobile app.
$mApp_{9}$	Once authenticated, the user does not have to re-authenticate within a reasonable period of time.
$mApp_{10}$	User can authenticate offline without connecting to the corporate server (such as Active Directory or other directory services). However, the credentials must be synchronized and updated with the corporate server within a reasonable period of time.
$mApp_{11}$	The mobile app must automatically lock itself after a specific number of incorrect user login attempts and delay the new attempt to authenticate.

$mApp_{12}$	The mobile app must automatically lock itself after a specific number of incorrect login attempts. Unlock is only possible by the administrator.
$mApp_{13}$	The access to information and functions of a mobile app must be checked via an access control.
$mApp_{14}$	The user of the mobile app is logged out after a specific period of inactivity (idle). The user must re-authenticate.
$mApp_{15}$	The mobile app data may be locally stored unencrypted on the mobile device.
$mApp_{16}$	The mobile app data must be encrypted if they stored locally on the mobile device.
$mApp_{17}$	The integrity of the mobile business process data must be maintained.
$mApp_{18}$	The app data must be protected against unauthorized identity.
$mApp_{19}$	The mobile app data may be accessible through other apps or the mobile OS.
$mApp_{20}$	The mobile app data may not be read, copied, or modified by third-party apps or other (security) apps.
$mApp_{21}$	When the mobile app is deleted, the app data must be completely and permanently deleted from the mobile device.
$mApp_{22}$	The mobile app is not allowed to call external resources (APIs, other applications) if these resources are irrelevant to the application's functionality.
$mApp_{23}$	The authenticity of the third-party mobile apps must be ensured.
$mApp_{24}$	The mobile app is not allowed to collect information about user usage. If collected, they must be anonymized.
$mApp_{25}$	Company-related login data may not be stored on the mobile device, the mobile OS or in the mobile app.

Table 25. Security requirements related to mobile applications

5.3.2 Security Level Definition

The enterprise has to define its own security levels[69] for its information as a starting point to use the CFMS. These security levels have to be considered for all information independent of how this information can be accessed, whether using mobile devices or traditional computers. However, each security level requires the fulfillment of a set of security

[69] The security levels defined in this thesis are only considered from the security management perspective. In this regard, deeper check regarding the quality of the implementation and regarding the specifications of the security measures as well as penetration testing to evaluate the security will be still needed. This check is out of scope of this work.

requirements, which can vary according to the type of access to the information, e.g. mobile or not mobile. CFMS focuses on the security requirements that are needed when information can be accessed via MEAs.

Information is an important business asset, so the enterprise might suffer great damage if its information falls into the wrong hands, if it is manipulated or not available at certain times. Therefore, it is important to be aware of the need to protect such information. The need for protection of information is classified into protection levels (or security levels) with regard to security objectives, confidentiality, integrity and availability.

Security Objective	**POTENTIAL IMPACT**		
	LOW	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 26. Potential impact definitions for security objectives

Source: (NIST, 2004)

Table 26 presents the definitions of these security objectives together with the potential impact of each objective being compromised classified into three categories, low, moderate and high. Furthermore, according to NIST, "*Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation*." (NIST, 2004). NIST defined a generalized format for expressing the security category (SC), of an information type:

*"**SC** information type = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}*

the acceptable values for potential impact are LOW, MODERATE, HIGH or NOT APPLICABLE[70]." (NIST, 2004)

The adverse effect can be for example, enterprise image loss, non-compliance with laws, financial loss, harm to individuals, degradation of task fulfillment or damage to business assets.

Security experts have first to define the intended security level for MEA and then administrate these levels within the CFMS by mapping them to the security requirements. As depicted on Figure 28, based on MEA use cases, the type of information that can be processed (read and/or write) by a MEA have to be determined first. The need for protection is mainly derived from the determination of the type of information involved in MEA. In this thesis, five dimensions are considered as most relevant to MEAs, namely, information classification dimension, legal dimension, policy dimension, technical dimension and user dimension. The first three dimensions are important to determine the needed security requirements for MEA, and they should be considered when determining the protection needs of the MEA.

[70] The potential impact value of not applicable only applies to the security objective of confidentiality.

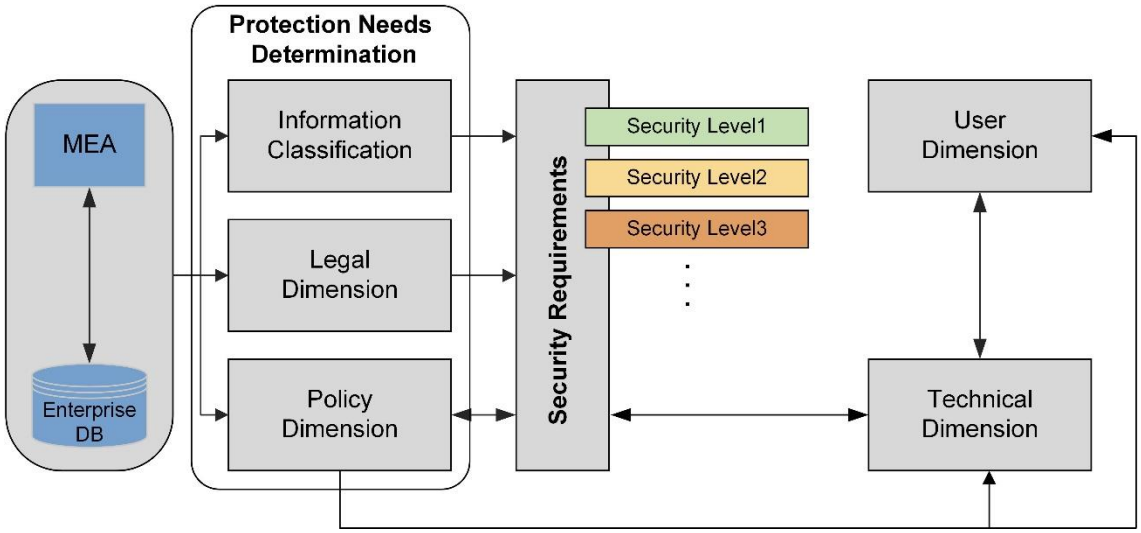

Figure 28. Multi-dimensional view of security levels

Information Classification Dimension: Classifying information into security levels is an essential key to determine the needed security requirements for a MEA and consequently to determine the security measures that have to be applied. In general information classification must be done by the owner of the information. As this thesis focus on MEAs, the enterprise is considered as the owner of the information.

Information can be classified based on its value and sensitivity into security levels. The CFMS supports the administration of three security levels, low, medium and high. However, the bigger and more complex the enterprise is, the more levels might be defined. The CFMS can be easily extended to enable the administration of additional categories, e.g. security level very high. In order to determine the intended security level (low, medium or high), it is essential to consider the potential impact (e.g. as classified in Table 26) by mapping each security level to a class of potential impact. Beside NIST, standards like ISO 27001 provides a classification scheme[71] that helps enterprises to classify information based on its confidentiality into three categories, namely, "public or open", "internal or proprietary" and "confidential or restricted".

Table 27 shows a possible definition of security levels along with examples of data classified in each level. For example, if an MEA can access information classified in security level high, the MEA should fulfill the security requirements associated with security level high.

[71] http://www.iso27001security.com/ISO27k_Information_classification_matrix.xlsx

Security Level	According to NIST	According to ISO 27001	Possible Examples
High	Max {(confidentiality, impact), (integrity, impact), (availability, impact)} = HIGH	Confidential	Personal data; Cryptographic Keys; Net Results before publication date; Strategic Planning; New Developments in terms of inventions / patents; Customer Data; etc.
Medium	Max {(confidentiality, impact), (integrity, impact), (availability, impact)} = MODERATE	Internal	Work Instructions; Company Policies and Standards; Phone Lists; Company Know How; Business and Marketing Plans; etc.
Low	Max {(confidentiality, impact), (integrity, impact), (availability, impact)} = LOW	Public	Annual Reports; Marketing Information; Company Profile; etc.

Table 27. Possible definition of security levels

Legal Dimension: This is the dimension which has an immense influence on information security, to ensure legal compliance to different directives and laws (Solms, 2001). For example, the General Data Protection Regulation (GDPR[72]), which defines and harmonizes data privacy laws across Europe, means it is now of more importance to keep this dimension highlighted. Thus, security experts must seriously consider such regulations when determining the protection requirements for MEA. This consideration is mandatory to derive protection requirements that are required by law.

Protecting persons against privacy violations through the handling of their personal data is the key concern in the GDPR. As defined by GDPR[73], *"personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*. GDPR is applied only in the case of processing of data which concerns personal data. As required by GDPR, enterprise should

[72] https://gdpr-info.eu/
[73] https://gdpr-info.eu/art-4-gdpr/

have a list of all types of personal information it holds and a list of places where personal information is stored.

Thus, security experts (here a security expert might be Data Protection Officer, who must provide professional knowledge in data protection law and IT security- as stated in the GDPR), should first define exactly which personal data can be involved in an MEA. Normally, enterprises define the personal data they process, assign a protection level to each data, and define the data subject (e.g. employee data or customer data). Table 28 shows an excerpt of possible personal information along with their needed protection level.

Personal Information	**Protection Level**
Name, gender, address, phone, date of birth, nationality, location data, search history, etc.	Medium
Personal Identification Number (like Identity card number, passport number, visa number), Social Security Number (like health insurance number), bank account, transaction record (like purchase, price, transactions, receipt number, receipt amount, invoice number, invoice amount), salary, credit card (including name cardholder, credit card number, validity, cvv), medical data (Physical and mental health, drug test results, disabilities, blood type, DNA code, prescriptions), etc. GDPR special category data, like racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic biometric, health data.	High

Table 28. Examples of personal information with assigned protection level

For each time t, the access matrix M_t presents the valid rights the subjects S_t have to access the objects O_t (Eckert, 2014).

$$M_t: S_t \times O_t \rightarrow 2^R; M_t(s,o) = \{r_1, r_2, \ldots, r_n\}$$

- O_t is a finite set of objects. In this thesis, $O_t = \{o_1, o_2, o_3\}$; o_1 represents personal data of employee, o_2 represents personal data of other employees, o_3 represents personal data of customer .
- R is a finite set of access rights. $R = \{read, store\}$.
- S_t is a finite set of subjects. In this thesis, S_t is defined according to processes an MEA can perform on the O_t, as follows: $S_t = \{MEA\text{-}Process\ 1, MEA\text{-}$

`Process 2, MEA- Process 3, MEA- Process 4, MEA- Process 5, MEA- Process 6, MEA- Process 7}`. These are presented in Table 29 as an access matrix.

For instance, according to this access matrix, if an employee uses an MEA that can perform the process P1, then the employee can read and locally store her/his personal data. She/he can also access personal data of other employee and customer. Further access scenarios are defined similarly. The process P7 means that an employee uses an MEA with no rights to read and store any personal data.

		Objects		
		o_1	o_2	o_3
Subjects	MEA- Process 1 (P1)	read, store	read, store	read, store
	MEA- Process 2 (P2)	read, store	read, store	
	MEA- Process 3 (P3)	read, store		
	MEA- Process 4 (P4)	read	read	read
	MEA- Process 5 (P5)	read	read	
	MEA- Process 6 (P6)	read		
	MEA- Process 7 (P7)			

Table 29. Access matrix of an MEA regarding the possible access of personal data

The personal data protection levels may differ from the overall security level of the MEA. For instance, Table 30 presents this difference taking into consideration further factors, like the possible types of personal data processing as defined in the access matrix (see Table 29).

MEA Required Security Level	Possible Types of Personal Data Processing							Personal Data Protection Level		
	P1	P2	P3	P4	P5	P6	P7	Low	Medium	High
High	✓	✓	-	✓	✓	-	-	-	✓	✓
Medium	-	-	✓	-	-	✓	-	-	✓	-
Low	-	-	-	-	-		✓	-	-	-

Table 30. Security levels considering the legal dimension – an example

Security experts must be involved in the translation of such laws into security requirements, to reduce the complexity behind such laws for other non-security expert roles. Employees who use mobile devices for work proposes might have concerns regarding their own privacy. For instance, when they use the same mobile device for private and business, EMM administrators can monitor the enrolled mobile devices and can therefore access the whole data stored on the mobile devices. Not only data on the mobile devices that is personal and private by nature, such as pictures, messages, emails and agenda items, qualifies as personal data, but also data that is related to the mobile device, such as environmental aspects (like mobile device's location), and data related to its usage, including logs containing usage data related to specific mobile applications (ENISA, 2017). For those reasons, employees might reject working using such managed mobile devices. In this regard, enterprises should address questions like: a) who is the owner of the data on mobile device? and b) who should have the right to wipe the data (partially or completely) on mobile device in case of security incidents? Thus, the enterprise should provide its employees with transparency when applying security measures (such as monitoring mobile devices) that might violate their privacy. For example, the enterprise can justify the need of such security measures by mapping these to the possible threats that might exist when using mobile devices for work purposes.

Policy Dimension: There are many definitions of the term "Policy". In general, policy is defined as *"A policy is a high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area"* (Peltier, 2002). A specific form of policy is security policy that defines a set of technical and organizational rules, instructions, responsibilities and roles to achieve the intended security objectives. It is often defined in text form and thus informally, so that one of the difficulties is to implement such informal statements in a controllable way (Eckert, 2014). Furthermore, when using mobile devices for work, enterprises should define a mobile device security policy that should be consistent with and complement security policy for non-mobile systems (Souppaya & Scarfone, 2013).

Mobile device security policy includes statements and rules for the general usage of mobile devices for work, examples can be:

- Data classified at a very high security level may not be stored locally on any mobile device.

- Data classified at a high security level can be stored locally on mobile device only when encrypted.
- In order to transfer sensitive data, appropriate encryption mechanisms must be used/provided.
- If the storage of private data on the mobile device is permitted, then measures must be taken to segregate company data and private data.
- Employees must immediately report all lost or stolen mobile devices to clearly defined contact persons.
- Employees may only load corporate data that is essential to their role onto their mobile devices.

However, the more detailed the policy, the more frequent the update requirements and the more complicated the training process for those who must adhere to it (Peltier, 2002). Thus, security experts should align the MEA security requirements and the security levels defined within the CFMS with statements and rules that are included in the enterprise's mobile device security policy. In addition, as security requirements continue to change, security experts, by keeping the mobile security requirements defined in the CFMS up-to-date, will support enterprises at the management level in defining mobile devices security policy, in particular, in defining which types of enterprise data may be accessed via mobile devices, and which types of mobile devices are permitted to access this data.

Technical Dimension: After defining the mobile device security policy and aligning it with security requirements, some security policies may be enforced via an EMM system and/or by applying technical security measures. These were discussed in Section 5.2. At this point, it is important to mention that some of these measures should be implemented with consideration of specific policies. For example, a policy might limit the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively, e.g. the use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

User Dimension: Applying security measures on mobile devices and enforcing policies can affect the employees' attitude towards using their mobile devices for work. This was discussed in Section 5.2. This dimension is of importance because both security and usability should be carefully considered when applying security measures on mobile devices. This dimension is connected to mobile device security policy that also includes organizational

rules of using mobile devices for work, e.g. the mobile device must not be lent to persons outside the enterprise even for a short period.

The security requirements included in the CFMS (see Table 23, Table 24, Table 25) have been classified into three security levels as shown in Table 31. This classification was performed based on the literature and through discussion with security experts. Such classification was needed to demonstrate the CFMS functionalities.

Security Level	Security Requirements
High	$mCom_{1, 2, 3, 4, 5, 7}$ $mOS_{1, 2, 4, 5, 6, 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23}$ $mApp_{2, 5, 7, 8, 12, 13, 14, 16, 17, 18, 20, 21, 22, 23, 24, 25}$
Medium	$mCom_{1, 2, 4, 7}$ $mOS_{1, 3, 5, 6, 7, 10, 11,12, 13, 14, 15, 16, 18,22, 23}$ $mApp_{1, 4, 9, 10, 11, 13, 14, 16, 17, 18, 21}$
Low	$mCom_{6}$ $mOS_{3, 8, 19}$ $mApp_{3, 15, 19}$

Table 31. Mapping security levels to security requirements

5.3.3 Summary

Enterprises should determine the intended security level for each MEA they use. This section has provided an overview on how to determine security levels including multiple dimensions that must be considered when defining security levels and determining the security requirements that have to be fulfilled to achieve these levels.

The CFMS includes a list of mobile security requirements that have been extracted and classified into security levels, based on literature review and discussion with security experts within enterprises. These requirements can be different from one enterprise to another. Furthermore, as security requirements can also be different from country to country because of different regulations and laws, the enterprise should define its own mobile security requirements taking into consideration multiple dimensions (see Figure 28). Thus, in this section, the list of mobile security requirements presented is not intended to be complete.

CFMS enables security experts to administrate their mobile security requirements and map them to related potential threats and security measures. In the technical dimension, the quality of the security measures and how these are implemented are out of the scope of this thesis.

6 Prototypical Implementation and Evaluation

The third phase of the research methodology described in chapter three is the development phase. It demonstrates the characteristics of the system by producing -as a proof of concept- the prototype that demonstrates the CFMS. Based on the conceptual specifications in chapters four and five, the CFMS has been implemented as a prototype in form of a web-based tool. The main goal behind this implementation is to demonstrate the framework's main functions, which in turn will enable a practical use of this framework in business sectors. In addition, the evaluation aspects of the prototypical implementations in different domains are presented here as well.

This chapter starts with a general overview of the prototypical implementation, where the UML diagrams and the database model of CFMS will be presented. A short explanation of the technologies adopted in this work is also provided. After that, the CFMS together with its guidance model and decision model are demonstrated. The chapter then shows the possible directions to evaluate this work in different domains. Finally, this chapter summarizes the main implementation issues explained in its sections.

6.1 General Overview of the Prototypical Implementation

The CFMS has been implemented in this thesis according to the requirements described in Chapter four, as a web-based prototype tool using up-to-date technologies. The selection of the specific technologies and products to use in developing the prototype depended on different factors like compatibility, performance, licensing and availability.

Due to many specific functions and the complexity of the data model of the CFMS, it does not make sense to use an existing system, e.g. to use an existing Content Management System (CMS) for the implementation, because the needed customization and adaption effort would be much higher in comparison to a new implementation of a web-based system. For implementation, the Model-View-Controller (MVC) framework was chosen in version 5 based on Microsoft ASP.NET. Choosing the C# programming language based on the Microsoft .NET Framework requires the selection of Microsoft Visual Studio which is the Integrated Development Environment (IDE) from Microsoft. Visual Studio provides an optimal integration of C# and supports the chosen ASP.NET MVC5 technology. Thus, Microsoft Visual Studio Community 2017 was used together with its integrated Microsoft

SQL Server 2016 LocalDB. For the design of the data model, the SQL scripts and procedures, Microsoft SQL Server 2016 Management Studio was used.

In addition, Table 32 presents further software products that were used for the implementation of the prototype:

Software Product	Description
Entity Framework[74] (Version 6.1.3)	Entity Framework is an open source framework for Object-Relational Mapping (ORM). It enables the use of relational data and facilitates database access for the .NET developers.
jQuery[75] (Version 1.12.4)	jQuery is a well-known free JavaScript library and offers several features for easy JavaScript usage and HTML DOM navigation and manipulation. It also offers many Asynchronous JavaScript and XML (AJAX) functions, which provides the ability to load data in the background and display it on the web page without having to reload the entire page.
DataTables[76] (Version 1.10.12)	DataTables is a free plugin for the jQuery JavaScript library and adds many features to HTML tables. It is a flexible tool which gives advanced interaction capabilities to HTML tables. In the context of this prototype, DataTables was used to represent the content of each component of the CFMS, with functions for sorting, searching, and page numbering.
Rotativa[77] (Version 1.6.4)	Rotativa is a C# library that provides a way to print PDF documents from ASP.NET MVC5 projects. The library offers functions for the creation of PDF documents based on views and it was used for the PDF export function.
Apache Subversion[78]	Apache Subversion is an open source version control system and becomes the central version management of files and directories. For the implementation of the CFMS prototype, Apache Subversion is used to manage the CFMS source code versions.

Table 32. Used software products for CFMS prototype

[74] https://docs.microsoft.com/en-us/ef/
[75] https://jquery.com/
[76] https://datatables.net/
[77] https://www.nuget.org/packages/Rotativa/
[78] https://subversion.apache.org/

6.1.1 UML Class Diagram of CFMS Meta-Model

The CFMS meta-model is shown in Figure 29 as a UML class diagram describing the framework components and the relations between them. This meta-model consists of nine classes defined as follows:

- class *SecurityLevel* defines the security levels of an MEA. This class includes attributes; mainly, id, name (e.g. low, medium or high), description (brief description of a security level), securityRequirements (as a set of security requirements), securityConcept (defines the MEA security concepts -i.e. the projects- that are classified in a security level). A *securityCheck* method is defined in this class, and checks if all the needed security requirements are considered. There is an association between class *SecurityLevel* and class *SecurityConcept*, where each security level classifies a set of security concepts. Furthermore, there is an association between class *SecurityLevel* and class *securityRequirement*, where the achievement of a security level requires the fulfillment of a set of security requirements.

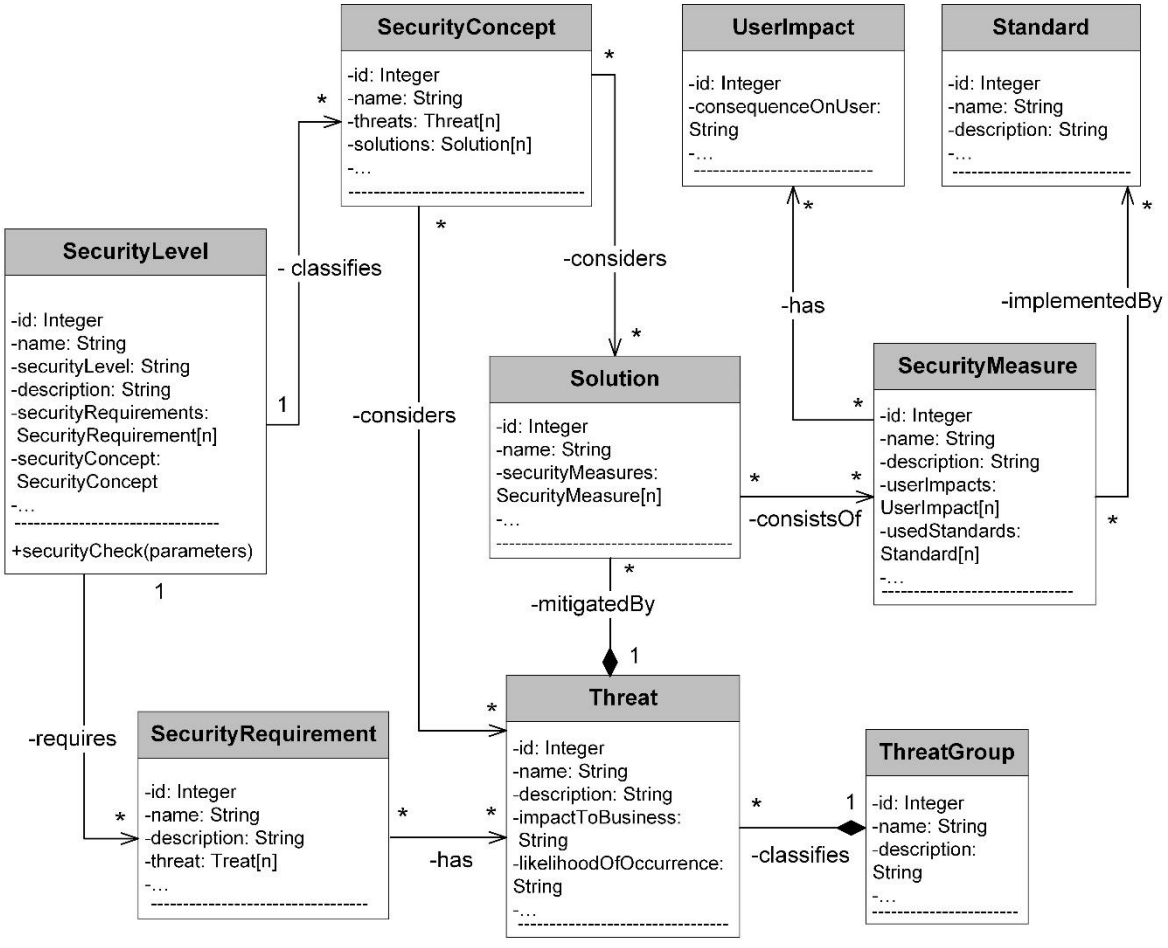

Figure 29. CFMS meta-model as UML class diagram

- class *SecurityRequirement* defines the security requirements related to MEAs. This class includes attributes, mainly, id, name (includes a prefix for the requirement category e.g. mOS_n for mobile OS category), description (brief description of a security requirement) and threat (a set of threats that need to be countered to meet the related security requirement). There is an association between class *SecurityRequirement* and class *Threat*, where each security requirement has a set of threats that need to be countered.
- class *Threat* defines security threats related to MEAs. This class includes attributes, mainly, id, name (threat name), description (threat briefly described), impactToBusiness and likelihoodOfOccurrence. There is a composition between class *Threat* and class *ThreatGroup*, where each threat is classified in a threat group. Furthermore, there is a composition between class *Threat* and class *Solution*, where the potential risks caused by each threat are mitigated by one or more security solutions.
- class *ThreatGroup* defines threats categories. This class includes attributes, mainly, id, name (name of threat group/category), description (brief description of a threat group).
- class *SecurityMeasure* defines security measures that can be applied on mobile devices. This class includes attributes, mainly, id, name (security measure name), description (describes the measure briefly), userImpacts (a set of potential consequences when applying this security measure) and usedStandards (a set of Standards that should be used to implement this security measure). There is an association between class *SecurityMeasure* and class *UserImpact*, where each security measure has a set of potential consequences on the user. Furthermore, there is an association between class *SecurityMeasure* and class *Standard*, where each security measure can have a set of standards needed for its implementation.
- class *Standard* defines security standards that are needed for the implementation of the security measures. This class is included in the CFMS meta-model, however it was not included the resulting prototype. This class can be implemented in future work.
- class *Solution* defines a set of potential security solutions alternatives that should be applied to secure MEAs. This class includes attributes, mainly, id, name (solution name) and securityMeasures (a set of security measures included in a security solution). There is an association between class *Solution* and class *SecurityMeasure*, where each security solution consists of one or more security measures.

- class *SecurityConcept* defines the security concepts of the created projects of MEAs. This class includes attributes, mainly, id, name (project name), threats (a set of potential threats that are related to the project), solutions (a set of the security solutions that should be applied for the project). The class *SecurityConcept* also has associations with the class *Threat* and the class *Solution,* where each security concept considers a set of related threats together with the needed security solution for each threat.

6.1.2 Main CFMS Interactions

This section presents the main CFMS interactions between its models and users. First, the main interactions when a non-security expert user creates a new project -the security concept of MEA- are depicted as a UML sequence diagram in Figure 30. It shows the message exchange between the business user, decision model and guidance model. The communications flow starts from the business user sending a request to decision model to create a new project. Then, the guidance model responses by presenting all the potential mobile security requirements to the decision model, which in turn displays these to the business user.

The business user has then two options, he/she can select the intended security level or select the needed requirements and the decision model will determine the security level based on the selected security requirements.

In the next step, the decision model will display the potential threats and possible solutions to counter these threats after requesting them from the guidance model. The business user can select between alternative security solutions based on the associated impacts on user. The decision model then sends a security check request -along with the threats and requirements as parameters- to the guidance model, which in turn checks if all the needed security requirements are selected and if there is a solution selected for each related threat. After that, the decision model displays the security check result to the business user.

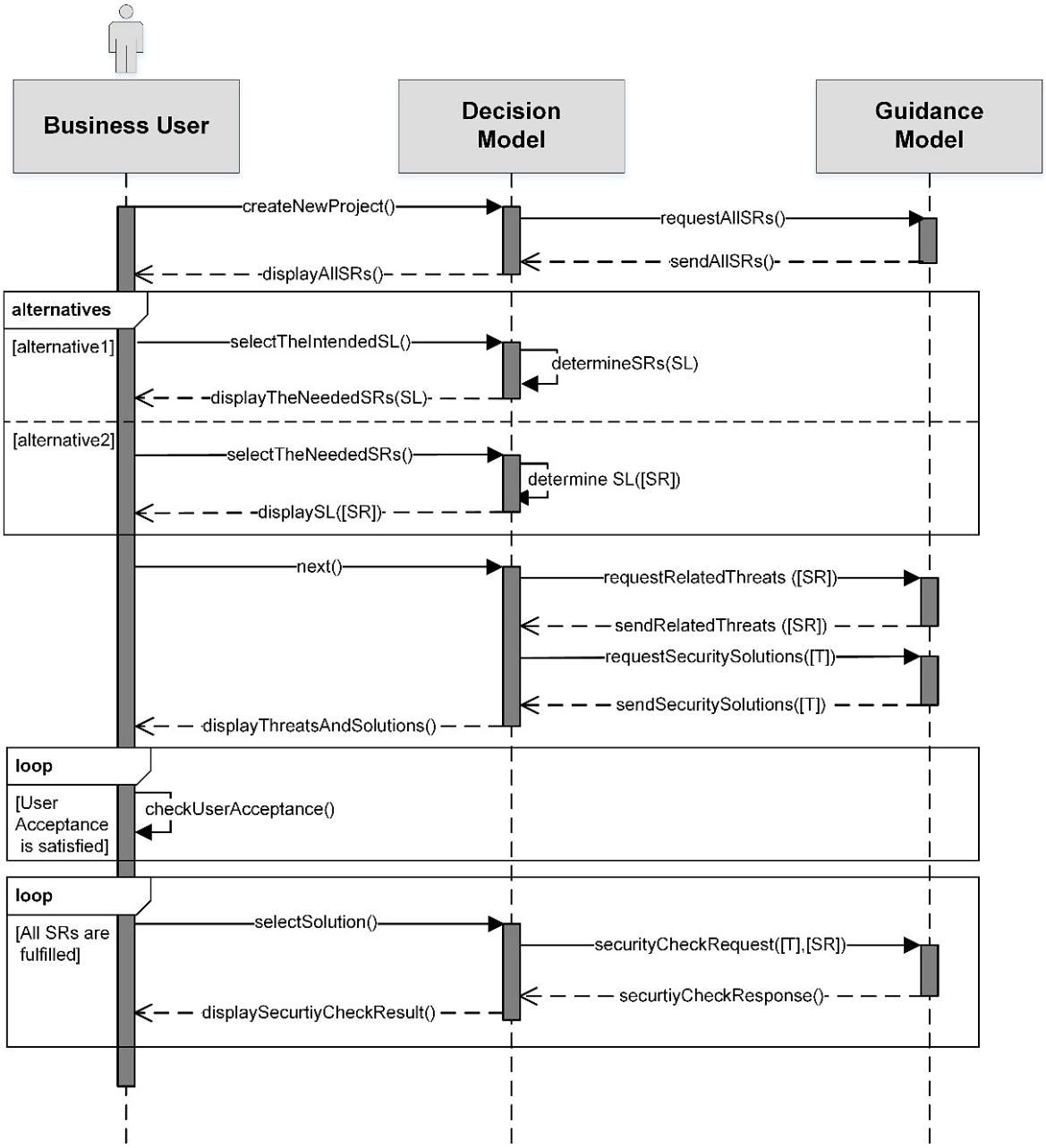

Figure 30. Main interactions to create a new project

Furthermore, the business user will have the possibility to add adjustments to the threats and solutions. These adjustments should be reviewed by a security expert before including them in the guidance model. Figure 31 shows further CFMS interactions, where the business user can include new threats and their solutions within the project. This is a very important process to include possible additional threats not covered in the guidance model in its current version.

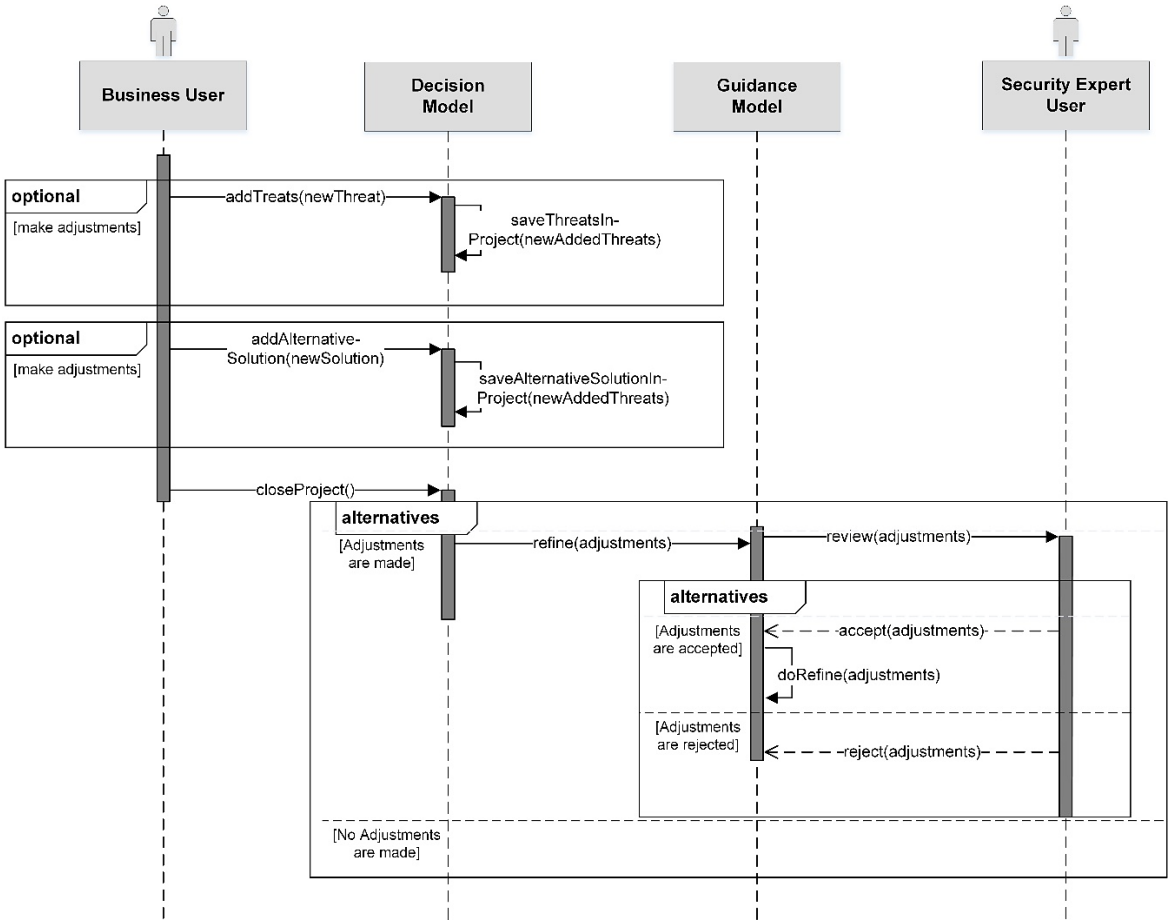

Figure 31. Main interactions to refine the guidance model

Finally, when the business user closes the project, the newly added threats and solutions will be sent through the guidance model to the security expert user to review them. If the added threats and/or solutions are accepted, they will be included in the guidance model draft and will be available to other projects in the next release of guidance model.

6.1.3 Database Model of CFMS

The CFMS database model was designed to determine the logical structure of the CFMS database and to fundamentally determine in which manner data can be stored, organized and manipulated. Hence, the method "Database First" of the Entity Framework with ASP.NET was chosen. This means that the database tables were first created in the SQL database and then the C# model classes were created using a function of the entity framework. Figure 32 shows the main tables in the database relational model of CFMS.

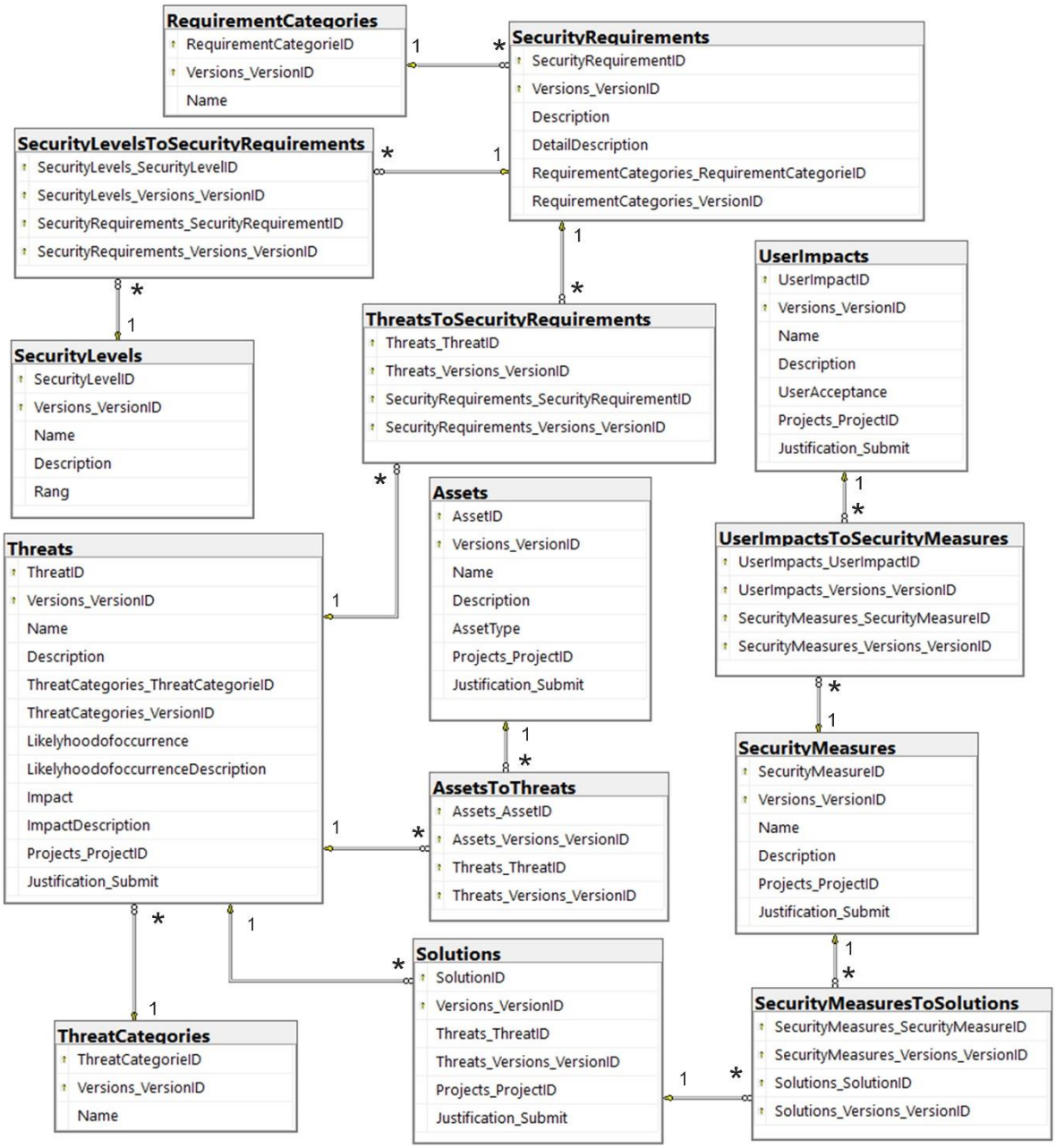

Figure 32. Database relational model of the CFMS

6.2 CFMS Demonstration

All the CFMS functionalities listed at the phase of requirement definitions (see Chapter 4) are implemented as a web application. The main GUI is shown in Figure 33, where the user can register/login as a specific role, e.g. security expert user or business user.

Figure 33. CFMS home page

After the registration as 'role security expert' for example, the user can login using email address and password. Figure 34 shows the login screen.

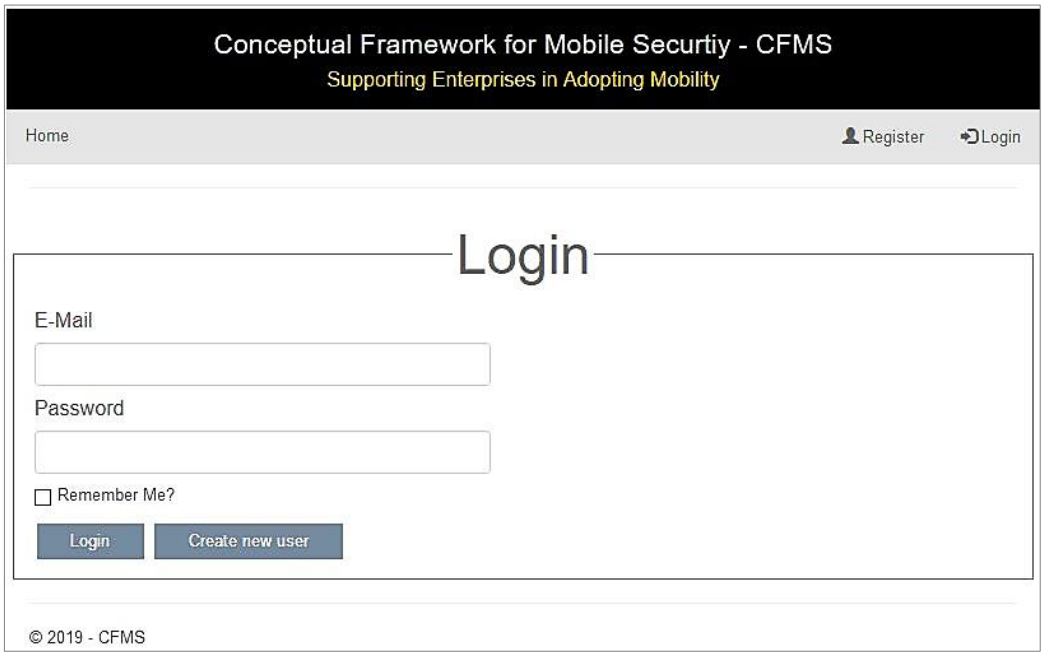

Figure 34. CFMS login screen

After a successful login as security expert, both models, the guidance model and the decision model, will be available for the user. Figure 35 shows the main page after the login in as security expert user.

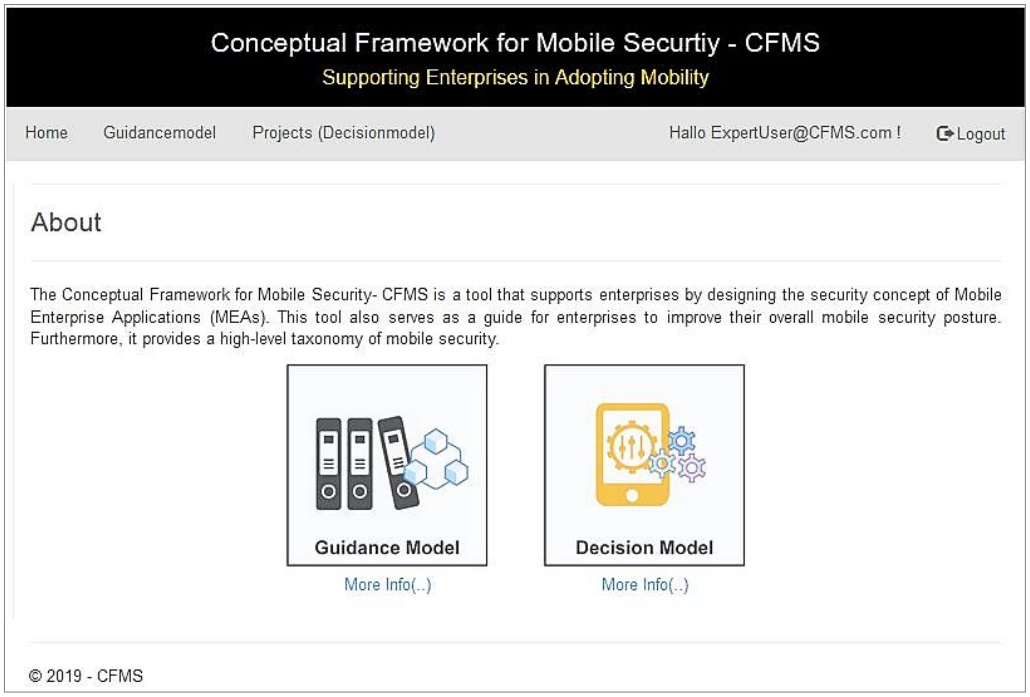

Figure 35. Main page after logging as security expert

Logging as business user (or any other role excepting the role security expert), the user would have access to decision model only, as shown in Figure 36.

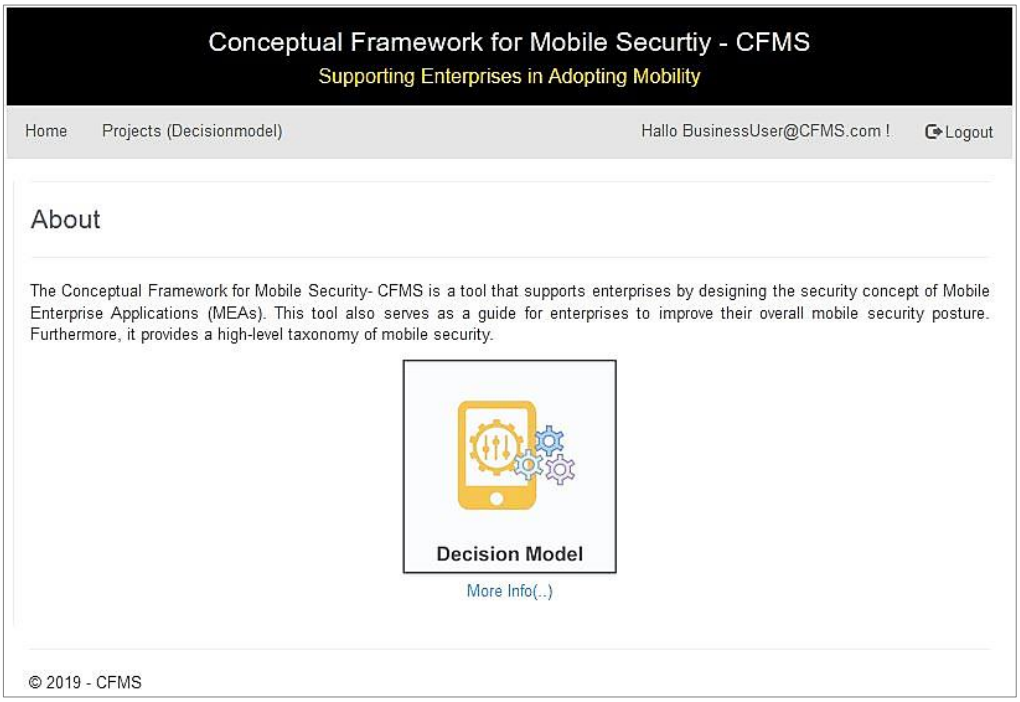

Figure 36. Main page after logging as non-security expert

In the following two subsections, the guidance model and the decision model are presented by demonstrating their main functionalities.

6.2.1 CFMS Guidance Model

The guidance model is available for security experts only. Figure 37 shows this model GUI where security experts can administrate its content and its versions. It is divided into two areas, "Versioning" and "Content Administration". In the "Versioning" area, as shown in the Figure, the security expert works on the guidance model version 1.8 (draft), which means that this version is not available yet to the decision model. Security experts can also load old versions of the guidance model by selecting that version and clicking on "Load".

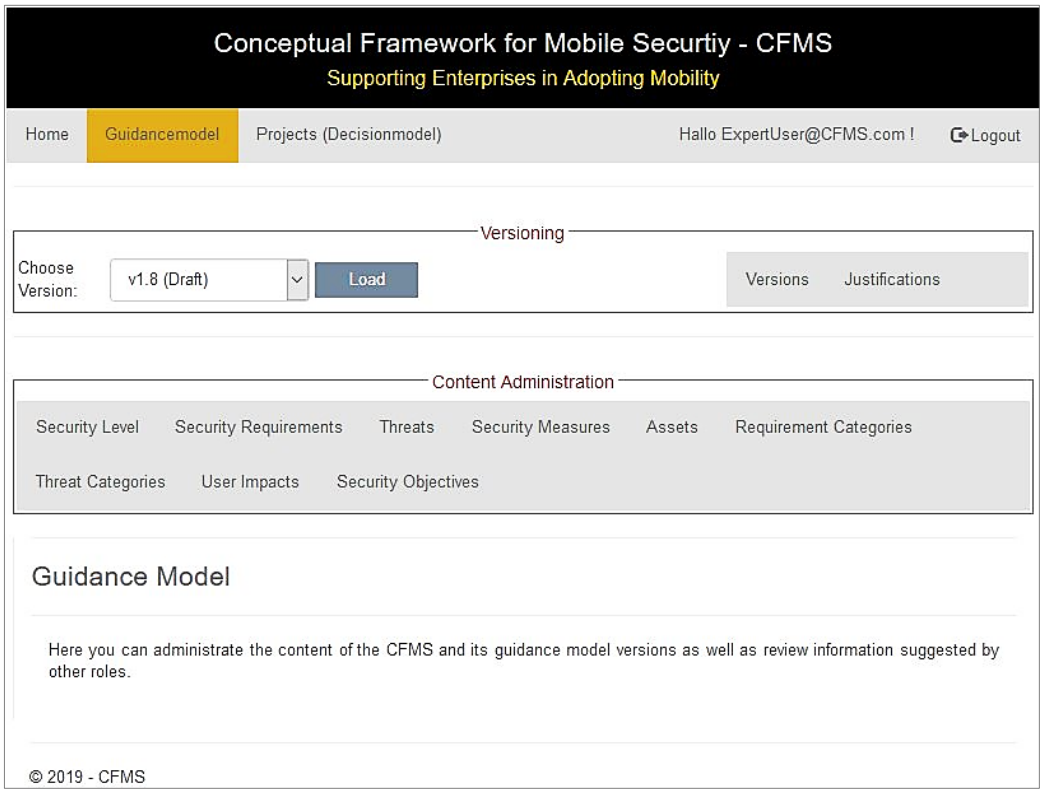

Figure 37. Main page after logging as security expert

In addition, an expert user can review suggested changes that were sent from the other roles via the decision model. Such changes will be shown when the security expert clicks on "Justifications". Here, the security expert can review the suggested changes and he/she has the option to accept or reject them. If these changes are accepted, they will be added to the draft version of the guidance model i.e. "v1.8 (draft)". These changes will be available to the decision model once a new version of the guidance model is created.

Figure 38 shows where to create a new version of the guidance model, where a list of all guidance model versions is shown along with the version type and creation date for each version. Creation date is important to keep a history of the actions when new versions of the

guidance model have been created. An improvement here would be to also log which user has created/released each version.

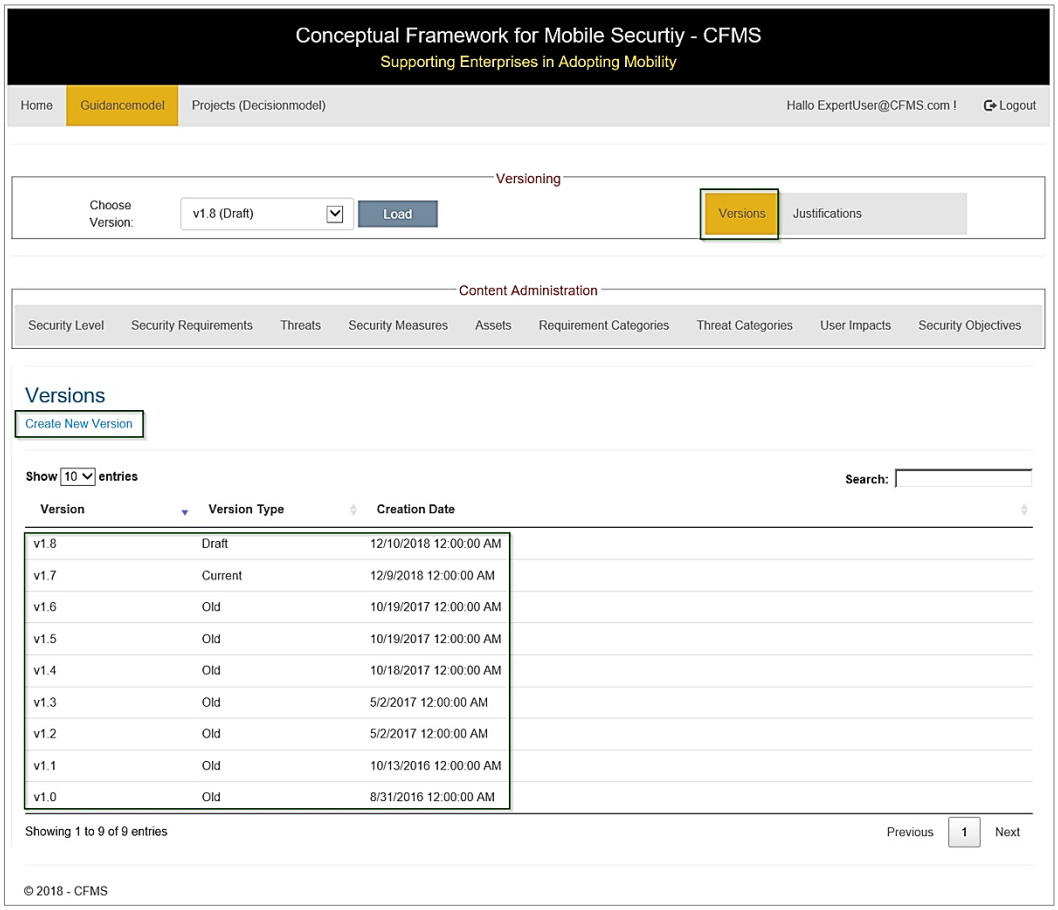

Figure 38. CFMS versions administration

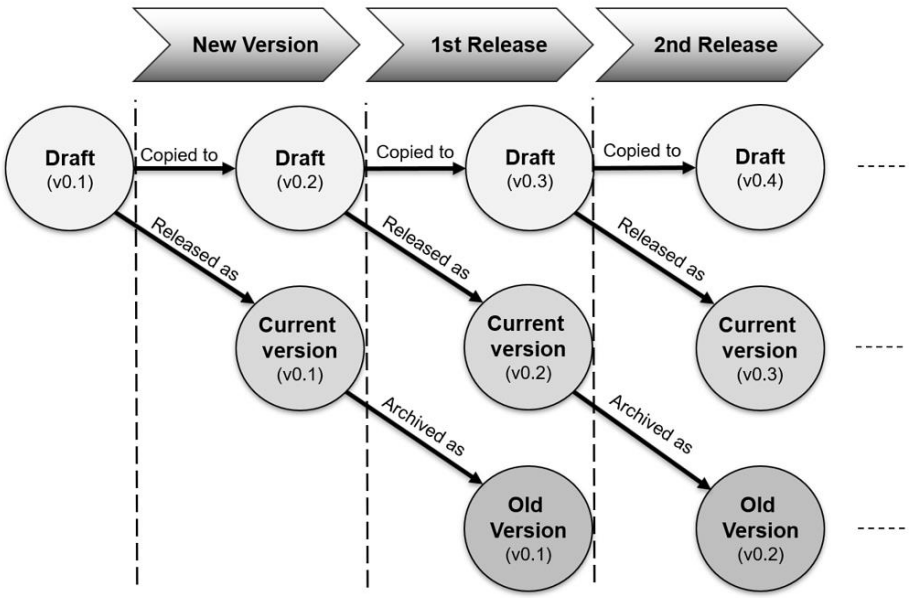

Figure 39. Management of guidance model versions

What happens in the background when creating a new version of the guidance model is illustrated in Figure 39. Starting with version v0.1 (draft), creating a new version of the guidance model will first copy version v0.1 (draft) to version v0.2 (draft) and then version v0.1 (draft) will be released as version v0.1 (current), which will be then available to the decision model. Repeating this process when version v0.2 (draft) is ready to be released, version v0.2 (draft) will be copied to version v0.3 (draft), version v0.2 (draft) will released as version v0.2 (current) and version v0.1 (current) will be archived as version v0.1 (old). The SQL stored procedure that creates a new version of the CFMS guidance model is presented in Appendix C. In the CFMS, only the content of the latest version type "current" will be available to the decision model.

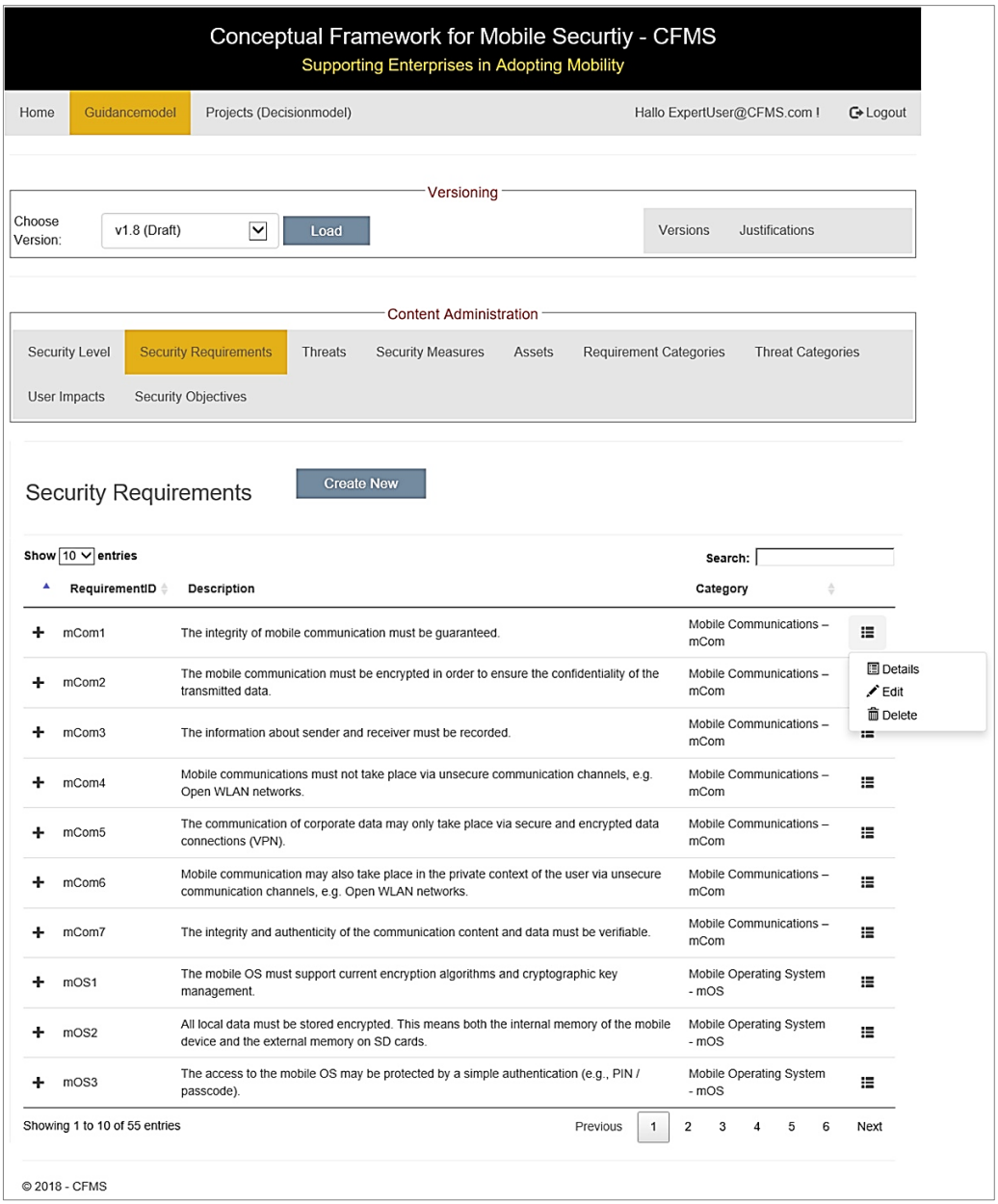

Figure 40. Screenshot of administrating the content of the guidance model

Finally, security experts can administrate the content of the guidance model by adding, editing and deleting functions. Figure 40 presents a screenshot where security expert user can administrate the mobile security requirements. In addition, security experts can perform the mapping between the components of the guidance model according to their relationships as already illustrated in the CFMS meta-model as UML class diagram (see Figure 29, Page 111).

6.2.2 CFMS Decision Model

The decision model is available for all the roles of the CFMS, i.e. for security experts and non-security experts as well. However, the main targeted group for the decision model is the non-security experts. Figure 41 shows a project list created along with the status and the related guidance model version for each project. For example, "MEA Project A" is a closed project (with status "Final") and the project had been created according to the guidance model version v1.0.

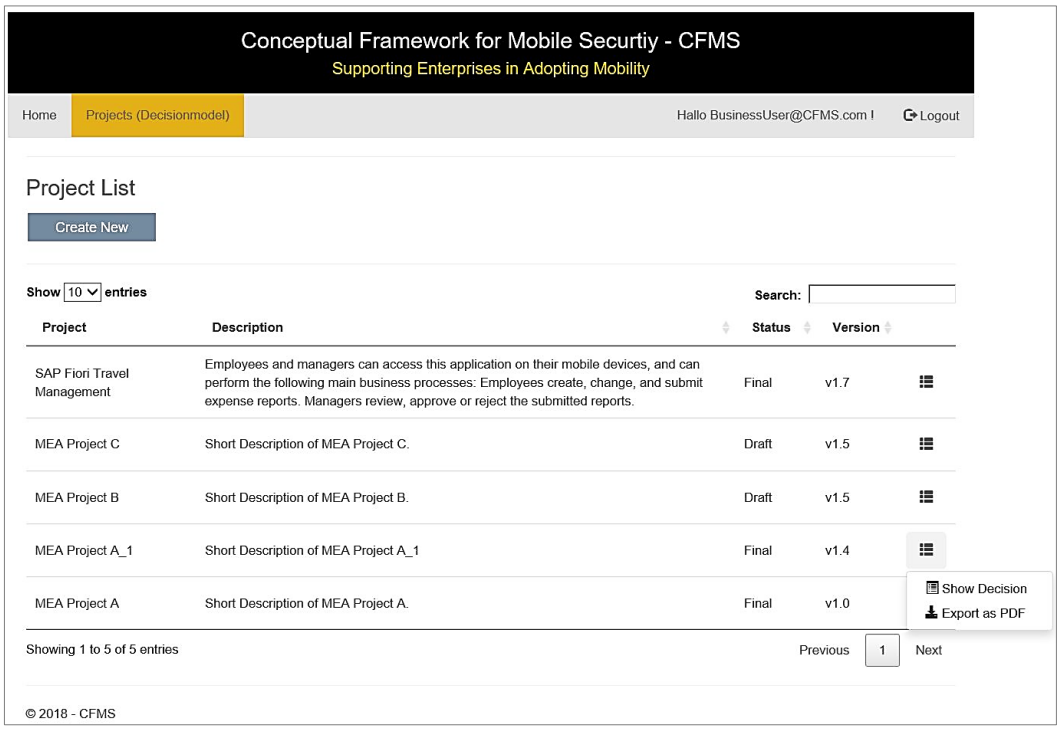

Figure 41. Project list in the decision model

The closed projects can be presented or exported as PDF that includes all the information related to that projects, including the mobile security requirements, the related threat and security solutions (with the individual security measures in each solution). Finally, new projects can be created via this model. This is illustrated in Section 6.3.2 based on MEA use case.

6.3 Evaluation

Based on the research methodology presented in Chapter three, this section gives the final discussion of the CFMS evaluation. The evaluation is an important process, in which, the utility, quality, and efficacy of the artifact must be rigorously demonstrated via well-executed evaluation methods (Hevner et al., 2004; Hevner & Chatterjee, 2010). Thus, the choice of evaluation methods is driven by the type of the artifact, which lend themselves to evaluation with particular methods (Peffers, Rothenberger, Tuunanen, & Vaezi, 2012). To evaluate the CFMS, the following evaluation methods were chosen:

- Functional testing: The CFMS was implemented as prototype to demonstrate its utility. Section 6.3.1 presents how the CFMS functionalities have been tested and demonstrated within enterprises.
- Illustrative scenarios: The CFMS was also evaluated by constructing business scenarios to demonstrate its utility (see Section 6.3.2). Furthermore, Section 6.3.3 illustrates how the CFMS can be utilized in another domain, namely, Smart Cities applications, to address issues related to privacy concerns.

6.3.1 Functional Testing and Conducted Workshops

The functional testing was conducted in two phases. In the first phase, the CFMS was implemented as a prototype and it was tested against its functional requirements through function tests. Thus, all CFMS functional requirements defined in Section 4.4.2 were fulfilled. In this phase, feedback from many discussion-sessions in Lufthansa Industry Solutions GmbH & Co. KG were also taken into consideration within the development phase of the CFMS.

In the second phase, the CFMS together with its functions was demonstrated and discussed in three workshops with different roles present, including, IT security officer, IT operation manager, and managing director within three German enterprises, namely, BTC AG, EWE AG and Lufthansa Industry Solutions GmbH & Co. KG. Each workshop took about 120 Minutes, divided into two sessions, theoretical and practical. In the theoretical session, the CFMS was presented, including short background information about MEAs and mobile security as well as explaining the idea behind this work. Moreover, the main outcomes behind CFMS were also presented in that session. After that, the practical session of the

workshop took place. Here, the CFMS prototype was presented via live demonstration of its models, guidance model and decision model, along with the functionalities that are supported in each model. This was done based on two prepared scenarios (a scenario demonstrated at BTC AG is presented in Section 6.3.2). After the presentation sessions, open discussions took place. For the workshop conducted at BTC AG, the discussions were partly based on a prepared questionnaire (see Appendix D).

Output from all interviewees showed the CFMS to be a very useful tool that is ideally suited for deriving the necessary security measures needed to achieve a security level. This derivation is nowadays not an easy task. The interviewees also found that the use of the CFMS can significantly accelerate the adoption of new MEAs by supporting business users with their decision-making process. They added that operational issues are often excluded from the decision-making process, but these can be easily included in that process using the CFMS. Moreover, the administration of the guidance model's versions, and the adjustments that may be provided by business users, support the continuous extension of the guidance model by including new content. In addition, as the security requirements can be different for each enterprise, depending on its size and domain, each enterprise can generate and administrate its own versions of guidance model. It was also confirmed that for enterprises that outsource their mobile technologies, the CFMS can serve as a communication interface between such enterprises and their external service providers. Besides business users, expert users like IT security officers, who have good IT security expertise, can benefit from the CFMS, since it enables a sustainable and structured documentation of the decisions made.

To conclude, further comments and suggested potential extensions from the participants in the workshops were as follows:

- Documenting security knowledge in the way presented, including mapping between security levels, security requirements, potential threats and security measures, is nowadays a challenge for enterprises, because there are no suitable data structures to store these in an adequate, structured and transparent manner. Tools such as Microsoft Word and Excel are used to include such knowledge, however, they are usually unstructured, confusing and difficult to review. Through the functionalities of the guidance model, the CFMS offers a possibility to store and administrate information about mobile security, adapted to each enterprise. In addition, all the participants found that the CFMS would be a good supporting tool for mobile security management.

- The means used to transfer the security knowledge to business users is very important. Through the listing and mapping of the CFMS content, business users might even be encouraged to add further information to the framework (in form of adjustments). Moreover, the CFMS would help security experts to justify the implemented mobile security measures and restrictions to the business users.
- The continuous adaptability and the inclusion of adjustments (justifications) as information feedback from projects were regarded as very positive. First, adjustments can be suggested by business users through the decision model, then the expert users can review these adjustments (quality control) in the guidance model before these are adopted in the next release of the guidance model.
- A feedback system for implementation projects was suggested, in order to obtain the follow-up on the decisions taken, especially with regard to the mobile security measures that need to be implemented. For example, it is conceivable that the implementation manager can provide feedback on the implemented security measures, so that a backflow to the framework is possible. This gives enterprises a structured overview of the security measures implemented.
- In addition, in case that certain mobile security measures could not be implemented, due to lack of available technologies, a feedback (report) from security expert users to risk management would also be a conceivable extension, to enable decisions on the risk acceptance.
- Instead of creating a project (security concept) for each MEA, a project including classes of MEAs that share the same security requirements could be created. It was suggested that such a project can serve as a template for other MEAs.
- Further, a suggested extension is to enable the CFMS to include other application types than MEA, for example, backend or desktop applications. On the one hand, the functionality of the guidance model can be so extended that the relevant components of the CFMS, such as security threats and measures, can be associated to one or more application types. On the other hand, the decision model can be extended to enable users to select a specific application type when creating a new project.

- The PDF export function was seen as a possible way to communicate the security requirements and the security measures to the implementation projects, so such documents would include the needed requirements clearly set out and justified.

Finally, according to the feedback obtained from the workshops, the CFMS was perceived as a useful tool that supports enterprises at security by design and security management when adopting MEAs. Furthermore, the maintenance of the guidance model is crucial, so that the CFMS will be applicable for enterprises with a good IT security department, where the security experts can take over the maintenance of the guidance model. However, for enterprises that outsource their mobile technologies, the CFMS can serve as a communication interface to justify and manage the mobile security requirements between that enterprises and their external service providers.

6.3.2 Business Scenarios from Praxis

This section illustrates possible utilization of the CFMS based on business scenarios at the enterprise BTC AG, which provides its employees with an application called SAP Fiori[79] for travel management. Employees need the chance to work productively on the move within business trips. Instead of having to travel to their offices to enter travel costs and other expenses, they should be able to enter them on the move. As discussed at BTC, this application can be accessed on windows PCs via a web portal or on mobile devices via a mobile application client. The second case is relevant here, employees and managers can access this application on their mobile devices, and can perform the following main business processes: a) Employees create, change, and submit expense reports, b) Managers review, approve or reject the submitted reports.

With this application, personal data (such as name, address, location data) of the employee can be accessed by managers, including information about trips and expenses. In addition, this application allows expense reports to be stored on mobile devices so that the application does not have to retrieve the data from the server every time it is opened. As this application enables managers to access personal data for employees, the security level required for the application data should be high as required by the legal dimension (see Table 30 in Section 5.3.2). After the security level was defined, the CFMS decision model was demonstrated

[79] https://experience.sap.com/fiori-design-web/fiori-client/

including the following workflow: In the first step, business user created new project by entering a project name with a brief description, as shown on Figure 42.

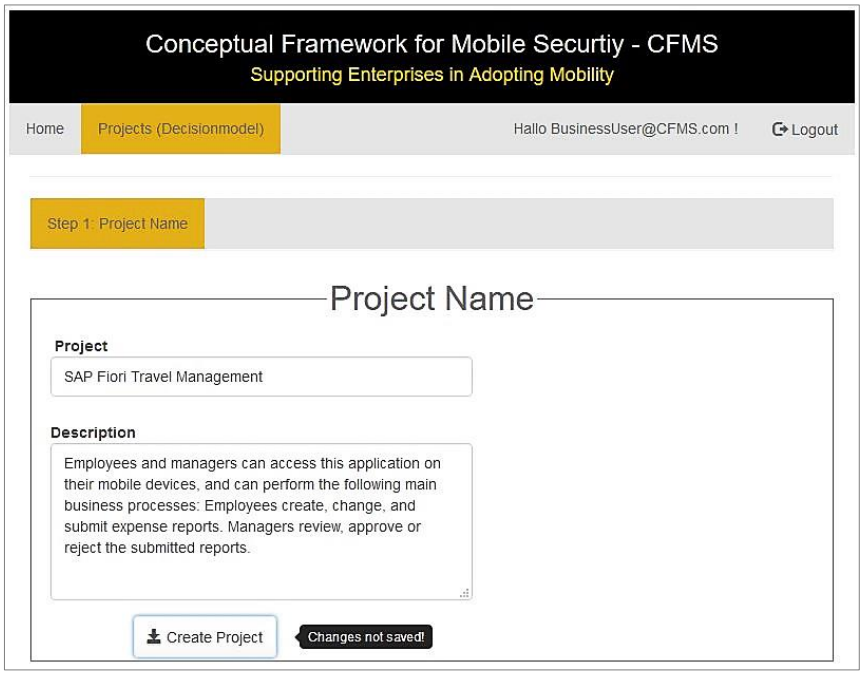

Figure 42. CFMS decision model – create a new project

In the second step, the decision model showed the next screen, where an intended security level can be chosen. As depicted on the Figure 43, the decision model shows a label "Security Level Undefined", i.e. that the security level was not chosen yet.

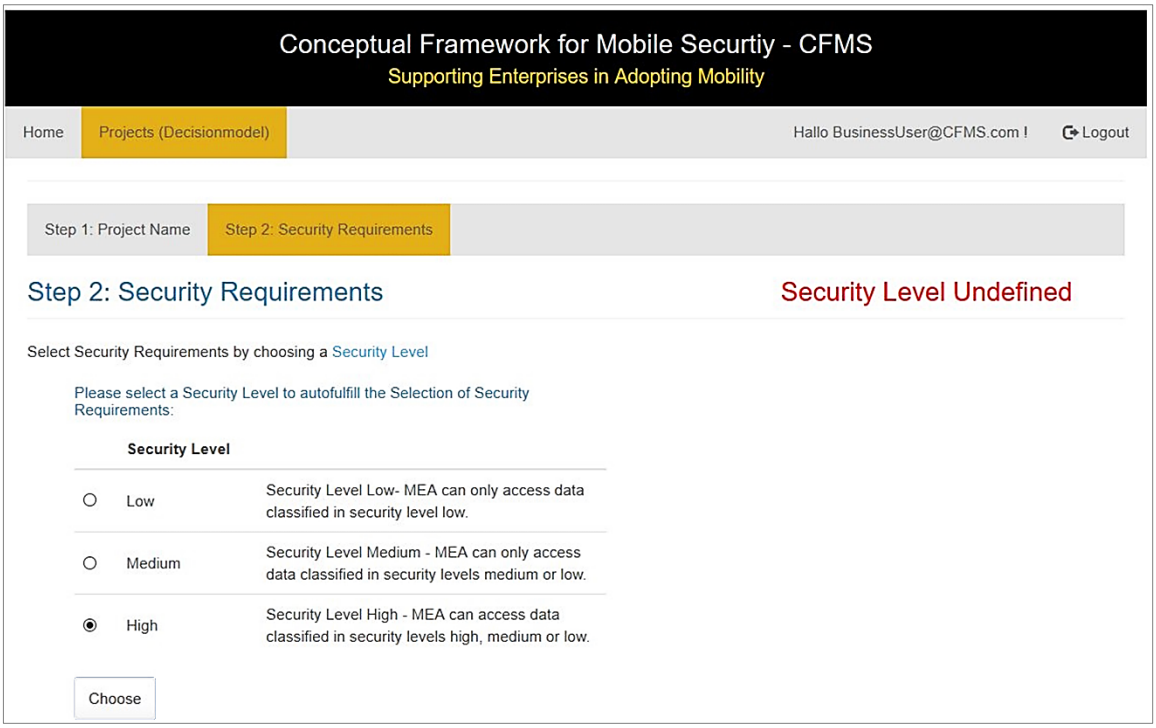

Figure 43. CFMS decision model – choosing a security level

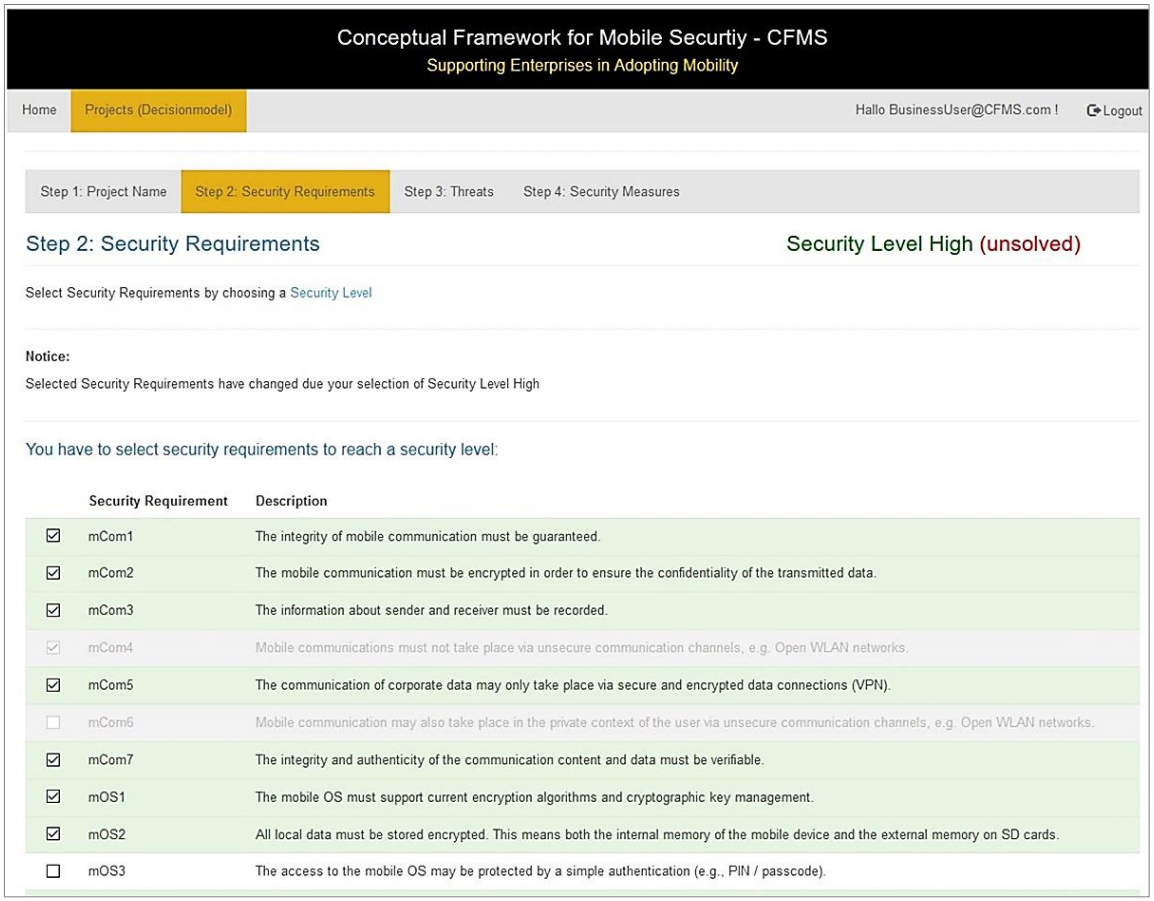

Figure 44. CFMS decision model – presenting the security requirements

As the security level needed for the application data was determined as high, the security level high was chosen in the CFMS and consequently the mobile security requirements needed were presented. Figure 44 shows a screenshot of this step, where a label "Security Level High (unsolved)" was also shown, i.e. that the security measures needed were not yet selected. This is done in the next steps. This label shows the result of a security check method, so that the security level will be shown as "unsolved" until both the needed security requirements and measures are selected.

In the third step, the decision model showed the potential threats and in the fourth, recommended security measures to counter each threat. After security measures were selected for each threat, a label "Security Level High" was shown. Figure 45 presents the final step, where the project can be closed by clicking on the button "Make Decision". The created project can be exported as PDF that includes the security requirements needed, the relevant threats and the security measures selected along with possible consequences for user.

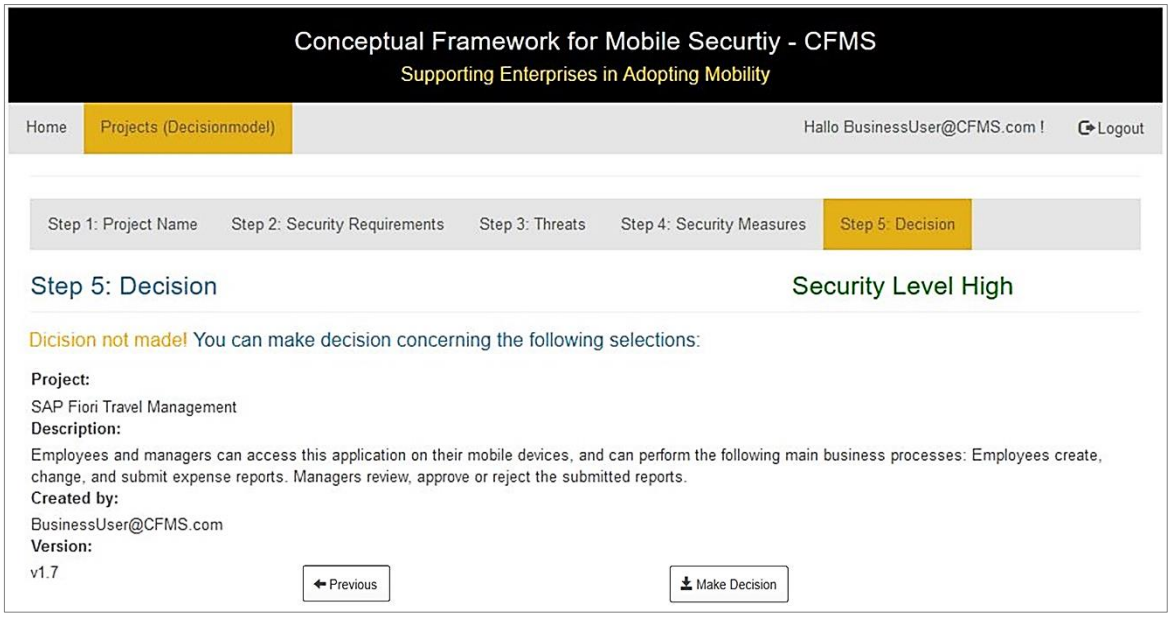

Figure 45. CFMS decision model – overview on the project being created

The above-mentioned scenario was presented for an existing MEA that is already used by BTC. The discussion at BTC concluded that that the information included in the created project will be useful to check if the security measures selected are indeed already applied. In addition, for an enterprise that wants to provide its employees with such an MEA, the information included will provide a checklist for the design and implementation phase.

Two more MEAs, Enterprise File Sharing (EFS)[80] and Sovanta Executive Cockpit[81], were discussed at BTC, but these cannot be included in this thesis, because the relevant information is confidential and therefore, BTC did not permit its inclusion.

6.3.3 Utilization of CFMS in Smart Cities Applications

Beside the demonstration of the CFMS within enterprises, the concept of CFMS was discussed in the 10th CEMIS-Days conference (Corporate Environmental Management Information Systems) with the aim of utilizing the CFMS to address issues relates to privacy concerns in Smart Cities (Hasan & Amin Rezaei, 2018).

[80] EFS is an application used to exchange data with external users who do not belong to corporate network. External users can be business customers, external service providers, or other contracting parties. EFS can be accessed via web portal or mobile app.

[81] https://sovanta.com/de/executive-cockpit

The next following subsections present the privacy concerns in Smart Cities applications, define the related problem, and finally illustrate how the CFMS can be utilized to address the defined problem.

6.3.3.1 Privacy Concerns in Smart Cities Applications

Population increase, climate change, and scarcity of resources have resulted in the fastest urban growth the world has experienced in recent decades (Biswas & Muthukkumarasamy, 2016). Recent studies have shown that more people live in cities (54 percent) than rural areas (46 percent) and by 2050, 66 percent of the world's population is predicted to be urban (United Nations, 2014). This urban growth leads to excessive usage of resources, which, in turn, triggers cities to employ modern technologies aiming to use resources optimally, reduce costs, monitor energy usage and to create a smart urban environment, called Smart City. Examples of such technologies are the Internet of Things (IoT) (an ubiquitous interconnected network of computing devices, software, smart sensors) and big data analytics. Such interconnected devices and sensors are mostly used to collect information, which is communicated in real time using wired or wireless networks. Analyzing the collected data would help a Smart City to understand what is happening now and what is likely to happen next. These processes promise to make cities safer and more sustainable. Such processes use and produce massive amounts of data. In recent years, the number of Smart Cities applications has been steadily increased in many domains, like smart environment, smart mobility, smart economy and smart governance (AlDairi & Tawalbeh, 2017).

However, as citizens are more and more dependent on IoT devices, with data available about their location and activities, privacy seems to disappear (Elmaghraby & Losavio, 2014). A crucial point is to provide citizens with transparency on how to maintain their privacy, when data is being collected from everywhere around them. Moreover, an essential key in the success of the Smart City concept is that citizens participate and trust the infrastructures. However, this requires that they can be assured that their privacy and security remain intact.

The emerging city data landscape presents additional challenges for public sectors like local governments. With respect to data, six concrete and operational issues are identified, namely, data sources, information sharing, data quality, costs, security and privacy (Al Nuaimi, Al Neyadi, Mohamed, & Al-Jaroodi, 2015; van Zoonen, 2016). Moreover, due to the increasing

number of Smart Cities worldwide, security and privacy concerns have become more important than they are for any technological phenomenon (AlDairi & Tawalbeh, 2017).

A crucial point to be considered here is the continuous change in laws and regulations that might demand stricter privacy. For instance, in Germany, the current Federal Data Protection Act[82] (dt. Bundesdatenschutzgesetz) aims at protecting the individual against his/her right to privacy being impaired through the handling of his/her personal data. As stated in that act, "*Personal data means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)*". Such information includes, but is not limited to, name, gender, Hobby, IP addresses (static and dynamic). This act has been replaced by a new EU regulation, the General Data Protection Regulation (GDPR)[83], which went into effect on May 25th, 2018 in all member states to harmonize data privacy laws across Europe. The new regulation has become stricter, e.g. instead of 300,000 Euros fine according to the current act, the administrative offences shall be punishable by a fine of up to 20 million in the new regulation, or up to 4 percent of the total worldwide annual turnover of the organization involved in the preceding financial year, whichever is higher. Applying the (EU) GDPR demands that companies consider further security and privacy requirements. However, communicating these requirements between different parties and managing them are very important.

With rising interest in Smart Cities, the concerns over potential privacy violations are increasing as well. In recent years, a rising trend of warnings and hints has been reflected in social media and papers, reported by activists, journalists, non-governmental organizations (NGOs) as well as non-profit organizations and some political parties in regard to privacy breaches in Smart Cities. Because of the increasing pressure from the afore-mentioned sources, politicians are taking privacy issues into consideration more seriously. Moreover, studies have shown that the participation of the citizens plays an essential role in success of Smart Cities, and this cannot not take place, unless they trust the concept of Smart Cities and are sure that their security and privacy rights will not be ignored (Martinez-Balleste, Perez-martinez, & Solanas, 2013). The nature of the security and privacy flaws in Smart Cities emerges due to two aspects: 1) sharing of multiple datasets between different organizations - which might apply different policies, and 2) the profit-driven nature of the private sector.

[82] https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0013
[83] https://gdpr-info.eu/

Because of budget deficits, public organizations mostly relying on private sectors for many of their internal and external processes and services. In terms of IT infrastructure, this means: sharing multiple datasets with each other (which is technically known as Data Mashup - a technique that combines the use of multiple data sets with a common subject of interest). Thus, multiple datasets can join in a manner which alters the existing data (Belleau, Nolin, Tourigny, Rigault, & Morissette, 2008). Through literature review, three common security and privacy issues can be defined regarding high dimensional data mashups: 1) by combining together multiple private data sets, the resulting data set would reveal more sensitive information to the other data providers, 2) the integrated data set could make identification of individuals easier by providing more data points for re-identification, and 3) mashup data from multiple sources may contain so many data attributes that traditional privacy models, like K-anonymity (Samarati, 2001; Sweeney, 2002), would render the protected data useless for analysis (Braun, Fung, Iqbal, & Shah, 2018).

Different studies have shown that the K-anonymity model is vulnerable to a range of attacks, including: Definetti attacks (Kifer, 2009), compositions attacks (Ganta, Kasiviswanathan, & Smith, 2008), and foreground knowledge attacks, where the attacker has some background knowledge of the individuals in dataset (Chen, Fung, Desai, & Sossou, 2012). To address issues related to high dimensional data mashups, differential privacy technology is applied. Differential privacy has been considered as one of the strongest privacy models because it empirically guarantees privacy regardless of an attacker's background knowledge (Dwork, 2008), and it provides a mean to measure and quantify the privacy level (Biryukov et al., 2011). Although such a model can address many privacy issues, communication between private and public sectors remains an essential element to facilitate the application of the privacy requirements.

6.3.3.2 Problem Definition

To define the problem at an abstract level, it is the matter of communication between two or more different parties, who are using different business protocols regarding their security and privacy. Thus, there should be a mean in between, which functions as an interface to facilitate the communication. In case of Smart Cities, the privacy and security requirements should be communicated between public and private sectors.

As depicted in Figure 46, the public sector provides public services to citizens and their perceived level of privacy plays a very important role in their decisions on participation in Smart Cities. The public sector is more concerned about citizens' privacy, but on the other hand, to fulfil their processes, they are dependent on services, which are offered by private sectors. Such a dependency forces them to share their data set with other third parties.

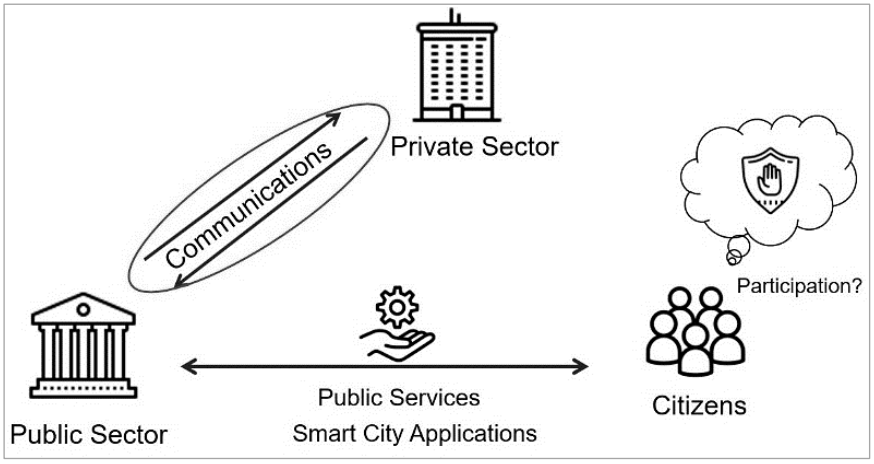

Figure 46. Need of communications between public and private sectors

The private sector, which tends to maximize profit, normally provides only the minimum level of privacy protection measures (Braun et al., 2018); therefore, they might compromise the level of privacy which the public sector is eager to maintain. Accordingly, to enable an effective communication between different parties, public and private sector organizations need cybersecurity and cyber privacy professionals with good communication skills, vendor understanding and business analysis, to communicate the level of requirement and measures that have to be taken (Andreasson, 2012; Braun et al., 2018; Carr, 2016).

To address this problem, the following section suggests the use of the CFMS[84] that can facilitate and make the communication of the security and privacy requirements between public and private sectors more efficient.

6.3.3.3 Possible Utilization of CFMS in Smart Cities

One of the possible scenarios for use of the CFMS in context of Smart Cities applications is described in the following.

[84] In this context, CFMS can be used for mobile and non-mobile applications.

The public sector should have a role of "security expert", which has specialized knowledge in security and privacy. Firstly, security experts in the public sector determine the security and privacy requirements that are needed to comply with the current regulations and laws. These requirements are included in an entity "requirement" in the CFMS guidance model. Secondly, security experts map each security requirement to a set of security measures that are need to fulfill the related requirement. These security measures are included in an entity "security measures" in the guidance model.

Through the CFMS decision model, the guidance model can be instantiated in the form of projects, which in turn form the security concept of the Smart City application. The CFMS provides the functionality of exporting these projects as PDF files. A PDF file includes two lists –mapped to each other, the security and privacy requirements and the needed security measures. Hence, these can be used as checklist for other roles in the private sector, e.g. app developers and Project managers. Figure 47 shows this scenario, where the CFMS acts as a communication interface between private and public sectors.

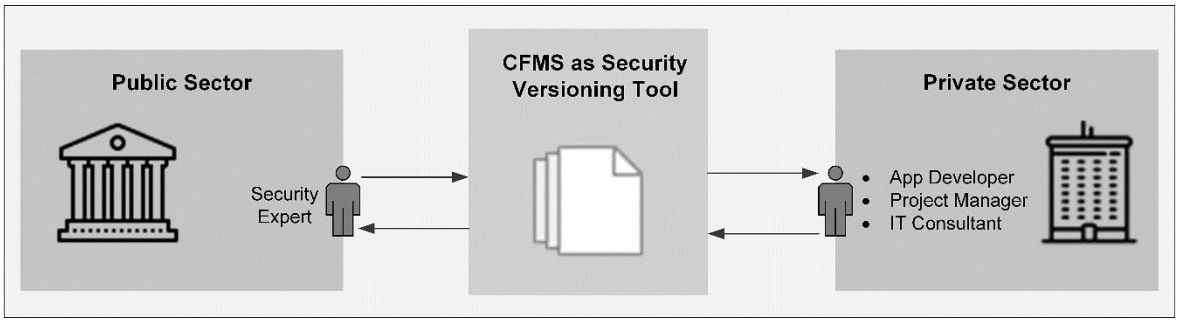

Figure 47. CFMS as communication interface between public and private sectors
Source: (Hasan & Amin Rezaei, 2018)

In this regard, the most import functionality of the CFMS is the administration of the versions of the guidance model. In the case of new security and privacy requirements, the security expert can include these in the next version of the guidance model.

For instance, the new EU GDPR sets strict rules for the legitimate usage of personal data, offers a stronger position to citizens to control their data (including, among other things "The right to be forgotten") and imposes high fines for data abuse, for which the data processor will be held responsible (van Zoonen, 2016). The new requirements – that are needed to comply with those new regulations – can be included in the guidance model, refining it in a new version. The new version of the guidance model will then be considered for all new Smart Cities applications. Furthermore, all the existing applications can be then evaluated

against the new version of the guidance model, to show whether some applications need to be enhanced with further measures to fulfill the new security and privacy requirements. Hence, once the new version of the guidance model is available, the decision model will notify the related users from the private sector about the newly added requirements as well as the updated ones. These requirements have to be fulfilled to comply with the new version of the guidance model, which has been already updated by the security experts from public sector to reflect the new regulations and laws.

Last but not least, as the security and privacy requirements can be different from one application to another, the guidance model can be instantiated in a number of projects, each of them representing a security concept for an application or for a class of applications that have the same security and privacy requirements.

Another use case scenario is that the public sectors can involve more roles beside security expert role, e.g. project manager role. CFMS will be used then to transfer the security and privacy knowledge from security expert to the project manager, and the second will communicate the security and privacy requirement to other roles from private sector.

To sum up, using CFMS can provide advantages as follows:

- Eliminating the need of privacy and security experts on the private sector side; this in turn reduces the costs for the private sector
- Providing a means of documentation and administration of the changes in requirements over time, manifested here as a versioning tool
- Due to the nature of the framework, which is designed for communication between security experts and non-security experts, it can be also used to communicate the security and privacy requirements as well as the security measures, that have to be applied for a specific application, to the end user (the citizen), thus building trust with higher level of transparency
- Since the framework provides two levels of guidelines as mentioned, laws to requirements and requirements to technical measures, it makes a direct communication with managerial level and developer level in private sector feasible
- The flexibility of the framework to accommodate changes in the case of the enforcement of the new laws and regulations

6.4 Summary

In this chapter, the main CFMS implementation details have been presented. Initially, technologies and software products used for the implementation of the CFMS prototype were discussed, followed by a UML class diagram that described the CFMS meta model, the UML sequence diagrams that illustrated the main interactions between CFMS models and its roles, and the CFMS database model that showed the relations between its components. Then, the CFMS as web-based tool was demonstrated together with its guidance model and decision model.

The last section of this chapter was dedicated to the evaluation aspects of this work. Two evaluation possibilities were discussed. First, functional testing was presented together with the workshops conducted within three enterprises (BTC AG, EWE AG and Lufthansa Industry Solutions GmbH & Co. KG) to demonstrate the CFMS functionalities. Subsequently, the main outcomes of these workshops were listed and suggestions for further potential improvements for future work were introduced. Second, in the Smart Cities applications domain, how the communications of security and privacy requirements between private and public sectors can be facilitated and managed using CFMS were discussed.

The next chapter is the final chapter in this thesis, and sums up the main contributions of this work and tries to give an outlook of possible future directions.

7 Conclusion and Outlook

This chapter summarizes the ideas, concepts and approaches presented over this dissertation. In addition, it provides a summary of contributions and introduces directions for potential future work that can be derived from this research. Thus, Section 7.1 summarizes the conducted research with its main contributions, after that, Section 7.2 gives some highlights on how the CFMS can be extended, opening directions for potential future work.

7.1 Research Summary

In order to delineate the topic at the beginning of this work, the mobile technology and its integration within enterprises were introduced to highlight important advantages that enterprises can obtain when adopting these technologies to enable their employees to work using mobile devices. However, due to security fears, this adoption has been slowed down. On the one hand, mobile devices are exposed to a wide range of threats and due to their significant resource constraints, many security measures from traditional computing domains do not translate well to mobile devices. On the other hand, the existing standards, catalogues and guidelines mostly target IT security professionals and therefore they are too complex for business users or users who do not have specialized know-how in security. Therefore, enterprises need to know which security level can be applied on mobile devices, and then can decide which data can be transferred to mobile devices. Thus, the research problem together with the research questions were defined. Subsequently, background information together with the related concepts needed for the understanding of the topic were presented to define the research landscape.

To address the defined problem and to answer the research questions, this thesis has developed a conceptual framework (called CFMS) that supports the enterprises when they adopt MEAs. The concept of the CFMS together with its structure, its models and its main requirements have been also defined to show the core functions of this framework. The CFMS was developed as web-based tool and was evaluated within workshops conducted in enterprises, where its functionalities were demonstrated. In addition, it was discussed how the CFMS can be utilized to address issues relates to privacy concerns in Smart Cities.

The main contributions that can be harvested from using the CFMS were explained in details throughout this thesis. These contributions are summarized as follows:

- Providing a tool that supports the transferring of the mobile security knowledge from security experts to non-security experts. This will increase security awareness within the enterprise.
- Documenting information about mobile security in a structured way and mapping threats to the mobile security measures required will help enterprises to justify these measures to employees, which help to increase their security awareness and consequently their acceptance of potential consequences of these measures.
- The CFMS helps to create security concepts for the MEAs the enterprise wants to adopt. In the case of an existing MEA, the mobile security requirements and measures included can be used as checklist to evaluate that MEA. Moreover, in the case of development of a new MEA, the mobile security requirements and measures can be used as checklist for the project implementation managers and app developers. However, this checklist helps to define a high abstraction level of the security requirements and measures needed.
- The CFMS is an application-based approach, and enterprises may use it to determine which enterprise applications and resources can be accessed over mobile devices. This approach gets its importance from the fact that mobile security requirements differ from one MEA to another, based on the importance of the data the MEA can access and consequently on the required security level. Furthermore, the needed mobile security measures can also differ between MEAs, and thus have different consequences. User acceptance of these consequences is also considered and investigated within this work.
- In case of non-IT enterprises, the CFMS can be used as a communication interface between these enterprises and their IT service provider. Section 6.3.3 illustrated such utilization in the context of Smart Cities application to communicate privacy requirements between public and private sectors.

Finally, because of constantly changing conditions and requirements determined by the environment, IT security is not something static, and therefore, the administration of the guidance model and its content is crucial for the efficient usage of the CFMS. Consequently, security experts within enterprises should continuously check the guidance model and update its content. This action is supported within the CFMS by its versioning concept of the guidance model.

Further interesting potential extensions are briefly highlighted in the following section. These extensions could not be included within this research, but they motivate further scientific discussion of the topic.

7.2 Outlook and Future Work

After the CFMS had been implemented and discussed within enterprises, it became very clear that enterprises demand a central tool to manage information security, not only for MEAs but also for all other application types that are used by employees. Having a huge number of documents about information security in form of PDF, Word or Excel is very confusing and it is difficult to follow up the dependencies between these documents, especially when one of these documents is updated. The questions would be:

- How these updates affect the existing applications?
- How to communicate these updates with employees using the affected applications?

The CFMS can be extended to include policies related to each security measure, e.g. encryption policy, password policy, etc. In this regard, the framework can be also connected to technical IT systems like EMM, so that changes in the content of the framework will be reported to these systems in form of notifications. For instance, in case of password security policy change, the new policy should be synchronized with the EMM to enforce the new policy. Further, this thesis has shown how an enterprise can define mobile security requirements and security levels based on multi dimensions. These dimensions can be included in the CFMS so each dimension can be mapped to a set of security requirements, making these more granular and clearer for both enterprises and regulators. In this regard, it would be possible to define an interface between the CFMS and the reporting system of the enterprise. Taking the above-mentioned issues into consideration, the CFMS builds the foundation to develop a holistic tool to manage information security within an enterprise.

The CFMS is platform-independent, i.e. the security requirements and measures included in this framework are not dedicated for a specific platform such as Android or iOS. Therefore, a potential extension here would be to include further information about the mobile platforms that can apply security measures and fulfill the related security requirements, enabling projects for specific mobile platforms to be administrated within this framework.

In addition, the CFMS can be extended by including technical security catalogues and guidelines (e.g. guides from ENISA or OWASP) that help app developers to develop secure MEAs. However, such extension should take into consideration the clear separation of the roles, so that such guidelines should be available for app developers only. Moreover, the projects that can be created via decision model should be available only for specific roles.

Finally, the framework can be adapted to support IT companies in developing secure applications e.g. in context of business to customer domain. In the last few years, agile software developments have become more common and most IT companies have started to apply agile processes within their software development. One of the most common agile frameworks is Scrum. There are different roles within each scrum team (like product owner, scrum master). OWASP has defined a role called security champion[85] (as defined by OWASP, "*Security Champions are active members of a team that may help to make decisions about when to engage the Security Team*").

Embedding a security champion in every scrum team is important to guarantee that there is some kind of security knowledge as part of every design decision when a team is discussing and building a software. This means that the centralized security experts in the company do not have to be everywhere and anytime. Developers would be responsible for building secure software, but they need the security knowledge. Sharing such knowledge within the team is a task of the security champion. However, according to the outcomes from security champions session from OWASP Summit 2017[86], the role of security champion can be filled by developers, testers, operation staff or anyone interested within the team. On the other hand, according to the same survey, security champions are expected to share security knowledge or conduct mini-trainings. The question here is how to enhance the security knowledge of the security champions. A potential solution would be by extending the CFMS by integrating the OWASP open source security knowledge framework to provide security check lists for security champions, who communicate these further with developers.

[85] https://www.owasp.org/index.php/Security_Champions
[86] https://github.com/OWASP/owasp-summit-2017/blob/master/Outcomes/Security-Champions/Security-Champions.md

References

Abura'ed, N., Otrok, H., Mizouni, R., & Bentahar, J. (2014). Mobile phishing attack for Android platform. In *2014 10th International Conference on Innovations in Information Technology (INNOVATIONS)* (pp. 18–23). https://doi.org/10.1109/INNOVATIONS.2014.6987555

Adeel, M., & Tokarchuk, L. N. (2011). Analysis of Mobile P2P Malware Detection Framework through Cabir & Commwarrior Families. In *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust (PASSAT) / 2011 IEEE Third Int'l Conference on Social Computing (SocialCom)* (pp. 1335–1343). https://doi.org/10.1109/PASSAT/SocialCom.2011.243

Akella, J., Brown, B., Gilbert, G., & Wong, L. (2012). Mobility disruption: A CIO perspective. *Insights & Publications, McKinsey & Company*. Retrieved from http://www.mckinsey.com/insights/business_technology/mobility_disruption_a_cio_perspective

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, *6*, 1. https://doi.org/10.1186/s13174-015-0041-5

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. *MIS Q*, *25*, 107. https://doi.org/10.2307/3250961

Albashrawi, M., & Motiwalla, L. (Eds.) 2016. *Adoption of Mobile ERP in Traditional-ERP Organizations: The Effect of Computer Self-Efficacy*: AIS eLibrary.

AlDairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109*, 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391

Alshalan, A., Pisharody, S., & Huang, D. (2016). A Survey of Mobile VPN Technologies. *IEEE Communications Surveys & Tutorials*, *18*, 1177–1196. https://doi.org/10.1109/COMST.2015.2496624

Amit, Y. (2014). The Invisible Profile: Patched in iOS 7.1. Retrieved from https://www.symantec.com/connect/blogs/invisible-profile-patched-ios-71

Amit, Y., & Sharabani, A. (2014). Mobile Security Attacks: A Glimpse from the Trenches. Retrieved from https://www.owasp.org/images/a/ab/AppSecIL_2014_Mobile_Security_Attacks_-_A_Glimpse_From_the_Trenches_-_Yair_Amit_-_Adi_Sharabani_-_Skycure.pdf

Andreasson, K. J. (2012). *Cybersecurity: Public sector threats and responses*. *Public administration and public policy: Vol. 165*. Boca Raton, FL: CRC Press.

AO Kaspersky Lab. (2015). Kaspersky Threats — Svpeng. Retrieved December 20, 2018, from https://threats.kaspersky.com/en/threat/Trojan-Banker.AndroidOS.Svpeng/

Apple Inc. (2017). iOS Security [White Paper]: iOS 10. Retrieved May 20, 2017, from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Arpaci, I., Yardimci Cetin, Y., & Turetken, O. (2015). Impact of Perceived Security on Organizational Adoption of Smartphones. *Cyberpsychology, Behavior and Social Networking*, *18*, 602–608. https://doi.org/10.1089/cyber.2015.0243

Asokan, N., Davi, L., Dmitrienko, A., Heuser, S., Kostiainen, K., Reshetova, E., & Sadeghi, A.-R. (2013). Mobile Platform Security. *Synthesis Lectures on Information Security, Privacy, and Trust*, *4*, 1–108. https://doi.org/10.2200/S00555ED1V01Y201312SPT009

Au, M. H., & Choo, K.-K.R. (2017). Mobile Security and Privacy. In *Mobile Security and Privacy* (pp. 1–4). Elsevier. https://doi.org/10.1016/B978-0-12-804629-6.00001-8

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. In *WOOT'10, Proceedings of the 4th USENIX Conference on Offensive Technologies* (pp. 1–7). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1925004.1925009

Bach, O. (2015). Mobile Malware Threats in 2015: Fraudsters Are Still Two Steps Ahead. Retrieved from https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead/

Barr, K., Bungale, P., Deasy, S., Gyuris, V., Hung, P., Newell, C., Zoppis, B. (2010). The VMware mobile virtualization platform: is that a hypervisor in your pocket? *ACM SIGOPS Operating Systems Review*, *44*, 124. https://doi.org/10.1145/1899928.1899945

Basole, R. (2007). Strategic Planning for Enterprise Mobility: A Readiness-Centric Approach. *AMCIS 2007 Proceedings. Paper 491*.

Basole, R., & Rouse, W. B. (2006). Mobile Enterprise Readiness and Transformation. *Idea Group Inc. IGI*.

Belleau, F., Nolin, M.-A., Tourigny, N., Rigault, P., & Morissette, J. (2008). Bio2rdf: Towards a mashup to build bioinformatics knowledge systems. *Journal of Biomedical Informatics*, *41*, 706–716. https://doi.org/10.1016/j.jbi.2008.03.004

Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., & Stamatiou, Y. (2014). User Acceptance of Privacy-ABCs: An Exploratory Study. In T. Tryfonas & I. Askoxylakis (Eds.), *Lecture Notes in Computer Science. Human Aspects of Information Security, Privacy, and Trust*

(Vol. 8533, pp. 375–386). Springer International Publishing. https://doi.org/10.1007/978-3-319-07620-1_33

Bhasker, D. (2013). 4G LTE security for mobile network operators. *Cyber Secur. Inf. Sys. Inf. Anal. Cent.(CSIAC), 1*, 20–29.

Bhatia, K., & Mittal, S. (2009). *Manpower development for technological change* (1st ed.). New Delhi: Excel Books.

Biryukov, A., Cannière, C. de, Winkler, W. E., Aggarwal, C. C., Kuhn, M., Bouganim, L., Smith, S. W. (2011). Differential Privacy. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of Cryptography and Security* (pp. 338–340). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-5906-5_752

Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1392–1393). IEEE. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Botha, A. C., Kourie, D., & Snyman, R. (2008). *Coping with continuous change in the business environment: Knowledge management and knowledge management technology*. Oxford: Chandos.

Braun, T., Fung, B. C.M., Iqbal, F., & Shah, B. (2018). Security and Privacy Challenges in Smart Cities. *Sustainable Cities and Society*. Advance online publication. https://doi.org/10.1016/j.scs.2018.02.039

Brockmann, T., Stieglitz, S., Kmieciak, J., & Diederich, S. (2012). User Acceptance of Mobile Business Intelligence Services. In *2012 15th International Conference on Network-Based Information Systems* (pp. 861–866). IEEE. https://doi.org/10.1109/NBiS.2012.129

Brodin, M. (2016). *Mobile Device Strategy: A management framework for securing company information assets on mobile devices*. Dissertation Series 15: University of Skövde.

BSI. (2008). BSI-Standard 100-1: Information Security Management Systems (ISMS). Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf

BSI. (2013). IT-Grundschutz-Catalogues. 13th version. Retrieved from https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

BSI. (2017). Mindeststandard des BSI für Mobile Device Management. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf

Budiu, R. (2013). Mobile: Native Apps, Web Apps, and Hybrid Apps. Retrieved from https://www.nngroup.com/articles/mobile-native-apps/

Buennemeyer, T. K., Gora, M., Marchany, R. C., & Tront, J. G. (2007). Battery Exhaustion Attack Detection with Small Handheld Mobile Computers. In *2007 IEEE International Conference on Portable Information Devices* (pp. 1–5). https://doi.org/10.1109/PORTABLE.2007.35

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*.

Burnett, M., & Kleiman, D. (2006). *Perfect passwords: Selection, protection, authentication*. Rockland, Mass.: Syngress.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*, 43–62. https://doi.org/10.1111/1468-2346.12504

Chatterjee, S., Paul, K., Roy, R., & Nath, A. (2016). A Comprehensive Study on Security issues in Android Mobile Phone - Scope and Challenges. *International Journal of Innovative Research in Advanced Engineering (IJIRAE), 3*.

Chen, R., Fung, B. C.M., Desai, B. C., & Sossou, N. M. (2012). Differentially private transit data publication: A Case Study on the Montreal Transportation System. In Q. Yang, D. Agarwal, & J. Pei (Eds.), *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '12* (p. 213). New York, New York, USA: ACM Press. https://doi.org/10.1145/2339530.2339564

Ciaramitaro, B. L. (2012). Introduction to Mobile Technologies. In B. L. Ciaramitaro (Ed.), *Mobile Technology Consumption* (pp. 1–15). IGI Global. https://doi.org/10.4018/978-1-61350-150-4.ch001

Cichonski, J., Franklin, J. M., & Bartock, M. (2016). Guide to LTE Security. (Draft) NIST Special Publication (SP) 800-187. Retrieved from http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf

CISCO. (2016). Cisco 2016 Annual Security Report. Retrieved March 10, 2016, from http://www.cisco.com/c/en/us/products/security/annual_security_report.html

Common Criteria. (2012). Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components. Retrieved from https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*, 104–126. https://doi.org/10.1007/BF03177550

Creswell, J. W. (1994). *Research design: Qualitative and Quantitative Approaches*: Sage Publications.

Croft, N. J., & Olivier, M. S. (2007). A Silent SMS Denial of Service (DoS) Attack. In *Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007) Proceedings.* Retrieved from http://mo.co.za/open/silentdos.pdf

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*, 297–334. https://doi.org/10.1007/BF02310555

Dalkir, K. (2005). *Knowledge management in theory and practice*. Amsterdam, London: Elsevier/Butterworth Heinemann.

Damopoulos, D., Kambourakis, G., Anagnostopoulos, M., Gritzalis, S., & Park, J. H. (2013). User privacy and modern mobile services: Are they on the same path? *Personal and Ubiquitous Computing*, *17*, 1437–1448. https://doi.org/10.1007/s00779-012-0579-1

Daojing He, Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. *Wireless Communications, IEEE*, *22*, 138–144. https://doi.org/10.1109/MWC.2015.7054729

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know / Thomas H. Davenport, Laurence Prusak*. Boston, Mass.: Harvard Business School Press.

David, S., Singh Dikhit, R., Shrivastava, J., & Sawlani, T. (2017). Enterprise Mobility Management: An Overview. *International Journal of Engineering Sciences & Research Technology*, 111–116.

Davis, F. D. (1986). A technology acceptance model for empirically testing new end-user information systems : theory and results. Diss. Retrieved from http://hdl.handle.net/1721.1/15192

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*, 319. https://doi.org/10.2307/249008

Denning, P. J. (1997). A new social contract for research. *Communications of the ACM*, *40*, 132–134. https://doi.org/10.1145/253671.253755

Denzin, N. K., & Lincoln, Y. S. (1994). *Handbook of qualitative research* (4th ed.). London, UK: Sage Publications.

Detken, K.-O., Diederich, G., & Heuser, S. (2011). Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC. *D.a.CH Security 2011: Bestandsaufnahme, Konzepte, Anwendungen Und Perspektiven; Syssec Verlag; Oldenburg*.

Disterer, G., & Kleiner, C. (2014). *Mobile Endgeraete Im Unternehmen: Technische Ansaetze, Compliance-anforderungen, Management*: Vieweg + Teubner Verlag.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches. *Information Resources Management Journal, 18,* 21–39. https://doi.org/10.4018/irmj.2005100102

Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile application security*. New York: McGraw-Hill.

Dwork, C. (2008). Differential Privacy: A Survey of Results. In M. Agrawal, D. Du, Z. Duan, & A. Li (Eds.), *Lecture Notes in Computer Science. Theory and Applications of Models of Computation* (Vol. 4978, pp. 1–19). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-79228-4_1

Eckert, C. (2009). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (6th ed.). München: Oldenbourg.

Eckert, C. (2014). *IT-Sicherheit: Konzepte, Verfahren, Protokolle* (9. Aufl.). *De Gruyter Studium*. Oldenbourg: De Gruyter.

Eilts, S. (2016). Technische Konzeption und prototypische Umsetzung eines Sicherheitsframeworks für mobile Unternehmensapplikationen (Master Thesis). Carl von Ossietzky University of Oldenburg, Oldenburg, Germany.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research, 5,* 491–497. https://doi.org/10.1016/j.jare.2014.02.006

ENISA. (2016). Smartphone Secure Development Guidelines. Retrieved from https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

ENISA. (2017). Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

Euler, M., Hacke, M., Hartherz, C., Steiner, S., & Verclas, S. (2012). Herausforderungen bei der Mobilisierung von Business Applikationen und erste Lösungsansätze. In S. Verclas & C. Linnhoff-Popien (Eds.), *Xpert.press. Smart Mobile Apps: Mit Business-Apps ins Zeitalter mobiler Geschäftsprozesse* (pp. 107–121). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22259-7_8

Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2012). Continuous mobile authentication using touchscreen gestures. In *2012 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 451–456). https://doi.org/10.1109/THS.2012.6459891

Fitzgerald, W. M., Neville, U., & Foley, S. N. (2013). MASON: Mobile autonomic security for network access controls. *Journal of Information Security and Applications*, *18*, 14–29. https://doi.org/10.1016/j.jisa.2013.08.001

Franklin, J. M., Brown, C., Dog, S., McNab, N., Voss-Northrop, S., Peck, M., & Stidham, B. (2016). Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue. Draft NISTIR 8144. Retrieved from http://csrc.nist.gov/publications/drafts/nistir-8144/nistir8144_draft.pdf

Ganta, S. R., Kasiviswanathan, S. P., & Smith, A. (2008). Composition attacks and auxiliary information in data privacy. In Y. Li, B. Liu, & S. Sarawagi (Eds.), *Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD 08* (p. 265). New York, New York, USA: ACM Press. https://doi.org/10.1145/1401890.1401926

Gartner. (2014). Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration. Retrieved from http://www.gartner.com/newsroom/id/2753017

Gartner. (2015). Gartner Forecasts 59 Percent Mobile Data Growth Worldwide in 2015. Retrieved from http://www.gartner.com/newsroom/id/3098617

Gartner. (2016). Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015. Retrieved from http://www.gartner.com/newsroom/id/3215217

Gasik, S. (2011). A Model of Project Knowledge Management. *Project Management Journal*, *42*, 23–44. https://doi.org/10.1002/pmj.20239

Godber, A., & Dasgupta, P. (2002). Secure wireless gateway. In D. Maughan & N. H. Vaidya (Eds.), *the ACM workshop* (pp. 41–46). https://doi.org/10.1145/570681.570686

Gramatica, M. de, Labunets, K., Massacci, F., Paci, F., & Tedeschi, A. (2015). The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals. In S. A. Fricker & K. Schneider (Eds.), *Lecture Notes in Computer Science. Requirements Engineering: Foundation for Software Quality* (Vol. 9013, pp. 98–114). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-16101-3_7

Gröger, C., Silcher, S., Westkämper, E., & Mitschang, B. (2013). Leveraging Apps in Manufacturing. A Framework for App Technology in the Enterprise. *Procedia CIRP*, *7*, 664–669. https://doi.org/10.1016/j.procir.2013.06.050

Grünendahl, R. T., Steinbacher, A. F., & Will, P. H.L. (2012). *Das IT-Gesetz: Compliance in der IT-Sicherheit*. Wiesbaden: Vieweg+Teubner Verlag.

Hardy, J. (2015). Mobilephobia: Is It Paralyzing Your Deployment of a Mobile Security Strategy? Retrieved from https://securityintelligence.com/mobilephobia/

Hasan, B., & Amin Rezaei, A. (2018). Enhancing Privacy in Smart Cities by Facilitating Communications between Public and Private Sectors. In J. Marx Gómez, A. Solsbach, T. Klenke, & V. Wohlgemuth (Eds.), *10. BUIS-Tage - Smart Cities / Regions.* Springer. Vieweg (In Press).

Hasan, B., Dmitriyev, V., Marx Gómez, J., & Kurzhöfer, J. (2014). A Framework along with Guidelines for Designing Secure Mobile Enterprise Applications. In *Security Technology (ICCST), 2014 International Carnahan Conference on* (pp. 1–6). IEEE. https://doi.org/10.1109/CCST.2014.6987030

Hasan, B., & Marx Gómez, J. (2017). Security Framework for Adopting Mobile Applications in Small and Medium Enterprises. In M. S. Obaidat (Ed.), *E-Business and Telecommunications: 13th International Joint Conference, ICETE 2016, Lisbon, Portugal, July 26-28, 2016, Revised Selected Papers* (pp. 75–98). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-67876-4_4

Hasan, B., Marx Gómez, J., & Kurzhöfer, J. (2013). Towards a Framework for Designing Secure Mobile Enterprise Applications. In *MOBILITY 2013, The Third International Conference on Mobile Services, Resources, and Users* (pp. 90–93).

Hasan, B., Rajski, E., Marx Gómez, J., & Kurzhöfer, J. (2016). A Proposed Model for User Acceptance of Mobile Security Measures – Business Context. In K. J. Kim, N. Wattanapongsakorn, & N. Joukov (Eds.), *Lecture Notes in Electrical Engineering. Mobile and Wireless Technologies 2016* (Vol. 391, pp. 97–108). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-10-1409-3_11

Hasan, B., Schäfer, P., Marx Gómez, J., & Kurzhöfer, J. (2016). Risk Catalogue for Mobile Business Applications. In *International Conference on e-Business* (pp. 43–53). https://doi.org/10.5220/0005968900430053

Hevner, A. R., & Chatterjee, S. (2010). *Design Research in Information Systems* (Vol. 22). Boston, MA: Springer US.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*, 75–105.

Hoos, E., Gröger, C., Kramer, S., & Mitschang, B. (2015). ValueApping: An Analysis Method to Identify Value-Adding Mobile Enterprise Apps in Business Processes. In J. Cordeiro, S. Hammoudi, L. Maciaszek, O. Camp, & J. Filipe (Eds.), *Lecture Notes in Business Information Processing. Enterprise Information Systems* (Vol. 227, pp. 222–243). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-22348-3_13

Hornbæk, K., & Hertzum, M. (2017). Technology Acceptance and User Experience: A Review of the Experiential Component in HCI. *ACM Transactions on Computer-Human Interaction*, *24*, 1–30. https://doi.org/10.1145/3127358

Howard, M., & Lipner, S. (2006). *The security development lifecycle: SDL, a process for developing demonstrably more secure software*. *Secure software development series*. Redmond: Microsoft Press.

Hurley, H., Lai, E., & Piquet, L.J. (2011). *Enterprise Enterprise Mobility Guide 2011*. Dublin CA: Sybase.

Huy, N. P., & van Thanh, D. (2012). Selecting the right mobile app paradigms. In *2012 Fifth IEEE International Conference on Service-Oriented Computing and Applications (SOCA)* (pp. 1–6). IEEE. https://doi.org/10.1109/SOCA.2012.6449450

IDC. (2014). IDC Reveals Worldwide Mobile Enterprise Applications and Solutions Predictions for 2015. Retrieved from http://www.businesswire.com/news/home/20141218006258/en/IDC-Reveals-Worldwide-Mobile-Enterprise-Applications-Solutions

Imgraben, J., Engelbrecht, A., & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy?: A survey of smart mobile device users. *Behaviour & Information Technology*, *33*, 1347–1360. https://doi.org/10.1080/0144929X.2014.934286

Internet Society. (2014). Global Internet Report 2014. Retrieved January 19, 2015, from https://www.internetsociety.org/wp-content/uploads/2017/08/Global_Internet_Report_2014_0.pdf

ISO 31000:2009. (2009). Risk Management—Principles and Guidelines.

ISO/IEC 17799. (2005). Information technology -- Security techniques -- Code of practice for information security management.

ISO/IEC 27001. (2005). *Information technology — Security techniques — Information security management systems — Requirements*: ISO/ICE.

Jackson, G. B. (1980). Methods for Integrative Reviews. *Review of Educational Research*, *50*, 438–460. https://doi.org/10.3102/00346543050003438

Jain, A. K., & Shanbhag, D. (2012). Addressing Security and Privacy Risks in Mobile Applications. *IT Professional*, *14*, 28–33. https://doi.org/10.1109/MITP.2012.72

Jain, S. (2014). Security Threats in Manets: A Review. *International Journal on Information Theory*, *3*, 37–50. https://doi.org/10.5121/ijit.2014.3204

Jankowska, A. M., & Kurbel, K. K. (2005). Service-Oriented Architecture Supporting Mobile Access to an ERP System. In O. K. Ferstl, E. J. Sinz, S. Eckert, & T. Isselhorst (Eds.), *Wirtschaftsinformatik 2005* (pp. 371–390). Physica-Verlag HD.

Jaramillo, D., Furht, B., & Agarwal, A. (2014). *Virtualization Techniques for Mobile Systems*. *Multimedia Systems and Applications*. Cham: Springer International Publishing.

Jermyn, J., Salles-Loustau, G., & Zonouz, S. (2014). An Analysis of DoS Attack Strategies Against the LTE RAN. *Journal of Cyber Security and Mobility*, *3*, 159–180. https://doi.org/10.13052/jcsm2245-1439.323

Jobe, W. (2013). Native Apps Vs. Mobile Web Apps. *International Journal of Interactive Mobile Technologies (IJIM)*, *7*, 27. https://doi.org/10.3991/ijim.v7i4.3226

Johnson, G., Scholes, K., & Whittington, R. (2011). *Strategisches Management - Eine Einführung: Analyse, Entscheidung und Umsetzung* (1., neue Ausg). *Pearson Studium - Economic BWL*. München: Pearson Studium ein Imprint der Pearson Education.

Johnson, M. (2011). *Mobile Device Management: What you Need to Know For IT Operations Management*: Lightning Source.

Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2014). Introducing touchstroke: Keystroke-based authentication system for smartphones. *Security and Communication Networks*, n/a-n/a. https://doi.org/10.1002/sec.1061

Kaneshige, T. (2015). Enterprise mobility slowed by security concerns. Retrieved from https://www.cio.com/article/2934333/mobile/enterprise-mobility-slowed-by-security-concerns.html

Kaspersky. (2013a). Kaspersky Security Bulletin 2013. Retrieved from http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

Kaspersky. (2013b). One in Every Six users suffer loss or theft of mobile devices. Retrieved March 10, 2016, from https://www.kaspersky.com/about/press-releases/2013_one-in-every-six-users-suffer-loss-or-theft-of-mobile-devices

Kennedy, M., & Sulaiman, R. (2015). Following the Wi-Fi breadcrumbs: Network based mobile application privacy threats. In *2015 International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 265–270). https://doi.org/10.1109/ICEEI.2015.7352508

Kersten, H., & Klett, G. (2012). *Mobile Device Management* (1. Aufl.). Heidelberg, München, Landsberg, Frechen, Hamburg: Mitp.

Kersten, H., & Wolfenstetter, K.-D. (Eds.). (2016). *Edition <kes>. Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden*. Wiesbaden, [Germany]: Springer Vieweg.

Kifer, D. (2009). Attacks on privacy and deFinetti's theorem. In U. Çetintemel, S. Zdonik, & D. Kossmann (Eds.), *Proceedings of the 35th SIGMOD international conference on Management of data - SIGMOD '09* (p. 127). New York, USA: ACM Press. https://doi.org/10.1145/1559845.1559861

Kizza, J. M. (2015). Mobile Systems and Corresponding Intractable Security Issues. In J. M. Kizza (Ed.), *Computer Communications and Networks. Guide to Computer Network Security* (pp. 491–507). London: Springer London. https://doi.org/10.1007/978-1-4471-6654-2_23

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly, 23*, 67. https://doi.org/10.2307/249410

Kohne, A., Ringleb, S., & Yücel, C. (2015). *Bring your own Device: Einsatz von privaten Endgeräten im beruflichen Umfeld - Chancen, Risiken und Möglichkeiten* (1. Aufl. 2015). Wiesbaden: Springer Fachmedien Wiesbaden; Imprint; Springer Vieweg.

Kolbe, L. M., & Ruch, T. J. (2014). Mobile Security: Herausforderungen neuer Geräte und neuer Nutzeransprüche. *HMD Praxis Der Wirtschaftsinformatik, 51*, 9–23. https://doi.org/10.1365/s40702-014-0005-4

Krcmar, H. (2015). *Informationsmanagement*. Berlin, Heidelberg: Springer Berlin Heidelberg; Imprint; Springer Gabler.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials, 15*, 446–471. https://doi.org/10.1109/SURV.2012.013012.00028

Lacerda, A., Queiroz, R. de, & Barbosa, M. (2015). A systematic mapping on security threats in mobile devices. In *2015 Internet Technologies and Applications (ITA)* (pp. 286–291). https://doi.org/10.1109/ITechA.2015.7317411

Landman, M. (2010). Managing Smart Phone Security Risks. In *InfoSecCD '10, Information Security Curriculum Development Conference* (pp. 145–155). ACM. https://doi.org/10.1145/1940941.1940971

Lederm, T., & Clarke, N. L. (2011). Risk Assessment for Mobile Devices. In S. Furnell, C. Lambrinoudakis, & G. Pernul (Eds.), *Lecture Notes in Computer Science. Trust, Privacy and Security in Digital Business* (Vol. 6863, pp. 210–221). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22890-2_18

Lee, S. (2016). User Behavior of Mobile Enterprise Applications. *KSII Transactions on Internet and Information Systems*, *10*. https://doi.org/10.3837/tiis.2016.08.030

Levinson, M. (2012). 6 Ways to Defend Against Drive-by Downloads. Retrieved from http://www.cio.com/article/2448967/security0/6-ways-to-defend-against-drive-by-downloads.html

Liotta, A., Tyrode-Goilo, D. H., & Oredope, A. (2008). Open Source Mobile VPNs over Converged All-IP Networks. *Journal of Network and Systems Management*, *16*, 163–181. https://doi.org/10.1007/s10922-007-9075-8

Liyanage, C., Elhag, T., Ballal, T., & Li, Q. (2009). Knowledge communication and translation – a knowledge transfer model. *Journal of Knowledge Management*, *13*, 118–131. https://doi.org/10.1108/13673270910962914

Lookout. (2011). Lookout Mobile Threat Report. Retrieved from https://www.lookout.com/img/images/lookout-mobile-threat-report-2011.pdf

Lookout. (2014). Phone Theft in America: What really happens when your phone gets grabbed. Retrieved May 17, 2016, from https://blog.lookout.com/blog/2014/05/07/phone-theft-in-america/

Lookout. (2015). Enterprise Mobile Threat Report: The State of iOS and Android Security Threats to Enterprise Mobility [Whitepaper]. Retrieved from https://info.lookout.com/rs/051-ESQ-475/images/Enterprise_MTR.pdf

Luenendonk. (2014). Mobile Enterprise Review: Mehr Strategie wagen.

Maan, J. (2012). Enterprise Mobility – A Future Transformation Strategy for Organizations. In D. C. Wyld, J. Zizka, & D. Nagamalai (Eds.), *Advances in Intelligent Systems and Computing. Advances in Computer Science, Engineering & Applications* (Vol. 167, pp. 559–567). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-30111-7_53

Major, E., & Cordey-Hayes, M. (2000). Knowledge translation: a new perspective on knowledge transfer and foresight. *Foresight*, *2*, 411–423. https://doi.org/10.1108/14636680010802762

Makki, S. K., Reiher, P., Makki, K., Pissinou, N., & Makki, S. (2007). *Mobile and Wireless Network Security and Privacy*. Boston, MA: Springer US.

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. In S. Jajodia, P. Shakarian, V.S. Subrahmanian, V. Swarup, & C. Wang (Eds.), *Advances in Information Security. Cyber Warfare* (Vol. 56, pp. 173–206). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-14039-1_9

Martin, T., Hsiao, M., Ha, D., & Krishnaswami, J. (2004). Denial-of-Service Attacks on Battery-powered Mobile Computers. In *PERCOM '04, Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04)* (pp. 309–318). Washington, DC, USA: IEEE Computer Society. Retrieved from http://dl.acm.org/citation.cfm?id=977406.978701

Martinez-Balleste, A., Perez-martinez, P., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*, 136–141. https://doi.org/10.1109/MCOM.2013.6525606

Mayron, L. M. (2015). Biometric Authentication on Mobile Devices. *IEEE Security & Privacy*, *13*, 70–73. https://doi.org/10.1109/MSP.2015.67

McAfee Labs. (2014). McAfee Labs Threats Report. Retrieved March 10, 2016, from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf

McLellan, C. (2014). Enterprise mobility in 2014: App-ocalypse Now? Retrieved March 10, 2016, from https://www.zdnet.com/article/enterprise-mobility-in-2014-app-ocalypse-now/

Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. In M. Jakobsson & A. Perrig (Eds.), *the 2004 ACM workshop* (p. 90). https://doi.org/10.1145/1023646.1023662

Michaelis, P. (2012). Enterprise Mobility – A Balancing Act between Security and Usability. In H. Reimer, N. Pohlmann, & W. Schneider (Eds.), *ISSE 2012 Securing Electronic Business Processes* (pp. 75–79). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-00333-3_8

Mintzberg, H. (1978). Patterns in Strategy Formation. *Management Science*, *24*, 934–948. https://doi.org/10.1287/mnsc.24.9.934

Moonsamy, V., & Batten, L. (2014). Mitigating man-in-the-middle attacks on smartphones - a discussion of SSL Pinning and DNSSec. In *The 12th Australian Information Security Management Conference* (pp. 5–13). Perth, WA: Edith Cowan University. Retrieved from http://hdl.handle.net/10536/DRO/DU:30071675

Morrissey, S. (2010). *iOS forensic analysis for iPhone, iPad and iPod touch*. Berkeley, Calif.?: Apress.

Mowafi, Y., Abou-Tair, D., Al-Aqarbeh, T., Abilov, M., Dmitriyev, V., & Marx Gómez, J. (2014). A Context-aware Adaptive Security Framework for Mobile Applications. In W. Mansoor, Z. Maamar, & F. Rabhi (Eds.), Proceedings of the 3rd International Conference on Context-Aware Systems and Applications. ICST. https://doi.org/10.4108/icst.iccasa.2014.257495

Mulvehill, T. (2016). The Risk From Mobile Malware Is Real — and Growing. Retrieved from https://securityintelligence.com/the-risk-from-mobile-malware-is-real-and-growing/

Murauer, R. (2013). *Mobile Medien und die Kompetenzen oberösterreichischer Lehrkräfte: Eine empirische Analyse*. [S.l.]: Disserta Verlag.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat Modeling as a Basis for Security Requirements. In *Symposium on Requirements Engineering for Information Security (SREIS)*. Retrieved from http://d-scholarship.pitt.edu/16516/

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47–66. https://doi.org/10.1016/j.cose.2012.11.004

Newman, A. (2014). Multi-Factor Authentication on Mobile Devices. Retrieved June 05, 2017, from https://www.kaseya.com/2014/09/29/multi-factor-authentication-on-mobile-devices/

Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A Novel Approach for Rogue Access Point Detection on the Client-Side. In *2012 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA)* (pp. 684–687). https://doi.org/10.1109/WAINA.2012.108

NIST. (2004). Standards for Security Categorization of Federal Information and Information Systems. Retrieved from http://csrc.nist.gov/

NIST. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Nonaka, I., & Konno, N. (1998). The Concept of "Ba": Building a Foundation for Knowledge Creation. *California Management Review*, *40*, 40–54. https://doi.org/10.2307/41165942

Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. *Long Range Planning*, *33*, 5–34. https://doi.org/10.1016/S0024-6301(99)00115-6

Oğul, M., & Baktır, S. (2013). Practical Attacks on Mobile Cellular Networks and Possible Countermeasures. *Future Internet*, *5*, 474. https://doi.org/10.3390/fi5040474

Olaleye, S. B., Ranjan, I., & Ojha, S. (2017). SoloEncrypt: A Smartphone Storage Enhancement Security Model for Securing users Sensitive Data. *Indian Journal of Science and Technology*, *10*, 1–8. https://doi.org/10.17485/ijst/2017/v10i8/104511

Oluwatimi, O., Midi, D., & Bertino, E. (2017). Overview of Mobile Containerization Approaches and Open Research Directions. *IEEE Security & Privacy*, *15*, 22–31. https://doi.org/10.1109/MSP.2017.12

Omar, K., & Marx Gómez, J. (2017). An investigation of the proliferation of mobile ERP apps and their usability. In *2017 8th International Conference on Information and Communication Systems (ICICS)* (pp. 352–357). IEEE. https://doi.org/10.1109/IACS.2017.7921997

Omar, K., Rapp, B., & Marx Gómez, J. (2016). Heuristic evaluation checklist for mobile ERP user interfaces. In *2016 7th International Conference on Information and Communication Systems (ICICS)* (pp. 180–185). IEEE. https://doi.org/10.1109/IACS.2016.7476107

Osman, N. B. (2013). Extending the Technology Acceptance Model for Mobile Government Systems. *Development*, *5*, 16.

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., . . . Sinz, E. J. (2010). Memorandum on Design-oriented Information Systems Research. *European Journal of Information Systems*, *20*, 7–10. https://doi.org/10.1057/ejis.2010.55

Padgette, J., Chen, L., & Scarfone, K. (2012). Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-121r1

Park, J. H., Yi, K. J., & Jeong, Y.-S. (2014). An Enhanced Smartphone Security Model Based on Information Security Management System (ISMS). *Electronic Commerce Research*, *14*, 321–348. https://doi.org/10.1007/s10660-014-9146-3

Pattnaik, P. K., & Mall, R. (2015). *Fundamentals of Mobile Computing*: PHI Learning Pvt. Ltd.

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. In *Lecture Notes in Computer Science* (pp. 398–410).

Peltier, T. R. (2002). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton: Auerbach Publications.

Peters, T., Işık, Ö., Tona, O., & Popovič, A. (2016). How system quality influences mobile BI use: The mediating role of engagement. *International Journal of Information Management*, *36*, 773–783. https://doi.org/10.1016/j.ijinfomgt.2016.05.003

Pierer, M. (2016). *Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises*. Wiesbaden: Springer Fachmedien Wiesbaden, Imprint: Springer Vieweg.

Ponzi, L. J., & Koenig, M. (2002). Knowledge management: another management fad? *Information Research*, *8*, 145.

Pu, S., Chen, Z., Huang, C., Liu, Y., & Zen, B. (2014). Threat analysis of smart mobile device. In *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)* (pp. 1–3). https://doi.org/10.1109/URSIGASS.2014.6929439

Ramu, S. (2012). Mobile Malware Evolution, Detection and Defense. *EECE 571B, Term Survey Paper*.

Ranjan, J., & Bhatnagar, V. (2009). A Holistic Framework for mCRM – Data Mining Perspective. *Information Management & Computer Security*, *17*, 151–165.

Rao, U. H., & Nayak, U. (2014). Malicious Software and Anti-Virus Software. In U. H. Rao & U. Nayak (Eds.), *The InfoSec Handbook* (pp. 141–161). Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4302-6383-8_7

Rashid, M.A., Hossain, L., & Patrick, J.D. (2002). The evolution of ERP Systems: A historical perspective. *Enterprise Resource Planning: Global Opportunities & Challenges*, 1–16.

Rhee, K., Won, D., Jang, S.-W., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *Electronic Commerce Research*, *13*, 243–256. https://doi.org/10.1007/s10660-013-9121-4

Rogowski, M., Saeed, K., Rybnik, M., Tabedzki, M., & Adamski, M. (2013). User Authentication for Mobile Devices. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, S. Wierzchoń (Eds.), *Lecture Notes in Computer Science. Computer Information Systems and Industrial Management* (Vol. 8104, pp. 47–58). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40925-7_5

Roth, J. (2005). *Mobile Computing: Grundlagen, Technik, Konzepte*. *Dpunkt. Lehrbuch*. Heidelberg: dpunkt-Verl.

Rowles, D. (2014). *Mobile Marketing: How Mobile Technology is Revolutionising Marketing, Communications and Advertising*. London: Kogan Page.

Rowley, J., & Slack, F. (2004). Conducting a literature review. *Management Research News*, *27*, 31–39. https://doi.org/10.1108/01409170410784185

RSA. (2016). Two-Factor Authentication Is a Must for Mobile. Retrieved June 05, 2017, from https://www.rsa.com/en-us/blog/2016-06/two-factor-authentication-is-a-must-for-mobile

Sahd, L.-M., & Rudman, R. (2016). Mobile Technology Risk Management. *Journal of Applied Business Research (JABR)*, *32*, 1079. https://doi.org/10.19030/jabr.v32i4.9723

Samarati, P. (2001). Protecting respondents identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, *13*, 1010–1027. https://doi.org/10.1109/69.971193

Sathyan, J., Narayanan, A., Narayan, N., & K V, S. (2013). *A comprehensive guide to enterprise mobility*. *Infosys Press*. Boca Raton, FL: CRC Press.

Sauter, M. (2018). *Grundkurs Mobile Kommunikationssysteme*. Wiesbaden: Springer Fachmedien Wiesbaden.

Seals, T. (2017). Most Mobile Devices Are Out of Date and Need Patching. Retrieved October 05, 2018, from https://www.infosecurity-magazine.com/news/most-mobile-devices-are-out-of-date/

Sekaran, U. (2003). *Research methods for business: A skill-building approach* (4th ed.). New York, Great Britain: Wiley.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2014). *Operating system concepts essentials* (Second edition). Hoboken, NJ: Wiley.

Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, Mass.: MIT Press.

Smith, R., Taylor, B., Bhat, M., Silva, C., & Cosgrove, T. (2017). Magic Quadrant for Enterprise Mobility Management Suites.

Sodanil, M., Quirchmayr, G., Porrawatpreyakorn, N., & Tjoa, A. M. (2015). A knowledge transfer framework for secure coding practices. In *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 120–125). IEEE. https://doi.org/10.1109/JCSSE.2015.7219782

Solms, B. von. (2001). Information Security — A Multidimensional Discipline. *Computers & Security*, *20*, 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

Souppaya, M., & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-124r1

Srinivasan, A., & Wu, J. (2012). SafeCode – Safeguarding Security and Privacy of User Data on Stolen iOS Devices. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, W. Zhou (Eds.), *Lecture Notes in Computer Science. Cyberspace Safety and Security* (Vol. 7672, pp. 11–20). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-35362-8_2

Stango, A., Prasad, N. R., & Kyriazanos, D. M. (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 262–267). IEEE. https://doi.org/10.1109/SECURWARE.2009.47

Stieglitz, S., & Brockmann, T. (2012). Increasing Organizational Performance by Transforming into a Mobile Enterprise. *MIS Quarterly Executive*, *11*, 189–204.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

Sun, Z., Wang, Y., Qu, G., & Zhou, Z. (2016). A 3-D hand gesture signature based biometric authentication system for smartphones. *Security and Communication Networks*, *9*, 1359–1373. https://doi.org/10.1002/sec.1422

Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*, 571–588. https://doi.org/10.1142/S021848850200165X

Symantec. (2014). Fraud Alert: Phishing — The Latest Fraud Alert: Phishing — The Latest Tactics and Potential Business Impacts – Phishing [White Paper]. Retrieved from http://www.symantec.com/content/en/us/enterprise/white_papers/b-fraud-alert-phishing-wp.pdf

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling Design Processes. *AI Mag*, *11*, 37–48. Retrieved from http://dl.acm.org/citation.cfm?id=95788.95795

Téllez, J., & Zeadally, S. (2017). Mobile Device Security. In J. Téllez & S. Zeadally (Eds.), *Computer Communications and Networks. Mobile Payment Systems* (Vol. 11, pp. 19–33). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-23033-7_2

Teufl, P., Zefferer, T., & Stromberger, C. (2013). Mobile Device Encryption Systems. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *IFIP Advances in Information and Communication Technology*. *Security and Privacy Protection in Information Processing Systems* (Vol. 405, pp. 203–216). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39218-4_16

Torraco, R. J. (2005). Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, *4*, 356–367. https://doi.org/10.1177/1534484305278283

Tsichritzis, D. (1997). The Dynamics of Innovation. In P. J. Denning & R. M. Metcalfe (Eds.), *Beyond Calculation* (pp. 259–265). New York, NY: Springer New York. https://doi.org/10.1007/978-1-4612-0685-9_19

Tu, G.-H., Li, C.-Y., Peng, C., Li, Y., & Lu, S. (2016). New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks. In E. Weippl, S. Katzenbeisser, C. Kruegel, A. Myers, & S. Halevi (Eds.), *the 2016 ACM SIGSAC Conference* (pp. 1118–1130). https://doi.org/10.1145/2976749.2978393

Tupakula, U., & Varadharajan, V. (2013). Securing Mobile Devices from DoS Attacks. In *IEEE 16th International Conference on Computational Science and Engineering (CSE)* (pp. 34–41). https://doi.org/10.1109/CSE.2013.16

Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2015). E-Commerce Security and Fraud Issues and Protections. In E. Turban, D. King, J. K. Lee, T.-P. Liang, & D. C. Turban (Eds.),

Springer Texts in Business and Economics. Electronic Commerce (pp. 457–518). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-10091-3_10

Unhelkar, B., & Murugesan, S. (2010). The Enterprise Mobile Applications Development Framework. *IT Professional*, *12*, 33–39. https://doi.org/10.1109/MITP.2010.45

United Nations. (2014). World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352), Department of Economic and Social Affairs.

Uskov, A. V. (2012). Information security of mobile VPN: Conceptual models and design methodology. In *IEEE International Conference on Electro/Information Technology* (pp. 1–6). IEEE. https://doi.org/10.1109/EIT.2012.6220739

V Do, T., Lyche, F. B., Lytskjold, J. H., & van Thuan, D. (2015). Threat Assessment Model for Mobile Malware. In K. J. Kim (Ed.), *Lecture Notes in Electrical Engineering. Information Science and Applications* (Vol. 339, pp. 467–474). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-46578-3_55

Vaishnavi, V., & Kuechler, W. (2004). *Design Research in Information Systems*. Retrieved from http://desrist.org/design-research-in-information-systems/

Vaishnavi, V., & Kuechler, W. (2007). *Design science research methods and patterns: Innovating information and communication technology*. Boca Raton, FL, New York: Auerbach Publications, Taylor & Francis Group.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*, 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Venkatesan, D. (2016). Android ransomware variants created directly on mobile devices. Retrieved from http://www.symantec.com/connect/blogs/android-ransomware-variants-created-directly-mobile-devices

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*, 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Verclas, S., & Linnhoff-Popien, C. (Eds.). (2012). *Xpert.press. Smart Mobile Apps: Mit Business-Apps ins Zeitalter mobiler Geschäftsprozesse*. Berlin, Heidelberg: Springer Berlin Heidelberg.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (Eds.) 2009. *Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process.*

Wächter, M. (2016). *Mobile Strategy: Marken- und Unternehmensführung im Angesicht des Mobile Tsunami*. Springer Science and Business Media.

Wang, H., & Xu, Q. (2012). Improving M-Commerce through Enterprise Mobility. In *Management of e-Commerce and e-Government (ICMeCG), 2012 International Conference on* (pp. 211–215). https://doi.org/10.1109/ICMeCG.2012.13

Wang, Z., & Stavrou, A. (2010). Exploiting smart-phone USB connectivity for fun and profit. In C. Gates, M. Franz, & J. McDermott (Eds.), *the 26th Annual Computer Security Applications Conference* (p. 357). https://doi.org/10.1145/1920261.1920314

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q*, *26*, xiii–xxiii. Retrieved from http://dl.acm.org/citation.cfm?id=2017160.2017162

Wixom, B., & Watson, H. (2010). The BI-Based Organization. *International Journal of Business Intelligence Research*, *1*, 13–28. https://doi.org/10.4018/jbir.2010071702

Wohlin, C., Höst, M., & Henningsson, K. (2003). Empirical Research Methods in Software Engineering. In G. Goos, J. Hartmanis, J. van Leeuwen, R. Conradi, & A. I. Wang (Eds.), *Lecture Notes in Computer Science. Empirical Methods and Studies in Software Engineering* (Vol. 2765, pp. 7–23). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-45143-3_2

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2000). *Experimentation in Software Engineering: An Introduction*. Norwell, MA, USA: Kluwer Academic Publishers.

Wójtowicz, A., & Joachimiak, K. (2016). Model for adaptable context-based biometric authentication for mobile devices. *Personal and Ubiquitous Computing*, *20*, 195–207. https://doi.org/10.1007/s00779-016-0905-0

Wright, T., & Poellabauer, C. (2012). Improved Mobile Device Security through Privacy Risk Assessment and Visualization. In *Data Engineering Workshops (ICDEW), IEEE 28th International Conference on* (pp. 255–258). https://doi.org/10.1109/ICDEW.2012.80

Zhauniarovich, Y., Russello, G., Conti, M., Crispo, B., & Fernandes, E. (2014). MOSES: Supporting and Enforcing Security Profiles on Smartphones. *Dependable and Secure Computing, IEEE Transactions on*, *11*, 211–223. https://doi.org/10.1109/TDSC.2014.2300482

Zimmermann, O. (2011). Architectural Decisions as Reusable Design Assets. *IEEE Software*, *28*, 64–69. https://doi.org/10.1109/MS.2011.3

Publications

Hasan, B., Amin Rezaei, A. (2018): Enhancing Privacy in Smart Cities by Facilitating Communications between Public and Private Sectors. In J. Marx Gómez, A. Solsbach, T. Klenke, & V. Wohlgemuth (Eds.), 10. BUIS-Tage - Smart Cities / Regions. Springer. Vieweg (In Press).

Hasan, B., Marx Gómez, J. (2017): Security Framework for Adopting Mobile Applications in Small and Medium Enterprises. In: Obaidat M., Lorenz, P. (Eds.): E-Business and Telecommunications, Cham: Springer International Publishing (Communications in Computer and Information Science), pp 75-98.

Hasan, B., Schäfer, P., Marx Gómez, J., Kurzhöfer, J. (2016): Risk Catalogue for Mobile Business Applications. In: 13th International Joint Conference on e-Business and Telecommunications. Lisbon, Portugal, pp. 43–53.

Hasan, B.; Rajski, E.; Marx Gómez, J.; Kurzhöfer, J. (2016): A Proposed Model for User Acceptance of Mobile Security Measures – Business Context. In: Kim, K.; Wattanapongsakorn, N.; Joukov, N. (Eds.): Mobile and Wireless Technologies 2016, vol. 391. Singapore: Springer Singapore (Lecture Notes in Electrical Engineering), pp. 97-108.

Hasan, B., Mahmoud, T., Pramod, R., Marx Gómez, J., Kurzhöfer, J. (2015): User Acceptance Identification of Restrictions Caused by Mobile Security Countermeasures. In: MOBILITY 2015, The Fifth International Conference on Mobile Services, Resources, and Users. Brussels, Belgium: ThinkMind.

Hasan, B., Dmitriyev, V., Marx Gómez, J., Kurzhöfer, J. (2014): A Framework along with Guidelines for Designing Secure Mobile Enterprise Applications. In: Security Technology (ICCST), 2014 International Carnahan Conference on. Rome, Italy: IEEE Xplore.

Hasan, B., Marx Gómez, J., Kurzhöfer, J. (2013): Towards a Framework for Designing Secure Mobile Enterprise Applications. In: MOBILITY 2013, The Third International Conference on Mobile Services, Resources, and Users. Lisbon, Portugal: ThinkMind.

Appendix A

An excerpt of risk Catalogue for MEAs.

Mobile Device Category – MD		
Threat	**Description & Risk Estimation**	
MD-T1	Unintentional loss of the mobile device. The following possibilities may exist: - The lost mobile device is found by incapable entity - The lost mobile device is found by capable entity - The lost mobile device is completely unsecured	
Loss and theft of mobile devices	Likelihood of Occurrence	High
	According to the Kaspersky survey in 2013, one in every six users has experienced loss, theft or catastrophic damage to a mobile device (such as laptop, smartphone or tablet) in the last 12 months. According to the same survey, 32% of smartphones and 28% of tablets had work emails, 20% of smartphones and 29% of tablets had business documents (Kaspersky, 2013b). A survey conducted by IDG Research on behalf of Lookout revealed that one in ten smartphone owners were victims of smartphone theft (Lookout, 2014).	
	Possible Impact	High
	Lost or stolen mobile devices could be used to gain access to user data stored on the device or they could be used as an entry point into the user's corporate network (Imgraben et al., 2014) (Au & Choo, 2017). Since most mobile platforms allow a mobile device to be connected to a PC as a USB storage device, lost or stolen mobile devices can be fully compromised via mobile device's USB as an attack vector (Wang, Z. & Stavrou, 2010). Potential affected assets: B1-11; P1-5; T1-6	
	Risk Level	High
MD-T2	Unattended mobile devices are those mobile devices that are left temporary, unlocked and unsupervised.	
Unattended mobile devices	Likelihood of Occurrence	Medium
	There are no available statistics on this threat. However, due to the small size of mobile devices, they can often be left unattended for a short time.	
	Possible Impact	Medium
	A mobile device unattended for a short time is not such a great threat, because of the limited time and probable lack of intention of the unauthorized user to cause severe damage to the business. Therefore, the direct impact to business from temporary loss of mobile devices can be estimated as low. However, as leaving a mobile device unattended also increases the possibility of theft, the potential impact of this threat is estimated as medium. Potential affected assets: B1-11; P1-5; T3	
	Risk Level	Medium

MD-T3	Every piece of the hardware (e.g. battery, network adapter, flash memory…etc.) can break at any time, because of defects in the production process or because of mishandling through the user.	
Physical damage	Likelihood of Occurrence	Low
	As physical damage of mobile devices is unintentional and the motivation and capability to threaten the business is low, the likelihood of occurrence of such threats is estimated as low.	
	Possible Impact	Low
	The direct financial loss is the mobile device itself. However, this threat can result in an indirect financial loss in terms of lower productivity of the employee due to inability to use the mobile device. Moreover, if the mobile device's data storage is broken, important business data stored locally can be lost. As most business data are not only stored on the device, but they are synchronized with the company system, the potential impact on business is therefore estimated as low. Potential affected assets: T1,2,4	
	Risk Level	Low
Third-Party Mobile Applications Category – MA		
Threat	**Description & Risk Estimation**	
MA-T1	Mobile malware are malicious mobile applications that are mostly unintentional downloaded by mobile device's user. Examples for mobile malware: Trojans (AO Kaspersky Lab, 2015), (Pu et al., 2014) Worms (Adeel & Tokarchuk, 2011) spyware (Lookout, 2011) ransomware (Venkatesan, 2016) SMS Abuse (Tu et al., 2016)	
Malware	Likelihood of Occurrence	High
	As typical users may have banking, credit card, hotel, airline and corporate applications installed on their mobile devices (Mulvehill, 2016), the attackers will be highly motivated to target mobile devices and their applications. Therefore, the likelihood of occurrence of such threats is estimated as high.	
	Possible Impact	High
	Malware can perform very different malicious actions depending on the type of malware. This ranges from the collecting of user patterns, over denial of certain services to the theft and leakage of critical business information like customer data or production data. Therefore, the impact on business is estimated as high. Potential affected assets: B1-11; P1-5; T2-6	
	Risk Level	High
Mobile OS Category – MOS		
Threat	**Description & Risk Estimation**	

MOS-T1	Gaining root access and rights of mobile operating system. This is not a threat itself, but increases mobile OS vulnerability. Rooting of mobile OS is usually used to remove preinstalled, unwanted applications, customize the theme and functions of the mobile OS or so that the user can access unofficial app markets and install unofficial mobile applications.	
Rooting / Jailbreaking	Likelihood of Occurrence	High
	Rooting of mobile OS does not require high technical capability. Users can be also motivated to root their mobile devices to access unofficial app markets and install unofficial mobile applications, which are mostly offered for free.	
	Possible Impact	High
	Gartner predicted that by 2017, 75% of mobile security breaches will be the result of mobile application misconfigurations like jailbreaking or rooting (Gartner, 2014). With Rooting, users do not only bypass their mobile device's built-in security, but they also extremely increase the risk of downloading malware. Recent reports reveal that up to 32% of apps on unofficial markets contain malicious content (Bach, 2015). Potential affected assets: B1-11; P1-5; T2-6	
	Risk Level	High
MOS-T2	As with rooting, missing a mobile OS updates is not a threat itself, but increases the mobile OS vulnerability. Missing updates can cause risk because they often include patches and security updates.	
Missing updates	Likelihood of Occurrence	High
	As reported by Skycure, 71% of mobile devices still run on security patches that are more than two months old, because the carriers are slow to make them available to users (Seals, 2017).	
	Possible Impact	Medium
	Malware and other kinds of mobile threat can depend on unpatched vulnerabilities to be successful. Therefore, missing updates can open the door for other threats (especially malware) that might cause high impact. Potential affected assets: B1-11; P1-5; T5	
	Risk Level	High
Wireless Networks Category – WN		
Threat	**Description & Risk Estimation**	
WN-T1	DoS attacks deny performing a certain service or running a certain software or application. DoS attacks do not only focus on the denial of services, they can reduce the ability of valid users to access resources (Myagmar et al., 2005) or they can induce incorrect operation (Rhee et al., 2013).	
Denial of Service	Likelihood of Occurrence	Low
	There are no available statistics yet on DoS attacks, which target MEAs. As the motivation of an attacker is estimated as low, the likelihood of occurrence of such threat is also estimated as low.	
	Possible Impact	Medium

	Business data are not exposed. The worst-case scenario is that the employee will not be able to perform business processes for a specific period of time. For some cases, DoS can downgrade the mobile device's performance, which in turn can lead to low employee productivity when the service needed is very slow or not available at all. Potential affected assets: B9	
	Risk Level	Medium
WN-T1.1 Abuse of SMS	DoS can be performed against mobile devices via sending thousands of silent SMS (or stealth SMS), which are indicated neither on the display nor by an acoustic signal (Croft & Olivier, 2007). Moreover, the intended victims will not be aware of such an attack, but they will recognize an abnormal decline in battery charge capacity and the inability to perform other mobile services.	
	Likelihood of Occurrence	Low
	See Threat "WN-T1"	
	Possible Impact	Medium
	See Threat "WN-T1" Potential affected assets: B9, T2	
	Risk Level	Medium
WN-T1.2 Sleep deprivation	Sleep deprivation or battery exhaustion particularly targets battery-powered devices by trying to drain their battery, preventing these devices from saving battery in sleep modes or similar through constant service requests (Martin et al., 2004) (Buennemeyer et al., 2007).	
	Likelihood of Occurrence	Low
	See Threat "WN-T1"	
	Possible Impact	Low
	No significant impact is found. Potential affected assets: T2	
	Risk Level	Low
WN-T1.3 DoS attack on MANETS	DoS-attacks also target Mobile Adhoc Networks (MANETs) like direct Peer-to-Peer Wi-Fi or Bluetooth-connections. Bluetooth is susceptible to DoS and impacts include making a device's Bluetooth interface unusable and draining the device's battery (Padgette et al., 2012). A flooding attack in MANETs can also be used to perform a sleep deprivation attack, where either a specific node or a group of nodes are targeted by forcing them to use their vital resources (e.g. Battery) (Jain, S., 2014).	
	Likelihood of Occurrence	Low
	See Threat "WN-T1"	
	Possible Impact	Low
	These types of attack have no significant impact due to the required close range, and therefore they can easily be avoided by simply moving out of range (Padgette et al., 2012). Potential affected assets: B9; T2	
	Risk Level	Low

WN-T2 MitM Attack	Man-in-the-Middle (MitM) attacks intercept communications in networks to eavesdrop, alter, or delete the exchanged data. The attacker is placed in the middle between the client and the server. For instance, (Moonsamy & Batten, 2014) described three popular MitM attacks (SSL Hijacking, SSL Stripping, DNS Spoofing) that targeted at smartphone applications.	
	Likelihood of Occurrence	Medium
	No available statistics are found yet on MitM attacks, which target MEAs. In general, as such attack can take place anywhere and anytime, its likelihood of occurrence is estimated as medium.	
	Possible Impact	High
	A successful attack can capture and manipulate sensitive information in real-time. Therefore, the potential impact is estimated as high. Potential affected assets: B1-11, P1-5	
	Risk Level	High
WN-T2.1 MitM Attack on unsecured WLAN	A type of such network attack is captive portals, that typically use encryption to secure user's credentials when authenticating to the network, but the network traffic is not encrypted and can be sniffed over the air (Godber & Dasgupta, 2002).	
	Likelihood of Occurrence	Medium
	Mobile devices connected to unsecured Wi-Fi hotspots increase the threat of communication interception, such MitM attacks and password eavesdropping (Fitzgerald et al., 2013) (Landman, 2010).	
	Possible Impact	High
	See Threat "WN-T2" Potential affected assets: B1-11, P1-5	
	Risk Level	High
WN-T2.2 MitM Attack on mobile Internet connection	MitM attack can also take place on other mobile Internet networks that use cellular system like the 2G (GSM) and 3G (UMTS) (Meyer & Wetzel, 2004). Moreover, 4G (LTE) networks might be vulnerable to MitM attack by impersonation of user International Mobile Subscriber Identifier (IMSI) (Bhasker, 2013). Although LTE is widely used and it is considered to be more secure than UMTS and GSM against MitM attack, using a rogue base station broadcasting at a high-power level, an attacker can force a user to downgrade to either GSM or UMTS (Cichonski et al., 2016).	
	Likelihood of Occurrence	Low
	This threat requires high capability to be performed. Moreover, NIST stated: "At the time of this writing, there are no significant, publicly-known weaknesses in the cryptographic algorithms used to protect the confidentiality and integrity of the UMTS air interface." (Cichonski et al., 2016).	
	Possible Impact	High
	See Threat "WN-T2" Potential affected assets: B1-11, P1-5	
	Risk Level	Medium
Mobile User Category – MU		

Threat	Description & Risk Estimation	
MU-T1	Through phishing, the attacker tries to steal login and personal data from the user, e.g. using mails, SMS, or advertisements as channels. These are used to trick the user into entering private information and login data in replica websites of commonly known websites or through the offering of free downloads or low-price shopping.	
Phishing	Likelihood of Occurrence	High
	Attackers are motivated to target mobile devices for several different reasons, one of which is the mobile device's display constraints that could be used to hide the URL bar (Abura'ed et al., 2014).	
	Possible Impact	High
	If the attacker succeeds in obtaining the login credentials (username, password und PIN, credit card data, etc.), then he might be able to perform all actions authorized to the mobile device's owner. Potential affected assets: B10; P5	
	Risk Level	High
MU-T2	The most known form of such threat is called drive-by download, that works by exploiting vulnerabilities in web browsers, plug-ins or other components that work within browsers (Levinson, 2012).	
Downloading of untrusted mobile applications	Likelihood of Occurrence	Medium
	This kind of threats tries to prompt users through advertisements or adverse websites to take an action that downloads malware on their mobile devices.	
	Possible Impact	High
	As the drive-by download can install and launch a malware, the impact to business is estimated as high. Potential affected assets: B1-11; P1-5; T2-6	
	Risk Level	High
MU-T3	Granting privilege to third-party mobile applications can be done without the knowledge of the mobile user.	
Unaware privilege granting	Likelihood of Occurrence	Medium
	Most mobile OSes inform the user about the access rights required while installing a mobile application. Although users are warned or informed about that, they tend to overlook this information and just grant the access privileges to the mobile application.	
	Possible Impact	High
	As granting privileges without checking if they are needed for the purpose of the installed application increases the possibility of installing malware, the impact to business is estimated as high. Potential affected assets: B1-11; P1-5; T2-6	
	Risk Level	High

Appendix B

The questionnaire used to investigate user acceptance (0 = no acceptance to 6 = very high acceptance).

1. How old are you? ----------
2. Do you use mobile devices (smartphones, tablets) for work?
   ○ Smartphone ○ Tablet ○ Both ○ None
3. Do you use the same mobile device privately as well?
   ○ Yes ○ No
4. Do you use your private or corporate-owned mobile device for work?
   ○ Private ○ Corporate-owned ○ None
5. In the case of password authentication, the user must confirm his identity by entering a password of a certain length. Depending on the implementation, this can consist of letters, numbers and special characters, e.g. P4s8W0!Rd.
   What time interval do you feel is reasonable to request the authentication with a long and complex password?
   Less than 30 minutes

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

   30 to 60 minutes

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

   12 to 24 hours

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

   Daily or longer

   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6
6. How useful do you feel this measure is?
   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6
7. Would you prefer using biometric authentication, like a fingerprint, instead?
   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6
8. How restricted do you feel in your work, when using VPN to get corporate data on your mobile device, considering a possible restriction on your usual internet connection?
   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6
9. Do you feel more secure using VPN when accessing critical corporate data?
   ○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

10. Considering the increased security when completely encrypting data storage (like SD-Card), how accepting are you of longer loading and saving time when using this kind of encryption?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

11. How much do you prefer single file/folder-encryption in comparison to the completely encryption of data storage, considering the faster loading and saving time?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

12. How acceptable for you is the containerization of mobile enterprise applications (sandbox), considering the strict separation of private and business applications?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

13. How much would you like a sandboxed application that still allows some kind of export (e.g. backups) and import (e.g. contact list) functionality?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

14. To what extent would you accept the increased battery/memory consumption (10% higher) if you use protection software like antivirus?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

15. How much do you feel your privacy is violated, when your employer monitors your mobile device only to check its compliance to the security policy?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

16. How much do you feel your privacy is violated, when your employer can monitor all your activities (e.g. Internet activities, e-mails, etc.) on your mobile device?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

17. How much would you accept that you can install applications from a corporate app-store only? Considering that some of your favorite applications are there as well.

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

18. How much would you prefer to use the original app-store in addition to the corporate one?

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

19. To what extent do you prefer implementing personalized policies on your mobile device?
    (i) For personalized policies, the company implements policies depending on the task or department of the employee in varying degrees of restriction (more restrictions when working with sensitive data, less restrictions when working with non-sensitive data).

○ 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

20. Would you give the mentioned security measures a positive, negative or no impact on your productivity?

○ -3 ○ -2 ○ -1 ○ 0 ○ 1 ○ 2 ○ 3

Appendix C

The SQL stored procedure that creates a new version of the CFMS guidance model:

```
DECLARE @VersionID_Current int
DECLARE @Version_Name NVARCHAR(15)
DECLARE @Version_Name_Main NVARCHAR(15)
DECLARE @Version_Name_Sub NVARCHAR(15)
DECLARE @Current_Date date

SET @VersionID_Current = (SELECT TOP 1 VersionID FROM Versions WHERE VersionType = 1 ORDER BY VersionID DESC)

SET @Version_Name = (SELECT TOP 1 Name FROM Versions WHERE VersionID = @VersionID_Current ORDER BY VersionID DESC)

SET @Version_Name_Main = (SELECT SUBSTRING(CAST(@Version_Name AS NVARCHAR), 2, CHARINDEX('.', @Version_Name, 1) - 2))

SET @Version_Name_Sub = (SELECT SUBSTRING(@Version_Name, CHARINDEX('.', @Version_Name, 1) +1 , 3))

DECLARE @Version_Current int
SET @Version_Current = (SELECT TOP 1 VersionID FROM Versions WHERE VersionType = 2 ORDER BY VersionID DESC)
IF @Version_Current IS NOT NULL
   BEGIN
      /* Update latest Current Version to VersionType OLD */
      UPDATE Versions SET VersionType = 3 WHERE VersionID = @Version_Current
   END

UPDATE Versions SET VersionType = 2 WHERE VersionID = @VersionID_Current

SET @Current_Date = (SELECT CAST(GETDATE() As datetime ))
SET @VersionID_New = @VersionID_Current + 1

IF @Version_Name_Sub = 9
   BEGIN
      SET @Version_Name_Main = @Version_Name_Main + 1
      SET @Version_Name_Sub = 0
   END
ELSE
```

```
   BEGIN
      SET @Version_Name_Sub = @Version_Name_Sub + 1
   END


/* Create new Version ID in Versions Table */
INSERT INTO [dbo].[Versions] VALUES
   (@VersionID_New, 'v' + @Version_Name_Main + '.' + @Version_Name_Sub, 1,
    @Current_Date, @VersionID_Current);


/* Copy Dataset (all tables) for new VersionID */
INSERT      INTO      [dbo].[SecurityMeasures]      ([SecurityMeasureID],
[Versions_VersionID], [Name], [Description])
   SELECT [SecurityMeasureID], @VersionID_New, [Name], [Description] FROM
    [dbo].[SecurityMeasures] WHERE Versions_VersionID = @VersionID_Current
    AND [Projects_ProjectID] is NULL;


INSERT   INTO   [dbo].[Solutions]   ([SolutionID],   [Versions_VersionID],
[Threats_ThreatID], [Threats_Versions_VersionID])
   SELECT [SolutionID], @VersionID_New, [Threats_ThreatID], @VersionID_New
   FROM [dbo].[Solutions] WHERE Versions_VersionID = @VersionID_Current
   AND [Projects_ProjectID] is NULL;


/*… Similar for all other tables */


/* Copy Dataset (cross-reference tables) for new VersionID */
INSERT              INTO              [dbo].[SecurityMeasuresToSolutions]
([SecurityMeasures_SecurityMeasureID],
[SecurityMeasures_Versions_VersionID],            [Solutions_SolutionID],
[Solutions_Versions_VersionID])
   SELECT      [SecurityMeasures_SecurityMeasureID],      @VersionID_New,
    [Solutions_SolutionID], @VersionID_New FROM
    [dbo].[SecurityMeasuresToSolutions]
   WHERE
    [SecurityMeasures_Versions_VersionID] = @VersionID_Current;


/*… Similar For all other cross-reference tables */
GO
```

Appendix D

Carl von Ossietzky Universität Oldenburg

Interview-Leitfaden zur Expertenbefragung zum Thema:

A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility

Ansprechpartner:

Basel Hasan

basel.hasan@uni-oldenburg.de

Supervisor:

Prof. Dr.-Ing. habil. Jorge Marx Gómez

Fakultät II – Informatik, Wirtschafts- und Rechtswissenschaften

Wirtschaftsinformatik / Very Large Business Applications

Ammerländer Heerstr. 114-118, 26129 Oldenburg

Einführung

Im Rahmen einer Doktorarbeit an der Universität Oldenburg wurde ein konzeptionelles Framework für mobile Sicherheit konzipiert und entwickelt, welches dem Unternehmen beim Einsatz von mobilen Unternehmensapplikationen unterstützen wird. Das Ziel dieses Workshops ist zuerst die Vorstellung und die Diskussion des entwickelten Frameworks sowie dessen implementierten Prototyp. Im Anschluss würden die Einsatzmöglichkeiten und die weiteren Evaluationsschritte des Frameworks bei BTC diskutiert werden. Zur Evaluation und Diskussion der Arbeit dienen die Fragen in nächsten drei Teilen.

Allgemein Informationen des Gesprächspartners *

Unternehmen: _____

Abteilung: _____

Position / Rolle: _____

Ort, Datum: _____

Weitere Information / Anmerkung:

_____

Darf ich Ihr Unternehmen in meiner Arbeit nennen?

☐ Ja ☐ Nein

_____

** Für die Teilnehmer werden die Namen anonymisiert.*

Teil 1: Allgemeine Frage

1. Haben Sie bereits Tools, die die Security Knowledge strukturiert verwalten?

   ☐ Ja ☐ Nein

   Falls Ja, welche?

   _____

   _____

Teil 2: Fragen zur Bewertung und Feedback der vorgeschlagenen Lösung

(ggf. bitte begründen Sie Ihre Antworten)

1. Wie beurteilen Sie die Klarheit der Visualisierung sowie der Strukturierung und Verknüpfung von Framework's Inhalte?

Visualisierung:	☐	Sehr klar	☐	Klar	☐	Weniger klar	☐ Unklar
Strukturierung:	☐	Sehr klar	☐	Klar	☐	Weniger klar	☐ Unklar
Verknüpfung:	☐	Sehr klar	☐	Klar	☐	Weniger klar	☐ Unklar

   _____

   _____

2. Halten Sie das Framework für geeignet, um für die Unterstützung des Unternehmens beim sicheren Einsatz von mobilen Unternehmensapplikationen eingesetzt zu werden?

   ☐ Sehr geeignet ☐ Geeignet ☐ Weniger geeignet ☐ Nicht geeignet

   _____

   _____

3. In wie fern kann das Framework den Security-expert Users dabei unterstützen, die mobilen Sicherheitsmaßnahmen gegen Business Users zu begründen?

   ☐ Erheblich unterstützen ☐ Unterstützen ☐ Teilweise unterstützen ☐ Nicht unterstützen

   _____

   _____

4. In wie fern kann das vorgeschlagene Framework dem Management von mobiler Sicherheit unterstützen?

   ☐ Erheblich unterstützen ☐ Unterstützen ☐ Teilweise unterstützen ☒ Nicht unterstützen

   _____

   _____

5. Welche Verbesserungsmöglichkeiten haben Sie noch zum vorgeschlagenen Framework? (Optimierungen oder Erweiterungen)

   _____

   _____

6. Welche Vor- und Nachteile sehen Sie in das vorgeschlagene Framework?

   a. Vorteile:

      _____

      _____

   b. Nachteile:

      _____

      _____

Teil 3: Fragen zur Einsatzmöglichkeiten des Frameworks beim BTC

1. Welche weiteren Evaluationsschritte wären bei Ihrem Unternehmen möglich?

   _____

   _____

2. Wie lässt sich das vorgeschlagene Framework in Ihrem Unternehmen eingesetzt werden?

   _____

   _____

Vielen Dank für Ihre Unterstützung

Ich versichere, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichungen, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

Basel Hasan, 21.05.2019