Usability, Security, and Mobility for Mobile Devices in Healthcare Information Systems

Doctoral Dissertation by

Jelena Mirkovic

Submitted to the Faculty of Mathematics and Natural Sciences at the University of Oslo in partial fulfillment of the requirements for the degree Philosophiae Doctor (Ph.D.) in Computer Science

November 2012

Series of dissertations submitted to the
Faculty of Mathematics and Natural Sciences, University of Oslo
No. 1308

ISSN 1501-7710

Cover: Inger Sandved Anfinsen.
Printed in Norway: AIT Oslo AS.

Produced in co-operation with Akademika publishing.
The thesis is produced by Akademika publishing merely in connection with the
thesis defence. Kindly direct all inquiries regarding the thesis to the copyright
holder or the unit which grants the doctorate.

Abstract

Recent advances in telecommunication and networking have a potential to influence healthcare management and healthcare delivery processes in a manner that was not possible several years ago. Numerous wireless and mobile networks, emerging mobile devices, platforms, and operating systems available today are starting to be used to collect, transfer, and analyze patient medical data in a transparent and controlled manner independent of time and place.

This dissertation investigates problems and issues related to successful development, adoption, and integration of mobile services in healthcare information systems for patients. In the context of the development of mobile application that enables access to the CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment) system, the following research questions are addressed:

- What are the main functionality and user interface requirements for developing user-friendly, adaptable and well-accepted applications that enable the patient's mobile access to a patient support system such as the CONNECT system? (Paper II)
- What are the security requirements for enabling secure mobile access to a patient support system such as the CONNECT system, and how can they be properly met without compromising usability of the system? (Paper III)
- What is the best approach for enabling seamless and context aware access to patient support system such as the CONNECT system over different types of terminals and access network on secure and user friendly manner? (Paper IV)

The main challenge of the presented work has been to encompass the complex and interdisciplinary field of utilization of mobile technology in a healthcare information for patients such as the CONNECT system. The presented work makes contributions in the areas of: development and integration of user-friendly and useful mobile services in healthcare information systems for patients, development of secure and user-friendly solutions for enabling access to patients' private health-related information, and development context adapted patient support systems that provide secure and user-friendly access to patient data over various types of terminals and access networks. During the research work conducted as part of the dissertation, different system stakeholders were involved and user's design and functionality requirements from mobile healthcare services for patients were identified, the current technical and legislation environment in healthcare information systems in Norway were researched, and different options and technologies for integrating various types of (mobile) access platforms to healthcare information services were studied. Even thought the contributions presented in the dissertation are gained

through work on the CONNECT project and are closely related to development of the CONNECT Mobile application, the results can be applied to a wide range of healthcare information systems with similar design and functionality requirements that handle sensitive and private data and require high level of user-friendliness and usefulness.

Preface

This dissertation has been submitted to the Faculty of Mathematics and Natural Sciences at the University of Oslo (UiO), as partial fulfillment of the requirements for the degree Philosophiae Doctor (Ph.D.). The work has been carried out at the Center for Shared Decision Making and Collaborative Care Research at the Oslo University Hospital as a part of larger study (PI, C. Ruland). The main supervisors were Dr. Haakon Bryhni and Professor Cornelia Ruland. The work was financially supported by the Norwegian Research Council through the project 176823/S10 called "Communication and Information Sharing between Patients and their Care Providers".

This dissertation consists of four chapters. Chapter 1 introduces the research topic and main research areas, defines the research methodology, outlines the motivation for the dissertation, and presents the research questions. Chapter 2 introduces the theoretical background and main concepts used in the dissertation. Chapter 3 presents short summaries of the four papers contained in the dissertation and describes related work in the specific research areas. Chapter 4 summarizes final conclusions and main contributions of the dissertation and presents areas for future work.

The results of this research have already been presented at conference publications. The last part of the dissertation contains four papers: a survey paper of relevant projects using mobile devices and mobile applications in healthcare (Paper I), a paper that addresses research issues in the development and design of a user-friendly mobile healthcare application that enable mobile access to patient support system (Paper II), a paper that proposes a secure solution for mobile access to patients' private medical information (Paper III), and a paper that describes a framework for development of ubiquitous patient support systems (Paper IV).

Acknowledgements

I would like to thank my supervisors, Dr. Haakon Bryhni and Dr. Cornelia Ruland, for their contributions to this work. Haakon, as my main supervisor, provided me with help and guidance throughout the work on this dissertation, and his broad knowledge and expertise added significant value to the presented work. Cornelia provided me with constant help, support, and new inspiration for further work and improvements in different parts of the dissertation. Thank you both for believing in me and giving me your guidance and support whenever I needed it.

I would like to thank all the people from Center for Shared Decision Making and Collaborative Care Research for all the help and support they provided me with during my work. I would also like to give special thanks to my colleagues in the information technology section of the research center for their help and cooperation on this project.

Additionally, I would like to thank the companies Faster Imaging and Encap for enabling me to use their technologies in my work, and for helping me during the development and implementation process.

I would also like to thank my family and friends for their support during the last few years. Moving away from my home country and family was difficult for all of us, but you always provided me with your support and love wherever I was.

Finally, I would like to thank Dr. Sandor Seres first for helping me find the PhD position in Norway, and, when I came here, for always providing me with interesting and inspiring discussions related to work, personal common interests, and topics involving our home country. You always reminded me that I should never settle for average, and to always strive to improve myself in every possible way.

Jelena Mirkovic

Oslo, Norway, November 2012

List of Papers

Paper I Jelena Mirkovic, Haakon Bryhni, and Cornelia M. Ruland. **Review of projects using mobile devices and mobile applications in healthcare**. In Scandinavian conference on Health Informatics, pp. 49-54, 2009, Arendal, Norway.

Paper II Jelena Mirkovic, Haakon Bryhni, and Cornelia M. Ruland. **Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management**. In The Third International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED 2011), pp. 64-71, 2011, Gosier, Guadeloupe, France.

Paper III Jelena Mirkovic, Haakon Bryhni, and Cornelia M. Ruland. **Secure Solution for Mobile Access to Patient's Health Care Record**. In 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (Healthcom 2011), pp. 296-303, 2011, Columbia, Missouri, USA.

Paper IV Jelena Mirkovic, Haakon Bryhni, and Cornelia M. Ruland, **A framework for the development of ubiquitous patient support systems**. In 6th International Conference on Pervasive Computing Technologies for Healthcare, 2012, San Diego, California, USA.

Table of Contents

Chapter 1: Introduction to the research topic and research methodology

Mobile devices are becoming more and more popular and accepted as an important part of our everyday life. They provide access to numerous services and allow us to stay connected independent of location and time. There has been an increase in the utilization of mobile services in many application areas such as learning, government, and business. The healthcare sector is also slowly starting to recognize and leverage the advantages of ubiquitous and seamless information systems. This dissertation addresses some of the main challenges and problems in order to enable user-friendly, secure, ubiquitous, and timely healthcare information delivery at the point of need, and provides some answers to why acceptance and wide deployment of mobile services in the healthcare sector is still low despite great potential.

There is a large body of research that demonstrates how utilization of mobile and wireless technologies in the healthcare sector can provide higher efficiency and quality of healthcare delivery and ensure lower cost of healthcare services [1-4]. Some of the areas where mobile healthcare services can provide a great advantage in comparison to traditional ways to deliver care, as described by Shieh and colleagues [1], are: home-based telemedicine for chronic and long term illness care (vs. traditional communication which requires clinical visits), mobile wireless devices for displaying up-to-date clinical information at the point of care (vs. traditional desktop PC applications or paper based systems), systems for emergency situations in remote locations where patient information is retrieved and treated by specialists from a remote location (vs. traditional emergency systems that lack correct and complete data at the time of service), and electronic health records that can be shared by both patient and healthcare provider (vs. standard paper-based healthcare records available just to healthcare provider).

Mobile access to healthcare services can provide a great advantage to various stakeholders, such as patients, healthcare personnel, and healthcare institutions. For example, patients can monitor their condition on their own, be more involved in their medical treatment and decision-making process, and stay connected with the healthcare provider at all times. By introducing mobile and wireless technologies, healthcare organizations can cut communication and treatment costs by reducing the number of patient hospital visits and hospital stays while increasing availability and productivity [2]. Healthcare providers can be offered ubiquitous, timely access to patients' health records, medical knowledge databases, and consultation with other experts in the specific fields at the point of need. Emerging technologies can be also used for gathering healthcare related data and transforming them to electronic form, making the healthcare information in this manner more centralized, accessible, and always up-to-date both for healthcare providers and patients (e.g., a repository of healthcare related information in digital format accessible from different settings inside healthcare institutions called Electronic Healthcare Record (EHR) [5-7], or a personal self-managed medical record where individuals update their own health related data usually referred as Personal Healthcare Record (PHR) [8-10]).

Norway, among other countries, has recognized the potential of new and evolving information and communication technologies for solving emerging healthcare related issues. The Norwegian Directorate of Health reports an increase in the aging population in recent years and as a result anticipates a higher prevalence of dementia, chronic illness, cancer, heart and lung insufficiency and musculoskeletal illness in the near future [11]. In addition, changes are expected in distribution between major groups of diseases as well as the appearance of new medicine and treatment methods. To address these challenges, Norwegian health authorities have set up numerous national plans and strategies in the last few years with the goal of improving healthcare services (e.g., The Coordination Reform [12], National Health Plan for Norway (2007-2010) [13], Interaction 2.0 - National eHealth strategy 2008-2013 [14]). All of these plans and strategies report a requirement for developing and improving healthcare services using new and emerging technologies, such as eHealth. In the literature, the term eHealth is often used to represent utilization of Internet and other related information sources and communication technologies in the healthcare industry to improve access, efficiency, effectiveness, quality of healthcare systems, and improving the health status of patients [15]. For example, Interaction 2.0 puts a strong focus on: network based services for patients and the general public, patient access to summarized medical information, electronic exchange of information and knowledge, and telemedicine and new information and communication technologies [14].

However, even though the advantages and needs for integrating mobile technology and advanced mobile services in the healthcare sector are identified and recognized, their wide deployment is still a work in progress. Before mobile services in healthcare can live up to their full potential, many issues and challenges must be addressed and resolved. Some of them are: privacy, security, and protection of highly private and sensitive data; limited capabilities of wireless and cellular communication networks; limited capabilities of mobile devices (e.g., display, processing power, and input characteristics); a large diversity of mobile devices and their specific capabilities; low interoperability; the complexity of different healthcare services and healthcare information systems, as well as numerous stakeholders in the healthcare system (e.g., providers, insurers, consumers, employers, and government entities), and legal and regulatory aspects [16-19]. The problem is not just the large number of identified issues, but also the high interrelationship between them. For example, the usefulness and user-friendliness of mobile services is related and often determined by limited capabilities of wireless and cellular communication networks and mobile terminals. Limited characteristics of networks and terminals are further related to how security and privacy issues are addressed, and security and privacy mechanisms, which are related to legal and regulatory rules, further can affect user-friendliness and usefulness of the mobile services. As a result, addressing one research issue in isolation without considering related challenges and problems is usually not possible. Due to the complex problem space and the numerous inter-correlated research issues further research work is needed to address these issues in relation to each other, as done in this dissertation in the context of the CONNECT research project.

1.1 CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment) project

The work presented in the dissertation is part of the CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment) research project. The main goal of the CONNECT project is to identify key factors that are related to successful adaptation, implementation, and maintenance of Internet-based support systems for communication and information sharing between and among patients and care providers. To address these challenges as part of the CONNECT project, a patient portal was developed that integrates a suite of Internet-based tools designed to support patients in illness management (referred to in this dissertation as the CONNECT patient support system). Here patients can monitor their symptoms, obtain individually tailored evidence-based self-management support, ask questions to a clinical nurse specialist, communicate with other patients in a forum, and use a diary. By providing patients with around the clock access to important health information, the goal of the CONNECT system is to help patients to better understand and manage their illness, become more engaged in their own health care and the decisions they face, and improve communication with their care provider [20-22]. The system is currently adapted in order to support patients with chronic or serious long-term illnesses, but the general principles can be implemented in a wide range of diagnoses. Several randomized clinical trials tested different parts of the system, and the results show improved patient provider communication, less symptom distress and depression, and better self-efficacy for patients with access to the CONNECT system [3, 20-25].

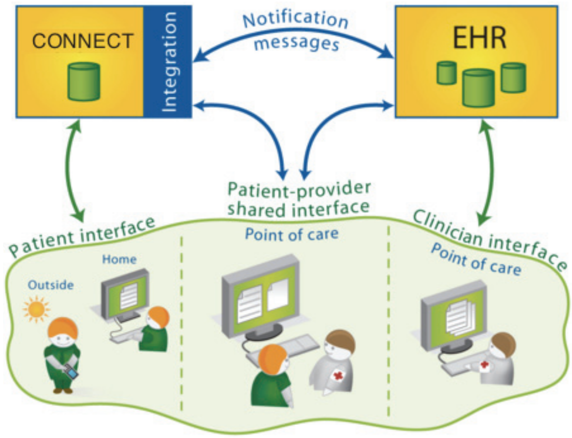


Figure 1. The CONNECT system architecture [26]

The CONNECT system architecture is shown in Figure 1. The CONNECT patient support system consists of several modules providing patients with different functionalities as described above. The purpose of an Integration layer is to provide connection with EHR system and other services in a hospital information system. Implementation of the Integration layer is part of the current research conducted as part of the CONNECT project. The messaging system based on the EbXML framework as proposed by the Norwegian Centre for Informatics in Health and Social Care [26, 27] is used to enable communication between multiple systems. To preserve security of the communication, messages are transferred over a secure network (The Norwegian Health Network [28]), while special proxy servers are used for translation and integration of the message files in different parts of the hospital information systems. The goal of the proposed architecture is to provide both clinicians and patients with access to the system through a joined interface (for both clinicians and patients) or through separate, more private interfaces (for patients only). The system is designed with the goal to enable patients to gain access over different terminals (web application, mobile application(s)) and communication networks, and receive information adapted to their specific needs and context of use.

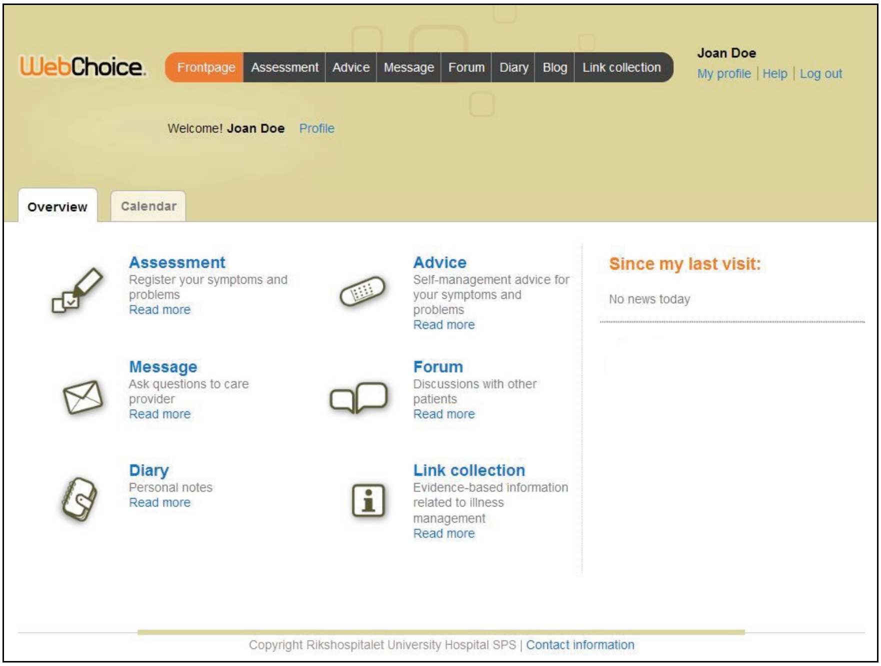


Figure 2. CONNECT application – a screenshot of the application's main menu showing the included supported functionalities

The underlying CONNECT web-based application adapted for running on standard PCs and laptops (interface shown on Figure 2) was previously developed and tested as part of the research work in the CONNECT project [3, 20-25]. The dissertation presents a continuation of this work where the main goal was to enable mobile access to the CONNECT system and to transfer and adapt functionalities of the CONNECT web application for use on mobile terminals. Ruland and colleagues gave a short overview on the research topic of development and deployment of mobile services in healthcare in the context of the CONNECT patient support system and discussed some research issues (such as security and mobility), before the work on this dissertation and development of mobile application commenced [26]. Additionally, before the work on the dissertation started only the initial design and functionality issues are researched through development of the first draft of the design screenshots. The research work conducted as part of this dissertation presents the further work on the discussed research topics and development process, and shows how the main challenges for implementation, deployment, and integration of mobile services are addressed in the projects through development of the CONNECT Mobile application.

1.2 Methods

As stated in the introduction, the challenges of development, deployment, and integration of mobile services in healthcare information systems (e.g., security, privacy, numerous types of terminals with different characteristics, numerous stakeholders, legal issues, limited capabilities of mobile terminals and mobile networks) are significant and highly inter-correlated. In this dissertation various challenges are addressed through different phases of the performed research work, and in this chapter the design science Information System (IS) Research Framework is used to frame and describe the performed research process in a unified approach.

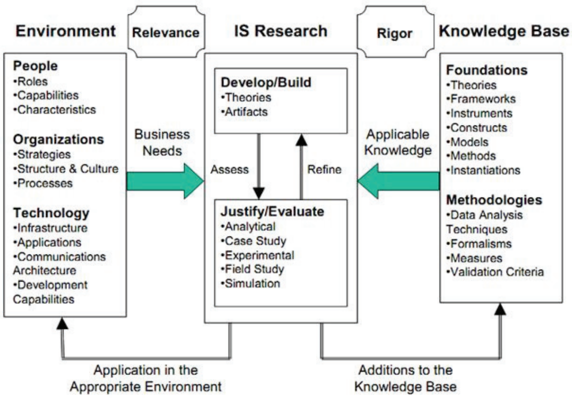


Figure 3. Information System Research Framework [29]

The design science IS Research Framework describes the design circle where an artifact is built [29-32]. Figure 3 shows the design science IS research framework as defined by Hevner and colleagues in [29]. The design circle contains two phases: Development/Build and Evaluation/Justification, and the framework supports development of the artifact through cycles of empirical and theoretical validation and improvement. The problem space is derived from the environment, composed of people, general organizations, and the implemented technologies. Identifying business needs as part of the research ensures research relevance. The knowledge base is used to provide means (foundations and methodologies) for developing the artifact. Correctly applying the existing knowledge base ensures rigor of the research results. Peffers and colleagues introduced a design science research process model to help researchers in performing and presenting design science research in information systems [30]. The process consists of six steps: (1) problem identification and motivation, (2) objectives of a solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication. These research process steps are used in next section as a framework for presenting the performed research process.

1.2.1 Problem identification and motivation

In the introduction it is noted how mobile services can be utilized in healthcare and what advantages they can provide to patients and healthcare personnel using some examples found in the literature (e.g., [1-3, 33]). However, despite the numerous successful research studies and trials that show the emerging need for these kind of services and recognized potential by national health authorities in different countries including Norway, mobile devices and applications are still not widely used in the healthcare sector as a standard way for delivering healthcare services to patients and healthcare providers and managing health related information. On the other hand, numerous stand-alone applications offering people health management services on mobile devices can be found on the market. For example there is a great number of health related applications available in the iTunes Store for iOS and in the Google Play store for Android devices. However, these applications are not connected to other health related services and information available on public healthcare information systems, and they usually do not implement specific security mechanisms and protections to ensure information confidentiality and privacy. The existence of the health related mobile applications shows a recognized potential and need for mobile healthcare services and presence of technologies that can be used for their implementation and delivery. At the same time the lack of their integration with other services in hospital information systems outlines the requirement for further research work and existence of what design science research framework calls business needs.

1.2.2 Objectives of a solution (research questions)

In the initial phase of the research work conducted in this dissertation the main goal was to identify what is state of the art in mobile healthcare application development and what are the key factors and requirements influencing successful implementation, adaptation, and deployment of mobile services in the healthcare sector and how they can be addressed. As noted before, some previous work on the CONNECT projects was performed to give a short overview of the problem space in the context of this specific project [26]. However, to gain a better additional understanding and more thorough knowledge of the current state of the research field of development and deployment of mobile services in healthcare in general, a literature survey was performed at the beginning of this research process. The goals of the survey were to: (1) identify technologies used today for development of mobile healthcare services, (2) identify advantages and disadvantages that different technologies offer and how they are suited for healthcare service delivery, (3) identify which technological approach is best suited for development of the research artifact in this research process, and (4) identify the main challenges and research issues that must be addressed when developing and integrating mobile services in healthcare information systems as well as their correlation, and based on these findings refine the objectives for the next phases of the research process previously defined by the project description.

The literature survey results were published in Paper I under the name "Review of projects using mobile devices and mobile applications in healthcare" [34]. The literature survey also identified numerous projects introducing mobile services in different healthcare areas, confirming a recognized potential of mobile healthcare services and the existence of business needs. The survey presented the possible technologies that were used for development of mobile healthcare applications. Through a review of other projects and their results and experiences, different technology approaches was evaluated and the appropriate technology approach for the specific problem space in the context of CONNECT systems was selected.

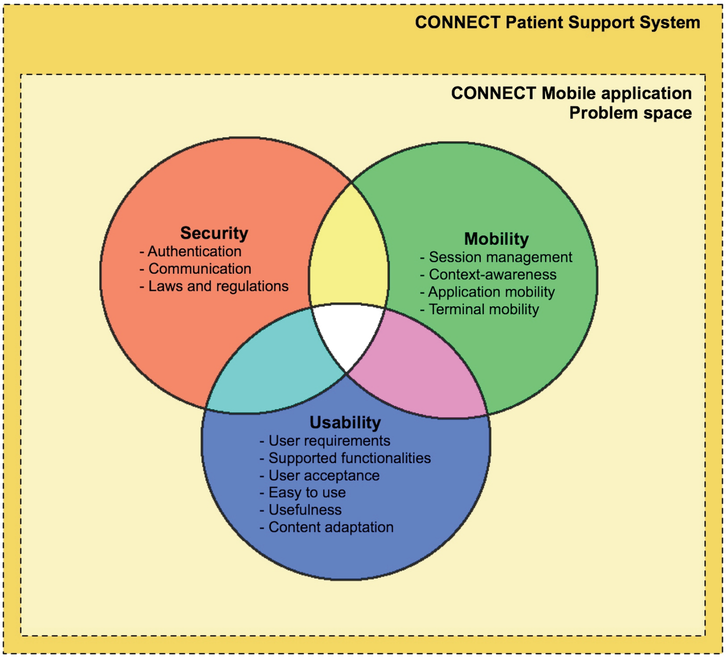


Figure 4. Graphical presentation of the research objectives in the context of development and deployment of CONNECT Mobile application

Additionally, some of the main development and deployment issues were identified through a survey (e.g., security, usability, user acceptance, mobility, training, cost, and organizational and legislation issues [1, 33, 35]). The research project specification defined the three main research issues: usability, security and mobility that are main the topics of this dissertation. Since the goal was to address these three identified research issues through the phases of the single research process and development of one main research artifact (the CONNECT Mobile application introduced below) they needed to be addressed in relation to each other, rather than in isolation. When addressing challenges introduced by one research issue other research issues must also be indirectly considered and addressed. Figure 4 shows a graphical presentation of these three research issues in the context of development and deployment of mobile services in the CONNECT patient support system. The Figure also presents the specific challenges related to the main research issues identified and addressed through the research work presented in this dissertation.

Based on previously defined research issues and their identified correlation, the knowledge gained through the survey, and previous research work that discussed the specific problem space in [26] the research questions are further refined to the following key objectives:

Research Question 1. What are the main functionality and user interface requirements for developing user-friendly, adaptable and well-accepted applications that enable the patient's mobile access to a patient support system such as the CONNECT system?

Research Question 2. What are the security requirements for enabling secure mobile access to a patient support system such as the CONNECT system, and how can they be properly met without compromising usability of the system?

Research Question 3. What is the best approach for enabling seamless and context aware access to patient support system such as the CONNECT system over different types of terminals and access network on secure and user friendly manner?

Each of these research questions is addressed through research work described in the papers contained in the dissertation. The Research Question 1 related to development of user-friendly and useful mobile application is addressed in the Paper II "Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management" [36]. The Research Question 2 related to enabling secure and user-friendly mobile access is addressed in the Paper III "Secure Solution for Mobile Access to Patient's Health Care Record" [37]. The Research Question 3 related to enabling user-friendly, secure, and seamless access to CONNECT system adapted to current context of use is addressed in the Paper IV "A framework for the development of ubiquitous patient support systems" [38].

The research work performed in the dissertation is limited to studying the provision of mobile access to services implemented in the CONNECT patient support system that is deployed as part of the hospital information system. The presented work does not address issues related to the development and deployment of the whole CONNECT patient support system and its functionalities. Through the research process described in the dissertation, the goal was to investigate how mobile access to such systems can be implemented to increase the availability, mobility, and usability of the patient supported system, and to research how new challenges can be properly addressed. The research questions regarding the development of the underlying patient support system functionality, integration and communication with other parts of the hospital information systems, content selection, adaptation and quality control, as well as influence on patient health and recovery are addressed in other research works conducted as part of the larger study [3, 20, 26, 39, 40].

1.2.3 Design and development, demonstration and evaluation

The defined research objectives are addressed through the process of building and evaluating the key artifact namely the CONNECT Mobile application. Each of the main research objectives is addressed through a single IS research process (or design cycle) described in the design science research framework using the following phases: Develop/Build and Justify/Evaluate. For different IS research processes different methodologies and foundations from the knowledge base for previous and related work, were used to address the defined objectives. More description and discussion of the specific methods used and contributions gained through design and development, demonstration, and evaluation phases is given in the next chapters. Each of the research processes is also described in detail in the research papers contained in this dissertation [36, 37, 41].

Chapter 2: Overview of the theoretical background

This chapter outlines the relevant theoretical background and explains the main concepts used in the presented work.

2.1 Usability

The standard for ergonomics of human-system interaction [42] defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use". In other words, usability is the measure that shows how user interface fits the user's requirements and how easy it is for the user to use it.

Different usability definitions and standards define usability in different usability components. For example, Shackel in [43] defines usability in terms of effectiveness, learnability, flexibility, and attitude. Jordan in [44] defines usability as guessability, learnability, experienced user performance, system potential, and re-usability. In the previously mentioned standard for ergonomics of human-system interaction [42] the main usability components are effectiveness, efficiency, and satisfaction. One often used definition is given by Nielsen [45] and Shneiderman [46], where usability is defined in five quality components:

Learnability

Learnability of the system design shows how easy it is for the user to perform the main system functionalities the first time that he/she uses it.

Efficiency

Efficiency of the system design shows how quickly the user can perform the system functionalities once he/she has learned the basic system design and become familiar with it.

Memorability

Memorability of the system design shows how easily the user can start using the system again after a period of not using it.

Errors

This component shows how often the user makes errors while using the system functionalities, how serious these errors are, and how easy it is for him/her to recover from the performed errors.

Satisfaction

A satisfaction component shows how pleased the user is with the system design.

Due to the development of new technologies that have the ability to support people in their everyday activities and their wide acceptance, Preece, Rogers and Sharp [47] have additionally identified advanced usability goals in addition to the general usability goals. According to them, the main usability goals are: easy to learn, have good utility, are safe to use, are effective to use, are efficient to use, and that is easy to remember how to use. The advanced usability goals (that describe users' experiences when using the system) are: satisfying, enjoyable, entertaining helpful, motivating, aesthetically pleasing, supportive of creativity, rewarding, emotionally fulfilling, and fun.

Different definitions of usability introduce many different usability components and goals. It is important to understand the difference between different usability components, and bear in mind that not all of them apply to all types of the interaction systems. Which usability requirements and goals that are most important in one system, depends on the type of the system, the context in which it is used, the functionalities it implements, and the types of potential users [47]. When the usability requirements that are most important in one system are identified, they are usually formulated in the form of questions. In this manner usability goals are turned into usability criteria that are then used for assessing the usability of a system in terms of how it can improve a user's performance. Some examples of usability criteria are: time to complete the task (efficiency), time to learn a task (learnability), and the number of errors made when performing a given task over time (memorability).

2.1.1 Usability evaluation methods

Numerous usability evaluation methods are widely used today for identifying end-users requirements and developing highly user-friendly systems. Different evaluation methods can be used in different situations, and the choice is usually closely related to: usability criteria identified for the system, the phase in the development process, and the type of participants available for evaluation process.

Not just end-users can be involved in the design process. Multidisciplinary experts and various stakeholders in the system (e.g., software developers, usability experts) can also give valuable contributions to the system development. Several usability evaluation methods can be used to include different types of stakeholders in the different phases of application design and in the implementation process. The approach that is generally recommended is to use different evaluation methods during one system design and development process, with the goal of identifying and addressing the requirements of different stakeholders, and of more efficiently creating a system that is highly effective and user-friendly [48, 49].

The following are short descriptions of some types of evaluation methods.

Usability testing

The usability testing process involves recruiting potential users and asking them to perform a carefully prepared set of tasks on the actual or prototype interface while measuring the typical user's performance (e.g., reaction times, behaviors, and errors) [47].

Interviews and Questionnaires

Interviews and questionnaires are usually used to assess users' subjective satisfaction and possible problems, which are generally hard to measure using objective methods. They are also particularly useful for studying how users use the system and which are the parts of the system they most like or dislike [45]. Interviews and questionnaires are considered as indirect methods, since they do not involve rating the user interface but rather the user's opinions about the interface. Therefore they are usually used together with usability testing, where results gained from both methods are merged and interpreted together. In the literature different types of standard usability questionnaires can be found that can be used to measure user satisfaction. These types of questionnaires provide many advantages to practitioners, such as objectivity, reliability, and scientific generalization [50]. The most widely used standardized usability questionnaires are: System Usability Scale (SUS) [51], Questionnaire For User Interaction Satisfaction (QUIS) [52], Computer Usability Satisfaction Inventory (CUSI) [53], and Software Usability Measurement Inventory (SUMI) [54].

Focus groups

Focus groups are considered a more informal technique and they are usually used before the interface is designed or after it has been in use for a period of time in order to identify the users' needs and requirements [45]. A focus group session is usually semi-structured, where the moderator typically follows a previously prepared script. However, group discussions and interactions between participants are encouraged. In this manner, users are able to develop and express an opinion within a social context and this is the main advantage of this approach over others.

Cognitive walkthrough

A cognitive walkthrough consists of simulating a user's problem solving process at each point in the system design where human-computer dialog is performed [55]. The cognitive walkthrough is developed for interfaces that are intuitive and where users could learn them by browsing, but can also be utilized for interfaces requiring intensive training of users [46]. It is usually performed by experts, but results are commonly discussed in group meetings with future users, designers, and developers to initiate discussion and a joint problem solving process [46].

Heuristic evaluation

Heuristic evaluation is performed by reviewing the system design according to predefined rules and guidelines, and identifying interface elements that do not comply with these defined rules so that they can be modified and adapted through an iterative design process [45] [47]. Heuristic evaluation is usually performed by design experts, but the evaluation can be also performed by some application domain experts with usability experience to gain even more valuable and effective feedback [56]. In the literature it can be found both generic heuristics that can be used for different types of system design (e.g. [55]) and more specific heuristics that are adjusted for one type of terminal and/or system (e.g., [47], [57]).

2.1.2 Participatory design

Participatory design is a system design approach where different stakeholders of the system are actively involved as full partners in a cooperative design process, with the goal to develop systems that are useful for end users, and meet their requirements. The method also aims to ensure that the system under development fits in the context and situation of how the system is to be used [58]. By involving users in the design process, the goal is not to fit users in as one additional component to an existing system development process, but to introduce new techniques and practices that can be used to facilitate a collaborative design process between different parties. However, a challenge present when using participatory design methods is how to resolve different views of problems or solutions by different users and user groups, and who should be chosen to have their logic represented in the overall system design (especially if the system is intended to be used by a large group of users with very different interests) [59, 60].

In participatory design, different methods can be used to enable cooperation and better understanding between different players in the design process. Some of the most frequently used methods are: cooperative action in order to understand the system and the users needs instead of a formal description of the system, mutual learning between users and system designers and developers, utilization of tools in the design process that are familiar to the users, a description of future work situations, and starting the design process with an understanding of the current practice of users [58]. Some of the techniques that can be used in this process are: *workshops* where different stakeholders can brainstorm about their current knowledge and practices and discuss how current system usage scenarios can be optimized and improved; *mockups* and *prototypes* as a low level and high level system presentation that can be used to envision system characteristics and help in choosing different directions for further system development; *contextual interviews and user observations* supported by video and audio recording can be used to gain more understanding about different aspects of the system and its context of use and to develop a shared understanding about system functionalities [58, 61, 62].

2.2 Security

In general, security means preserving and protecting property or interests from intrusions [63] [64]. The main principle used to achieve this is to restrict access to the specified resources, and allow access only to trusted parties that are able to prove their identity. Given this definition, security is based on these main issues.

Authentication: ensuring that the provided credentials from the user are in order,

Confidentiality: prevention of unauthorized disclosure of information,

Integrity: prevention of unauthorized modification of information,

Availability: prevention of unauthorized and unwanted withholding of information or resources.

Since the work described in this dissertation is based on authentication of the user for mobile healthcare services, further text will describe the theoretical background of authentication mechanisms in more detail.

2.2.1 Authentication

As a prerequisite for enabling access to any system that contains private information it is required that the user is identified and authenticated. Through identification the user announces who he/she is, and through authentication the user proves who he/she claims to be. In order to perform user identification, some type of unique user identifier, such as a username or user ID number, is required. When it comes to performing a user authentication process some of the traditional approaches used are:

Something a user knows (the user has to know some “secret”, e.g. password or PIN number),

Something a user holds (the user has to have a physical token, e.g. One-Time Password (OTP) generator or identification card)

Something a user is (utilization of biometric schemes that use unique physical characteristics of a person, e.g. a fingerprint reader or face scanner),

Something a user does (the user performs some mechanical tasks that are repeatable and specific to the user, e.g. signature or gait),

Where a user is (the user is authenticated based on his/her location).

Each authentication mechanism can provide different levels of security. The level of security implemented through a specific authentication method can depend on: the characteristics of the specific security mechanism implemented (e.g., length of the password, the type of token, or sensitivity of biometrics system), the user's understanding and acceptance of the authentication mechanism (e.g., how the user manages his/hers passwords, where the user keeps security tokens), and the characteristics of the information system that deploys a specific authentication mechanism (e.g., how data are managed inside of the system). In order to provide a higher level of security multiple mechanisms can be combined, and this type of authentication is called multi-factor authentication.

When authentication is performed successfully the user can be granted or denied access to the requested resources based on the security policy implemented in the system. How the security policy will be defined and which security mechanisms will be implemented in one system can vary, and are mainly related to the type of information system and sensitivity of the data stored in the system.

2.2.2 Security standards and regulations regarding personal health data

National and international laws and regulations specify various aspects of security in healthcare computer systems. Different security requirements and regulations are used in different countries, and this situation results in very difficult integration between healthcare information systems and a lack of standard and widely accepted security solutions. In theory, introducing regulations that apply for different countries, like the European Union Regulative, can reduce this diversity. However, federal security regulations today usually delegate certain regulatory authority to its member countries, thus requiring additional local regulations that may have to be taken into account when ensuring security and privacy of sensitive medical information as described below in the case of The European Union regulations [65].

Some of the standards and regulations most relevant for security and privacy protection in healthcare information systems and services are described in the following sections.

ISO standards

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) defines in the ISO/IEC 27000-series standard rules and best practice recommendations on addressing information security risks, management, and control [65]. The ISO/IEC standards define fundamental requirements and implementation guidelines and principles for the development of information management systems [66]. The most important standards related to the development of healthcare information systems are: (1) the ISO 27799:2008 standard (Health Informatics - Security management in health) which describes guidelines for design and development of health sector specific information management systems [67] and the ISO/TR 27809:2007 standard (Health informatics - Measures for ensuring patient safety of health software) which provides control guidelines for ensuring patient safety within healthcare information systems [68]. Some other standards related to security management in healthcare information systems are: the ISO/TS 22600-2:2006 Health informatics - Privilege management and access control that is developed with the goal to provide support for implementing rules and protocols for sharing healthcare information between various healthcare providers and organizations, health insurance companies, their patients, staff members and trading partners [69], and ISO/TS 13606-4:2009 Health informatics -- Electronic health record communication - Part 4: Security that describes a methodology for specifying the privileges necessary to access data from EHR [70].

Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)

HIPPA is a US law designed to establish standardized mechanisms for providing security and confidentiality of all healthcare-related data [71]. It consists of two main sets of rules known as the privacy and security rules. HIPPA privacy rules define how health information should be properly used and disclosed, and ensures the flow of health information required for provision of quality care [72]. HIPPA security rules define a set of security standards for protection of health information in electronic form during storage and transfer [73].

The HITECT Act sets more stringent regulatory requirements under the security and privacy rules of the HIPAA Act, and provides legal liability for non-compliance with HIPAA requirements. Additionally it addresses the issues related to notification of breaches and the access to electronic health records [74].

The European Union regulations

In Europe there are numerous rules and legislations regarding the handling of medical data, due to the different sources of regulation (a regulation authority can be the European Union, as well as the legislation of the member states) [65]. The European Union issues directives that describe in general how medical data should be protected, and the directives than have to be implemented into national law by each member state. The most important directives addressing protection of personal (medical) data are:

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data – This directive describes the minimum requirements that must be guaranteed when processing personal data [75]. Some of the requirements set by this directive are: (1) The user of the system must give consent before private data are allowed to be processed and he/she has the right to know all details related to processing activities, (2) The private data must be protected against "accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access", (3) The security mechanisms and measures implemented to protect private data must be "appropriate to the risks represented by the processing and the nature of the data to be protected", and (4) The service provider must inform the national authority in charge of supervision about planned processing of private data before the process is started [76, 77].

EU Directive 2002/58/EC (Directive on privacy and electronic communications) – The directive complements the directive 95/46/EC and addresses issues related to the protection of privacy when processing personal data using new telecommunication technologies [78]. Some of the main requirements set out in this directive are: (1) The service provider must provide confidentiality and integrity of private data and define and deploy the appropriate security policies that enable protection of data during processing, (2) The service provider must inform the users of the system if a breach occurs and explain the possible risks and measures, (3) All member states must define national legislations stating that confidentiality of private data is assured, (4) The private data must be destroyed or made anonymous after processing is finished and they are no longer needed [78].

Norwegian regulations

In order to regulate security and privacy issues in the healthcare sector in Norway, specific acts and regulations are defined in accordance to regulations set by European Union (more specific Directive 95/46/EC and EU Directive 2002/58/EC introduced previously). The Norwegian Data Protection Authority or Data Inspectorate (Datatilsynet) is an independent administrative body under The Ministry of Government Administration, Reform, and Church Affairs which is in charge of enforcing legislation regarding personal data, and ensuring "that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life, and to ensure that personal data are of adequate quality" [79]. Some of the most important regulations are:

- The Personal Data Act [80],
- Personal Data Regulations [81],
- Regulations on the use of Information and Communication Technology [82],
- The Personal Health Data Filing System Act [83],
- The Health Personnel Act [84],
- The Act relating to Patients' Rights [85],
- Code of Conduct for information security in the healthcare, care, and social services sector ("The Norm") [86].

2.2 Security

The introduced regulations define several requirements for providing security and protection of private (healthcare) data defined as sensitive data per se. The summary of acts and regulations and their sections that address security issues related to private (medical) data is outlined in Appendix 1 of the dissertation. The key security requirements can be summarized as follows:

- Personal data may be processed only if the processing satisfies certain conditions (e.g., data subject gives his/her consent, it is necessary to protect person's interest but he/she is incapable of giving personal consent, data are previously made public by data subject).
- All systems processing personal sensitive data must implement security measures to protect sensitive data against confidentiality, integrity, and accessibility threats.
- Integrity and confidentiality of personal data must be protected using encryption mechanisms, strong authentication or by other means during transmission beyond the physical control of the service provider.
- Appropriate techniques for identification, authentication, and authorization must be employed as part of security mechanisms protecting the information system to prevent unauthorized access to sensitive data.
- The service provider must define an acceptable risk level associated with the processing of personal data, and carry out a risk assessment with the goal to determine the probability and consequences of a breaches of security, and the risk level for each threat. The risk level is determined by combining the probability and consequence of the threat. The security measures must then be defined and implemented according to the probability and consequence of breaches of security compared to an acceptable risk level. The Data Protection Authority may issue additional orders regarding the protection of personal data.
- The service provider must implement security mechanisms in order to detect any attempt of system misuse (e.g. tamper-proof logs). All use of the system must also be logged.
- The service provider must physically protect the equipment, system, and information against damage, misuse, unauthorized access and modification.
- The service provider is allowed to transfer the personal data only to external systems that satisfy all set requirements.
- The personal data should not be stored longer than required, and if there is a need for storage in longer periods the data must be properly anonymized.
- All security measures implemented in the information system must be documented.

The presented regulations define security measures that must be in place when providing a person with access to private and sensitive (medical) information. However, in the acts and regulations it is not defined which security mechanisms must be used to provide the required protection and which level of security must be provided. Thus, the Norwegian government introduced additional requirements for implementing electronic services in the public sector, according to inter alia Code of Conduct for information security in the healthcare, care, and social services sector or “The Norm” [86]. Related to security of authentication mechanisms, four different security levels are defined for the protection of personal data, and it is described which level must be implemented for services processing different types of information. Protection of applications and services in the public sector processing sensitive personal information, such as health information, require implementation of security mechanisms of the highest security level (also called “Person Høy og Virksomhet”), which require authentication systems based on Public Key Infrastructure (PKI) or an equivalent security level. The PKI based security solution must meet defined requirements for user authentication and identification, signature, and encryption [87]. The service provider of each PKI solution considered to be on the highest security level must submit a self-declaration voucher to the Norwegian Post and Telecommunications Authority claiming and substantiating that the requirements defined by The Ministry of Government Administration [88] are met. The Norwegian Post and Telecommunications Authority publish a list of providers they believe fulfill the requirements.

The next section will focus on describing current authentication mechanisms currently available in Norway that are accepted as being secure enough for providing access to sensitive (medical) data.

2.2.4 Secure authentication mechanisms in Norway

Today, two authentication mechanisms are approved for the highest security level in Norway [89]. One is the Buypass solution [90] that uses a smartcard with a stored BuypassID identifier based on a PKI certificate. The second system is the Commfides solution [91] that delivers a private key to each user which can be used for authentication, signing, and encryption on CD media. Both solutions provide certificates on a specific authentication device and, for now, do not support storage of the certificates on mobile phones. The Buypass solution today supports registration of the user’s phone number and relates it to the specific smartcard with stored credentials [92]. The Buypass mobile authentication system is acceptable only for lower security levels of authentication (not approved for person sensitive data), since with the Buypass mobile authentication system the user is not authenticated by using the BuypassID, but just by using the regular username/password authentication that is not based on the PKI.

An authentication method that is not approved for the highest security level for access to personal health information but is very popular and well accepted in Norway is the BankID solution [93]. BankID is a personal electronic identity used for secure identification and signing on the Internet used by the majority of banks in Norway. The BankID system has a version for mobile phones called “BankID for Mobile” in addition to the PC-based version. In “BankID for Mobile”, the user’s private information is stored on the SIM card of the mobile phone where it is protected against modification and unauthorized access [94]. In this solution the mobile network operator manages and stores the user credentials needed for user verification in the SIM card, and authentication in the terminal is done using a SIM Application Toolkit and not integrated with an application in the terminal. For this security mechanism to be utilized in the public sector, a Service Level Agreement (SLA) must be established between each public institution using the service and each mobile network provider (since a key part of the user credentials needed for access resides in the SIM card provided by mobile network operator). In the SLA, all parties must agree to all required security policies and measures that should be implemented in order to protect users’ accounts and login credentials. One disadvantage of this approach is the fact that currently only one network operator in Norway supports “BankID for Mobile” (Telenor) and the users must use BankID issued by a specific bank. This is not acceptable for a public information services, since a main prerequisite for an authentication solution used for providing public sector services, and healthcare information services in particular, is its ability to enable access for all potential users [85]. Recently, BankID Norge launched a mobile application that enables mobile phone and tablet users to perform authentication for services using mobile web browsers. When the authentication process is started from a web browser, the BankID application is automatically activated and user authentication is taken care of by the application. When the authentication has finished successfully, the user is redirected back to the mobile web browser and can access the requested services. This mobile authentication system has so far had limited deployment (only one service provider has implemented this service until today) and currently only supports iOS devices.

Today there is no authentication mechanism that is approved for the highest security level in the public sector, and adjusted for use on mobile phones. The closest solution we found is “BankID for Mobile”, which stores users’ credentials on the SIM card, and a new service launched by BankID Norge recently that is still in early deployment stage. However, these solutions are not officially approved for the highest security level and introduce additional issues that must be addressed (operator lock-in, bank dependency, and support for a limited number of users/devices).

2.3 Mobility

The word mobility can be defined as the movement of people, changing location or changing roles. Mobility as such is not in itself a service offered by a system because mobility has no value for a user if not combined with other services. As a result, mobility is rather defined as a capability of the system that can be added to any network system.

2.3.1 Levels of mobility

Mobility of the devices could be viewed at different levels of granularity. The three main levels of mobility described by Dixit Prasad [95] are:

Macro mobility

Macro mobility addresses issues when nodes move globally, or to another domain (inter-domain mobility). On the macro mobility level there are fewer handoffs, and communication is not seamless (ongoing transmission is interrupted and the communication channel must be reconnected). There are two standard approaches for addressing macro mobility issues: one is on the transport or application layer and the other is on the network layer. When using the transport or application layer approach every application must be aware of the mobility of the terminal to support session continuity. One example of handling macro mobility issues on the application layer is Session Initiation Protocol (SIP) [96]. When using the network layer solutions, additional services from the network layer are used to handle session management and the end application can be kept unaware of the mobility issues. An example of the network layer approach is the Mobile IP standard [97].

Micro mobility

Micro mobility addresses issues when nodes move in one single administrative domain (intra-domain mobility). Micro mobility is usually performed in smaller geographical areas, and handoffs are more frequent, faster, and seamless. Micro mobility issues are usually addressed on the link layer (for example, cellular networks, such as GSM and UMTS, have their own micro mobility handling mechanisms implemented).

Ad hoc mobility

Ad hoc mobility addresses mobility issues in the infrastructure-less collection of communication devices. In the ad hoc network all the network intelligence is situated in the devices that make up the network, and the mobile devices do not only act as hosts but also as a routers [95]. In ad hoc networks, mobility of the devices causes constant changes in the network topology and communication is frequently established through a number of nodes (multi-hop communication). One example of utilization of an ad hoc network is the Personal Area Network (PAN). A PAN is a group of interconnected devices within the range of an individual person (typically within a range of 10 meters) [98]. The PAN networks are gaining popularity today, and much research is done to address challenges and requirements for their deployment in different utilization areas (e.g., business, learning, and healthcare).

2.3.2 Mobility types

There are several types of mobility, and different literature and standards such as IETF and ETSI uses different definitions and meanings for the different types of mobility. The following discuss definitions of different mobility types and define the mobility terms that are used throughout the dissertation. The ETSI TEDDI database and the IETF RFC database are used as references.

Terminal mobility

IETF RFC3753 "Mobility Related Terminology" defines terminal mobility to be the same as host mobility, or "the function of allowing a mobile node to change its point of attachment to the network, without interrupting IP packet delivery to/from that node" [99]. European Telecommunications Standards Institute in [100] define terminal mobility as "1) The possibility of geographically moving a terminal, from which different TCP sessions have been established, and maintaining those sessions irrespective of the terminal move (or in other words, without the need for releasing those sessions due to the moving of the terminal); 2) The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal". The same standard also call this session mobility. In this dissertation we define terminal mobility as allowing the terminal to change its point of attachment to the network while maintaining all services on the same terminal.

The process that occurs when the mobile terminal change its point of attachment to the network is called handover [99]. Different types of handover are defined in the literature and meanings of definitions are not always the same. In the next part we give some definitions of main types of handovers.

Vertical handover is according to European Telecommunications Standards Institute handover across heterogeneous access networks [101, 102]. IETF RFC 3753 defines vertical handover as mobile nodes moving between access points of different type, such as, UMTS to WLAN, and it may or may not be noticed at the IP layer [99]. This dissertation defines vertical handover as mobility across network technologies.

Horizontal handover is according to European Telecommunications Standards Institute handover within homogeneous access networks [101, 102]. IETF RFC 3753 defines horizontal handover as mobile nodes moving between access points of the same type (in terms of coverage, data rate and mobility), such as, UMTS to UMTS, or WLAN to WLAN, and it may or may not be noticed at the IP layer [99]. This dissertation defines horizontal handover as mobility within the same network technology.

Inter-domain (or Inter-Access Network) handover is according to European Telecommunications Standards Institute generally the same as vertical handover, handover across heterogeneous access networks [101]. According to IETF RFC 3753 Inter-Access Network handover is "a handover where the MN moves to a new Access Network" [99]. In this definition since domain is changed this type of handover involve the assignment of a new IP access address to the mobile node, and it require support for macro mobility management. This dissertation defines inter-domain handover as mobility across access networks and involve IP address change).

Intra-domain (or Intra-Access Network) handover is according to European Telecommunications Standards Institute generally the same as horizontal handover, handover within homogeneous access networks [101]. According to IETF RFC 3753 Intra-Access Network handover is "a handover where the MN changes Access Routers inside the same Access Network" [99]. In this definition this type of handover is not necessarily visible outside the Access Network, since the mobile node is preserving the IP address, and it requires only micro mobility management. The only change it can result is in the routing paths. This dissertation defines intra-domain handover as mobility inside one access network.

Session mobility

European Telecommunications Standards Institute define in [103] session mobility as a "network ability that enables a user to maintain an active session while switching between terminals or changing to another subnet or access network". In the IETF definitions, discussing of session mobility session mobility involves changing of terminals. As an example, in [104] it is stated that "session mobility involves both transfer and retrieval of an active session. Transfer means to move the session on the current device to one or more other devices. Retrieval means to cause a session currently on another device to be transferred to the local device. This may mean to return a session to the device on which it had originally been before it was transferred to another device". In [105] session mobility is defined as "the ability for a communication session to be moved from one device to another under the control of the user". In this dissertation, we define session mobility as the transfer of media and context information of an ongoing communication session from one device to another.

Application mobility

According to Victor Charles Zandy [106] application mobility is the ability for an application to travel with its user, moving between computers or moving with a computer between locations. Thus, terminal mobility and session mobility has many similarities with application mobility. Bardram and colleagues introduce a similar term "application roaming" as the "alternation between multiple devices an be done 'on-the-fly' by moving a task from one device to another in a fast pace" [107]. In this thesis, we regard application mobility, application roaming and session mobility as synonyms and defined as transfer of media and context information of an ongoing communication session from one device to another.

Chapter 3: Usability, Mobility, and Security in mobile healthcare applications

This chapter presents short summaries of each paper and gives a brief discussion about the contributions and limitations of the performed research. Additionally, as part of the presentation of the paper I, the updated literature overviews are added.

3.1 Paper I: Review of projects using mobile devices and mobile applications in healthcare

Summary: In the paper the results of a literature survey of projects that research the development and deployment of mobile applications and devices in healthcare are described. The goal of the review is to show which technologies can be utilized for the development of mobile healthcare information services and what are the main challenges influencing their wide acceptance and utilization in everyday healthcare delivery. Mobile applications and devices for both patients and healthcare providers are taken into consideration. The review covers all projects found in the literature, both from developed and developing countries. An electronic search was undertaken of the relevant scientific library databases (IEEE Xplore and ACM Digital Library) as well as a manual search of the reference sections of relevant articles for related topics and reviews of the literature. The search was performed using keywords such as “mobile”, “application”, “service”, “health”, “healthcare”, “usability”, “usability testing”, and “security”, and their combination depended on the search topics (mobile applications and services in healthcare, usability, and security). Quality assurance of how to identify the most important papers was done by identifying the most cited papers and reviewing references of all papers that appeared in the different search topics.

Our literature survey paper provides an overview of the projects that use different technology approaches to deliver healthcare services to end-users. A preview of the performed clasification is given in Table 1. The first group of projects develops new mobile devices and specific applications implementing required functionalities adjusted to the characteristics of the new device. The projects in the second group use standard mobile devices and mobile services available on them (such as voice calls and SMS messages) for delivering healthcare services. The last group of projects develops specific applications that perform required functionalities and run on legacy devices.

3.1 Paper I: Review of projects using mobile devices and mobile applications in healthcare

Table 1. Classifications of the projects introducing mobile devices and services in healthcare [34]

	New device	New application	Based on legacy mobile services
Specific mobile devices with a custom application	Yes	Yes	No
Standard mobile devices and legacy mobile services	No	No	Yes
Mobile applications for legacy mobile devices	No	Yes	No

The paper additionally reveals the related work that address existing challenges for development, deployment, and integration of mobile services in healthcare information systems, and gives a short discussion with focus on two main challenges namely security and usability by presenting projects addressing these key requirements. Finally, it briefly describes the CONNECT project, its characteristics and plan for mobile service development, combining terminal adaptation, ease of use, and security.

Contributions: The main goal of this paper is to give an overview of the current situation and future trends in research, implementation, and deployment of mobile services in healthcare. The review shows how different projects utilize different technologies to fit different contexts of use and different usage scenarios. Advantages and limitations of each technology approach is additionally discussed to identify what is the best technology to be used for development of the CONNECT Mobile application (the main research artifact in this research project). The conclusion was that creating dedicated mobile terminals for healthcare services does not scale, while using only standard features such as SMS and voice calls is inadequate for advanced healthcare applications where user interaction is a key element. The technology approach that fitted this specific project and problem space best was developing a mobile application for standard mobile devices. The development of a native application is chosen over development of a mobile web site mainly because the native application can provide better support for adaptation of its design and functionalities to the specific device characteristics, functionalities, and context of use, and it also enables utilization of standard features implemented on the phone itself such as camera or location services (a more detailed discussion related to development of natives application versus development of mobile web site and its adaptation is given in the usability literature overview in the next section). Java ME platform was selected as the targeted development platform since it provides support for creating a user-friendly and well-designed user interface that is easy to understand and manage, and it also supports the use of security features such as encryption and derstand and manage, and it also supports the use of security features such as encryption and HTTPS connection. Additionally, Java ME is a widely used developer platform supported on a wide range of standard mobile phone at the time of publication. The client has later been ported to iOS and Android, however this work is not part of the dissertation.

Besides a technology review, the work on the survey also revealed the open research issues that must be addressed when adding mobile services and devices to healthcare information services. Two research areas, usability and security, were identified in the survey as being most important and have been covered in more detail. The paper gives an overview of how usability and security are addressed in some of the projects identified in the literature review. The projects underlined the high importance of utilizing participatory design, and involving potential users in the application development process to ensure identification and implementation of system design and functionalities that comply with the user’s requirements. With regards to security, the most important factor is the existence of widely accepted and approved security mechanism adapted to mobile devices’ characteristics that guarantee high security and protection of privacy of personal data, and in the same time do not downgrade the usability and accessibility of the healthcare information services. When developing mobile services that manage sensitive patient data additional work must be done in complying with legislation on state and regional level, making sure that security mechanisms can be implemented according to the law. Gained knowledge of the current research work in this research field was afterwards used together with previous research work that discussed the problem space in the context of CONNECT Mobile application [26] to refine the research question and objectives for further stages of the research process (as described in the introduction of the dissertation).

Limitations: The literature review identified several requirements that must be considered when implementing mobile services, not just in healthcare, but also for general utilization (e.g., mobility of the user and service, limitations of the mobile devises and communication networks, compatibility with standards and technologies that are used in communication process, and control of the quality of the information that users access). However, only usability and security issues are discussed in more detail, while other issues are only identified and noted in the paper. Since the next three papers in the dissertation focus on the three main topics: usability, security and mobility issues for developing and integrating mobile service to the CONNECT system and their correlation, a more detailed literature review of related research work done in these research areas is added in the continuation of this section.

In the performed survey the projects are classified only by the technology they use to provide mobile services and by the main research challenges they address (usability and security).

3.1 Paper I: Review of projects using mobile devices and mobile applications in healthcare

The choice to perform this specific organization of the projects is guided by the main requirements in this phase of the research process: to identify the best suited technology for development of the CONNECT Mobile application and to research how different research issues (security and usability) are previously addressed in the related research work. No additional classification of projects based on other characteristics is performed (e.g., types of service, effect on user's health condition, user acceptance, and cost efficiency). Examples of other types of surveys can be found in literature (e.g., [2, 108-110]), however these topics are currently outside of the research areas addressed in this dissertation.

In addition to the first three groups of projects using different technology approaches for delivering mobile healthcare services reported in the paper, mobile devices connected to the sensor network were also identified. Due to paper size limitations and the CONNECT project characteristics and defined problem space, a description of this type of projects was not added to the original paper. However, the potential of sensor technology for development of mobile healthcare services with advanced patient monitoring and context adaptation features is shortly discussed in the final chapter of the dissertation.

3.1.1 Additional literature overview

Since the literature review described in this paper was performed at the beginning of the research project, in this chapter a new literature overview for each main research issue that is addressed in the next papers (usability, security, and mobility) is presented. Literature overviews mainly present general research work addressing the main challenges in the context of development and utilization of mobile devices and services. However, we also try to keep the main focus on mobile healthcare services since they are the main topic of this dissertation.

Usability literature overview

One of the conclusions of the literature overview presented in the survey paper [34] was that the best solution for developing a research artifact in this research project is by developing a dedicated mobile application for legacy mobile devices, since the mobile application can implement advanced functionalities and the user will be able to use a mobile device he/she is already familiar with. Due to this reason, the presented literature overview is focused on the related research work addressing issues and challenges when it comes to developing user-friendly, useful, and well-accepted mobile (healthcare) applications for legacy mobile devices.

Two general approaches can be used for developing applications for standard mobile devices: the development of a web site that is accessible over a mobile web browser, and the development of native mobile application. The development of (mobile) web sites enables easy deployment over a wide range of terminals since standard mobile browsers are used for accessing the application. Recent research can be found discussing weather websites should be adapted to the limitations of the mobile terminal (e.g., small screens, limited input features). Maurer and colleagues in [111] argue that new hardware and interaction techniques such as multi-touch gestures can enable a more effective way of browsing the original websites, and that limiting full web sites and their functionalities to fit to mobile devices is not necessary required. On the other hand, Schmiedl and colleagues show that mobile websites adapted to the limited characteristics of mobile devices are still highly important and highly appreciated by users, however special care must be taken to understand the mobile usage scenarios and optimize the site functionality in the right manner [112]. The usability studies done by Nielsen proved the great value of mobile web sites and conclude that “a specific mobile site is a must” [113]. The results of the usability studies show that even when a web site is adapted for use on mobile devices, user performance is even better when using native mobile applications [114]. The main reason for this is the fact that only limited optimization is possible during website design, while native application can be adjusted to the specific limitations and abilities of each individual device. Additionally, the development of a native application enables utilization of device’s specific features (e.g., camera, microphone, location services). The shortcoming when choosing the native mobile application approach is much more development and maintenance work since the development process must be done for each mobile platform. Recently different cross-platform development tools that can be used to provide easier development of a single native mobile application that is compatible for running on different devices have started to emerge (e.g., [115-118]). Since these tools are still rather new and under development they have some unresolved issues (e.g., inconsistent support for different functionalities across different platforms, application performance speed) however we believe they will in future present good alternatives for more efficient development of more effective and flexible mobile (healthcare) applications.

Today most mobile applications developed as a version of a standard PC (web) application are adapted to the limited characteristics of the mobile devices. In the literature there can be found numerous different general rules and design principles on how to adapt a PC (web) application for use on mobile devices since these two terminals have very different functionality and design characteristics (e.g., [119-124]). However, the great variety of mobile devices and their characteristic makes development of standard applications that run on different devices and offers the same look-and-feel very difficult. Mobile device manufacturers, mobile platform manufacturers, and design standardization organizations have defined numerous rules and guidelines for development of mobile applications and their adaptation for use on different types of mobile devices with specific characteristics and features (e.g., [46, 125-131]). As a result, there can be found numerous mobile application design and functionality guidelines that often do not comply with each other and are more device and/or platform specific. Due to this reason, in the literature there can be found different projects that are working on adjusting the general design guidelines and rules and creating the new ones to address the design and functionality requirements set by specific types of services and context of use (e.g., m-commerce services, E-book applications, multimedia services, m-learning [132-135]). The design guidelines can be also found for development of mobile healthcare services. For example, Luckmann and colleagues define design requirements for developing handheld patient diaries to record a patient's pain experiences and provide information about pain, treatments, and functionality [136]. Palmblad and colleagues describe design requirements for developing handheld computer systems for the electronic collection of patient diary and questionnaire data in clinical trials [137]. Falchuk and colleagues outline visual development themes for design and interaction design in mobile healthcare [138]. Consolvo and colleagues show design requirements and general practices in order to encourage physical activity of persons [139]. Lorenz and colleagues define design guidelines in terms of the development of a mobile system for monitoring personal parameters for the elderly [140]. Siek and colleagues describe design guidelines for the development of personal health applications for older adults and their caregiver in order to manage prescriptions and medication intake [141], while Ahmad and colleagues note the interface design guidelines for designing mobile health assistant applications for elderly [142]. Liu and colleagues present design guidelines to support effective communication and promote social support for parents with high-risk infants [143]. Mendoza-Gonzalez and colleagues outlines the guidelines for design graphical user interfaces of mobile E-Health communities [144]. The majority of projects found in the literature are mainly focused in researching design and functionality rules for systems with specific functionalities (e.g., patient diaries and questionnaires, wellness application, personal parameters monitoring, patient medication intake management, E-Health communities) and they often target the specific user groups (e.g., elderly, parents of infant, women). Additionally, most of them are working on the development of stand-alone mobile application. However, the research work such as [145-148] are arguing that that the mobile application in the healthcare domain should not be seen as an alternative to the use of stationary desktop or laptop terminals, and conclude that the mobile applications should be developed rather as a supplement for desktop applications for providing access to valuable and context-adapted information in the different usage environment. Research work addressing integration of mobile application as part of the bigger and more complex healthcare information systems can be also found (e.g., porting a web-based cancer treatment prediction tool to a mobile device [149], development of a new e-healthcare system for depression treatment available over multiple access terminals [150], development of a universal platform for continuous patient health education [151], developing mPHR system for diabetics where mobile phone is used to upload health records and access their data over Internet [152], development of a multi platform system that enables interactive, structured, and multi-modal delivery of clinical advice and the authoring of such a content [153]). The related research projects focus on addressing system performance and functionality implementation and adaptation issues for special types of healthcare services and use cases (cancer prediction tool, depression treatment, diabetes management system), and none of them are researching design and usability guidelines related to development and integration of mobile services in already existing healthcare information services.

In the literature different projects can be found that are researching users' acceptance of mobile healthcare services. Some of the studies report very good acceptance (e.g., [154-156]), unlike others (e.g., [157, 158]). One of the main factors that have been identified to have a direct influence on the potential acceptance of mobile information technology innovations in healthcare is perceived usefulness, ease of use and the user's perception of technology design approach (especially navigation and data presentation) [159, 160]. The best way to ensure usefulness and user-friendliness' of the (mobile) application, besides following the proposed design guidelines, is to involve different system stakeholders in the application development process, and in this manner identify different end-user requirements and adjust mobile services design and functionality to users' capabilities, needs and expectations during the development process. The importance of involving different stakeholders and utilization of usability evaluation and participatory design method is also previously identified and discussed in the survey paper in the dissertation [34]. Some of the usability evaluation methods often used are: user needs assessment through workshops and focus groups with participants, usability testing using low-fidelity prototyping and high-fidelity prototyping, pilot field testing, structured and semi-structured interviews with users, expert reviews – cognitive walkthroughs and heuristic evaluations [136, 140-142, 161-164]. However, some of the research work can be found that is concluding that using just standard usability testing methods in the new context of a mobile application is not sufficient and that new and adapted usability evaluation methods must be developed. For example, adaptation of different standard usability testing methods is proposed to better suit mobile device characteristics and frequent change of usage context (e.g., workshops where end users were involved in mobile system design process through scenario building, role playing, and low-fidelity prototyping [165], conceptual framework for generating usage scenarios with specific focus on change of context of use when using mobile application [166], new techniques for development of mobile application low fidelity prototypes [167, 168], different methods for collecting emotional responses to evaluate mobile applications in mobile settings [169], and a contextual usability evaluation framework for a mobile computing environment [170]). Additionally, research work such as [133, 171, 172] is working on the development of methodologies, frameworks, and tools to facilitate and automate the process of design development and evaluation of mobile applications. The further development of standard and widely accepted evaluation methods adapted just for mobile applications and devices could help developers and researchers in future to more easily and efficiently identify user needs and expectations from the mobile applications and services (specially during a change of the usage context) and thus ease development of useful and user-friendly mobile applications.

Besides a variety of standard users, people with specific needs must be taken into consideration when developing mobile healthcare services (e.g., users with vision or motorical problems). In order to meet their special requirements, universal design methods are usually employed [173-175], and different projects today are working on development of general interface adaptation mechanisms for supporting users with special needs (e.g., [176-180]). Applying this knowledge to the mobile healthcare service could greatly influence wider user acceptance and utilization. Additional importance for adaptation of healthcare information services to user group with special needs is outlined by research such as [181, 182] that shows how treatment of different patients influences their ability to use an online healthcare system and which specific issues must be considered when developing healthcare information services. Perhaps the most important group of potential users of (mobile) healthcare applications is the elderly, and separate research area can be found that address design and development issues for the development of mobile healthcare information services specifically for this types of users and discuss the service adaptation needs due to the group's limited expertise in using new technologies and poorer cognitive and perception abilities (e.g., [183-191]).

Due to a great number of potential user groups of healthcare information services (the key objective of these services is to be available for all people) and their different characteristics and requirements, it can be very difficult to identify functionality and design requirements of one specific application that should match needs of all users. One approach to address this issue is described in research work such as [141, 190] that outlines that developing one single solution would not fit the needs of all users and recommends the development of different interface versions for different user groups. The disadvantage of this approach is that development of different user interfaces requires much more development and maintenance work, but enable easy adaptation of interface and functionalities to specific user needs. The other approach proposed by some of the found research work in the literature is implementing dynamic interface adaptation to different contexts of use and enabling users to perform modifications and personalization of the services before they start using them (e.g., [192-196]). While dynamic interface adaptation can provide more flexible interfaces and do not require development and adaptation of different application version, it requires implementation of specific context adaptation and management logic and can put additional requirement on user to do the final adjustments of the application before it can be used. Additional discussion about adaptation of (healthcare) services to various different contexts of use (not just type of users) can be found in the next section presenting "Mobility literature overview".

Since the research work found in the literature addressing issues related to integration of mobile application as part of the bigger and more complex healthcare information system is limited to special types of healthcare services and use cases and none of them outlines general design and usability guidelines, the research work presented in the paper II in this dissertation is performed with the goal to identify what design rules and guidelines should be applied when developing and integrating mobile application(s) to a patient support system such as CONNECT and adapting both the interface design and the system functionalities to a mobile device's limited characteristics [36]. By using different usability evaluation and participatory design methods (low fidelity usability testing, high fidelity usability testing, semi-structured interviews, heuristic evaluation) the users' expectations and requirements from the CONNECT Mobile application are identified and addressed, and the final version of the mobile application is evaluated by the group of potential users in the context of the whole CONNECT patient support system to investigate relation to other parts of the system (web application) and users' acceptance.

Security literature overview

Since the research work done as part of the dissertation is addressing mainly issues related to enabling secure and user-friendly authentication of the user when accessing mobile healthcare information services, this literature overview will present a short overview of different authentication mechanisms and current research related to their adaptation to mobile devices and a new context of use. At the end it is discussed in more detail multi-channel authentication mechanisms.

A most common approach to provide secure mobile access to mobile information services used in a majority of studies and projects today is to adapt and integrate standard authentication mechanism(s) (such as password authentication, token-based authentication, Public Key Infrastructure, and biometrics) into existing security architecture of the information system. Due to specific characteristics of mobile devices, some of the standard authentication mechanisms can be made more user-friendly for use on mobile devices than in the case for stationary computers. A good example is usage of mobile phones as authentication tokens when performing user authentication, since mobile phones are widely accepted as highly personal devices that people always carry. There are numerous research projects that propose using a mobile phone as an authentication token for accessing different services on stationary computers. For example, many systems use SMS messages instead of dongles and cards for delivery of One-Time Password (OTP) [197]. However, delivery of OTP over SMS introduces additional security issues since security of the OTP is based on the security of the SMS message, which is not guaranteed by cellular operators. Additionally, verification of the sender of the SMS message should be performed to provide verification that the sender of the message is authentic. Instead of sending OTP over SMS in clear text, recently several research projects propose developing and using mobile applications that generate OTP (e.g., [198, 199]). In this manner additional parameters (such as a mobile device identifier, a mobile phone number, or time stamp) can be used to provide more secure authentication over a second communication channel (multi-channel authentication is described in more detail in the next section). Moreover, new emerging technologies such as Near Field Communication (NFC) [200, 201], Quick Response (QR) codes [202-204], or Bluetooth communication [75, 205] can be used to make communication between mobile phones and stationary computers during the authentication process easier and more user-friendly. The disadvantage of the discussed mechanisms is that the authentication mechanism is adapted and done on the mobile phone, but not for mobile services. Mobile device is used as an authentication device, while the main access terminal is still stationary PC.

Another approach to adapt the standard authentication mechanism to mobile devices is to store a client's private key, that is part of a PKI security architecture, in the internal memory of the device. The private key can be subsequently used for secure user authentication, and the signing and encryption of data that is exchanged between mobile application and server. One example of this approach is shown by Pitsillides, et al. [206] and Panteli, Pitsillides, Pitsillides, and Samaras [207], in which a security framework is described for the provision of end-to-end security of e-health mobile applications supporting the networked collaboration of healthcare professionals. Authentication of the user is implemented in two stages. First, the user performs authentication on the device using a strong PIN number. Then the user is authenticated for the application through a digital certificate and a strong password. Digital certificates are installed on all mobile devices and, in addition to authentication; they are used for the encryption of sensitive data during transmission and integrity control of information exchanged over the Internet. Another example of how PKI can be used for providing user authentication is proposed in the work described in [208] where a novel scheme for mutual client and server authentication based on the exchange of messages encrypted with private keys is described. The proposed scheme uses PKI to provide bidirectional authentication and non-repudiation and uses a session key to provide high security. Utilization of PKI architecture in mobile services can provide a high level of security and data protection, but the major drawback is the cost of the security architecture establishment and maintenance. Certificates and private keys must be installed and maintained on each client device, and procedures for revocation, renewal and destruction must be established. Also, additional security mechanisms must be implemented on mobile devices to enable secure storage of private keys.

Mobile device hardware security components can be used for improving performance and security of implemented security mechanisms. However, developing specific hardware is a demanding and costly process that requires adaptation of the entire mobile device hardware and it is difficult to reach a common standard across manufacturers. Therefore, work on improving security features of legacy mobile devices and a SIM card's hardware is usually done by mobile device manufacturers and operators themselves. One example of a hardware component that provides support for hardware based security is the Trusted Platform Module (TPM) [209, 210]. The TPM provides various security functions, such as random number generation, asymmetric key generation, encryption/decryption, generation/verification of digital signatures, hash algorithms, identification and authentication mechanisms, and secure storage. The TPM security specification defines security services common to all platforms and allows them to be adapted for implementation for specific platforms. Today TPM is integrated just into limited number of hardware platforms (such as PCs and servers), and support for mobile devices is not currently available. However, many industry players are planning to integrate Mobile Trusted Module (MTM) in the coming generation of devices such as mobile phones and PDAs. The MTM is a revised version of TPM specification adapted for usage on mobile phones [211]. Research work as [212, 213] shows how MTM can be integrated in mobile security and authentication provision services. The general conclusion is that security features built into mobile device hardware can help developers to implement and improve advanced security mechanisms and provide better protection of users' private data without requiring additional development efforts. However, they introduce additional dependency of mobile device hardware, which can result in delivery of (healthcare) services to only a group of users with newer mobile terminals. Thus, software-based solutions are usually better suited to ensure wide delivery of services in addition to high security.

Another approach to implementing secure authentication is to take advantage of existing technologies in the cellular network. Cellular operators implement various standard security mechanisms. For example, projects such as [214-216] propose authenticating users by using the Generic Bootstraping Architecture (GBA) mechanism implemented by the mobile network operator. GBA is a framework for mutual authentication of users and network applications, and consists of a single authentication infrastructure that can be used for all of the potential services on a mobile device [217]. The user is authenticated based on long-term credentials present in the SIM, which are protected from unauthorized access. More work can be found that proposes utilization of different SIM based authentication mechanism for user authentication when accessing mobile information services (e.g. [218-220]). Standard security solutions provided by mobile network providers can offer benefits such as easy integration of well-established and approved security solutions without the need for additional development and maintenance. However, they also introduce drawbacks such as less control and flexibility because cellular operators as a third party are controlling security features that protect access to private data, which is usually not acceptable for services managing highly sensitive (medical) data. An additional problem can be the numerous mobile network providers in each country, entailing cooperation agreements and a need for all of the mobile providers to define and agree on the security policies to enable access to mobile services for all potential users. Experience from other authentication solutions, such as BankID for Mobile in Norway, show that such coordination is very difficult, and may be impossible without regulatory intervention.

Limited computational capacity and power supply of mobile devices has resulted in research related to utilizing external services for performing security and authentication algorithms in mobile services, such as cloud computing [221, 222] and agent technologies [209, 223, 224]. Using external services such as cloud computing and mobile agents has the potential to enable developers to improve the security capabilities of mobile healthcare applications and overcome existing mobile device limitations. However, security mechanisms utilizing these technologies are still not accepted as standard mechanisms for providing everyday security solutions thus showing the need for further research and development work in this area before wide deployment is possible.

One standard approach to implement user authentication is based on identification and verification of humans by their unique characteristics and traits (also called biometrics) introduced in the theoretical background in chapter 2.2.1. One of the main limitation of this approach is that the technology that is used for providing biometric authentication is usually very expensive mainly due to expensive infrastructure required to process authentication data [225]. Also, in general people are not comfortable in using this type of authentication mechanism for everyday services due to its intrusiveness [226, 227]. Functionalities available on the mobile phone can be used to ease the gathering of biometric data in a less intrusive manner and result in a better user acceptance and proliferation of this type of authentication mechanisms. In the literature can be found different research approaches suggesting how mobile devices can be used for biometrics authentication (e.g., voice recognition [228-230], fingerprint recognition [231], face recognition [232-234], patient ECG recognition [235]). Additionally, using advanced sensor features of smart phones (e.g., accelerometer, location sensors) has enabled the development of new authentication mechanisms that were not previously available on a PC, such as location based authentication [236, 237], gesture recognition [238, 239] and gait recognition [240, 241]. Using advanced authentication mechanisms based on biometrics that are adapted to mobile device characteristics has a potential to improve the security of mobile services in the future without influencing the usability of the system. However, these mechanisms can also introduce additional privacy issues, since they require gathering sensitive private data people generally are not willing to share.

Multi-channel authentication

In a previous part of this section it is discussed how different single authentication mechanisms could be adapted and used on mobile devices. As described in the theoretical background in chapter 2.2.1 multifactor authentication that combine couple of authentication mechanisms is used to offer better protection against security attacks. However, the one channel used in multi-factor mechanisms is usually the weakest part of the system since if the channel is compromised all factors exchanged between user and the system can be captured. To overcome this vulnerability, the multi-channel authentication is introduced, where different authentication factors are transferred over independent channels. Multi-channel authentication mechanisms offer better protection then using only one channel for delivery of authentication factors, since with using multi-channel authentication attacks must compromise both communication channels to gain access to protected resources. Most commonly a web channel is combined with a mobile network channel. One example of the multi-channel authentication approach is an authentication mechanism that enables strong authentication of the user using a non-trusted communication channel (e.g., a PC in an Internet cafe) by using a trusted communication channel (a private mobile phone) proposed by Shintaro and colleauges [242]. The user reads a session ID from the primary communication channel (web channel) using a bar code reader on a mobile terminal, and it sends the session ID through a mutually authenticated secure channel over the mobile phone network to the authentication server. The authentication server can then match the session ID and bind the successfully authenticated user to the main communication channel. Another approach that uses the cellular phone network as a second channel for user authentication is sending OTP over SMS or generating OTP in a mobile application (this security mechanism is more discussed in a previous part of the section).

Additionally, commercial products that rely on the security of the closed switched telephone network can be found, such as SAINTlogin [243], Identrica [244], Lloyds TSB [245]. In the SAINTlogin solution, the system provides the user with a random phone number unique for each incoming authentication request. The one-time telephone number is used to identify each started authentication session, and the user is authenticated on the second authentication channel by checking the calling number which is previously registered in the system and linked to the user. The Identrica System requests a user to enter the mobile number into a login page together with other access login details. To complete the login process the user is asked to call a given number belonging to the company. The caller number is used to authenticate the user over the secondary channel by matching it with the number given on the primary web channel. In the Lloyds TSB solution the bank calls the customer on the previously registered phone number and provides a one-time PIN number that must be entered and sent over the main communication channel.

A more general multi-channel solution is proposed in [246, 247] where the user can choose one or more independent secondary access channels, which are used to verify user identity (e.g., mobile phone, a landline phone, e-mail, or Nintendo Wii) and authenticate the transaction. In this solution much more flexibility and security management is given to the user since he/she will be able to increase and decrease security according to his own desire and understanding of the system. Additionally, the service provider can define some initial security requirements and limitations enforcing minimal protection of the user sensitive data.

The literature survey found lacking related research work on developing multi-channel authentication solutions that can be used on one device, more specifically on mobile phones. Mobile phones used today provide the user with the ability to connect to different networks at the same time and to use different communication channels. A common understanding and requirement set from legislators making security requirements is that the terminal providing second authentication channel or serving as an OTP device must be separated from the terminal used to access private data. The research work described in Paper III [37] in the dissertation shows how a mobile phone can be used as the terminal for accessing the user's private data and at the same time provide additional user authentication over an independent second communication channel, making the terminal and the code calculator/OTP device the same device. The main advantage of the proposed security solution compared to other proposed multichannel authentication mechanisms is that it can be used without reducing the security and in the same time providing superior ease of use since it does not require additional device/token from the user.

Mobility literature overview

This section investigates how related work address session mobility issues when providing seamless access to mobile information systems and shows how security issues are addressed in this context. Also, it is discussed some of the standard mechanisms for enabling macro mobility (or Inter-Access Network handover). Additionally, it is presented overview of some techniques proposed for enabling context adaptation of healthcare applications and information services and discussed how related research work proposes combining context adaptation with mobility management for mobile healthcare information services.

For enabling terminal mobility across different access networks and administrative domains standard technologies (such as Mobile IP, Mobile VPN, and Session Initiation Protocol - SIP mentioned in the chapter 2.3) exist today. Each technology offers a different approach for handling macro mobility issues, but also introduces limitations that must be additionally considered. The Mobile IP protocol allows location-independent routing of IP packets on the Internet and provides support for seamless connectivity across heterogeneous networks [97]. However, the protocol also has some major limitations such as: performance overhead due to triangle routing, the requirement for implementation of additional support mechanisms by an operator or service provider (e.g. hosting of a home/remote agent), the requirement of a user to install the additional client software on the mobile device, and security considerations (e.g., denial of service attack, passive eavesdropping, reply attacks [248-250]). Additional research work, such as [251, 252], is conducted to improve the performance of Mobile IP protocol and provide a more efficient macro mobility handling mechanism. However, Mobile IP is still not widely accepted on mobile terminals, and only few operators and enterprises use the technology today. Mobile IPv6 address some of the shortcomings of Mobile IPv4, but do not solve all infrastructure requirements, which so far has limited commercial deployment. Mobile VPN is a popular technology for handling terminal mobility issues of mobile devices in enterprise environments. It provides mobile devices with continuous access to network resources and software services in their home network while they are on the move. However, the advanced security mechanisms provided by Mobile VPN technology (e.g., encryption, authentication, and user provisioning) adds also to the communication overhead. Also, in the same way as for Mobile IP, the additional Mobile VPN client software must be installed and/or configured on the client (mobile device) and server (service provider) for the service to be available to the end users. In general, standard network layer protocols, such as Mobile IP and Mobile VPN, can be used for enabling terminal mobility. However, the software supporting these protocols is still not widely present and accepted on mobile devices, resulting in extra requirements from users to install and configure their mobile device before they can use the service. Additionally, these protocols can add extra performance and communication overhead on mobile devices that already have power and processing constrains. For handling macro mobility issues on the application level, the SIP protocol can be used. The SIP protocol enables registration of a mobile client so the user can initiate and receive communication and services from any location [96]. The disadvantage of the SIP protocol is that it does not provide seamless connectivity when the user is on the move since the protocol is designed more for reaching a mobile terminal from the network side using a unique user's identifier (SIP URIs). Different research efforts are being made to adapt the SIP protocol for more effective handling of macro mobility (e.g,. enabling soft handover by adding SIP proxies with content buffering and filtering features to the base stations [253, 254], combination of SIP with Mobile IP protocol [255], enhancing the architecture with Session Border Controls and extending application and/or media layer functions [256], and re-establishing SIP session after establishing network layer connection using re-INVITE message from the client or creating multiple sessions between two end-points [257]). However, the SIP protocol is still mostly used for enabling peer-to-peer communication (mostly multimedia content streaming) and it is not usually deployed as a standard solution for providing seamless access over heterogeneous access networks. Besides handling macro mobility on network (Mobile IP, Mobile VPN) and application (SIP) layers, there are also proposals for handling macro mobility on the transport layers such as [258, 259]. However, this approach usually suffers from the drawback that it has to modify the standard Internet transport protocols implementation, such as TCP, for all the hosts, which is not practically feasible for a generally available (healthcare) service. Handling terminal mobility at a transport layer is usually proposed and implemented as a part of research projects and still not standardized as general technology solution.

Session mobility as defined in previous chapters ensures that the active session is preserved while the user is accessing the same service over different terminals. Canfora and colleagues in [260] describe three main architectural schemes noting how session mobility can be achieved for web applications. The first option is to add functionalities for tracking and managing session information to a client device or client application. When a session is transferred, the session data is transported to the other client usually by implementing peer-to-peer communication between clients or adding a server that temporary stores the session data (e.g., [261-269]). The advantage of this approach is that complete and precise session information can be obtained since the client poses all session information (even the information that was never transmitted over the network to the server). On the other hand, the disadvantage is that enabling recovery of session information when the communication channel with the original client is lost can be very demanding or even impossible. Additionally, changes must be implemented for all client devices (in the form of e.g., web browser add-ons or client mobility agents). If the session mobility functionalities are developed as separate add-ons and not integrated as part of the client application, additional installations and configurations must be performed usually by mobile device users.

The second option is to create an intermediate proxy server that will intercept all communication between the client and server side (e.g., [260, 264, 270-272]). In this case the session information is stored and managed on the proxy server, and when the session should be transferred the proxy server performs all the session handling work. The advantage of this approach is that a proxy server can usually be added without big changes to client and server applications, making it a very attractive solution for adding session handling features for existing web applications. However, since a proxy server is added as a new point in the communication, additional protection mechanisms must be implemented to protect the system's overall security, data privacy and confidentiality (e.g., the proxy server should perform additional identification and authentication of the user to be able to restore the right session state and all communication from and to the proxy server and the data stored on the server should be protected from intruders using an appropriate mechanisms such as encryption). Additionally, if the client application is not additionally adapted to support session handling features the proxy server will not be able to gather session information that is not previously transmitted (e.g., uncommitted forms).

The third option is to store session information on the server. In this case the server is responsible for restoring the proper session information for the client. Besides research work addressing this topic for supporting web applications (e.g. [273-276]), the desktop virtualization technology called Virtual Desktop Interface (VDI) is implemented and provided by the majority of technology vendors today (e.g., Citrix, Microsoft, Oracle, RedHat and others) to enable easy transfer of complete user desktop environments to different servers. The VDI technology provides support for storing and running a virtualized desktop on a remote server. In this manner, all of the used programs, applications, process, and data are kept on the server and run centrally and a user can connect and run the same personalized operating system in the same state from different devices. The advantage of storing session information on the server side is that session data is managed as part of the server architecture and the additional protection of session data and communication is not needed. Also, session handling mechanisms are configured on the server and are easier to maintain. The disadvantage of this approach is that it requires additional implementation and/or modifications on the server side for adding support for handling sessions. If the client application is running on one server this overhead is not significant, but since web applications can be implemented on numerous servers that share the information about the user session, implementing and coordinating session handling among different servers can be challenging. Also, this approach has the same problem as the proxy server solution; session information from the client not transferred to the server will be lost.

Besides these three identified approaches, some projects propose implementation of specific mobility handling middleware. For example, Bagrodia and colleagues in [277] present the iMASH architecture for enabling a session to move seamlessly between heterogeneous platforms. The iMASH solution proposes middleware services hosted by additional platforms (proxies) placed between clients and legacy servers and require additional implementation on clients while the legacy servers are unchanged. All communication between client and server is mediated by middleware on proxy servers that also manages the application session state to facilitate fast application session handoff between client devices. A similar approach is proposed in [278] where a middleware solution named OPEN Migration Service Platform is proposed. The platform contains a server side proxy implemented as modified SOCKETSv5 proxy, and a light-weight mobility client on the end-user devices. Similar to the previous example, all network communication related to session migration between the client and application server will have to go through the proposed proxy. Another example is described in [279] where Mockets are introduced, a communication middleware designed to support session mobility in terms of seamless handover and migration of services session endpoints from one node to the other. The Mockets middleware is designed as an application-level library that must be installed on both the client and server side. The middleware provides support for rebinding the open sessions to the network attachment point and network interface that provides the best performance. Additionally, it also provides support for adding mechanisms that enable moving the object representing the saved session state to another device and resuming a previously suspended session. In [280, 281] an activity-based computing architecture framework developed to support clinical hospital work is described. The architecture is based on handling activities that gather all information and applications related to one entity (e.g. one patient) and provides support for discovering, suspending, resuming, roaming and sharing the selected activity. The framework has a hybrid architecture using client-server communication for activity and state management. On the client side activity management functionalities are implemented as part of the integrated OS layer and a pluggable user-interface layer. On the server side framework is implemented through an infrastructure layer that handles activity storage, roaming, and sharing. The main advantage of the middleware solution is that it usually offer the better support for management of session mobility since they provide more specific session management functionalities that can be used by different services on both client and server side. However, they also require additional installation, configuration and maintenance of middleware software on the server, client, proxy or on multiple devices. If the middleware is not accepted as a standard and widely adopted solution in an operating system architecture, then the additional work for setting up the middleware environment on each device must be performed by the service provider or user.

A key consideration when providing session mobility for services that handle sensitive private data (such as healthcare information services) is security. The session handling mechanism must be implemented so confidentiality, integrity and privacy of data are preserved. From the above discussion we saw that adding a proxy server for session handling can require implementing additional security mechanisms on the new server. Implementing session handling mechanisms as part of server and client applications introduce less overhead since security mechanisms are already implemented and handled as part of the standard client/server application. Specific middleware added on client, server, and proxy for handling session transfer must also implement security mechanisms for protecting data during the session transfer and management process. In the next part a short overview of related work that proposes different ways for implementing secure authentication and communication when enabling session management in (healthcare) information systems is given.

The iMASH project addresses security issues as part of the middleware by creating three types of communication channels between the client and the proxy namely a device control channel, a session control channel, and a session data channel [282]. The device control channel performs mutual authentication between the client's and proxy's middleware using a unique certificate issued from a trusted authority and encrypts data during transfer using symmetric encryption over WTLS communication channel. On the session control channel user authentication is performed during session creation based on a username and password, after which if the user is successfully authenticated the client application will be activated. The session data channel is used to transfer session data. The approach that divides the authentication process on two communication channels provides an advantage during session handoff since only user authentication is required, while device authentication is performed automatically by the middleware. However, this approach requires a valid certificate to be installed on each device on which the session handoff is performed, and additional security techniques must be implemented on device to provide tamper-proof container and secure storage and management of these sensitive data. Additionally, the proposed architecture do not discuss how the middleware security management implemented in the proxy are related and integrated to authentication and security mechanisms on the legacy server. The OPEN Migration Service Platform project authenticates a client to the application server middleware based on application ID and device ID. The application and device IDs are registered on the server during the registration process that is required for each client before they can use the session migration functionality. The paper does not specify if some stronger (user) authentication is required during the registration process, so the conclusion is that the provided authentication is very weak since the user of the service is not specifically authenticated when session transfer is performed and if the device is stolen the intruder will be able to request session migration and access the service. For enabling migration of an authenticated session, Suoranta and colleagues propose implementing a client-side session migration mechanism [283]. The proposed solution uses Single-Sign On (SSO) techniques that manage user authentication over different services and describe migration of authentication sessions between a desktop computer and mobile device web browsers. They propose and implement a browser add-on that performs transfer of cookies between devices using a secure Bluetooth connection. The disadvantage of the proposed client-side session migration mechanism is that it does not provide seamless session transfer since it requires the user to initiate and accept the session transfer and establish connection between two active devices. Also, managing of sessions through cookies in different web browsers can be highly demanding due to the lack of a standard for accessing and naming cookies for different types of servers and services. Additionally, as the authors noted some servers bind cookies to IP addresses to prevent reply attacks which disable utilization of proposed mechanisms. In [260] it is described how security can be handled when using proxy based solution for managing web browser sessions. For providing user privacy and confidentiality the proxy server performs standard HTTP authentication of the user (using Basic or Digest scheme). If the web server requires user authentication, the user must be authenticated again and all authentication processes are performed through a proxy server. For optimizing the process the authors propose potential storage of user credentials on the proxy server the first time they are used (if the Basic scheme is used), and enabling the proxy server to automatically authenticate the user in future. Storing user credentials on the proxy server introduces a very high risk, since the intruder who gains access to the information on the proxy server can gain full access to the system and information from all users. Additionally, in this approach it must be ensured that the user authentication on the proxy server is of the same security level as for original service to preserve enough protection against unauthorized access. Each of the discussed projects propose implementation of the specific security mechanism to enable secure session mobility management, however none of the them provide support for adaptation of these mechanisms to the different context of use (for example enabling one authentication mechanism when a user access the system over the web browser application on public PC while adapting authentication mechanism when session is transferred to native mobile application running on a private mobile phone device). The solutions for enabling context aware user authentication can be found in the literature, but for general information systems that do not provide session management (e.g., [284-288]). Integrating support for adaptation of authentication mechanisms in systems that enable session management handling can be valuable for services that manage sensitive (medical) data and require user-friendly and context aware services accessible over various terminals.

Adaptation of the mobile services functionalities and design to different context of use (e.g., different device characteristics, location) is a key element of any mobile application development process. In the literature there are numerous researchers addressing this issue. For example in the healthcare domain, different studies have investigated how context-awareness can be implemented and integrated in mobile electronic patient records used in hospital by healthcare providers and what advantages these systems can provide (e.g., [289-292]). The results showed that adapting mobile applications for accessing electronic patient records to the context related information (e.g., knowledge about the users of the system, the location, work process, the social context, and the context of the specific system) could provide valuable benefits for this type of services. Additional recommendation is that since every system is different, the key requirement when adding context adaptation support is to utilize design methods that employ a high degree of user involvement such as user-centered or participatory design methods when implementing a context-aware system [289, 293]. For example, Bardram in [293] outlined lessons learned trough a user-designed process carried out in cooperation with clinicians and patients about applying context-awareness to clinical work. Some of the conclusions are: context-awareness data should be used for helping navigation through large amounts of medical data, and the context-aware application should only suggest the course of action and let the user make the final choice. Dahl and Svanæs in [294] compare some location and token-based interaction techniques for systems that provide point-of-care access to medical information. The results show that the usability of the interaction techniques greatly depend on specific physical and social conditions of the use situations, and they propose to designers to consider a large number of potential sensor-based interaction techniques and to implement the few ones that show the best results. In this way, healthcare providers can choose the one that fits the best their current needs at the time of use.

However, even thought there can be found numerous research identifying principles how context aware services should be developed, designing and implementing context aware services still present highly challenging and difficult task due to users continuous and pervasive interaction [295]. In the literature different projects can be found that are describing how context aware services should be designed and developed. For example, Bardram proposed and developed a conceptual and technical framework for creating context-aware clinical computing application called Java Context-Awareness Framework with a small set of interfaces that provide support for development of robust, event-based and service-oriented healthcare services [293, 296]. Projects as [291, 297, 298] propose using agent technology that acts on behalf of users, service providers, devices, and sensors in the medical IT environment and implement complex functionalities that are in this manner hidden from the users. Paganelli and colleagues propose using an ontology-based context model and rule-based reasoning for representing patient health status and adaptation of the system functionalities to the patient's health plan and specific needs [299]. As part of the AWARENESS project it is developed infrastructure for supporting context-aware application that provide a generally applicable context model with implemented quality and time-critical context reasoning and user centered dynamic privacy control [300]. In Match project [301] it is proposed using policy-based home care system, where policy rules are used to specify the behavior of a system and adaptation to the current context.

Previous examples show that there are different project addressing session adaptation and context adaptation issues independently. However very few projects that address both of these issues together is found. One example in healthcare domain is project called Activity Based Computing that proposes and develops an architecture supporting local mobility within hospitals [107]. The proposed architecture supports local mobility of medical personnel in one hospital. The focus of the project is managing application mobility across different terminals (called by authors “application roaming”) and content adaptation, while terminal mobility and support for roaming between different network types and administration domains is not managed by proposed architecture since the service is used only inside of one hospital internal network. The access to the system is enabled only using web browsers on devices, while support for development and integration of native mobile applications is not provided. Additionally, the transfer of session is not performed automatically (the original application must initiate session transfer and provide the address of the device where session should be transferred). Another example is project Ubidoctor that propose a middleware-based service infrastructure that enable doctors accessing hospital information system independent of their current place and time [302]. The proposed middleware architecture provides support for handling session mobility and content adaptation for healthcare applications and enables access to the system from outside of local hospital networks. However, the proposed middleware does not provide support for protecting sensitive data stored and managed by the middleware services and implementing security mechanisms as part of the middleware solution.

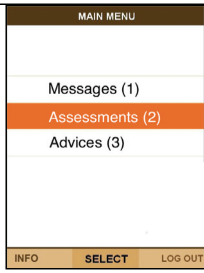
The related work presented in this chapter shows the research and industry solutions for providing secure, context aware (healthcare) information services that support session and macro mobility management. We found different projects addressing these issue independently, however we found lacking the related work that combine all these features in one proposed solution. For example, different approaches for handling session mobility are showed and different authentication mechanisms are proposed for protecting unauthorized access to these systems, but none of the related projects enable adaptation of these security mechanisms to the context of use. Also several projects that are addressing session mobility and context adaptation issues in healthcare information services are described, but they do not provides support for integrating security management functionalities as part of the proposed solutions. Due to this reason, in the paper IV in the dissertation [38], we researched how a patient support system can be developed and adapted to allow session mobility and secure seamless access, and propose a generic architecture framework called CONNECT framework that provides support for implementing context aware authentication, session management and content adaptation when developing context sensitive patient support systems. The proposed framework supports implementing session mobility in a secure and user-friendly manner and simplifies further development and integration of different (mobile) platforms to the current CONNECT patient support system.

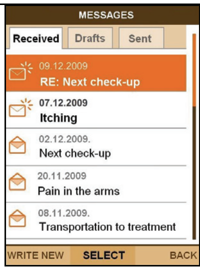
3.2 Paper II: Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management

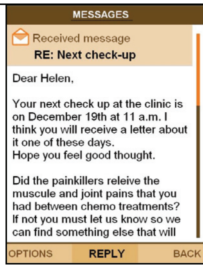
Summary: The research work presented in the paper address research issues related to: (1) identifying interface design and functionality requirements needed for the CONNECT Mobile application to provide patients with easy, user-friendly, context adapted mobile access to health related information in the CONNECT system, (2) identifying how previous knowledge and experience with other parts of the CONNECT system affect users understanding and operation of the mobile application, and (3) researching patients acceptance and opinions regarding the usefulness of the mobile application as part of the CONNECT system. During development of the CONNECT Mobile application various participatory design and usability evaluation methods (semi-structured interviews, usability testing with low fidelity and high fidelity prototypes, and heuristic evaluation) were used and the detailed analysis of gathered quantitative and qualitative data was performed. Various types of system stakeholders (patients, design and software development experts, and medical personnel) were included in different phases of the iterative design and development process.

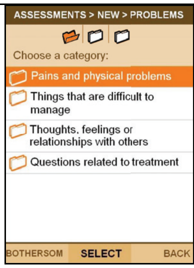
The low fidelity usability testing combined with semi-structured interviews with patients was performed in the beginning of the application design development process to get initial feedback from potential users regarding the system's interface design and functionalities. The low fidelity prototype is developed by adapting the first version of the application design screenshots developed in previous phase of project to comply with general design guidelines and recommendation defined by mobile device manufacturers, mobile platform manufacturers, and design standardization organizations (e.g., [46, 122, 126-129]). The feedback from potential users was used to gain better understanding of the new context of use for the CONNECT patient support system and to identify users requirements and expectations from this type of mobile health management system. The results and design rules gained from the user feedback in this phase are described in the paper, and a more detailed description is presented in the Appendix 2 of the dissertation. The feedback gained from participants in this phase was used to adapt the application interface design and functionalities before the application development process had started. In order to develop of the CONNECT Mobile application Java Platform, Micro Edition (Java ME) developer platform [303] was used. To provide additional support for adaptation to any mobile terminal without any specific requirements from a device and user software library from Faster Imaging [304] was used during development. The software library provided new methods for text manipulation and dynamic adaptation of commands and navigation elements with automatic adaptation to device capabilities (e.g., support for arbitrary fonts with arbitrary size scaling and support for various navigation methods such as buttons, stylus, soft-keys, numeric keys, and touch screens in a consistent way). In this manner, every user could use his/her private mobile phone to access the same service, while the interface is automatically adjusted to each specific device and its capabilities. Developers and design experts participated in group sessions, where system design, functionality, and adaptation issues were discussed. As a result of this phase, a fully functioning high fidelity prototype was created based on a previously developed and adapted interface and functionality design. In the next phase expert reviews with nurses were performed on the high-fidelity prototype. The heuristics evaluation method is used in this phase to get valuable feedback from healthcare personnel not just on interface inconsistencies but also on interface and functionality implementation design based on their previous experience with development of the CONNECT system. Most of the comments received in this phase were related to small interface adjustments and more convenient organization of the content on the screen (the summary of the comments are showed in the paper and the detailed description of received feedback is given in the Appendix 3 of the dissertation). The feedback received in this phase was used for final adjustments and improvements of the high fidelity prototype before the final usability evaluation phase with patients had begun. The results of the final high fidelity usability testing showed that the patients did not have any major complaints or problems performing the tasks in the CONNECT Mobile application. However, for patients that had used the CONNECT web application before, previous knowledge and experience helped them to understand and perform tasks with higher efficiency and make fewer errors. All the participants agreed that the functionalities provided on the mobile application were sufficient, and that adding more functionalities and options would result in a more complicated system that is harder to understand and use. The final interviews performed after completed high fidelity prototype testing showed that patients found the mobile application useful and were ready to accept it as part of the CONNECT patient support system in their everyday health management process. Additionally, participants described new usage scenarios and contexts where using mobile services is more suitable than using a standard web application. For example, one patient stated that now she has much more free time (e.g., waiting for treatment, in the transport to and from hospital) when she cannot use a PC, and in this situation she finds the mobile application very useful. Another participant said that the web application can be used only when she is at home and sits in front of PC, while a mobile application she can use anywhere and anytime since she always has her mobile phone with her (e.g., going to the shop, sitting outside in the garden). Additionally, one participant reported that she very often did not have enough energy to sit long in front of computer, while a mobile phone she could use to access the system even when resting and laying down. A more detailed description of results recorded in the high-fidelity usability testing together with semi-structured interviews can be found in chapter 5 of the paper.

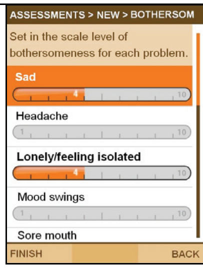
<table>
<tr><th>Functionality</th><th>Screenshots</th></tr>
<tr><td>Login and main menu</td><td>

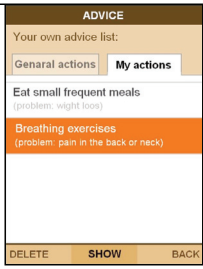



</td></tr>
<tr><td>Messaging</td><td>




</td></tr>
<tr><td>Registration</td><td>




</td></tr>
<tr><td>Advice</td><td>


</td></tr>
</table>

Figure 5. Screenshots of the final mobile application interface (part of the figure is taken from [36])

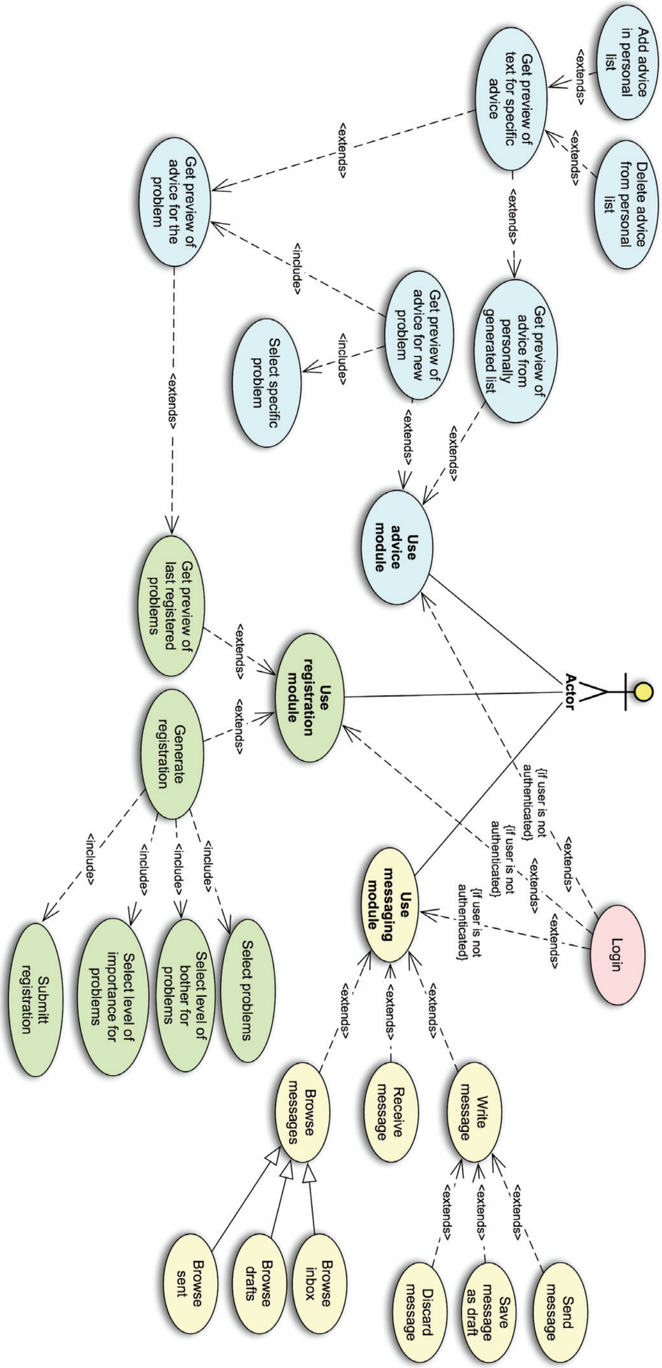


Figure 6. Use case diagram of the functionalities provided by the CONNECT Mobile application

3.2 Paper II: Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management

Through the described development and evaluation phases a user-friendly, adaptable, and well-accepted CONNECT Mobile application that enables mobile access to the CONNECT patient support system is created. The mobile application screenshots that demonstrate final application interface design and functionalities are shown in Figure 5.

Figure 6 shows a use case diagram of the functionalities provided in the CONNECT Mobile application. The main functionality modules supported are:

The messaging module where a patient can exchange messages with medical personnel.

The registration module where a patient can register and manage problems that are bothering him/her. For each selected problem the patient additionally registers the level of bother and importance level. Additionally, there is an option where the patient can get a preview of the last registered problems.

The advice module where a patient can get information about how to manage his/her symptoms, how to psychologically deal with the illness, the challenges it brings, and what his/her rights are as a patient (all information in this module is evidence-based and quality assured by healthcare personnel). The patient can also create a personalized list of advice that he/she finds most useful and valuable.

Contributions: The main goal of this paper was to address the research issues related to the development of a useful and user-friendly application that enables mobile access to a patient support system such as the CONNECT system and research the acceptance and usefulness of a mobile application integrated as part of the CONNECT system. In this context, the first objective has been to identify mobile application interface design requirements and adjustments. The general design guidelines in the literature were found insufficient and in many cases contradictory, while research work related to "mobilizing" web based healthcare systems is limited to addressing functionality adaptation and performance analysis of specific types of information system intended for limited user groups (see the literature survey in Chapter 3.1.1). To identify the main design and functionality requirements when enabling mobile access to the CONNECT system different participatory design and usability evaluation methods were used during the design and development process. By involving various types of system stakeholders different types of feedback and comments are received, and different user requirements and design principles that are applied during the application development process are identified. The first contribution in this research area is a set of guidelines and interface requirements that should be used when developing and integrating mobile services in healthcare information systems with similar functionality and design requirements (detailed description of the guidelines can be found in the paper).

The next objective of the paper has been to identify the users' functionality requirements and acceptance of the CONNECT Mobile application as one part of a larger patient support system. Most mobile healthcare applications and services that can be found in the literature and mobile markets today are stand-alone systems and all functionalities are provided only through a single application. However, based on the feedback received from patients, it was concluded that most patients accepted and appreciated a mobile application in addition to a web application. They still recognized and preferred the web version as the main application with full functionality support, but also they identified the new usage scenario where the mobile application can be found more useful and appropriate compared to utilization of a standard web application. Also, the patients stated that they do not require all functionalities of the system when using a mobile terminal; it is enough to have a selected subset. Based on this user feedback, we came to the conclusion that the mobile application should constitute just a part of a more complete system including other types of terminals such as web or tablet for home/hospital use. In this manner, it is possible to provide a user with numerous different functionalities and features over different access terminals, and keep the (mobile) applications very simple, easy to use and context adapted. This conclusion is consistent with the results presented in the related work such as [145-148] showed and discussed in the literature review. Additionally, in the paper guidelines are suggested regarding how the mobile application should be developed in accordance with other parts of the patient support system, so the user can use the previously gained knowledge and experience with the system when a mobile application is introduced.

Finally, it is researched what are patients' opinions regarding the final CONNECT Mobile application usefulness and ease of use. All patients that participated in the final high fidelity usability testing phase found the mobile application together with the other parts of the CONNECT patient support system very useful. Also, they did not have any major difficulties when using the mobile application that is developed applying design and functionality requirements identified in the previous phases of the research process, and they agreed that it was easy to use the application and perform the requested tasks. Based on the feedback gained from participant through the research process, we concluded that the standard patient support services offered in Norway today (phone calls and hospital visits) should be extended with advanced and more flexible patient support systems (such as CONNECT system) that take advantage of new and emerging technologies (including mobile technology) with the goal to fulfill rising patients' requirements and provide healthcare information delivery and support at the point of need.

Limitations: One of the participants in the usability study suggested that the CONNECT

Mobile application should be offered only to potential users between 20 and 50 years old, which are more accustomed to using mobile technologies. The good acceptance and easy understanding of the CONNECT Mobile application interface and functionalities by this user group is also showed in the results of this study (the mean age of the users who participated in the high fidelity usability study was 46.5). However, the general conclusion of the study is that mobile information services in healthcare sector should not be limited just to specific user groups (e.g., younger people). Reaching the elderly and other user groups (e.g., users with special needs such as people with vision and motoric problems) would mean identifying new system requirements by including a wider user group of potential users in the development process, and additionally adapting the services for the new usage context. For future work in the CONNECT project utilizing the universal design principals and adjusting and improving the (mobile) application(s) and service(s) to supports needs of a larger user group is planned.

The targeted user group participating in high fidelity usability testing was women between 20 and 50 years of age in treatment for breast cancer. This additional limitation must be taken into consideration when discussing the reported results. Another limitation is that the number of users that participated in the high fidelity usability testing was only ten. Even though the literature suggests that a lower number of users is adequate for performing qualitative usability studies [305], due to the sensitive nature of the healthcare systems, future work requires identifying more design guidelines and user requirements from different users by recruiting a higher number and greater variety of potential users during usability testing phases.

While performing high fidelity usability testing, the participants used the mobile application installed on a Nokia 5110 Express Music testing phone, not on their own private mobile phone. This fact probably adversely influenced performance and the number of errors participants performed, and we believe that using their own mobile phones would provide more personal and valuable feedback since the participants are better acquainted with the devices' legacy functionalities and features.

The heuristics evaluation, as a type of expert review, is usually performed by usability experts (as noted previously in Chapter 2.1.1). However, the theory overview of the heuristic evaluation by Jaspers in [56] shows that application domain experts with usability experience can be also highly efficient in identifying usability problems in the system. For this reason, during the CONNECT Mobile application development process nurses from our research center were recruited to perform the heuristic evaluation. We found that these nurses, who worked previously on developing different parts of the CONNECT systems, possessed very valuable knowledge of the patients' needs and requirements and can be used as a good replacement for design experts in this phase of system design.

During development of the CONNECT Mobile application standard usability evaluation and participatory design methods are used. Besides these standard methods, the literature review described in the chapter 3.1.1 identified the research efforts working on adaptation of the standard evaluation methods to the specific characteristics of the mobile devices and frequent change of usage context. Utilization of new and more context-adapted evaluation methods is considered for future work on the CONNECT Mobile application(s) to more efficiently identify new users' requirements for the new usage scenarios.

During the high fidelity usability testing one of the standardized usability questionnaires was additionally used to measure system usability and user satisfaction. The questionnaire that was used was Software Usability Measurement Inventory (SUMI). However, the authors of this tool did not perform analysis of the data as we had previously agreed on, and we were unable to present the results of performed testing in the paper. The results of the questionnaires would, nevertheless, present just preliminary results in this application development stage, and to gain more valuable quantitative usability results more users must be included in the final phase of the application testing [306].

The paper describes how the mobile application is developed and integrated as part of the CONNECT patient support system, which also provides a web based application adapted for use on standard PCs. Based on feedback received from patients during the development and evaluation phase it is proposed to implement only a limited number of functionalities on the mobile application to preserve application simplicity and user-friendliness. Here must be noted that the application was developed for standard mobile phones with limited interface and input capabilities (the testing phone was a standard Nokia phone). Today, we can see wide penetration and acceptance of smart phones and tablets with advanced interfaces and interaction capabilities and higher performance capabilities. The newly emerged question is whether the proposed design guideline applies also to these new devices with advanced features, or whether the new mobile devices are able to deliver all system functionalities on their own. This topic will be further investigated in the continuation of the CONNECT project, and is not addressed through research work presented in the dissertation.

The next stage in the CONNECT project is to start a pilot study where the group of patients will be offered both mobile and web access to the CONNECT patient support system during one time period, and answer research questions regarding differences in usability, usefulness, and usage patterns for different types of access terminals and context of use. By testing the system in real world practice the main goal is to gain research results that show how mobile services add to the system's mobility and utilization in people's everyday life, and what further advantages they can provide in addition to standard web version.

3.3 Paper III: Secure Solution for Mobile Access to Patient's Health Care Record

Summary: There are many standards that describe guidelines for implementing security protection in healthcare information services and their secure integration (as seen from Chapter 2.2.3), and literature review showed a substantial amount of research work that is done on adaptation of standard security mechanisms (more specifically authentication) to the specific characteristics of the mobile terminals and networks. However, mainly due to high requirements set by national laws and policies for protection of patients' private data there are still no standard and widely accepted mechanisms that enable secure mobile access to healthcare information system in Norway.

The paper proposes a security architecture for mobile access to healthcare information systems that enables secure authentication and communication between a mobile device and a healthcare service provider through the usage of a two-factor authentication method on a mobile phone (Confirm-by-PIN solution implemented by the Encap company [307] [308]) and encryption. The Confirm-by-PIN security solution was previously used for enabling two-factor authentication of the user in (bank) web services running on a PC, where OTP is delivered to the user's phone through a dedicated mobile application. In this paper it is proposed a new approach to use the Confirm-by-PIN authentication services and integrate the authentication functionalities as part of the CONNECT Mobile application. In this manner, the CONNECT Mobile application is utilized not just for providing the service functionalities to the user but also for initializing and performing the authentication process using Confirm-by-PIN programming libraries. The proposed solution adapts the existing Confirm-by-PIN authentication solution to provide multifactor authentication without the traditional requirement from the user to have an additional authentication token, so the use of the authentication mechanism is simplified without compromising security.

The paper shows a reference model of the proposed security architecture and explains communication scenarios for the authentication process. Additionally, we describe how the proposed security architecture provides support for different security features (authentication, confidentiality, integrity, protection against session hijacking, meeting local privacy laws, and usability).

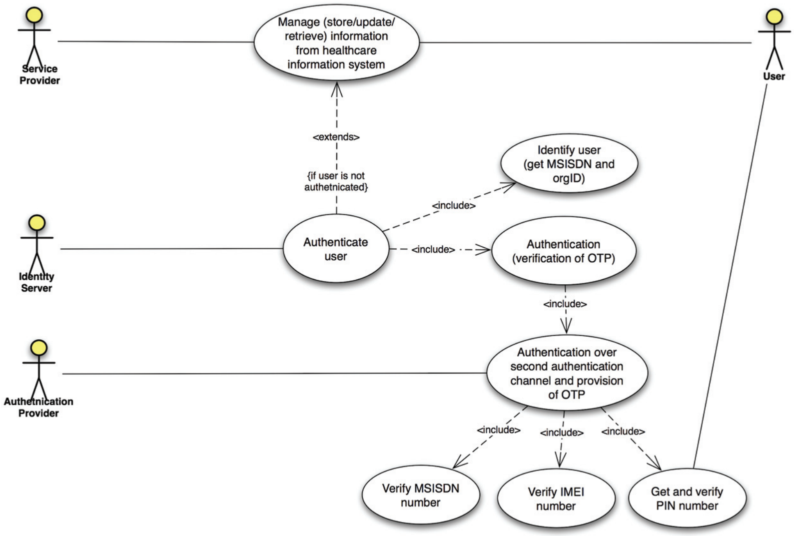


Figure 7. Use case diagram of authentication process

Use case diagram of authentication process is showed in Figure 7. Four actors participate in the authentication process:

The User is the patient with an installed mobile application on his/her mobile phone,

The Service Provider stores and manages patients medical information and provides service functionalities,

The Identity Server performs the authentication of the user,

The Authentication Provider performs authentication of the user through a second communication channel and delivery of a One Time Password (OTP).

The user first sends a request for private data to the Service Provider over a secure HTTPS channel. If the user is not previously authenticated, the request is forwarded to the Identity Server who performs authentication and informs the Service Provider if the user is who he/she claims to be. The user is identified using MSISDN (the telephone number uniquely identifying a subscription in a GSM or a UMTS mobile network as defined by the E.164 standard [309]) and orgID (the code that identifies type of user), which is specific to the authentication system. Authentication of the user is performed over two communication channels. Over one communication channel the user’s personal PIN number, mobile device identifier (International Mobile Equipment Identity - IMEI), and user’s private MSISDN are verified and OTP is generated. The main HTTPS-based communication channel is later used to verify the OTP.

For testing purposes a mobile application and a server architecture test bed were developed to simulate the proposed solution, prove its feasibility and evaluate performance. The test bed is developed based on the description of the security architecture of the University Hospital in Oslo. In this manner the feasibility of the solution is shown and demonstrated how the proposed architecture could be deployed and adapted for one real life hospital information system. For development of the mobile application the Java ME developer platform is used, and for server side implementation the XenServer virtualization platform that provides capabilities required to create and manage a virtual infrastructure is utilized.

During the testing process the system's performance, scalability, and processing requirements on a mobile device is measured. The performance analysis identified communication bottlenecks and places for further work and optimization. Additionally, in the paper it is suggested how the authentication process could be optimized without decreasing security. The system's performance has been tested when multiple users performed authentication simultaneously and the results showed that there were no significant changes in performance. Due to the limited capabilities of the mobile devices, power consumption and CPU load on the phone when authentication process is performed is additionally measured. The results showed that power and memory consumed do not pose a problem, nor is the authentication process more demanding than running any other standard mobile application that use Internet connection. Due to the nature of the proposed authentication mechanisms and its security features, just preliminary scalability testing with eight simultaneous users was performed and results showed that the system performance is not considerably affected.

Contributions: The first objective of the research work presented in the paper has been to identify the security requirements for enabling mobile access to a patient support system such as the CONNECT system in Norway, and to find out which security mechanisms are implemented and used in practice today and how they correspond to the requirements. Norway has set very strict security requirements and corresponding legislation for protecting access and processing of patients' private medical data (see Chapter 2.2.3). In cooperation with the hospital IT department, we studied how the general security architecture implemented in the hospital information system that fulfill the set security requirements can be utilized and adapted for providing mobile access to patient sensitive information. The security architecture implemented in the hospital information system is divided in two zones: (1) a Demilitarized zone (DMZ) containing a main access proxy server, called Access Manager, which performs user authentication and access control functionalities and prevents outside users from getting direct access to sensitive data and services and (2) a Safe Patient Zone containing servers that provide healthcare information services and manage patient sensitive data. All user communication is performed through the Access Manager proxy server, which uses external authentication services for verifying user credentials. Today the hospital information system supports BankID and BuyPass authentication mechanisms for PC terminals. If the Access Manager successfully authenticates a user, it forwards the user requests to a specified server in the Safe Patient Zone. The WebChoice server implements the functionalities of the CONNECT patient support system and manages patient sensitive data. This server is located in the Safe patient zone and the patients are allowed to access the serves only if they are successfully authenticated and authorized by the Access Manager proxy server.

We concluded that additional adaptations and changes are required before the security architecture implemented in the hospital information system used for enabling secure access to the CONNECT system over web application can be used for enabling mobile access. We proposed adding one additional server (the CONNECT Mobile server) in the Safe patient zone and using this server as a proxy for mobile communication with the WebChoice server. The CONNECT Mobile server performs only an additional adaptation of data that should be sent to the mobile application and it does not store any sensitive data. Since the proxy server is located in the Safe Patient Zone and it does not store private data, the implementation of additional security mechanisms on the server is not required. Thus, the original CONNECT patient support system can be extended with mobile access with a minimal set of changes. We identified that the biggest obstacle for enabling mobile access to sensitive healthcare data using existing security architecture was providing secure user authentication over mobile devices. The hospital security architecture implemented today does not provide support for secure user authentication over mobile devices. The main reason is the lack of user authentication mechanisms that are adapted for mobile devices and accepted at the highest security level required for protection of patient personal data. As a result, no healthcare information services provided by the hospital information system today are accessible over mobile devices. For this reason we have focused our research on the development of a security architecture that enables secure user authentication for mobile devices and still supports full integration with an existing hospital information system that enables protection of patient privacy, confidentiality, and integrity according to the national security requirements. In the Appendix 4 of the dissertation, it is showed how the proposed security architecture integrated with hospital information system complies with national regulations and acts, and which security mechanisms are employed for protection of patients' private data in hospital information system. The content in Appendix 4 present the summary of a more detailed description of the complete IT system architecture that can be found in the risk assessment document that was developed as part of the approval process with the hospital security authority in dialog with the Norwegian Data Inspectorate.

As we noted before, besides general requirements for protecting sensitive (healthcare) data the Norwegian government set additional requirements for using a PKI based authentication solution for enabling access to sensitive information (including healthcare related information). The review of the authentication mechanism available and in use in Norway (described in the Chapter 2.2.4) revealed that there is no authentication mechanism that is approved for the highest security level in the public sector adapted for use on mobile phones. The proposed architecture that utilizes Encap's Confirm-by-PIN solution for enabling mobile access to the CONNECT system is not based on the PKI and since PKI is a requirement, the requirements must be changed or a secure storage of private keys must be employed. Two technology approaches are considered to address the requirement for a PKI:

(1) Use one of the approved strong authentication methods (based on PKI-based authentication) for authenticating a user during the application download and activation process over a secure web page. When the user is successfully authenticated using strong authentication method a new user account (MobileID) is created. The new user account is synchronized with the original user account for the strong authentication solution and used for performing the user authentication process using Confirm-by-PIN solution in the further use of the mobile application.

(2) Securely store private key, which can be used as an additional factor in authentication, encryption, and signing processes, on the mobile device. The one option is to store the private key on the SIM card. The example of this solution is BankID Mobile authentication mechanism (introduced in Chapter 2.2.4). The other option is to store the private key in the mobile devices' secure internal storage. As previously noted in the literature review in the chapter 3.1.1, many industry companies are planning to develop a revised version of TPM specification adapted for use on mobile devices and integrate it to the new generations of mobile devices in future. TPMs can also be implemented in software, for extending the authentication mechanisms for mobile devices with software-based secure storage for user's credentials similar to TPMs used in servers and workstations.

The first proposed solution resolves the requirement for utilization of a strong authentication mechanism (such as PKI) just for the application download and activation process and not for regular application usage. The proposed strong authentication is usually not very user-friendly. However, considering that the activation and installation process is not performed very often (just when starting or reactivating the application) and that the provided security level is proved as very high we claim that utilization of these types of mechanisms will improve the system's security level and make users feel safer and more protected when using mobile healthcare services. The disadvantage of this approach is that it adds extra work for linking and implementing synchronization of the two accounts. In the second proposed approach the private key is stored on the mobile device, so the requirement for PKI can be fully resolved. However, the problem with storing private data on the SIM card is the dependency from the operator and possible limitation of accessibility for all users if all operators do not support the solution. Replacing security of SIM storage with TPM hardware or software solutions avoids the dependency on an operator provider. However, TPM hardware is still not present on mobile devices and the only way to employ TPM on all mobile devices is to implement software-based secure storage for a user's credentials using cryptography libraries available for different developer platforms. This type of implementation also raises the question of how the user should be authenticated before he/she can get access to the private key (e.g. ask an additional password, use a physical token or prove identity by some other means), and how this new authentication mechanism influences the security architecture. Utilization of PKI systems additionally introduces the requirement for implementing standard mechanisms for distribution and management of private keys that should be present on all mobile devices of all potential users.

For our specific problem space the paper proposes utilization of strong authentication of the user for the application activation process (the first proposed approach). In this manner the requirement for strong authentication can be fulfilled for the activation process, and afterwards the more user-friendly security solution is used for general utilization of the application. We claim that introducing a requirement for PKI-based user authentication, after the activation process is performed successfully, is too high a demand for mobile systems that should be used on a daily basis by a large number of users. This paper describes one approach how security of the system can be enabled and preserved using advanced security mechanisms without influencing user-friendliness and accessibility of the system. We think that it is necessary to adapt the security requirements in Norway to support not just secure but also user-friendly access to the public (healthcare) services over mobile devices. Security mechanisms for mobile systems must be adapted to the new context of use and characteristics of the mobile devices, so the main advantages the mobile services offer to users and their main purpose (enabling more user mobility and accessibility to services anytime and anyplace) can be preserved. Additionally, the regulation must also focus on solutions that are general and available for all people using different mobile devices/operators /network types, enabling better accessibility to healthcare services.

The next research objective has been to propose authentication mechanisms that can be used to provide secure access to a patient's private medical data without decreasing usability of the system. During the development work on the proposed security architecture, in addition to security, usability issues were also taken into consideration. The described authentication solution is independent of mobile operator, device, and network type. In this way users can utilize the systems independent of their current time and location as long as they have their private mobile phone with them and know their PIN number. We claim that the authentication mechanism used for mobile healthcare services should not depend on the mobile operator (SIM card) or any particular terminal in order to be available for all potential users.

The proposed architecture enables users to securely access the CONNECT patient support system from mobile devices without the need for any additional tokens and devices. A multifactor authentication process requires from the user something that he/she knows (PIN number) and something that he/she has (his/her private mobile phone with the SIM card). The user is simultaneously protected from: compromising the PIN number, losing their private mobile phone, and losing their private SIM card. If the user loses the mobile phone he/she can revoke the mobile access permission to the healthcare services. Additionally, when the SIM card is re-issued by their mobile operator, the mobile application will automatically stop working until it is activated again, simplifying the revocation process. Protection from brute force attacks is implemented by blocking the user account after three unsuccessful login attempts. If this happens the user must activate the account again to be able to use the mobile application (the PIN number is not stored anywhere, and it must be set again by going through the whole activation process). Additionally, no private data are stored on the mobile device. In this manner, it is made sure that intruders will not be able to access any private data just by being in possession of the user's mobile phone. Besides these security mechanisms the proposed architecture also enables protection of confidentiality and integrity of private data, and protection against security attacks such as session hijacking. A detailed description of the whole security architecture and security mechanisms can be found in the paper.

The proposed security solution is implemented as part of the CONNECT patient support system, and the main purpose of the research work was to enable secure access to medical information stored in the CONNECT patient support system. However, the same architecture could be used for any type of mobile healthcare information system and services, independent of who the potential users are.

Limitations: A formal test of security measures and system security features was outside the scope of this work. For future work it is planned to test further the security mechanisms and the security architecture against attacks and attempts of unauthorized access.

The performed tests measured how much time that is used in the system for a typical authentication process. The results were subsequently evaluated through comparison with the time needed to authenticate the user of an online banking system, because we considered that the two systems share many security requirements (we did not find any publicly available security architecture implemented today that was more similar to the one we have proposed). However, to properly evaluate performance, it would be best to perform usability testing with potential users. This is planned in future work. In this manner the goal is to measure acceptance of the implemented security mechanisms and authentication procedure compared to similar systems, and identify users' awareness and understanding of security and privacy issues when using mobile services in healthcare.

Scalability of the system is currently measured when only eight users performed an authentication process simultaneously. In a real life system the number of users that must be supported at the same time is much higher. However, due to limited resources and demanding requirements for creating a testing environment with a large number of clients (testing can be done only using real phones with SIM cards) the current work shows just the initial scalability testing results with eight simultaneous users. Additional scalability and performance testing is planned for future work to ensure that the system can scale well when the load on the server is increased.

As part of future work, the plan is to implement the security architecture in the real life system when the proposed adaptations are performed, and use it for providing secure and user-friendly mobile access to CONNECT patient support systems.

3.4 Paper IV: A framework for development of ubiquitous patient support systems

Summary: Considering the current wide acceptance and popularity of different user terminals (both stationary and mobile) and presence of a large number of different communication networks, one of the key goals set in the initial phase of the research project has been to enable access to the CONNECT patient support system from most relevant mobile terminals and in this manner make the system more available to patients independent of time and place. The main challenges addressed in the paper are: seamless access over different types of terminals and access networks, session management and migration, application security and content adaptation to the context of use. To address these challenges in the paper a generic and modular architecture and design framework called CONNECT framework is introduced. The CONNECT framework provides support for implementing seamless application mobility and content adaptation for healthcare information services across different terminals. The CONNECT framework is not dependent on any type of developer platform, operating system, or terminal type. The framework also provides supports for managing terminal mobility issues in a secure and user-friendly manner. The authentication process is handled as part of the framework, enabling easier integration and utilization of various authentication mechanisms that are adapted to the context of use.

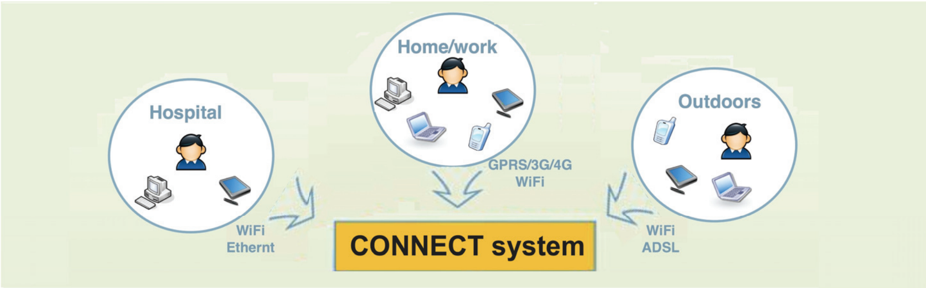


Figure 8. Mobility of the patient support system – possible implementation [38]

Figure 8 shows different usage scenarios for the CONNECT patient support system that implements the proposed CONNECT framework. The goal is to enable development of the system that enables the patient user-friendly, secure, and context adapted access to the system from a hospital, home, workplace, or outdoor location using different types of terminals (e.g., PCs, tablet PCs, mobile phones, and laptops) and different access networks (e.g., WiFi, Ethernet, GPRS, 3G, 4G, and ADSL) without interrupting the current session.

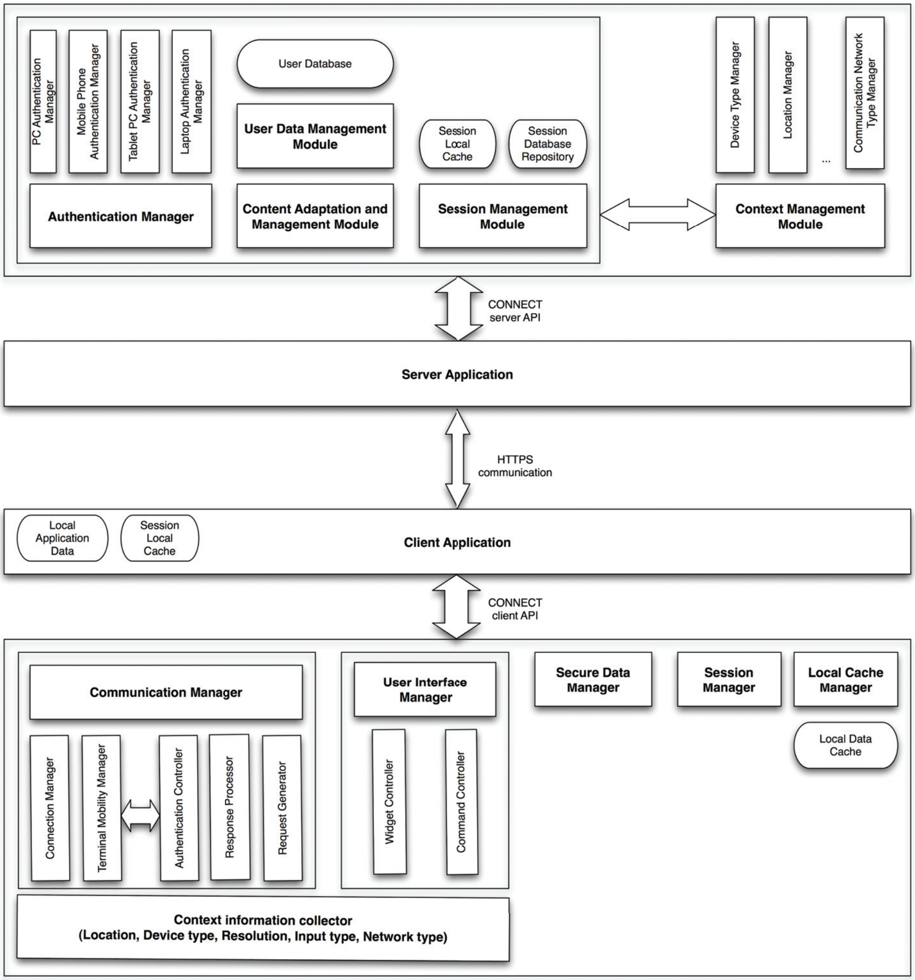


Figure 9. The mobility framework [38]

The framework consists of both the server and client modular architectural and design framework is showed in Figure 9.

The server architecture framework consists of the following modules:

The Context Management Module that process information regarding the context in which a service is used and provides this information to other modules,

The Session Management Module that performs storage, maintenance, and retrieval of session data,

The User Data Management and Content Adaptation and Management Module that is responsible for accessing and managing user data and for generating responses for a client application adapted to the current context of use, and

The Authentication Manager Module that performs authentication of the user, and makes sure that the user is who he/she claims to be before access to the service is enabled.

The client architecture framework consists of:

The Context Information Controller that gathers and provides context information to other application modules,

The Communication Manager that performs communication with the server side,

The Terminal Mobility Manager that is in charge of sensing the change of the access network and initiating authentication of the user ensuring that the user is properly authenticated to the service provider when the inter-access network handoff is performed,

The User Interface Manager that is responsible for the interface organization and adaptation and for implementation of events and actions related to a user's commands,

The Secure Data Manager that is in charge of secure management of a user's private data,

The Session Manger in charge of managing session related data, and

The Local Cache Manager responsible for storing application related data in permanent device storage.

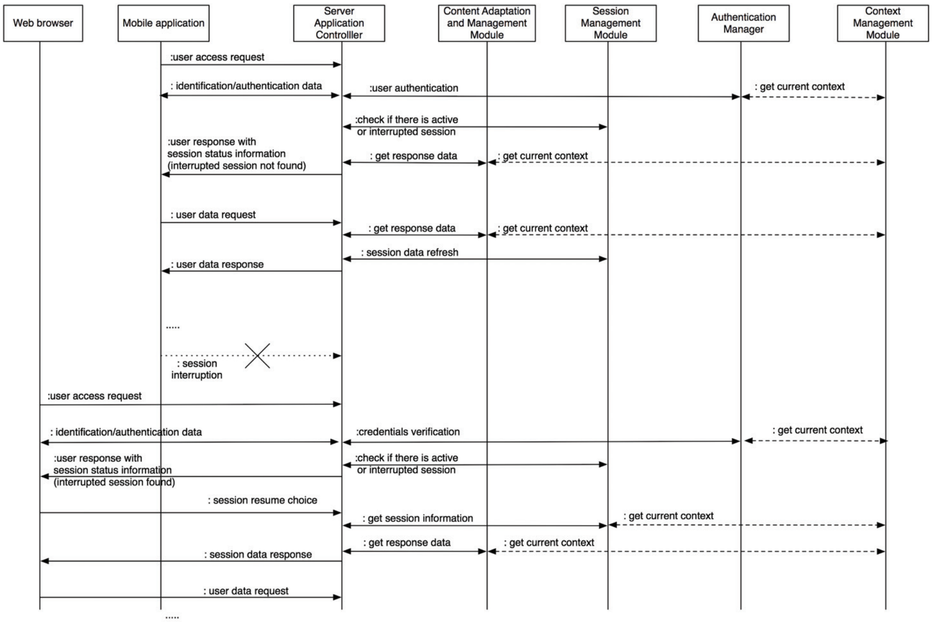


Figure 10. Mobility scenario – message flow [38]

One possible session mobility management scenario updated from the paper is described in Figure 10. First, the user sends a request to the server using the application on his/her private mobile phone. When the Server Application Controller receives the request from the client application, it forwards the request to the Authentication Manager. To identify the right authentication mechanism the current user's context is identified using the Context Management Module. In this specific testing implementation, a user's context information is the type of client application that accesses the service, and this information is transferred in an HTTPS request header. The user is asked for credentials, and if the user is successfully authenticated, Server Application controller checks if there is an active or an interrupted session for this user by contacting Session Management Module. If there is no session data stored, the client request is forwarded to Content Adaptation and Management Module, which get data regarding the current context using the Context Management Module services and generate a response for the user based on this information. The response is sent to the user, and he/she can start using the application. During further communication the Server Application Controller performs a session refresh operation each time it receives the request from the client and sends the response. If there is an interruption in the session, and the user tries to login from the other device (his/her computer) after a delay, a login procedure will start in the same manner. However, because an interrupted session is found by the Session Management Module, a response from the user request will notify the client application about the current session, and the user will be prompted if he/she wants to continue the previous session, and if he/she confirms the session information will be gathered from the Session Management Module, and the response containing the session data will be sent to the client application. When the session data is received on the client application, the last saved session state can be loaded.

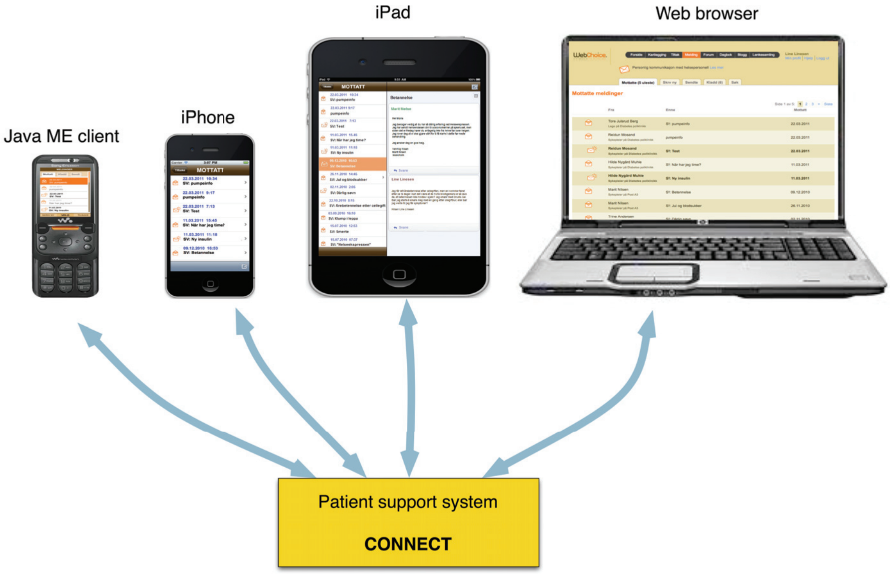


Figure 11. Different client types [38]

By using the proposed framework we implemented a server application using a Java Standard Edition platform (deployed on an Apache Tomcat server) and three types of client applications (a Java ME client application, an iOS client application, and a web client application) on which was performed a series of tests measuring performance and scalability of the system when session management functionality is provided. For testing purposes only messaging functionality is implemented in the test environment.

The developed testing environment and different client applications demonstrated how a proposed framework could be adapted and used on different developer platforms. For example, in Figure 11 it is shown how the interface for accessing the CONNECT system can be adapted for different (mobile) device types and their characteristics using the proposed framework.

During the testing phase session management time overhead was measured on different types of client applications and it was concluded that measured time does not present a problem.

Additionally, system scalability was determined by measuring time overhead when there were 10, 20, 50, 70 and 100 simultaneous users. The results showed that measured time overhead is acceptable and that scalability of the system is not substantially affected by adding session and content management functionality based on the described framework.

Contributions: The paper proposes the generic and modular architecture and design framework that provides support for the development of user friendly and context-specific interfaces with advanced security, session, content, and mobility management features. The framework enables easier implementation, maintenance, and adaptation of patient support systems for different types of terminals, networks, and system functionalities. Utilization of the proposed framework enables the seamless delivery of context-adapted information at the point of need independent of the user's current location and time, thus enabling utilization of the full potential of mobile device features in a patient support system such as CONNECT system. In addition to mobility management functionalities, the framework is also adapted to support interface, security, and application logic.

During the research work we studied how efficient support for application mobility can be implemented. The literature review showed different approaches regarding how session (application) mobility can be supported (client side, server side, proxy server, middleware) and revealed limitations and advantages of each approach (mobility literature review is presented in the chapter 3.1.1). In this project we decided to place session management functionalities as part of the client and server architecture framework (the CONNECT mobility framework). The main reason for choosing this approach is since it enabled secure and user-friendly session management functionalities with minimum requirements from the user (implementation of session management functionality allows a user to start interacting with the service over one device and when the user changes a device and opens a new communication channel the session is adapted and transferred automatically). Additionally, this approach does not require implementing extra functionalities on the client side (e.g., establishing and managing a communication channel between (mobile) devices for transferring the session data) or proxy server (e.g., deploying security architecture to protect user sensitive data on the proxy server).

Additionally, the CONNECT framework is not dependent on any specific developer platform, access network, or device type. Consequently, developers are fully supported to develop applications for different terminals utilizing devices, developer platforms, and/or OS specific features and interface design elements. The modular architecture enables better organization of the system functionalities, easy implementation and adaptation for different systems, easy integration with external systems and their functionalities, as well as the possibility of re-utilizing the same modules for different services and applications. The proposed framework facilitates the implementation of a more consistent and easily managed application that can automatically adapt interface and application content to the characteristics of device. The framework does not define a specific context adaptation mechanism that must be utilized during implementation, but rather support integration and utilization of different mechanisms found in the literature to provide adaptation of content and security mechanisms (such as [284-288, 291, 293, 295-301] described in the literature overview in the chapter 3.1.1) for specific usage scenarios.

In this paper, we have chosen to focus mainly on enabling session mobility (or application mobility / application roaming) since this functionality is currently not widely supported. However, we also investigated how terminal mobility (change of point of attachment to the network) can be efficiently managed in a secure and user-friendly manner. Handover and roaming across different technologies (and possibly also network providers) means crossing domains that are not equally well protected. Since the CONNECT framework provides end-to-end security using secure HTTPS connection and strong authentication, the paper focused mainly on preserving secure and user-friendly access to a patient support system when mobile node changes the access network that results in change of mobile node's IP address and requirement for reestablishing the new communication channel. The intra-access network handover can be provided by standard mobility management features of the wireless network (for example, cellular networks such as GSM and UMTS have their own micro mobility handling mechanisms) while communication between client and server is preserved and protected by end-to-end security provided by an HTTPS connection. Utilization of standard macro mobility software and services on the network layer (such as Mobile IP and Mobile VPN) was considered to enable macro mobility management. However, this approach was found not appropriate for this specific problem space for two main reasons:

Security. If the client device changes network, the security management during reconnection is transferred to the particular mobility software such as Mobile IP or Mobile VPN and the reconnection is not further controlled by the Security Management Module in the application. This can raise security related issues during session persistence and management process if the third party software providers do not support required security and privacy protection mechanisms. If this approach is chosen, a specific agreement between the CONNECT service provider and a third party mobility provider must be established making sure that the data is managed properly and according to the security policy during reconnection.

Usability. Third party mobility management services can require some additional information from the user during connection re-establishment and for user re-authentication, and this type of user interaction would not be controlled by the Interface Management module of the framework. As a result, inconsistency of the system interface design would probably occur because different systems do not use the same interface elements design.

An alternative would be to include management of Mobile IP or Mobile VPN as part of the CONNECT framework and place it under the same security policy and interface design rules. However, this alternative was not chosen since it would not enable high enough level of flexibility and the possibility to develop a generic solution that is applicable to all types of client devices and communication networks without an extra requirement for installations and adjustments from users.

Due to this reason, in the paper we propose that change of access networks should be handled in the CONNECT mobility framework on the application layer (by the Terminal Mobility Manager). The Terminal Mobility manager is in charge of sensing the access network change and initiating user re-authentication over the new communication channel when network change occurs, while intermittent connectivity is performed only by retransmission capabilities in the TCP protocol. After user is successfully authenticated, the application can continue communication over the new HTTPS connection. Since the new user authentication must be initiated when the HTTPS channel is reestablished on the new communication channel, putting mobility management logic as part of the framework can leverage security and interface functionalities implemented in other modules, protecting users' privacy while preserving an unified application design. Additionally, no extra software and services are required from a third party to provide support for terminal mobility management, simplifying deployment.

Usage of the proposed framework can simplify development of mobile healthcare applications with similar security and mobility requirements. However, the framework must be implemented specifically for each development platform to fully utilize the potential of the mobile terminal functionalities and specific interface characteristics. For this reason, in the paper it is proposed to standardize functionalities for enabling application mobility in the manner that is described through the CONNECT framework for both client and server operating systems, and by creating the dedicated middleware functionalities as part of the client and server operating system make mobility features more available.

Limitations: The CONNECT patient support system and CONNECT Mobile application developed as part of the CONNECT project offer different functionalities to patients. However, session management functionalities are currently supported and tested only for the messaging module. Since acceptable performance and scalability results were gained through the system testing so far, the plan is to implement session management functionalities also for other functionalities, and perform and compare further testing results making sure that there are no bottlenecks and unidentified performance issues.

For the testing purpose the client applications are developed for three different developer platforms: Java ME (available on a wide range of currently sold mobile phones), iOS (supported by iPod Touch, iPhone and iPad) and web based (support access over different terminals using web browser). Consequently, context adaptation features of the framework could be utilized and tested to a further extent. Additional support can be easily added for Android, Mobile Windows, and other (mobile and stationary) developer platforms, and further work in this area is planned in the future. Utilization of the support tools for cross-platform development (e.g., [116], [117], [118]) can be used to automate this process further and translate once written application logic code to different mobile developer platforms.

During the testing process the system performance and scalability is measured with the goal to identify overhead introduced by session management functionality. Testing of terminal management functionalities is not performed so far. Further tests and comparisons of the performance of the mobility management functionalities provided by the CONNECT framework and other standard mobility support services is planed to provide additional evaluation of the proposed mobility management solution. Additionally, the final testing of the proposed system is planned during the pilot study by the real potential users, with the goal to assess the usefulness and acceptance of the proposed mobility management solution.

Chapter 4: Conclusion and future work

This chapter contains the summary and discussion of the research contributions presented in the dissertation. The last section shows a short overview of future work in the research area of development and deployment of mobile healthcare services and potential directions for further development the CONNECT project and mobile application(s).

4.1 Discussion of the contributions

The dissertation addresses research issues and challenges related to development, deployment, and integration of the mobile services in healthcare information systems, by putting them in the more specific context of patient support systems such as CONNECT. In the initial phase of the research process through the performed survey of the related research work we researched how mobile services are and how they can be used in the healthcare sector, identified the main challenges that influences wide deployment and acceptance of the mobile devices and services, and investigated how the identified issues could be addressed in accordance with specific characteristics of mobile devices and in the context of the CONNECT patient support system (Paper I). The survey paper revealed the existence of the business need for development of mobile healthcare services and their integration with healthcare information systems that is recognized in both research domain and industry, and described some of the current research that is addressing current challenges introduced by specific characteristics and new contexts of use of mobile terminals for delivery of healthcare related information and services. The main objective of the research work presented in the dissertation was to solve issues related to enabling mobile access to healthcare information system by development and analysis of a research artifact - CONNECT Mobile application, and through this process to address the main challenges that are related to wide deployment, user-acceptance, and integration of mobile services to the CONNECT system. Different research issues regarding usability, security, and mobility and their correlation is addressed in the next three research papers contained in the dissertation (Papers II-IV).

In the research area of development of user-friendly and useful mobile healthcare information services (Paper II), through involvement of different system stakeholders and by using several usability evaluation and participatory design methods in the system development and evaluation process, the user requirements and expectations from the CONNECT Mobile application were identified and this information is used to develop and adapt application's design and functionality. The knowledge gained in this process can be further used for future development of the CONNECT system to support user-friendly access over new types of mobile terminals (e.g., smart phones, tablets) and the development and "mobilizing" of other healthcare information services for patients with similar functionalities and design requirements. The feedback from patients showed that they accept the CONNECT Mobile application in addition to a web application. Even though the full web version is still preferred when they have access to a PC, they found the CONNECT Mobile application useful and identified new usage scenarios for the mobile application (e.g., when outside in garden, on the way to treatment and back, when relaxing at home, etc.), confirming the need for enabling additional mobile access to the CONNECT system besides standard web application. Based on the received feedback the general recommendation is that healthcare information services for patients should be developed as a single system that can be accessed through different types of terminals (PCs, laptops, mobile phones, smartphones), while design and functionalities of different applications are adjusted to the current context of use (e.g., type of terminal, terminal capabilities, type of access network) preserving in this manner user-friendliness and usefulness of the service for different usage scenarios.

Security issues are identified as a significant challenge when developing and integrating mobile services in healthcare information systems. Due to this reason it is researched the security requirements in Norway defined to ensure security and privacy of personal (medical) data. The main conclusion was that due to the lack of a mobile authentication mechanisms that is accepted for protection of sensitive patient data, none of the information services currently implemented in the hospital information system in Oslo University Hospital is accessible over mobile terminals (access is limited only to PC usage). For this reason, we have proposed a security architecture for enabling mobile access to healthcare information systems that ensures secure authentication and communication between the CONNECT Mobile application and the hospital information system (Paper III). We also described how the proposed architecture can be integrated in the specific security architecture implemented at the Oslo University Hospital, and discussed how it complies with the security legislation. Besides security, the usability of the authentication solution is also considered during development, ensuring that the application is available and easily accessed for all potential users. The proposed solution does not introduce any additional binding to a network provider, mobile phone manufacturer, bank system or require additional installation and setup on the mobile device by potential users. The proposed security architecture is developed mainly for enabling patients mobile access to the CONNECT system, but it can be also used by any other healthcare services implemented in the hospital information system to enable mobile access. Additionally, even though the paper describes compliance and integration to one specific hospital information system, the security architecture can be easily transferred and adjusted to different (healthcare) information systems and contexts of use. The proposed architecture shows how authentication of the user can be provided without limiting and downgrading the usability and accessibility of the system, by utilizing specific characteristics of the mobile devices and adjusting them to the defined security requirements. This is an especially valuable feature for services that require availability and easy access to a great number of people, such as healthcare information services.

Usability and security issues are additionally addressed in the context of development of patient support systems that enable seamless application mobility and content adaptation across different terminals and/or access networks (Paper IV). We have developed a mobility framework that provides support for managing both application and terminal mobility in a secure and user-friendly manner. Since the importance of enabling access to the CONNECT system over various devices and adaptation of its functionalities and design to the current context of use is previously identified, this framework is developed with the goal to support easier transfer and adaptation of the system functionalities to different terminals and context of use. The framework is initially developed as a part of the CONNECT patient support system, but it can be also used for enabling session management and context adaptation for a wide range of (healthcare) services and applications that require these functionalities. The framework can be especially valuable for the systems that manage sensitive private information and require additional adaptation of the security mechanisms to different contexts of use.

The CONNECT Mobile application that enables mobile access to the CONNECT patient support system is the instantiation of the artifact created through the described research process. Throughout the development process, different research objectives are addressed and a user-friendly, useful, and well-accepted mobile application was created in the process. The artifact of the described research process, besides the CONNECT Mobile application, is also the proposed security architecture that enables secure access to the patient's private data without decreasing the usability of the system, and the CONNECT mobility framework that enables secure and user-friendly handling of mobility functionalities across different network types and access terminals. Even though the artifacts are created in the context of the specific research project and CONNECT patient support system the new knowledge that they provide can be easily applied to development and integration of mobile applications and services in other types of healthcare information systems. The research results gained through the work on the dissertation can be used for further development of more secure and user-friendly mobile healthcare applications that can extend the accessibility of the healthcare information services and provide services at the point-of-need. Additionally, since very similar challenges and research issues can be found in other research areas that are working on integration of mobile services in everyday practices (especially the ones that handle sensitive and private data such as government, banking, etc.), the contributions from the dissertation can be applied to an many other of use cases.

4.2 Future work in development, deployment, and integration of mobile services in healthcare

As part of the work on the dissertation, different issues regarding usability, security, and mobility in the research area of development and integration of mobile services in healthcare information services are addressed, but also numerous other challenges and issues are identified. This section will provide discussion regarding future work in this research area and possible directions for further work and improvements of the CONNECT Mobile application(s).

Adaptation for different users

Complying design and functionalities of mobile healthcare information services to fit the users requirements and expectations is one of the main prerequisites for wide acceptance and utilization of mobile services in everyday healthcare management and delivery, and an area that requires further research work. As noted in the usability literature overview in Chapter 3.1.1, when developing any type of service, especially for use in the healthcare sector, it is important to identify requirements and needs from different types of future users, and to develop a system adjusted for the majority of the population, including users with special needs. The literary review revealed many research projects that are studying how design requirements can be adapted and used to provide support for different user groups (e.g., users with specific vision or hearing problems and elderly). Utilization and adoption of this knowledge in the development of mobile healthcare applications could help to create services that are more accessible and easy to use for all users. The work presented in the dissertation addresses the issues of development of user-friendly and well-accepted mobile healthcare services, however one of the main limitation (as previously concluded in Chapter 3.2) is the limited number of users and user groups that participated in mobile application development and evaluation phases. Due to this reason, for future work in the CONNECT project it is planned to research what are further adaptations and developments of the mobile application required by different user groups (e.g., users with special needs and users in different gender and age groups) and how they are related to different contexts of use (e.g., using different devices, access networks, usage scenarios).

Adaptation for different contexts of use

In additions to patients, mobile services can bring equally useful functionalities and features to healthcare providers. In the literature there are numerous projects that show how mobile systems can improve productivity of healthcare providers and reduce costs of health institutions, and how identified issues can be addressed (e.g., [310-312]). Some of the potential usage scenarios can be: on-the-spot emergency, home care, and situations where care providers don't have a fixed place of work or need to look up relevant information resources such as clinical guidelines. For the future work on the CONNECT project development of an additional mobile application that will enable mobile access to CONNECT system for healthcare providers is also planned. Some challenges when developing mobile applications for healthcare providers are very similar to the ones where mobile services are used by patients (for example, there are similar problems related to usability [313, 314], acceptability [315, 316], security [317, 318], and mobility [319, 320]). However, implementation of different system features and identification and utilization of different set of design rules is required because types of users and usage scenarios differ. The further research work in the CONNECT project is planned to provide additional knowledge regarding new potential usage scenarios and new user requirements and expectations towards the utilization of the CONNECT system in the new context of use.

Even though the topic of implementation of mobile services in developing countries is not covered in the dissertation, this is also one usage scenario where mobile devices and services may make very valuable contributions. Mobility, low price of terminals, possibility for adaptation to different situations, and usage scenarios are just some of the factors that make mobile technologies the right choice for enabling easy and location independent access to healthcare information services in developing countries. However, challenges that must be addressed are very different from those in developed countries (e.g., power consumption and preservation, different user requirements, different cultural and educational environments, security problems when sharing a mobile terminal among a large number of users, and varying network coverage [321]). This problem space is identified and addressed through many research projects that investigate different issues and challenges for providing more efficient healthcare services at a lower cost, accessible to people living in rural areas of developing countries (e.g., [322-324]).

Utilization of new technologies

New types of mobile devices (such as smart phones and tablet PCs), mobile and broadband networks (such as 3G and 4G) and operating systems (such as iOS, Android, and Windows Mobile) introduce the possibility for further adaptations and improvements of current mobile (healthcare) services and their utilization in the new usage scenarios. However, before they can be widely used and integrated in healthcare information systems further research that address the new challenges introduced by their specific features and context of use is needed (e.g., identification of new design and functionality requirements and investigation of their correlation with existing system interfaces and implementation, investigation of implemented and supported security mechanisms and their compliance with security regulations and requirements, research what adaptation requirements are needed for the general healthcare information systems to provide support for the new contexts of use). This dissertation describes how some of these challenges are addressed in the context of deployment and integration of standard mobile phones in order to provide mobile access to the CONNECT patient support system. Additionally, the mobility framework introduced in [38] provides support for easy further development of the CONNECT system and for enabling new access methods over different types of (mobile) terminals and adaptation of their design and functionalities. The plan for future work on the CONNECT project is to apply the gained knowledge in the further studies that will research how new technologies can be used to make the healthcare information services for patients more accessible, useful, and user-friendly.

Even though the utilization of the sensor technology in (mobile) healthcare information services is not part of the dissertation, this technology has great potential to add valuable contributions in this area. Utilization of sensors for measuring of physiological parameters of patients (such as patients' vital signs, blood pressure, or heart rate) and continuous monitoring, and implementation of advanced context identification and management functionalities are just some of the new and advanced features that sensor technology can provide to mobile healthcare services. However, several concerns, such as interoperability, power consumption, security and privacy, usability, and user acceptance are still open issues related to wide utilization of this technology in (healthcare) mobile services [17, 325-327].

New and emerging security threats and issues

Improvements in technology also brings along new security threats and issues that require adaptation or replacement of existing security mechanisms. For example, the same authentication mechanism can be implemented and used differently on various terminals due to devices specific characteristics, adding more inconsistency and higher requirements for adaptation (one example is BankID authentication solution described in Chapter 2.2.4 that provides one general solution implemented for standard web browser and separate two solutions adapted for mobile device utilization). The security literature overview in chapter 3.1.1 discuss how different standard authentication mechanisms can be used and adapted to mobile devices and their characteristics and which limitations these adaptations can introduce. Additional requirement for security mechanisms implemented in (mobile) healthcare information services besides compliance with security requirements and legislation is the preservation of usability and mobility features of the system. We believe that the security solutions that provide high protection of private data and do not limit usability and mobility of the services will play a crucial role in the future of development and integration of mobile services in healthcare information systems. As part of the future research work in the CONNECT project a continuation of the efforts to enable secure and easy access to the patient support system over different terminals and access networks is planned. Utilization of new technologies to enable more flexible and accessible systems also introduces the requirement for the development of new security mechanisms or adaptation of ones already implemented. For example, providing access to the CONNECT system using a mobile application that runs on a tablet PC that does not have a SIM card slot requires implementation of the new authentication mechanisms since the security solution for mobile devices proposed in [37] is not applicable to this new context of use (the new device does not have a SIM card and access to a mobile network) and the standard security mechanism used for the web application on a PC such as Buypass and BankID is not accessible (due to the lack of standard card reader adapted for this type of devices and lack of support for a JavaScript plug-in for web browsers that run BankID services). To ease integration of new authentication mechanisms to the CONNECT system and their utilization in the new context of use the CONNECT Mobility framework introduced in [38] will be utilized.

Resolving the existing issues related to usability, security, and mobility in the context of mobile devices and their unique capabilities that differ them from stationary terminals, will provide the required knowledge needed for integration and deployment of mobile services in healthcare information systems, not just for patients but in general. Additionally, fast development and improvement of mobile devices and mobile technologies can further enhance the need for these services and speed up their integration, since the mobile devices already have a very central place in peoples every day life and organization of our activities, including health management. Many people already use healthcare mobile applications for management of health related issues, and a secure, mobile, and user friendly integration with other healthcare information systems and patients' health information can further improve their usefulness and efficiency, and enable them to reach their full potential in the delivery of healthcare services and information at the right place and in the right time.

Bibliography

[1] Y. Y. Shieh, *et al.*, "Mobile Healthcare: Opportunities and Challenges," in *International Conference on the Management of Mobile Business*, Toronto, Ont., 2007, pp. 50-50.

[2] N. S. Gollol Raju, *et al.*, "Status of Mobile Computing in Health Care: An Evidence Study," in *26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEMBS '04)* 2004, pp. 3274-3277.

[3] C. M. Ruland, *et al.*, "User requirements for a practice-integrated nurse-administered online communication service for cancer patients," *Stud Health Technol Inform,* vol. 146, pp. 221-5, 2009.

[4] B. Spring, *et al.*, "Multiple behavior changes in diet and activity: a randomized controlled trial using mobile technology," *Arch Intern Med,* vol. 172, pp. 789-96, May 28 2012.

[5] K. Yun Sik, "International standards for building Electronic Health Record (EHR)," in *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry, HEALTHCOM 2005*, 2005, pp. 18-23.

[6] International Organization for Standardization, "ISO/TR 20514:2005, Health informatics -- Electronic health record," in *Definition, scope and context*, ed, 2005.

[7] Y. Wan, "Application of EHR in Health Care," in *Second International Conference on Multimedia and Information Technology (MMIT)*, 2010, pp. 60-63.

[8] P. C. Tang, *et al.*, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," *J Am Med Inform Assoc,* vol. 13, pp. 121-6, Mar-Apr 2006.

[9] J. S. Luo, "Personal health records," *Primary Psychiatry,* vol. 13, pp. 19-21, 2006.

[10] M. I. Kim and K. B. Johnson, "Personal health records: evaluation of functionality and utility," *J Am Med Inform Assoc,* vol. 9, pp. 171-80, Mar-Apr 2002.

[11] Norwegian Directorate of Health. (2009, July 21). *Norway and Health. An introduction*. Available: www.helsedirektoratet.no

[12] Norwegian Ministry of Health and Care Services, "The Coordination Reform," Norwegian Ministry of Health and Care Services2008.

[13] Ministry of Health and Care Services, "National Health Plan for Norway (2007-2010)," Oslo2006.

[14] Ministry of Health and Care Services, "Interaction 2.0 - National eHealth strategy 2008-2013," Oslo2010.

[15] G. Eysenbach, "What is e-health?," *J Med Internet Res,* vol. 3, p. e20, 2001.

[16] U. Varshney, "Pervasive healthcare," *Computer,* vol. 36, pp. 138-140, 2003.

[17] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mob. Netw. Appl.,* vol. 12, pp. 113-127, 2007.

[18] S. Standing and C. Standing, "Mobile technology and healthcare: the adoption issues and systemic problems," *Int J Electron Healthc,* vol. 4, pp. 221-35, 2008.

[19] R. S. H. Istepanian, *et al.*, "Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity," *IEEE Transactions on Information Technology in Biomedicine,* vol. 8, pp. 405-414, 2004.

[20] C. M. Ruland, *et al.*, "Designing tailored Internet support to assist cancer patients in illness management," *AMIA Annu Symp Proc,* vol. 11, pp. 635-9, 2007.

[21] C. M. Ruland, *et al.*, "Effects of an Internet Support System to Assist Cancer Patients in Reducing Symptom Distress: A Randomized Controlled Trial," *Cancer Nurs,* vol. 9, p. 9, Apr 9 2012.

[22] L. Heyn, *et al.*, "Effects of an interactive tailored patient assessment on patient-clinician communication in cancer care," *Psychooncology,* vol. 15, Sep 15 2011.

[23] L. Heyn, *et al.*, "Effects of an interactive tailored patient assessment tool on eliciting and responding to cancer patients' cues and concerns in clinical consultations with physicians and nurses," *Patient Educ Couns,* vol. 86, pp. 158-65, Feb 2012.

[24] C. M. Ruland, "Clinicians' perceived usefulness of a support system for patient-centered cancer care," *Stud Health Technol Inform,* vol. 124, pp. 624-30, 2006.

[25] C. M. Ruland, *et al.*, "Effects of a computer-supported interactive tailored patient assessment tool on patient care, symptom distress, and patients' need for symptom management support: a randomized clinical trial," *J Am Med Inform Assoc,* vol. 17, pp. 403-10, Jul-Aug 2010.

[26] C. M. Ruland, *et al.*, "Developing a shared electronic health record for patients and clinicians," *Stud Health Technol Inform,* vol. 136, pp. 57-62, 2008.

[27] Helsedirektoratet. (2012, Oct. 30). *Elin-k prosjektet har bidratt til utvikling av standardiserte løsninger for elektronisk informasjonsutveksling mellom pleie- og omsorgstjenesten i kommunene, fastleger og sykehus*. Available: www.kith.no/templates/kith_WebPage____3666.aspx

[28] (2012, Oct. 01). *Norwegian Health Network, Norsk Helsenett*. Available: http://www.nhn.no/english-1

[29] A. R. Hevner, *et al.*, "Design science in information system research.," *MIS Quarterly,* vol. 28, pp. 75-105, March 2004 2004.

[30] K. Peffers, *et al.*, "The Design Science Research Process: A Model for Producing and Presenting Information Systems Research," 2006.

[31] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decis. Support Syst.,* vol. 15, pp. 251-266, 1995.

[32] J. G. Walls, *et al.*, "Building an Information System Design Theory for Vigilant EIS," *Information Systems Research,* vol. 3, pp. 36-59, 1992.

[33] S. Price and R. Summers, "Mobile Healthcare in the Home Environment," in *28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '06)* 2006, pp. 6446-6448.

[34] J. Mirkovic, *et al.*, "Review of projects using mobile devices and mobile applications in healthcare," in *Scandinavian conference on Health Informatics*, Arendal, Norway, 2009.

[35] W. Kai, *et al.*, "Pervasive and Trustworthy Healthcare," in *22nd International Conference on Advanced Information Networking and Applications - Workshops (AINAW 2008)* 2008, pp. 750-755.

[36] J. Mirkovic*, et al.*, "Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management," in *eTELEMED 2011, The Third International Conference on eHealth, Telemedicine, and Social Medicine*, Gosier, Guadeloupe, France, 2011, pp. 64 - 71.

[37] J. Mirkovic*, et al.*, "Secure Solution for Mobile Access to Patient's Health Care Record," in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, Columbia, Missouri, USA, 2011.

[38] J. Mirkovic*, et al.*, "A framework for the development of ubiquitous patient support systems," in *6th International Conference on Pervasive Computing Tech-nologies for Healthcare*, San Diego, California, USA, 2012.

[39] A. Jeneson*, et al.*, "Comparing Messages in an Online Communication Forum for Cancer Patients with Patients' Messages to a Clinical Nurse Specialist," in *Medinfo 2007 Congress*, Brisbane, 2007, pp. 1473-1474.

[40] R. Andersen*, et al.*, *Clustering techniques for organizing cancer-related concepts into meaningful groups for patients*, 2005.

[41] J. Mirkovic*, et al.*, "A framework for the development of ubiquitous patient support systems," *Journal of Pervasive and Mobile Computing,* 2011.

[42] International Organization for Standardization, "Ergonomics of human-system interaction -- Usability methods supporting human-centred design," ed, 2005.

[43] B. Shackel, "Usability: context, framework, definition, design and evaluation," in *Human factors for informatics usability*, ed: Cambridge University Press, 1991, pp. 21-37.

[44] P. W. Jordan, *An introduction to usability*: Taylor & Francis, 1998.

[45] J. Nielsen, *Usability Engineering*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1995.

[46] B. Shneiderman, *Designing the user interface: strategies for effective human-computer interaction*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1986.

[47] J. Preece*, et al.*, *Interaction Design*, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 2002.

[48] D. J. Mayhew, "The usability engineering lifecycle," presented at the CHI '99 extended abstracts on Human factors in computing systems, Pittsburgh, Pennsylvania, 1999.

[49] D. Norman, *The Design of Everyday Things*: Basic Books, 2002.

[50] J. R. Levis, "Usability testing," in *Handbook of Human Factors and Ergonomics*. vol. 3rd, ed New York, NY: John Wiley, 2006, pp. 1275 - 1316.

[51] J. S. Dumas, "User-based evaluations," in *The human-computer interaction handbook*, A. J. Julie and S. Andrew, Eds., ed: L. Erlbaum Associates Inc., 2003, pp. 1093-1117.

[52] J. P. Chin*, et al.*, "Development of an instrument measuring user satisfaction of the human-computer interface," presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, Washington, D.C., United States, 1988.

[53] J. Kirakowski and A. Dillon. (1988, The computer user satisfaction inventory (CUSI): Manual and scoring key.

[54] J. Kirakowski and M. Corbett, "SUMI: the Software Usability Measurement Inventory," *British Journal of Educational Technology,* vol. 24, pp. 210-212, 1993.

[55] J. Nielsen, "Usability inspection methods," presented at the Conference companion on Human factors in computing systems, Boston, Massachusetts, United States, 1994.

[56] M. W. Jaspers, "A comparison of usability methods for testing interactive health technologies: methodological aspects and empirical evidence," *Int J Med Inform,* vol. 78, pp. 340-53, May 2009.

[57] E. Bertini*, et al.*, "Appropriating and assessing heuristics for mobile computing," presented at the Proceedings of the working conference on Advanced Visual Interfaces, Venezia, Italy, 2006.

[58] *Design at Work: Cooperative Design of Computer Systems*: L. Erlbaum Associates Inc., 1991.

[59] T. Bratteteig and I. Wagner, "Epilogue: A Multidisciplinary Take on Digital Design," in *Exploring digital design : multi-disciplinary design practices*, ed: Springer, 2010, pp. 283 - 286.

[60] T. Bratteteig*, et al.*, "Research Practices in Digital Design
Exploring Digital Design," I. Wagner*, et al.*, Eds., ed: Springer London, 2010, pp. 17-54.

[61] F. Kensing and J. Blomberg, "Participatory Design: Issues and Concerns," *Comput. Supported Coop. Work,* vol. 7, pp. 167-185, 1998.

[62] K. Bodker*, et al.*, *Participatory It Design: Designing for Business and Workplace Realities*: MIT Press, 2004.

[63] D. Gollmann, *Computer Security*, 2nd ed. Chichester, West Sussex, England: John Wiley & Sons, 2006.

[64] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 1st ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2007.

[65] Christian Neuhaus*, et al.*, "Survey on Healthcare IT systems, Standards, Regulations and Security," Universitaatsverlag Potsdam, Potsdam2011.

[66] International Organization for Standardization and International Electro-technical Commision. (2009, June 15). *ISO/IEC 27000-series standard*. Available: http://www.27000.org/

[67] The 27000.org directory. (2008, June 15). *An Introduction To ISO 27799*. Available: http://www.27000.org/iso-27799.html

[68] International Organization for Standardization. (2011, June 15). *ISO/TR 27809:2007 Health Informatics -- Measures for ensuring patient safety of health software*. Available: http://www.iso.org/iso/catalogue_detail?csnumber=44320

[69] International Organization for Standardization, "ISO/TS 22600-1:2006 Health informatics -- Privilege management and access control," in *Part 1: Overview and policy management*, ed, 2006.

[70] International Organization for Standardization, "ISO/TS 13606-4:2009 Health informatics - Electronic health record communication," in *Part 4: Security*, ed, 2009.

[71] A. Appari*, et al.*, "HIPAA Compliance: An Examination of Institutional and Market Forces," in *The 8th Workshop on Economics of Information Security*, London, 2009.

[72] U. S. Department of Health and Human Services. (2003, June 6). *Summary of the HIPAA Privacy*

Rule. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[73] U.S. Department of Health and Human Services. (2003, June 06). *Summary of the HIPAA Security Rule*. Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[74] L. F. Freedman. (2009, June 1). *The Health Information Technology for Economic and Clinical Health Act (HITECH Act): implications for the adoption of health information technology, HIPAA, and privacy and security issues*. Available: http://www.nixonpeabody.com/publications_detail3.asp?ID=2621

[75] K. Peng*, et al.*, "An identity authentication system based on mobile phone token," in *IEEE International Conference on Network Infrastructure and Digital Content*, 2009, pp. 570-575.

[76] *Directive 95/46/EC,* The European Parlament and the council, 1995.

[77] European Parlament and The Council. (1995, Oct. 11). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[78] *Directive 2002/58/EC,* European Parliament and the Council, 2001.

[79] The Data Protection Agency. (2011, June 25). *About The Data Protection Agency*. Available: http://www.datatilsynet.no/templates/Page____194.aspx

[80] *LOV-2000-04-14-31 Lov om behandling av personopplysninger (personopplysningsloven),* Justis- og beredskapsdepartementet, 2000.

[81] *FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften)*, 2000.

[82] *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT),* Finanstilsynet, 2003.

[83] *LOV-2001-05-18-24 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven),* Helse- og omsorgsdepartementet, 2001.

[84] *LOV-1999-07-02-64 Lov om helsepersonell m.v. (helsepersonelloven),* Helse- og omsorgsdepartementet, 1999.

[85] *LOV-1999-07-02-63 Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven) [pasientrettighetsloven],* Helse og omsorgsdepartementet 2012, 1999.

[86] Helsedirektoratet. (2012, Oct. 11). *Code of Conduct*. Available: http://www.helsedirektoratet.no/english/topics/code-of-conduct/Sider/default.aspx

[87] Fornyings- administrasjons- og kirkedepartementet. (2008, June 25). *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*. Available: http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli.html?id=505958

[88] The Ministry of Modernisation Norway, "Requirements specification for PKI for the public sector," 2005.

[89] A. Haraldsen. (2010, June 25). *DIFI velger Buypass og Commfides som leverandører av eID*. Available: http://www.norstella.no/difi-velger-buypass-og-commfides-som-leverandoerer-av-eid.4779911-124296.html

[90] Buypass. (2011, June 25). *Buypass Securing Transactions*. Available: http://www.buypass.no/

[91] Commfides. (2011, June 25). *Commfides*. Available: https://www.commfides.com/

[92] Buypass. (2011, June 25). *Buypass mobil*. Available: http://www.buypass.no/Brukersted/Mobil

[93] Bankenes Betalings Sentral AS. (2005, June 23). *BankID COI, White Paper*. Available: http://www.eurim.org.uk/activities/pi/BankIDWhitePaper.pdf

[94] BankID. *BankID på mobil*. Available: https://www.bankid.no/Dette-er-BankID/BankID-pa-mobil/

[95] S. Dixit and R. Prasad, *Wireless IP and Building the Mobile Internet*. Norwood, MA, USA: Artech House, Inc., 2002.

[96] F. Panken*, et al.*, "Open Access Networks - Architecture for Sharing Residential Access with Roaming WLAN Users," *Telektronikk,* vol. 2, 2006.

[97] F. Steuer*, et al.*, "Seamless mobility over broadband wireless networks," in *IST Mobile and Wireless Summit*, Dresden, Germany, 2005.

[98] SearchMobileComputing.com. (2001, July 25). *Definition - Personal Area Network (PAN)* . Available: http://searchmobilecomputing.techtarget.com/definition/personal-area-network

[99] Network Working Group. (2004, Jun 2). *Mobility Related Terminology*. Available: http://www.ietf.org/rfc/rfc3753.txt

[100] European Telecommunications Standards Institute. (2002, Jun 2). *ETSI TR 170 002 V3.1.1 Project MESA; Service Specification Group - Services and Applications; Definitions*. Available: http://www.etsi.org/deliver/etsi_tr/170000_170099/170002/03.01.01_60/tr_170002v030101p.pdf

[101] European Telecommunications Standards Institute. (2009, Jun 2). *User Group; Analysis of current End-to-End QoS standardization state*. Available: http://www.etsi.org/deliver/etsi_tr/102800_102899/102806/01.01.01_60/tr_102806v010101p.pdf

[102] European Telecommunications Standards Institute. (2009, Jun 2). *User Group; End-to-end QoS management at the Network Interfaces; Part 1: User's E2E QoS - Analysis of the NGN interfaces (user case)*. Available: http://www.etsi.org/deliver/etsi_tr/102800_102899/10280501/01.01.01_60/tr_10280501v010101p.pdf

[103] European Telecommunications Standards Institute. (2006, Jun 2). *Corporate telecommunication Networks (CN); Mobility for enterprise communication*. Available: http://www.etsi.org/deliver/etsi_tr/102400_102499/102477/01.01.01_60/tr_102477v010101p.pdf

[104] Network Working Group. (2009, Jun 2). *Session Initiation Protocol (SIP) Session Mobility*. Available: http://tools.ietf.org/html/rfc5631

[105] European Telecommunications Standards Institute. (2011, Jun 2). *Universal Mobile Telecommunications System (UMTS); LTE; All-IP network (AIPN) feasibility study (3GPP TR 22.978 version 10.0.0 Release 10)*. Available: http://www.etsi.org/deliver/etsi_tr/122900_122999/122978/10.00.00_60/tr_122978v100000p.pdf

[106] V. C. Zandy, "Application mobility," The University of Wisconsin - Madison, 2004.

[107] J. Bardram*, et al.*, "Supporting local mobility in healthcare by application roaming among heterogeneous devices," in *5th International Conference on Human Computer Interaction with*

Mobile Devices and Services, Udine, Italy, 2003, pp. 161--176.

[108] S. Koch, "Home telehealth - Current state and future trends," *International journal of medical informatics,* vol. 75, pp. 565-576, 2006.

[109] G. Shobha, *et al.*, "Medical Applications of Wireless Networks," in *Second International Conference on Systems and Networks Communications*, 2007, pp. 82-82.

[110] K. Yamauchi, *et al.*, "3G Mobile Phone Applications in Telemedicine - A Survey," in *Proceedings of the The Fifth International Conference on Computer and Information Technology*, 2005, pp. 956-960.

[111] M.-E. Maurer, *et al.*, "Mobile or desktop websites?: website usage on multitouch devices," presented at the Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries, Reykjavik, Iceland, 2010.

[112] G. Schmiedl, *et al.*, "Mobile phone web browsing: a study on usage and usability of the mobile web," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Bonn, Germany, 2009.

[113] J. Nielsen. (2009, Aug. 1). *Mobile Usability, First Findings*. Available: http://www.useit.com/alertbox/mobile-usability-study-1.html

[114] J. Nielsen. (2011, June 27). *Mobile Usability Update*. Available: http://www.useit.com/alertbox/mobile-usability.html

[115] Adobe Systems Inc. (2012, June 27). *Easily create apps with the only free open source framework that supports 7 mobile platforms*. Available: http://phonegap.com/

[116] (2011, July 18). *MonoTools for Visual Studio*. Available: http://mono-tools.com/

[117] (2011, July 18). *Xamarin. Building Cross-Platform Mobile Apps using C# and .NET*. Available: **http://xamarin.com/**

[118] (2011, July 18). *MoSync. The Open Source SDK for universal mobile application development*. Available: http://www.mosync.com/

[119] H. N. Chua, *et al.*, "Web-page adaptation framework for PC & mobile device collaboration," in *19th International Conference on Advanced Information Networking and Applications*, 2005, pp. 727-732 vol.2.

[120] R. Mizouni, *et al.*, "Challenges in "mobilizing" desktop applications: a new methodology for requirements engineering," in *International Conference on Innovations in Information Technology*, 2009, pp. 225-229.

[121] J. Nichols and T. Lau, "Mobilization by demonstration: using traces to re-author existing web sites," presented at the Proceedings of the 13th international conference on Intelligent user interfaces, Gran Canaria, Spain, 2008.

[122] D. Zhang, "Web content adaptation for mobile handheld devices," *Commun. ACM,* vol. 50, pp. 75-79, 2007.

[123] L. Qiao, *et al.*, "Information presentation on mobile devices: techniques and practices," presented at the Proceedings of the 10th Asia-Pacific web conference on Progress in WWW research and development, Shenyang, China, 2008.

[124] S. Shrestha, "Mobile web browsing: usability study," presented at the Proceedings of the 4th international conference on mobile technology, applications, and systems and the 1st international symposium on Computer human interaction in mobile technology, Singapore, 2007.

[125] International Standard Organization, "ISO 9241 Ergonomics of human-system interaction," in *Part 210: Human-centred design for interactive systems*, ed, 2010.

[126] W3C. (2010, July 26). *Mobile Web Application Best Practices, W3C Recommendation 14 December 2010*. Available: http://www.w3.org/TR/mwabp/

[127] Nokia. (2007, July 1). *S60 UI Style Guide*. Available: http://www.forum.nokia.com/info/sw.nokia.com/id/04c58d5a-84c3-42db-83d5-486c1cf3e6b3/S60_UI_Style_Guide_v1_3_en.pdf.html

[128] Nokia. (2010, Dec. 15). *Mobile developing and design guidelines*. Available: http://wiki.forum.nokia.com/index.php/Mobile_developing_and_design_guidelines

[129] SonyEricsson. (2010, Dec. 15). *Sony Ericsson UI Rulebook*. Available: http://developer.sonyericsson.com/wportal/devworld/downloads/download/dw-102212-uirulebook?cc=gb&lc=en

[130] Android Developers. (2012, Aug. 01). *Android Design*. Available: http://developer.android.com/design/index.html

[131] IOS Developer Library. (2012, Aug. 1). *iOS Human Interface Guidelines*. Available: http://developer.apple.com/library/ios/#DOCUMENTATION/UserExperience/Conceptual/MobileHIG/Introduction/Introduction.html

[132] M. Seraj and W. Chui Yin, "A study of User Interface Design principles and requirements for developing a Mobile learning prototype," in *2012 International Conference on Computer & Information Science (ICCIS)*, 2012, pp. 1014-1019.

[133] N. Ayob, *et al.*, "Three Layers Design Guideline for Mobile Application," in *International Conference on Information Management and Engineering*, 2009, pp. 427-431.

[134] T. Tse-Ming, *et al.*, "Status and Trend of E-book Applications for iOS Devices: A Developer's Perspective," in *13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD)*, 2012, pp. 157-161.

[135] T. Yung-Chung, *et al.*, "Integrated usability model for the multimedia mobile device development," in *2011 International Conference on Multimedia Technology (ICMT)*, 2011, pp. 5904-5907.

[136] R. Luckmann and A. Vidal, "Design of a handheld electronic pain, treatment and activity diary," *J Biomed Inform*, vol. 43, pp. S32-6, Oct 2010.

[137] M. Palmblad and B. Tiplady, "Electronic diaries and questionnaires: designing user interfaces that are easy for all patients to use," *Qual Life Res*, vol. 13, pp. 1199-207, Sep 2004.

[138] B. Falchuk, "Visual and interaction design themes in mobile healthcare," in *Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous*, 2009, pp. 1-10.

[139] S. Consolvo, *et al.*, "Design requirements for technologies that encourage physical activity," presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada, 2006.

[140] A. Lorenz, *et al.*, "Personalized mobile health monitoring for elderly," presented at the

Proceedings of the 9th international conference on Human computer interaction with mobile devices and services, Singapore, 2007.

[141] K. A. Siek, *et al.*, "Designing a Personal Health Application for Older Adults to Manage Medications: A Comprehensive Case Study," *J Med Syst,* vol. 12, p. 12, May 12 2011.

[142] D. Ahmad, *et al.*, "Experiences in designing personal health assistants for the impending aged generation," presented at the Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 2, Liverpool, United Kingdom, 2008.

[143] L. S. Liu, *et al.*, "Improving communication and social support for caregivers of high-risk infants through mobile technologies," presented at the Proceedings of the ACM 2011 conference on Computer supported cooperative work, Hangzhou, China, 2011.

[144] R. Mendoza-Gonzalez, *et al.*, "Guidelines for designing graphical user interfaces of mobile e-health communities," presented at the Proceedings of the 13th International Conference on Interaccion Persona-Ordenador, Elche, Spain, 2012.

[145] S. Chatterjee, *et al.*, "Examining the success factors for mobile work in healthcare: A deductive study," *Decis. Support Syst.,* vol. 46, pp. 620-633, 2009.

[146] J. Kjeldskov and M. B. Skov, "Exploring context-awareness for ubiquitous computing in the healthcare domain," *Personal Ubiquitous Comput.,* vol. 11, pp. 549-562, 2007.

[147] E. Ammenwerth, *et al.*, "Mobile information and communication tools in the hospital," *International journal of medical informatics,* vol. 57, pp. 21-40, 2000.

[148] L. Xue, *et al.*, "Mobile phone-based health application for women: a Singapore study," presented at the Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, 2011.

[149] T. Gegg-Harrison, *et al.*, "Porting a cancer treatment prediction to a mobile device," in *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2009, pp. 6218-6221.

[150] M. Persson, *et al.*, "A new improved distributed e-healthcare system based on open standards for depression treatment," presented at the Proceedings of the 3rd International Conference on Information and Communication Systems, Irbid, Jordan, 2012.

[151] J. Finkelstein and J. Wood, "Information technology for continuous patient health education," presented at the Proceedings of the 2011 conference on Information technology education, West Point, New York, USA, 2011.

[152] I. C. Chang, *et al.*, "Building mPHR to assist diabetics in self-healthcare management," in *Service Systems and Service Management (ICSSSM), 2010 7th International Conference on*, 2010, pp. 1-5.

[153] M. S. Iyengar, *et al.*, "GuideView: a system for developing structured, multimodal, multi-platform persuasive applications," presented at the Proceedings of the 4th International Conference on Persuasive Technology, Claremont, California, 2009.

[154] R. Challenor and S. Deegan, "What service users want: a new clinic results service. Can we satisfy both patients' needs and wants?," *Int J STD AIDS,* vol. 20, pp. 701-3, Oct 2009.

[155] N. Luo, *et al.*, "Acceptance of information and communication technologies for healthcare delivery: a SingHealth Polyclinics study," *Ann Acad Med Singapore,* vol. 38, pp. 529-8, Jun 2009.

[156] B. T. Horowitz. (2010, Dec. 30). *Mobile Health Apps to Triple by 2012, Presenting Challenges for Mobile Networks: Report*. Available: http://www.eweek.com/c/a/Health-Care-IT/Mhealth-Apps-to-Triple-by-2012-Presenting-Challenges-for-Mobile-Networks-Report-869725/

[157] A. Kleiboer*, et al.*, "Monitoring symptoms at home: what methods would cancer patients be comfortable using?," *Qual Life Res,* vol. 19, pp. 965-8, Sep 2010.

[158] H. Pinnock*, et al.*, "Professional and patient attitudes to using mobile phone technology to monitor asthma: questionnaire survey," *Prim Care Respir J,* vol. 15, pp. 237-45, Aug 2006.

[159] A. H. H. M. Mohamed*, et al.*, "MoHTAM: A Technology Acceptance Model for Mobile Health Applications," in *Developments in E-systems Engineering (DeSE), 2011*, 2011, pp. 13-18.

[160] A. H. H. M. Mohamed*, et al.*, "Does e-Health technology design affect m-Health informatics acceptance? A case study," in *Biomedical and Health Informatics (BHI), 2012 IEEE-EMBS International Conference on*, 2012, pp. 968-971.

[161] M. Mikkonen*, et al.*, "User and Concept Studies as Tools in Developing Mobile Communication Services for the Elderly," *Personal Ubiquitous Comput.,* vol. 6, pp. 113-124, 2002.

[162] E. Kangas and T. Kinnunen, "Applying user-centered design to mobile application development," *Commun. ACM,* vol. 48, pp. 55-59, 2005.

[163] C. C. Tsai*, et al.*, "Usability and feasibility of PmEB: a mobile phone application for monitoring real time caloric balance," *Mob. Netw. Appl.,* vol. 12, pp. 173-184, 2007.

[164] E. Arsand*, et al.*, "Usability of a Mobile Self-Help Tool for People with Diabetes: the Easy Health Diary," in *IEEE International Conference on Automation Science and Engineering*, 2007, pp. 863-868.

[165] D. Svanaes and G. Seland, "Putting the users center stage: role playing and low-fi prototyping enable end users to design mobile systems," presented at the Proceedings of the SIGCHI conference on Human factors in computing systems, Vienna, Austria, 2004.

[166] M. d. Sa and L. Carrico, "Lessons from early stages design of mobile applications," presented at the Proceedings of the 10th international conference on Human computer interaction with mobile devices and services, Amsterdam, The Netherlands, 2008.

[167] M. d. Sa and L. Carrico, "Low-fi prototyping for mobile devices," presented at the CHI '06 extended abstracts on Human factors in computing systems, Montréal, Québec, Canada, 2006.

[168] D. Bolchini*, et al.*, "FEATURE: 'Paper in screen' prototyping: an agile technique to anticipate the mobile experience," *Interactions,* vol. 16, pp. 29-33, 2009.

[169] M. Isomursu*, et al.*, "Experimental evaluation of five methods for collecting emotions in field settings with mobile applications," *International Journal of Human-Computer Studies,* vol. 65, pp. 404-418, 2007.

[170] C. K. Coursaris and D. J. Kim, "A Meta-Analytical Review of Empirical Mobile Usability Studies," *J. Usability Studies,* vol. 6, pp. 117-171, 2011.

[171] F. Balagtas-Fernandez and H. Hussmann, "A Methodology and Framework to Simplify Usability Analysis of Mobile Applications," presented at the Proceedings of the 2009 IEEE/ACM International Conference on Automated Software Engineering, 2009.

[172] L. Baillie, "Involving users in the design of multimodal mobile applications," in *26th*

International Conference on Information Technology Interfaces, 2004, pp. 329-334 Vol.1.

[173] NC State University. (2012, Aug 1). *Center for Universal Design*. Available: http://www.ncsu.edu/project/design-projects/udi/

[174] O. Plos and S. Buisine, "Universal design for mobile phones: a case study," presented at the CHI '06 extended abstracts on Human factors in computing systems, Montreal, Quebec, Canada, 2006.

[175] R. Hellman, "Universal design and mobile devices," presented at the Proceedings of the 4th international conference on Universal access in human computer interaction: coping with diversity, Beijing, China, 2007.

[176] J. Jaeyeob, "The research of mobile user interface design components from the standpoint of universal design for learning," in *Wireless and Mobile Technologies in Education, 2005. WMTE 2005. IEEE International Workshop on*, 2005, p. 3 pp.

[177] H. K. Jansson*, et al.*, "Accessible User Interfaces in a Mobile Logistics System," presented at the Proceedings of the 5th International on ConferenceUniversal Access in Human-Computer Interaction. Part II: Intelligent and Ubiquitous Interaction Environments, San Diego, CA, 2009.

[178] B. Ruiz*, et al.*, "Design for All in multimedia guides for museums," *Comput. Hum. Behav.,* vol. 27, pp. 1408-1415, 2011.

[179] C. H. Liu*, et al.*, "Optimizing the usability of mobile phones for individuals who are deaf," *Assist Technol,* vol. 22, pp. 115-27, Summer 2010.

[180] B. M. Chaudry*, et al.*, "Mobile interface design for low-literacy populations," presented at the Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, Miami, Florida, USA, 2012.

[181] A. Das*, et al.*, "Interaction design for cancer patients: do we need to take into account the effects of illness and medication?," presented at the Proceedings of the 2011 annual conference on Human factors in computing systems, Vancouver, BC, Canada, 2011.

[182] P. Klasnja*, et al.*, "Blowing in the wind: unanchored patient information work during cancer care," presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA, 2010.

[183] P. Verhaeghen and T. A. Salthouse, "Meta-analyses of age-cognition relations in adulthood: estimates of linear and nonlinear age effects and structural models," *Psychol Bull,* vol. 122, pp. 231-49, Nov 1997.

[184] T. A. Poynton, "Computer literacy across the lifespan: a review with implications for educators," *Computers in Human Behavior,* vol. 21, pp. 861-872, 2005.

[185] J. C. Marquie*, et al.*, "Do older adults underestimate their actual computer knowledge?," *Behaviour & Information Technology,* vol. 21, pp. 273-280, Jul-Aug 2002.

[186] N. Charness and E. A. Bosman, "Human factors and design for older adults," in *Handbook of the psychology of aging (3rd ed.)*. ed: San Diego, CA, US: Academic Press, 1990, pp. 446-463.

[187] P. Rabbitt, "Does it all go together when it goes? The Nineteenth Bartlett Memorial Lecture," *Q J Exp Psychol A,* vol. 46, pp. 385-434, Aug 1993.

[188] C. K. Or and B. T. Karsh, "A systematic review of patient acceptance of consumer health information technology," *J Am Med Inform Assoc,* vol. 16, pp. 550-60, Jul-Aug 2009.

[189] T. Heart and E. Kalderon, "Older adults: Are they ready to adopt health-related ICT?," *Int J Med Inform*, vol. 8, p. 8, Apr 8 2011.

[190] A. Lorenz and R. Oppermann, "Mobile health monitoring for the elderly: Designing for diversity," *Pervasive and Mobile Computing*, vol. 5, pp. 478-495, 2009.

[191] A. C. Valdez, *et al.*, "Task performance in mobile and ambient interfaces. Does size matter for usability of electronic diabetes assistants?," in *Information Society (i-Society), 2010 International Conference on*, 2010, pp. 514-521.

[192] C. Bruninx, *et al.*, "Runtime Personalization of Multi-Device User Interfaces: Enhanced Accessibility for Media Consumption in Heterogeneous Environments by User Interface Adaptation," in *Semantic Media Adaptation and Personalization, Second International Workshop on*, 2007, pp. 62-67.

[193] J. Davis, *et al.*, "A user adaptable user interface model to support ubiquitous user access to EIS style applications," in *29th Annual International Computer Software and Applications Conference*, 2005, pp. 351-358 Vol. 2.

[194] D. Ying, *et al.*, "Context-Aware Learning for Intelligent Mobile Multimodal user Interfaces," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1-5.

[195] C. E. Cirilo, *et al.*, "Model driven RichUbi: a model driven process for building rich interfaces of context-sensitive ubiquitous applications," presented at the Proceedings of the 28th ACM International Conference on Design of Communication, Sao Carlos, Sao Paulo, Brazil, 2010.

[196] E. Vasilyeva, *et al.*, "Towards the framework of adaptive user interfaces for eHealth," in *Proceedings. 18th IEEE Symposium on Computer-Based Medical Systems*, 2005, pp. 139-144.

[197] P. Tanvi, *et al.*, "Token Based Authentication Using Mobile Phone," in *2011 International Conference on Communication Systems and Network Technologies (CSNT)*, 2011, pp. 85-88.

[198] S. Hallsteinsen, *et al.*, "Using the mobile phone as a security token for unified authentication," in *Second International Conference on Systems and Networks Communications*, 2007, pp. 68-68.

[199] F. Aloul, *et al.*, "Two factor authentication using mobile phones," in *IEEE/ACS International Conference on Computer Systems and Applications*, 2009, pp. 641-644.

[200] T. Mantoro and A. Milisic, "Smart card authentication for Internet applications using NFC enabled phone," in *International Conference on Information and Communication Technology for the Muslim World*, 2010, pp. D13-D18.

[201] J. Noll, *et al.*, "Admittance Services through Mobile Phone Short Messages," in *International Conference on Wireless and Mobile Communications*, 2006, pp. 77-77.

[202] R. d'Alessandro, *et al.*, "SC@CCO: a Graphic-Based Authentication System," presented at the Proceedings of the 1st European Workshop on System Security, Glasgow, Scotland, 2008.

[203] L. Kuan-Chieh, *et al.*, "A One-Time Password Scheme with QR-Code Based on Mobile Phone," in *Fifth International Joint Conference on INC, IMS and IDC*, 2009, pp. 2069-2071.

[204] K. Yung-Wei, *et al.*, "Physical Access Control Based on QR Code," in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2011, pp. 285-288.

[205] T. Do van, *et al.*, "Strong authentication with mobile phone as security token," in *IEEE 6th*

International Conference on Mobile Adhoc and Sensor Systems, 2009, pp. 777-782.

[206] A. Pitsillides, *et al.*, "Ditis: Virtual Collaborative Teams for Home Healthcare," *J. Mobile Multimedia,* pp. 23-26, 2006.

[207] N. Panteli, *et al.*, "An e-Healthcare Mobile Application: A Stakeholders' Analysis Experience of Reading," in *Handbook of Research on Advances in Health Informatics and Electronic Healthcare Applications: Global Adoption and Impact of Information Communication Technologies*, K. Khoumbati, *et al.*, Eds., ed, 2010, pp. 433-445.

[208] S. Minglei, *et al.*, "Mobile Authentication Scheme Using SMS," in *ITA International Conference on Services Science, Management and Engineering*, 2009, pp. 161-164.

[209] S. Ray and G. P. Biswas, "Design of Mobile-PKI for using mobile phones in various applications," in *International Conference on Recent Trends in Information Systems (ReTIS)*, 2011, pp. 297-302.

[210] Trusted Computing Group, "TPM Main Specification Level 2 Version 1.2, Revision 116 ", ed, 2006.

[211] Trusted Computing Group. (2012, June 23). *Mobile Trusted Module*. Available: http://www.trustedcomputinggroup.org/developers/mobile

[212] A. Mohammed, "The Mobile Phone as a Multi OTP Device Using Trusted Computing," in *International Conference on Network and System Security*, 2010, pp. 75-82.

[213] L. Ren and N. Dongxiao, "Content Protection Based on Trusted Computing in Mobile Terminal," presented at the Proceedings of the 2009 International Conference on Information Management, Innovation Management and Industrial Engineering - Volume 02, 2009.

[214] M. Shanmugam, *et al.*, "Enabling Secure Mobile Access for Electronic Health Care Applications," in *Pervasive Health Conference and Workshops*, 2006, pp. 1-8.

[215] D. van Thanh, *et al.*, "Simple Strong Authentication for Internet Applications Using Mobile Phones," in *IEEE Global Telecommunications Conference*, 2008, pp. 1-5.

[216] J. A. MacDonald, "Cellular authentication: key agreement for service providers," in *Second International Conference on Pervasive Computing Technologies for Healthcare*, 2008, pp. 69-72.

[217] The 3rd Generation Partnership Project. (2011, Sep. 23). *The Mobile Broadband Standards*. Available: http://www.3gpp.org/

[218] T. Do van, *et al.*, "NETp1-09: Enhancing Internet Service Security Using GSM SIM Authentication," in *IEEE Global Telecommunications Conference*, 2006, pp. 1-5.

[219] W. Audun, *et al.*, "Secured enterprise access with strong SIM authentication," in *10th IEEE International Enterprise Distributed Object Computing Conference*, 2006, pp. 463-466.

[220] D. van Thanh, *et al.*, "Pervasive service access with SIM-based VPN," in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, 2009, pp. 836-841.

[221] R. Chow, *et al.*, "Authentication in the clouds: a framework and its application to mobile users," presented at the Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA, 2010.

[222] M. T. Nkosi and F. Mekuria, "Cloud Computing for Enhanced Mobile Health Applications," in *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 2010, pp. 629-633.

[223] R. Sulaiman*, et al.*, "E-health Services with Secure Mobile Agent," in *Seventh Annual Communication Networks and Services Research Conference*, 2009, pp. 270-277.

[224] R. Sulaiman*, et al.*, "A Security Architecture for e-Health Services," in *10th International Conference on Advanced Communication Technology*, 2008, pp. 999-1004.

[225] J. D. Pierce*, et al.*, "A conceptual model for graphical authentication " in *Australian Information Security Management Conference*, Perth, Western Australia 2003, pp. 1-8.

[226] A. Albrecht, "Understanding the issues behind user acceptance," *Biometric Technology Today,* vol. 9, pp. 7-8, 2001.

[227] M. Boatwright and X. Luo, "What do we know about biometrics authentication?," presented at the Proceedings of the 4th annual conference on Information security curriculum development, Kennesaw, Georgia, 2007.

[228] K. Dong-Su and H. Kwang-Seok, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Transactions on Consumer Electronics,* vol. 54, pp. 1790-1797, 2008.

[229] B. D. Subudhi*, et al.*, "Embedded design of a remote voice control and security system," in *TENCON 2008 - 2008 IEEE Region 10 Conference*, 2008, pp. 1-6.

[230] H. Uzuner*, et al.*, "LSF Aliasing Removal for Improved Speaker Verification," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2006, pp. I-I.

[231] W. Yi*, et al.*, "Investigating Correlation-Based Fingerprint Authentication Schemes for Mobile Devices Using the J2ME technology," in *IEEE Workshop on Automatic Identification Advanced Technologies*, 2007, pp. 35-40.

[232] T. Xu-Sheng*, et al.*, "Optimal Gabor Features for Face Recognition," in *International Conference on Machine Learning and Cybernetics*, 2006, pp. 3266-3270.

[233] O. Al-Baker*, et al.*, "A GPRS-based remote human face identification system for handheld devices," in *Second IFIP International Conference on Wireless and Optical Communications Networks*, 2005, pp. 367-371.

[234] A. Hadid*, et al.*, "Face and Eye Detection for Person Authentication in Mobile Phones," in *First ACM/IEEE International Conference on Distributed Smart Cameras*, 2007, pp. 101-108.

[235] F. Sufi and I. Khalil, "An automated patient authentication system for remote telecardiology," in *International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, 2008, pp. 279-284.

[236] R. J. Hulsebosch and P. W. G. Ebben, "Enhancing Face Recognition with Location Information," in *Third International Conference on Availability, Reliability and Security*, 2008, pp. 397-403.

[237] C. Min-Hsao and C. Chung-Han, "Secondary User Authentication Based on Mobile Devices Location," in *IEEE Fifth International Conference on Networking, Architecture and Storage*, 2010, pp. 277-281.

[238] J. Guerra-Casanova*, et al.*, "A robustness verification system for mobile phone authentication based on gestures using Linear Discriminant Analysis," in *Third World Congress on Nature and*

Biologically Inspired Computing, 2011, pp. 157-162.

[239] J. Guerra-Casanova, *et al.*, "Time series distances measures to analyze in-air signatures to authenticate users on mobile phones," in *IEEE International Carnahan Conference on Security Technology*, 2011, pp. 1-7.

[240] D. Sugimori, *et al.*, "A Study about Identification of Pedestrian by Using 3-Axis Accelerometer," in *IEEE 17th International Conference on Embedded and Real-Time Computing Systems and Applications*, 2011, pp. 134-137.

[241] C. Nickel, *et al.*, "Using Hidden Markov Models for accelerometer-based biometric gait recognition," in *IEEE 7th International Colloquium on Signal Processing and its Applications*, 2011, pp. 58-63.

[242] S. Mizuno, *et al.*, "Authentication using multiple communication channels," presented at the Proceedings of the 2005 workshop on Digital identity management, Fairfax, VA, USA, 2005.

[243] SAINTlogin. (2003, June 29). *CellPhone Users Validation made easy*. Available: http://www.saintlogin.com/html/cosa.html

[244] Identrica. (2006, June 29). *identrica 2 factor authentication*. Available: http://www.identrica.com/

[245] Lloyds TSB. (2012, June 29). *Security Procedure*. Available: http://www.lloydstsb.com/security/authentication_procedure.asp

[246] R. C. Karen Renaud, Mohamed Al Fairuz "A SUPPORT ARCHITECTURE FOR MULTI-CHANNEL, MULTI-FACTOR AUTHENTICATION," in *IADIS International Conference e-Commerce*, Portugal, 2007, pp. 59-66.

[247] M. A. Fairuz and K. Renaud, "Multi-channel, Multi-level Authentication for More Secure eBanking," presented at the ISSA, 2010.

[248] A. R. Alkhawaja and H. Sheibani, "Security issues with Mobile IP," School of Information Science, Computer and Electrical Engineering Halmstad University 2011.

[249] H. Wang and S. Zheng, "The security issues and countermeasures in Mobile IP," in *International Conferences on Info-tech and Info-net*, Beijing, 2001, pp. 122-127 vol.5.

[250] J. Chandrasekaran. (2000, June 1). *Mobile IP: Issues, Challenges and Solutions*. Available: http://wireless6.com/download.php?id=2481

[251] R. Jan, *et al.*, "Enhancing survivability of mobile Internet access using mobile IP with location registers," in *IEEE Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, 1999, pp. 3-11 vol.1.

[252] A. Navichai and W. Benjapolakul, "Two-Step Paging for reducing signaling costs in Mobile IP," in *13th International Conference on Advanced Communication Technology*, 2011, pp. 50-55.

[253] H. Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 4, pp. 47-57, 2000.

[254] N. Banerjee, *et al.*, "Seamless SIP-based mobility for multimedia applications," *Network, IEEE,* vol. 20, pp. 6-13, 2006.

[255] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," presented at the Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia, Seattle, Washington, United States, 1999.

[256] K. Oberle, *et al.*, "Enhanced Methods for SIP based Session Mobility in a Converged Network," in *16th IST Mobile and Wireless Communications Summit*, 2007, pp. 1-5.

[257] A. Soomro and R. Schmitt, "A framework for mobile healthcare applications over heterogeneous networks," in *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, 2011, pp. 70-73.

[258] D. A. Maltz and P. Bhagwat, "MSOCKS: an architecture for transport layer mobility," in *Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies*, 1998, pp. 1037-1045 vol.3.

[259] M. Atiquzzaman and A. S. Reaz, "Survey and classification of transport layer mobility management schemes," in *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2005, pp. 2109-2115 Vol. 4.

[260] G. Canfora, *et al.*, "Proxy-based Hand-off of Web Sessions for User Mobility," presented at the Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005.

[261] P. Vijayakumar, *et al.*, "Application-independent session mobility between user terminals," presented at the Proceedings of the Second international conference on Mobility Aware Technologies and Applications, Montreal, Canada, 2005.

[262] R. Bolla, *et al.*, "An Integrated Mobility Framework for Pervasive Communications," in *IEEE Global Telecommunications Conference*, 2009, pp. 1-6.

[263] M. Barisch, *et al.*, "A Flexible Framework for Complete Session Mobility and Its Implementation," presented at the Proceedings of the 15th Open European Summer School and IFIP TC6.6 Workshop on The Internet of the Future, Barcelona, Spain, 2009.

[264] H. Song, "Browser Session Preservation and Migration," presented at the In Poster Session of WWW, Hawaii, USA, 2002.

[265] H. Song, *et al.*, "Browser State Repository Service," presented at the Proceedings of the First International Conference on Pervasive Computing, 2002.

[266] A. Alapetite, "Dynamic 2D-barcodes for multi-device Web session migration including mobile phones," *Personal Ubiquitous Comput.,* vol. 14, pp. 45-52, 2010.

[267] H.-h. Chu, *et al.*, "Roam, a seamless application framework," *J. Syst. Softw.,* vol. 69, pp. 209-226, 2004.

[268] Günther Hölbling, *et al.*, "AbSM: agent-based session mobility," in *Transactions on computational collective intelligence IV*, N. Ngoc Thanh, Ed., ed: Springer-Verlag, 2011, pp. 192-209.

[269] N. Suri, *et al.*, "Strong Mobility and Fine-Grained Resource Control in NOMADS," in *2nd International Symposium on Agents Systems and Applications and the 4th International Symposium on Mobile Agents (ASA/MA)*, 2000, pp. 2-15.

[270] M.-D. Hsieh, *et al.*, "Stateful session handoff for mobile WWW," *Inf. Sci.,* vol. 176, pp. 1241-1265, 2006.

[271] M. Adeyeye and N. Ventura, "A SIP-based web client for HTTP session mobility and multimedia services," *Computer Communications,* vol. 33, pp. 954-964, 2010.

[272] M. Adeyeye, *et al.*, "Converged multimedia services in emerging Web 2.0 session mobility

scenarios," *Wirel. Netw.,* vol. 18, pp. 185-197, 2012.

[273] P. Wonjoo*, et al.*, "The design of WCCS for synchronization web navigation contexts," in *2011 International Conference on ICT Convergence*, 2011, pp. 592-593.

[274] L. G. de Carvalho*, et al.*, "Synchronizing web browsing data with Browserver," in *IEEE Symposium on Computers and Communications*, 2010, pp. 738-743.

[275] D. MacCormac*, et al.*, "A thin client approach to supporting adaptive session mobility," presented at the Proceedings of the 2nd international conference on Advances in grid and pervasive computing, Paris, France, 2007.

[276] D. MacCormac*, et al.*, "Implementation of a Systemto Support Mobile Computing Sessions," in *2nd International Conference on Pervasive Computing and Applications*, 2007, pp. 521-526.

[277] R. Bagrodia*, et al.*, "iMASH: interactive mobile application session handoff," presented at the Proceedings of the 1st international conference on Mobile systems, applications and services, San Francisco, California, 2003.

[278] K. Hoojgaard-Hansen*, et al.*, "Session mobility solution for client-based application migration scenarios," in *Eighth International Conference on Wireless On-Demand Network Systems and Services*, 2011, pp. 76-83.

[279] C. Stefanelli*, et al.*, "Session mobility in the mockets communication middleware," in *IEEE Symposium on Computers and Communications*, 2008, pp. 596-603.

[280] J. E. Bardram and H. B. Christensen, "Pervasive Computing Support for Hospitals: An overview of the Activity-Based Computing Project," *IEEE Pervasive Computing,* vol. 6, pp. 44-51, 2007.

[281] J. Bardram*, et al.*, "Support for activity-based computing in a personal computing operating system," presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada, 2006.

[282] E. Skow*, et al.*, "A security architecture for application session handoff," in *IEEE International Conference on Communications*, 2002, pp. 2058-2063 vol.4.

[283] S. Suoranta*, et al.*, "Authentication session migration," presented at the Proceedings of the 15th Nordic conference on Information Security Technology for Applications, Espoo, Finland, 2012.

[284] M. J. Covington*, et al.*, "A context-aware security architecture for emerging applications," in *18th Annual Computer Security Applications Conference*, 2002, pp. 249-258.

[285] B. Malek*, et al.*, "A framework for context-aware authentication," in *IET 4th International Conference on Intelligent Environments*, 2008, pp. 1-8.

[286] J. Zhefan*, et al.*, "Design of a Security Management Middleware in Ubiquitous Computing Environments," in *Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2005, pp. 306-308.

[287] A. Staikopoulos*, et al.*, "Template-Based Adaptation of Semantic Web Services with Model-Driven Engineering," *IEEE Transactions on Services Computing,* vol. 3, pp. 116-130, 2010.

[288] T. Kindberg*, et al.*, "Context authentication using constrained channels," in *Fourth IEEE Workshop on Mobile Computing Systems and Applications*, 2002, pp. 14-21.

[289] Y. Dahl*, et al.*, "Context in care--requirements for mobile context-aware patient charts," *Stud Health Technol Inform,* vol. 107, pp. 597-601, 2004.

[290] J. Kjeldskov and M. Skov, "Supporting Work Activities in Healthcare by Mobile Electronic Patient Records," in *Computer Human Interaction*. vol. 3101, M. Masoodian*, et al.*, Eds., ed: Springer Berlin / Heidelberg, 2004, pp. 191-200.

[291] M. A. Munoz*, et al.*, "Context-aware mobile communication in hospitals," *Computer,* vol. 36, pp. 38-46, 2003.

[292] J. E. Bardram*, et al.*, "Experiences from real-world deployment of context-aware technologies in a hospital environment," presented at the Proceedings of the 8th international conference on Ubiquitous Computing, Orange County, CA, 2006.

[293] J. E. Bardram, "Applications of context-aware computing in hospital work: examples and design principles," presented at the Proceedings of the 2004 ACM symposium on Applied computing, Nicosia, Cyprus, 2004.

[294] Y. Dahl*, et al.*, "A comparison of location and token-based interaction techniques for point-of-care access to medical information," *Personal Ubiquitous Comput.,* vol. 12, pp. 459-478, 2008.

[295] L. Barkhuus and A. Dey, "Is Context-Aware Computing Taking Control away from the User? Three Levels of Interactivity Examined," in *UbiComp 2003: Ubiquitous Computing*. vol. 2864, A. Dey*, et al.*, Eds., ed: Springer Berlin Heidelberg, 2003, pp. 149-156.

[296] J. E. Bardram, "The java context awareness framework (JCAF) - a service infrastructure and programming framework for context-aware applications," presented at the Proceedings of the Third international conference on Pervasive Computing, Munich, Germany, 2005.

[297] M. D. Rodriguez*, et al.*, "Agent-based ambient intelligence for healthcare," *AI Commun.,* vol. 18, pp. 201-216, 2005.

[298] D. B. Hoang and C. Lingfeng, "Mobile Cloud for Assistive Healthcare (MoCAsH)," in *IEEE Asia-Pacific Services Computing Conference*, 2010, pp. 325-332.

[299] F. Paganelli*, et al.*, "ERMHAN: a context-aware service platform to support continuous care networks for home-based assistance," *Int. J. Telemedicine Appl.,* vol. 2008, pp. 1-13, 2008.

[300] M. J. van Sinderen*, et al.*, "Supporting context-aware mobile applications: an infrastructure approach," *Communications Magazine, IEEE,* vol. 44, pp. 96-104, 2006.

[301] F. Wang and K. J. Turner, "Towards personalised home care systems," presented at the Proceedings of the 1st international conference on PErvasive Technologies Related to Assistive Environments, Athens, Greece, 2008.

[302] J. R. B. Diniz*, et al.*, "An architecture of services for session management and contents adaptation in ubiquitous medical environments," presented at the Proceedings of the 2008 ACM symposium on Applied computing, Fortaleza, Ceara, Brazil, 2008.

[303] (2010, Dec. 10). *Java Platform, Micro Edition (Java ME)*. Available: http://java.sun.com/javame/downloads/

[304] Faster Imaging AS. (2011, July 25). *Fast, high quality imaging on any device*. Available: http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.fasterimaging.com%2Fpdfs%2Fwhitepaper_generaltechnology.pdf&rct=j&q=%22Fast%2C%20high%20quality%20imaging%20on%20any%20device%22&ei=NvIWToDRPJDusgbItcnTDw&usg=AFQjCNGHVyxuptkkP35HA7IJK69lx3UN1A&sig2=8HEoxB9YC9iApls0glL5yA&cad=rja

[305] J. Nielsen. (2000, July 18). *Why You Only Need to Test with 5 Users*. Available:

http://www.useit.com/alertbox/20000319.html

[306] J. Nielsen. (2006, July 18). *Quantitative Studies: How Many Users to Test?* Available: http://www.useit.com/alertbox/quantitative_testing.html

[307] A. Hagalisletto and A. Riiber, "Using the mobile phone in two-factor authentication," *UbiComp 2007 Workshop Proceedings*.

[308] H. Raddum, *et al.*, "Security Analysis of Mobile Phones Used as OTP Generators," in *Workshop in Information Security Theory and Practice*, 2010, pp. 324--331.

[309] International Telecommunciation Union, "The international public telecommunicaton numbering plan," ed, 2010.

[310] Microsoft Case Studies. (2011, July 19). *First Choice Home Health and Hospice of Utah, Home Health Provider Saves $500,000 Annually, Doubles Cash Flow, with Mobile Solution* Available: http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000010753

[311] Microsoft Case Studies. (2011, June 10). *Egyptian Ambulance Organization, Ambulance Agency Improves Emergency Service Delivery with Electronic Fleet Management* Available: http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000010726

[312] University of Cambrige, "Mobile Communication for Medical Care - Final Report. Case study A: mHealth in Guangdong Province," University of Cambrige, China Mobile2011.

[313] Z. Niazkhani, *et al.*, "Evaluating the medication process in the context of CPOE use: The significance of working around the system," *Int J Med Inform,* vol. 80, pp. 490-506, Jul 2011.

[314] H. J. Scholl, "Mobile computing in the public sector: practices, opportunities, and arduous challenges," presented at the Proceedings of the 10th Annual International Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government, 2009.

[315] G. J. Putzer and Y. Park, "The effects of innovation factors on smartphone adoption among nurses in community hospitals," *Perspect Health Inf Manag,* vol. 7, p. 1b, 2010.

[316] K. J. Ruskin, "Communication devices in the operating room," *Curr Opin Anaesthesiol,* vol. 19, pp. 655-9, Dec 2006.

[317] M. Hassinen and P. Laitinen, "End-to-end Encryption for SMS Messages in the Health Care Domain," *Stud Health Technol Inform,* vol. 116, pp. 316-21, 2005.

[318] G. Kambourakis, *et al.*, "PKI-based secure mobile access to electronic health services and data," *Technol. Health Care,* vol. 13, pp. 511-526, 2005.

[319] S. Lee, *et al.*, "An implementation of wireless medical image transmission system on mobile devices," *J Med Syst,* vol. 32, pp. 471-80, 2008.

[320] J. R. B. Diniz, *et al.*, "An architecture of services for session management and contents adaptation in ubiquitous medical environments," presented at the Proceedings of the 2008 ACM symposium on Applied computing, Fortaleza, Ceara, Brazil, 2008.

[321] S. N. Khalifehsoltani and M. R. Gerami, "E-health Challenges, Opportunities and Experiences of Developing Countries," in *International Conference on e-Education, e-Business, e-Management, and e-Learning*, 2010, pp. 264-268.

[322] Z. Omary, *et al.*, "Challenges to E-healthcare adoption in developing countries: A case study of Tanzania," in *First International Conference on Networked Digital Technologies*, 2009, pp. 201-209.

[323] L. JunHua, *et al.*, "mHealth for Influenza Pandemic Surveillance in Developing Countries," in *43rd Hawaii International Conference on System Sciences*, 2010, pp. 1-9.

[324] D. Vatsalan, *et al.*, "Mobile Technologies for Enhancing eHealth Solutions in Developing Countries," in *Second International Conference on eHealth, Telemedicine, and Social Medicine*, 2010, pp. 84-89.

[325] I. Crk, *et al.*, "Understanding energy consumption of sensor enabled applications on mobile phones," *Conf Proc IEEE Eng Med Biol Soc,* vol. 2009, pp. 6885-8, 2009.

[326] H. Baharin, *et al.*, "Mutuality: a key gap in the move to telecare," presented at the Proceedings of the 10th International Conference NZ Chapter of the ACM's Special Interest Group on Human-Computer Interaction, Auckland, New Zealand, 2009.

[327] A. Acharyya, *et al.*, "Hardware development for pervasive healthcare systems: Current status and future directions," in *Asia Pacific Conference on Circuits and Systems*, 2008, pp. 1304-1307.

Abbreviation

3G	3^{rd} generation mobile telecommunications standard
4G	4^{th} generation mobile telecommunication standard
ADSL	Asymmetric Digital Subscriber Line
CD	Compact Disc
CONNECT	Care Online: Novel Networks to Enhance Communication and Treatment project
CPU	Central Processing Unit
CUSI	Computer Usability Satisfaction Inventory
DMZ	Demilitarized zone
ebXML	Electronic Business using eXtensible Markup Language
ECG	ElectroCardioGram
EHR	Electronic Healthcare Record
ETSI	European Telecommunications Standards Institute
GBA	Generic Bootstraping Architecture
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HIPPA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IS	Information System
ISO	International Organization for Standardization
Java ME	Java Platform, Micro Edition

MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MTM	Mobile Trusted Module
NFC	Near Field Communication
OS	Operating System
OTP	One Time Password
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
PHR	Personal Healthcare Record
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QR Code	Quick Response Code
QUIS	Questionnaire For User Interaction Satisfaction
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SSO	Single-Sign On
SUMI	Software Usability Measurement Inventory
SUS	System Usability Scale
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
UMTS	Universal Mobile Telecommunication System
VDI	Virtual Desktop Interface
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WTLS	Wireless Transport Layer Security

Appendices

Appendix 1. Acts and regulations in Norway addressing security issues related to protection of personal (healthcare) data – short preview of most relevant sections and chapters

Act / Objective	Sections and chapters relevant to the protection of personal (healthcare) data	
Act: **Personal Data Act** *Objective:* The purpose of this Act is to protect natural persons from violation of their right to privacy through the processing of personal data. The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality (Section 1 – Purpose of the Act).	Definition (Section 2)	Personal data is any information and assessments that may be linked to a natural person. Information relating to health is considered as sensitive personal data.
	General rules for processing sensitive personal data (Section 9)	Sensitive personal data may only be processed if the processing satisfies certain conditions, e.g. that the data subject consents, there is statutory authority for such processing, it is necessary to protect a person's interest, but he is incapable of giving his consent, or the processing relates to data which the data subject has voluntarily and manifestly made public. Further, a license from the Data Inspectorate is required for the processing of sensitive personal data.
	Data Security (Section 13)	The controller and the processor shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data. The controller and processor shall document the data system and the security measures. Such documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to the Data Inspectorate and the Privacy Appeals Board.
	Prohibition against storing unnecessary personal data (Section 28)	The controller shall not store personal data longer than is necessary to carry out the purpose of the processing. If the personal data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased. The controller may, notwithstanding the first paragraph, store personal data for historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the person concerned. In this case, the controller shall ensure that the data are not stored in ways, which make it possible to identify the data subject longer than necessary.

	Supervision and sanction (Chapter VIII)	The Data Inspectorate is an independent administrative body subordinate to the King and the Ministry. The Data Inspectorate shall: (1) keep a systematic, public record of all processing that is reported, (2) deal with applications for licenses, receive notifications and assess whether orders shall be made in cases where this is authorized by law, (3) verify that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified, (4) keep itself informed of and provide information on general national and international developments in the processing of personal data and on the problems related to such processing, (5) identify risks to protection of privacy, and provide advice on ways of avoiding or limiting such risks, (6) provide advice and guidance in matters relating to protection of privacy and the protection of personal data to persons who are planning to process personal data or develop systems for such processing, including assistance in drawing up codes of conduct for various sectors, (7) on request or on its own initiative give its opinion on matters relating to the processing of personal data, and (8) submit an annual report on its activities to the King.
Act: **Personal Data Regulations** *Objective:* The chapter 2 of the regulation describes in more details security requirements when processing and using personal data.	Proportionality requirements relating to the protection of personal data (Section 2-1)	The planned and systematic measures taken pursuant to these Regulations shall be proportional to the probability and consequence of breaches of security.
	Orders from the Data Inspectorate (Section 2-2)	The Data Inspectorate may issue orders regarding the protection of personal data, including the establishment of criteria for acceptable risk associated with the processing of personal data.
	Security management (Section 2-3)	The purpose of the processing of personal data and general guidelines for the use of information technology shall be described in security objectives. Choices and priorities in security activities shall be described in a security strategy. Use of the information system shall be reviewed regularly in order to ascertain whether it is appropriate in relation to the needs of the enterprise, and whether the security strategy provides adequate data security.
	Risk assessment (Section 2-4)	The enterprise shall itself establish criteria for acceptable risk associated with the processing of personal data. The data controller shall carry out a risk assessment in order to determine the probability and consequences of breaches of security.
	Security audits (Section 2-5)	Security audits of the use of the information system shall be carried out regularly. A security audit shall comprise an assessment of organization, security measures and use of communication partners and suppliers.
	Discrepancies (Section 2-6)	Any use of the information system that is contrary to established routines, and security breaches, shall be treated as a discrepancy. If the discrepancy has resulted in the unauthorized disclosure of personal data where confidentiality is necessary, the Data Inspectorate shall be notified.

	Personnel (Section 2-8)	Members of the staff of the data controller shall only use the information system to carry out assigned tasks, and shall be personally authorized to make such use.
	Physical security (Section 2-10)	Measures shall be taken to prevent unauthorized access to equipment that is used to process personal data pursuant to these Regulations.
	Protection of confidentiality (Section 2-11)	Measures shall be taken to prevent unauthorized access to personal data where confidentiality is necessary. Personal data that are transferred electronically by means of a transfer medium that is beyond the physical control of the data controller shall be encrypted or protected in another way when confidentiality is necessary. As regards storage media that contain personal data where confidentiality is necessary, the need to protect confidentiality shall be shown by means of marking or in another way. If the storage medium is no longer used for the processing of such data, the data shall be erased from the medium.
	Securing of accessibility (Section 2-12)	Measures shall be taken to secure access to personal data where accessibility is necessary. Preparations shall be made for alternative processing in the event of the information system being unavailable for normal use.
	Protection of integrity (Section 2-13)	Measures shall be taken to prevent unauthorized changes in personal data where integrity is necessary. Measures shall be taken to prevent malicious software.
	Security Measures (Section 2-14)	Security measures shall prevent unauthorized use of the information system and make it possible to detect attempts to make such use. Attempts to make unauthorized use of the information system shall be registered. Security measures shall include measures that cannot be influenced or circumvented by members of the staff, and shall not be limited to actions that any individual member is supposed to carry out.
	Security in other enterprises (Section 2-15)	The data controller shall only transfer personal data by automatic means to a person who satisfies the requirements of these Regulations. The data controller shall have knowledge of the security strategy of communication partners and suppliers, and regularly make sure that the strategy provides adequate data security.
Act: **Regulations on the use of Information and Communication Technology** *Objective:* Define requirements from institutions when developing, integrating, maintaining, and outsourcing ICT systems.	Planning and organization (Section 2)	The institution shall establish overachieving objectives, strategies and security requirements of its ICT activity. A description shall exist of each individual process and of how responsibility for administration, procurement, development, operation, systems maintenance, protection of data and decommissioning is to be carried out in a satisfactory manner.
	Risk Analysis (Section 3)	The institution shall establish criteria for acceptable risk with regard to use of its ICT system. The institution should have a documented process for conducting risk analyses of its ICT activity, and the process must define responsibilities and monitoring of steps taken as a result of the analysis performed. The institutions must conduct risk analysis at regular basis (at least annually, or in the event of modifications of significance to ICT security), to ensure that that the risk is contained within acceptable limits in relation to the type of ICT system and information processed. The result of the analysis must be documented.

	Security (Section 5)	The institution shall prepare procedures designed to ensure protection of equipment, systems and data of significance to the institution against damage, misuse, unauthorized access and vandalism. Compliance with the requirements as to security in relation to personal data under Personal Data Act, shall be regarded as compliance with the provisions of this section.
Act: **Personal Health Data Filing System Act** *Objective:* The purpose of the Act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy, so as to ensure that medical assistance may be provided in an adequate, effective manner. The Act shall ensure that personal health data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and respect for private life and ensure that personal health data are of adequate quality.	Processing of personal health data (Section 5)	Personal health data may only be processed by automatic means when this is permitted in the Personal Data Act, or it is so provided by statute and is not prohibited on other special legal grounds. Before personal health data may be obtained for processing, the data subject must give his consent, unless otherwise provided by or pursuant to statute.
	Requirements regarding specification of purpose, objectiveness, relevance, etc. (Section 11)	All processing of personal health data shall have an explicitly stated purpose that is objectively justified by the activities of the data controller. The controller shall ensure that the personal health data that are processed are relevant to and necessary for the purpose of the processing of the data.
	Access to personal health data in the data controller's and the data processor's institution (Section 13)	Only the data controller, the data processors and persons working under the instructions of the controller or the processor may be granted access to personal health data. Access may only be granted insofar as this is necessary for the work of the person concerned and in accordance with the rules that apply regarding the duty of secrecy.
	Duty of secrecy (Section 15)	Any person who processes personal health data pursuant to this Act has a duty of secrecy pursuant to the Public Administration Act and the Health Care Personnel Act.
	Ensuring confidentiality, integrity, quality and accessibility (Section 16)	The data controller and the data processor shall by means of planned, systematic measures, ensure satisfactory data security with regard to confidentiality, integrity, quality and accessibility in connection with the processing of personal health data. To achieve satisfactory data security, the controller and the processor shall document the data system and the security measures. Such documentation shall be accessible to the staff of the controller and of the processor. The documentation shall also be accessible to the supervisory authorities. Any controller who allows other persons to have access to personal health data, e.g. a data processor or other persons performing tasks in connection with the data system, shall ensure that the said persons fulfill the requirements set out in the first and second paragraphs.
	The data processor's right of disposition over personal health data (Section 18)	No data processor may process personal health data in any way other than that which is agreed in writing with the data controller. Nor may the data be handed over to another person for storage or manipulation without such agreement.

	Prohibition against storing unnecessary personal health data (Section 27)	The data controller shall not store personal health data longer than is necessary to carry out the purpose of the processing of the data. Unless the personal health data shall thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased.
	Duty to notify the Data Inspectorate (Section 29)	The data controller shall notify the Data Inspectorate prior to processing personal health data by automatic means and prior to establishing a manual personal health data filing system.
Act: **Health Care Personnel Act** *Objective:* The objective is to contribute to safety for patients and quality within the health service, as well as trust in both health personnel and the health service.	General rule relating to the duty of confidentiality (Section 21)	Health personnel shall prevent others from gaining access to or knowledge of information relating to people's health or medical condition or other personal information that they get to know in their capacity as health personnel.
	Consent to give information (Section 22)	The duty of confidentiality is not to prevent information from being made known to the person that the information directly relates to, or to others, to the extent to which the person who is entitled to confidentiality gives his consent thereto.
	Restrictions in the duty of confidentiality (Section 23)	This duty of confidentiality is not stated to prevent information from being known to persons who already have knowledge of it, or from being provided when no valid interests indicate secrecy, or from being passed on when identifying characteristics have been omitted, or from being passed on if exceptional grounds make it legitimate to pass on the information.
	Information to co-operating personnel (Section 25)	Unless the patient objects thereto, confidential information may be given to co-operating personnel when this is necessary in order to provide responsible health care.
	Duty to provide patient access to records (Section 41)	The health care provider shall provide access to the patient records to anyone entitled thereto pursuant to the provisions of the Patients Rights Act section 5-1.
Act: **Act relating to Patients' Rights** *Objective:* Goal of the act is to ensure that all citizens have equal access to good quality health care by granting patients rights in their relations with the health service.	The right to protection against the dissemination of information (Section 3-6)	Medical and health-related information and other personal information shall be treated in accordance with the current provisions regarding confidentiality. The information shall be treated with caution and respect for the integrity of the person whom the information concerns. The duty of confidentiality ceases to apply to the extent that the person entitled to confidentiality so consents.

Appendix 2. Low fidelity usability testing results

Design rules reported in the paper	Participants feedback
The mobile application should be as simple as possible without using too many functionalities, options, and descriptive text.	• Most participants said that the option for changing font color and background contrast when reading long text will not be useful for them, and it would result in more complex interface with many not required options. • All participants said that introduction text on login page is not useful since the user should already know this information if he/she is using the application. • None of the participants suggested supporting additional functionalities in mobile application, nor had complaints that proposed functionalities should be extended.
Transferring the same colors from a web to a mobile version could result in low readability and clarity.	• Two participants thought that reading text in bright color on dark background (transferred from web version) would be difficult on real device. • One participant noted that it is better to use only limited set of more calming colors, while using more “fancy and colorful interfaces” would not be appropriate for this type of application.
Using images and icons should be limited, especially if they are used just for descriptive purpose, and not to provide additional information to user. However, the icons should be used to show some status or information to the user on the manner that is similar to the PC or other standard mobile applications. Images and other type of multimedia content can be used to support users with special needs.	• All participants said that additional images in the main menu (where they are used in addition to the text) are not required. • All participants found useful icons in the messaging module (e.g. type of message, message status). • One participant proposed using images and sound for supporting people with vision problems

The best approach when choosing the text size for mobile application is to adapt the size depending on the screen size, resolution and amount of information on the screen.	• Only one participant had objection that the font size is to small, while all other participant said that size is good enough for reading. • One participant noted that too big font size can result in bad organization of content on the screen.
When using submenus in different screens to implement extensive menus with deep structure, take special care to clarify connection between screens that correspond to the one functionality. We decided to solve this problem using icons that identify the hierarchical menu level since we concluded that putting whole menus would result in to complicated and heavy user interface.	• Two participant commented that the menus on multiple screens are too complicated. • One participant suggested to put all menus on the same screen
Using similar design rules (e.g. similar colors, application specific icons and command names) across different types of application can be useful for understanding and relating different applications that share same content and functionalities. However, it is more important to adjust screens to more resemble standard device functionalities (e.g. text input, menu organization and command organization adapted for mobile devices) and application types (e.g. messaging and email application).	• One participant that previously used web application noted that the fact that mobile application resembles to web application is very helpful to her, since she can more easily understand and use the system based on previous experience. • One participant stated that it is good that all navigation and control in the system can be done using just standard soft key buttons and arrows, keeping in this way system very simple and clean. • One participant provided us valuable insight how to adapt application for devices that support only pointers and keyboards. He proposed more extensive use of shortcuts from the keyboard when selecting menu items, and enabling options selection using numbers from keyboard in the same time as arrow buttons.

Mobile application should be made suitable for wide range of potential users, not just younger user group.	• Two participants said that they think the application is more suitable for younger population, and since they are more PC users they thought the application would not be useful for them. However, one participant proposed that receiving SMS message as notification of new message in CONNECT application would be very useful, and then it would be more convenient to use mobile application to check the new message then to go to web application (the option for receiving SMS message as notification is afterwards added to CONNECT system, due to identified requirements from the users of the web application). • Two other participants said that they find application very useful and intuitive and they would use it for everyday symptom management.

Appendix 3. Heuristic evaluation – testing results

Group of heuristics	**Comment**
Adaptation of application functionalities	Show notification if the message has attachment when previewing the message.
Adaptation of command names to better fit the context of use	Change names of back options for new registration functionality. Change names of next options for new registration functionality. Change names of back option for the mail functionality. Change names of middle soft key option for the mail functionality. Change names of back option in the advice menu.
Adaptation of navigation process through the application	Map numbers to the menu items in the main menu for easier navigation. When the user quits registration process go to main menu screen. Add option to go back to main menu when choosing advice. When selected option to open draft go directly to editing screen (no need for preview first).
Organization of the content on the screen	Make font size for login screen bigger. Make soft key menu little higher, text for the middle soft key little bigger. Change organization of the text for a problem item in a last registration report. Change feedback text when new registration is submitted. Bigger font size for the messages module. Make option for writing new mail more visible. Add name of the advice in text for asking the conformation for deleting advice. Make option for finding advice default for advice module. In report of last registration order problems by level of bother by default. No need to show number of new messages on the top of the inbox table. Set new registration tab option as default for registration module.
Issues regarding application compatibility with different mobile devices	Problems with viewing of text of the advice on different phones.

Appendix 4. Compliance of CONNECT system implementation with security rules and regulations (summary of the risk assessment documents)

Requirements	Implementation
Personal healthcare data may be processed only if the processing satisfies certain conditions, e.g. the person (subject) gives his/hers consent.	The patients will be informed about security measures and routines for managing personal data, and additionally they will be instructed how to use the mobile application in a secure manner. The patients will be asked to sign consent agreeing that their data can be used and processed in the research project. Support telephone will be provided so all users of the system can call and ask for help if they have problems or question regarding the system or its functionalities.
All systems processing personal sensitive data must implement security measures to protect sensitive data against confidentiality, integrity, and accessibility threats.	Secure HTTPS communication will be used for all communication between client application and hospital information system. Information that is received over HTTPS connection on the mobile phone will not be used by any other services and/or applications on the phone. When user logs out from the application no private data will be stored on the device. If the user forget PIN code or lose the mobile phone he/she can get information about how to get new PIN code or activate the service on the new phone by using support line.
Integrity and confidentiality of personal data must be protected using encryption mechanisms, strong authentication or by other means during transmission beyond the physical control of the service provider.	All information exchanged between the mobile application and the CONNECT mobile server (located in the "Secure patient zone") will be encrypted, and no private data will be permanently stored on the mobile device. No direct communication is allowed with other servers in the "Secure patient zone" except CONNECT server. All communication between the mobile application and CONNCT Mobile server must go through DMZ zone and the authentication server. Firewall servers are used for additional protection of communication.

Appropriate techniques for identification, authentication, and authorization must be employed as part of security mechanisms protecting the information system to prevent unauthorized access to sensitive data.	All data in the CONNECT system are located in the protected system, where users must log in using BankID or Buypass authentication (patients using CONNECT web application), Encap's Confirm-by-PIN authentication solution (patients using CONNECT Mobile application) or username and password (healthcare personnel inside hospital network).
The service provider must define an acceptable risk level associated with the processing of personal data, and carry out a risk assessment with the goal to determine the probability and consequences of a breaches of security, and the risk level for each threat.	In cooperation with hospital IT department it is made a risk assessment for the CONNECT system architecture and send to the hospital privacy official person for approval.
The service provider must implement security mechanisms in order to detect any attempt of system misuse (e.g. tamper-proof logs). All use of the system must also be logged.	All servers in the CONNECT system in "Secure patient zone" and Access Manager in DMZ zone performs logging of all requests and use of the system. Hospital IT department performs daily backup of the whole system.
The service provider must physically protect the equipment, system, and information against damage, misuse, unauthorized access and modification.	Physical access to the servers is allowed only for authorized personnel. Healthcare personnel (nurses, doctors) in hospital can access the CONNECT system only if they are logged in hospital network and they are registered users of the CONNECT system. Healthcare personnel will have access only to private messages that patient sends to their specific department, and symptom registrations and advice only if patient allows sharing. Access to the CONNECT system for healthcare personnel from outside of hospital network is be prohibited.
The service provider is allowed to transfer the personal data only to external systems that satisfy all set requirements.	The personal data is stored only inside the described security architecture, and today CONNECT system is not connected to other external systems outside the hospital information system.

The publications

Review of projects using mobile devices and mobile applications in healthcare

Jelena Mirkovic[a], Haakon Bryhni, PHD[a], Cornelia M. Ruland, RN, PHD [b]

[a] *Department of Informatics, University of Oslo, Oslo, Norway*
[b]*Center for Shared Decision Making, Rikshospitalet, University Hospital, Oslo, Norway*

Abstract

Increased demands for health care services in recent years have resulted in raised health care costs and greater demands from health personnel. Usage of new technologies has a potential to extend traditional health care services into patients' homes and thus increase health care efficiency and save costs. In this paper we present a review of projects that develop mobile applications and devices for use in health care. First, we present projects that used different technology approaches to deliver health care services to users. In this category are projects that develop a specific mobile device with a custom application, projects that use legacy mobile devices and services, projects that develop applications for already existing mobile devices. We further present projects that address the key requirements for security and usability of health care services. We finally briefly describe the CONNECT mobile project, its characteristics, and our approach to mobile service development combining terminal adaptation, ease of use and security.

Keywords: mobile device, healthcare, usability, security

Introduction

Research shows that total health spending has increased dramatically over the last 30 years in the EU [1]. There has also been a rise of the unit cost of healthcare inputs, more than prices in general [2], and higher demand for healthcare personnel [3]. New technologies can meet these challenges while at the same time saving costs, increase patient's quality of life and shorten recovery, by providing relevant, valuable and timely information at the point of need.

Mobile technology has the potential to offer many of these benefits to health care. In this paper we present projects that as goal have developing mobile healthcare service to patients and/or healthcare providers. Our goal is to show how mobile devices can be used in healthcare, which technologies can be used for mobile service development, and how are main functionality issues addressed.

Challenges using mobile devices in health care

The main characteristic of mobile technology in healthcare is to provide more efficient and location independent information delivery, that can enable more accessible and flexible care. Usage of mobile devices can also facilitate better and timely interaction among patients and health service providers. Furthermore, such devices and applications can help doctors and nurses to access information that is required for conducting their everyday jobs easier, quicker and independent of the location. Some of the areas in which this kind of applications can be used are: on-the-spot emergency, home care and situations where care provider don't have fixed place of work, or need to look up relevant information resources such as clinical guidelines [4]. In addition, mobile devices can bring benefits to patients who can stay connected with their care providers between clinical encounters, get help and advice for their symptoms and problems from outside of hospital, better understand and manage their illness, and become more engaged in their care.

Besides great benefits that mobile devices can provide, there are also important concerns related to their use in the healthcare services. A primary concern is security. The healthcare sector manages information about patients that are highly confidential, and need to be treated according to security policies. There is also a demand for high application usability due to the wide range of users. Applications should be very simple, straightforward and suitable for all users for whom they are intended. Other concerns are related to the development process, including: limitations and capabilities of the mobile terminals and mobile-networks, compatibility of standards and technologies that are used in communication, and control of the quality of the information that users are accessing.

Until recently, mobile phones did not have the power to accomplish the requirements for security and usability. Some of the drawbacks of the older wireless technologies and networks are: the high cost for cellular communication links, limited data transfer rate of the mobile telephone system, limited availability of mobile Internet connectivity and lack of information access due to the complexity of healthcare IT systems [3]. Recent development of wireless technology and mobile devices provides new possibilities and enables implementation of features that can address challenges that the healthcare sector demands. For instance, new technologies that can enhance security for mobile devices and enable secure interface with Electronic Health Record (EHR) system, as Generic Authentication System based on SIM (GAS) [5] and RFID (Radio-frequency identification) reader [6] are developed.

Survey of projects using mobile devices in health care

The projects that are presented are result of a search for related projects in the field of mobile terminals and applications in health care, including aspects of usability, mobility and security. During our search, the goal has been to find relevant and alternative approaches to how mobile devices are used in the healthcare sector, what technologies are used, and which are the biggest challenges in deployment. As a result we found many projects, using various technologies and addressing different challenges and requirements for successful utilization of mobile devices in healthcare.

We organize the projects according to technologies that are used for theirs development. Additionally we present projects that are addressing most important healthcare services requirements - usability and security.

Classification of the project according used technologies

According to the technology that is used for mobile service development we classified projects in three groups:

- Projects developing specific mobile devices with a custom application
- Projects using standard mobile devices and legacy mobile services
- Projects developing mobile applications for legacy mobile devices

Differences and characteristics of the projects classification groups are presented in Table 1.

Table 1 – Classification of the projects

	New device	New application	Utilizing legacy mobile services
Specific mobile devices with a custom application	Yes	Yes	No
Standard mobile devices and legacy mobile services	No	No	Yes
Mobile applications for legacy mobile devices	No	Yes	No

Projects developing specific mobile devices with a custom application

Projects in this group develop their own mobile device together with an application for the specific device with the goal to enable users to send and/or receive medical information and help them in their every day activities.

MOBY-DEV [7] presents a new generation of mobile devices intended for health care professionals working in and outside hospitals and giving them the possibility to edit medical history, handle pharmaceutical prescription by voice commands, receive and give orders related to medical/nursing care, store important medical information and programs, exchange e-mails and surf the Internet. These devices are based on palm PCs, wirelessly connected to the relevant databases and are able to enhance mobility, increase user-friendliness of the medical system, enforce security and confidentiality and reduce transcription error rates.

The Health Buddy system [8], developed by Health Hero Network Inc., is a system that serves as interface between patients at home and care providers, facilitating patient education and monitoring of chronic conditions. This system consists of a mobile device, with a specific interface, design and software which patients use for communication with a medical healthcare center and clinical information databases.

Creating a custom mobile device provides additional flexibility for the developers, and the terminal can be adapted for specialized functions. The system developers can address all system requirements with no limitation from the legacy mobile device hardware and software. The main problem of this approach is the usability of a device that is used only for a single purpose. A legacy mobile terminal is more useful as it can be used for many tasks, and is always available. We believe that adaptation to a legacy terminal represents a better application investment, since the application can be the same even if the mobile terminal is changed frequently.

Projects using standard mobile devices and legacy mobile services

This group consists of projects that are using only wide spread mobile devices, such as PDA and mobile phones, and their legacy functions, such as voice calls or SMS messages. Using this approach, projects try to utilize capabilities of a standard mobile device, to help patients and facilitate their daily life and/or recovery process.

The project NHS Direct [9] represent a nurse-led telephone information service providing basic healthcare advice to callers that is accessible twenty-four hours a day, seven days a week. The main aim of this project is to determine the impact that the usage of mobile phones is having on the service, and how new terminals enhance accessibility.

The literature also reports numerous projects that use SMS messages to provide help to patients. Project SweetTalk [10] schedules the automated delivery of a series of appropriately tailored messages to difficult-to-reach young age group of diabetes patients with the goal of exploring the impact of SMS-enabled behavioral support with intensive therapy. Queen Elizabeth Hospital in England introduced a system whereby patients who are waiting to collect their dispensed drugs are sent an SMS message to inform them when their prescription is ready for collection [11].

Using standard mobile devices and legacy functions for developing healthcare services adds great advantages for users and system owners. All functionalities that are needed for this type of systems are already enabled on the mobile device, and users know how to use them. However, this is also a disadvantage since the developer cannot adapt and change the services according to special requirements. We believe that the limitations of data types and presentation severely limit the usability of these services.

Projects developing mobile applications for legacy mobile devices

This group consists of projects that develop specific applications intended for running on already existing mobile devices, like mobile phones and PDAs. For this kind of projects the main goal is to use the mobile device that the patients as well as medical personnel already have and use, and add specific functionalities through individual application.

The DITIS (A Collaborative Virtual Medical Team for Home Healthcare of Cancer Patients) [12] is a system that is developed to address the difficulties of communication and continuity of care between the members of a home healthcare multidisciplinary team and between the team of oncologists often hundreds of kilometers away. It includes a set of tools for effective scheduling and coordination of team members, with features including automatic notification and alerting and provides secure access to e-records from anyplace and anytime via desktop computers or variety of mobile devices.

The LOTSE project [13] has set the goal of developing a health care application for mobile devices based on web pads, to enable recording information and reviewing patient records, and to perform remote diagnostics. This project wants to enable location-independent access to the required information to persons working in home care through usage of wireless connectivity and mobile terminals.

Most of the reported projects are intended for healthcare providers, but there are also projects that are intended for patients. Example of this kind of projects is Health-Related Quality of Life [14] with the aim to develop a new system for transmission of patients´ reported outcomes using mobile phones or Internet and to test the acceptability and the ability of patients using the system through mobile phones. The project Mobile Learning Tools for Children with Life-threatening Allergies [15] have as aim to enable supported learning and information giving to help anaphylactic children and their families live safer and more flexible lives.

Developing mobile application for legacy mobile device present a good solution regarding usability, because the user can use a standard, personal mobile device for accessing healthcare services. However, developing mobile applications that will work on all mobile phones and PDAs represent a great challenge, due to numerous types of mobile devices with different capabilities. The standard approach in these projects is to develop the mobile application for a specific kind of mobile phone or PDA, and this approach limits the number of possible users and reduces usability of the application.

Classification of the project according the main functionalities they address

During development of mobile healthcare services that should be used by patients and healthcare providers in real life situations, numerous requirements must be addressed. In this part of the paper we present some projects that are addressing two key requirements for mobile healthcare services: usability and security.

Projects addressing usability of applications in healthcare

When developing applications with the intention to be used in health care, usability requirements have to be specially addressed and implemented. Potential users of these applications are either patients or care providers. If the users are patients they may have different functional difficulties and little knowledge of mobile terminals and handling application on them. When users are healthcare providers, the most common situation is that they do not have much time for executing complicated and time consuming operations on a mobile device but need to focus on the patients. Participatory design methods to identify users' system requirements are therefore crucial in interface design. It is very important that user interface is very simple, intuitive and easy to use with support of all functionalities that are requested.

Project senSAVE [16] analyzes the usability requirements for elderly by first interviewing patients with different difficulties and health problems about their needs and requirements. After the interview, different user interfaces were developed, using patient's proposals as guidelines, and usability testing with patients was performed. Patients were afterwards through interviews and questionnaires asked about their impressions and satisfaction with clarity and simplicity of the user interfaces and about thoughts and insights regarding possibilities of improvement.

The Home Assistant project [17] develops a multimedia communication terminal, that will allow elderly and disabled people to keep in touch with relatives, friends and service providers. Their goal was to decide through interaction and interviews with patients, which functionalities are most useful and should be supported. Four possible application functionalities that could be implemented were suggested to patients and they were asked to grade their difficulty and usability.

Projects addressing security demands of healthcare applications

Information that is transferred between the healthcare provider and patient and stored on the mobile device and/or healthcare system represents highly personal data and must be protected with high security measures and techniques, consistent with relevant security policies. Very strong authentication is demanded so that a third party, without access permission, cannot access the application and its data and jeopardize confidentiality. Also, during communication all data that are transferred should be protected against eavesdropping and interference with the transmissions by intruders. Including security measurements like strong encryption and access control helps to secure confidentiality and compliance with privacy laws.

One example of security services in a mobile e-Health Application is the security architecture of the MobiHealth project [7]. A range of security mechanisms is implemented in this project. First, encrypted communication between the mobile terminal and sensors is implemented, if connected over a Bluetooth connection. For external communication between the mobile device and the remote server Transport Layer Security (SSL/TLS) is used. The public key cryptography techniques used with SSL/TLS generally require that at least the server authenticates itself by means of an X.509 certificate, issued by a Certification Authority trusted by the client. This project additionally to server certificate authentication use the X.509 certificate assigned to each patient's mobile terminal for the terminal authentication. Additional authentication for the client can optionally be implemented through usage of a password or PIN code.

In the DITIS system [18] authentication is achieved on two levels. The first level of authentication is between the user and the device through a strong PIN number/password. The second level of authentication is between the user and the healthcare application and is achieved by using a digital certificate and a strong password. An appropriate Public Key Infrastructure (PKI) system is implemented and managed to provide certification service.

Also, electronic data security standards have been created to guarantee protection of the security and privacy of personal data in the healthcare systems. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA has released its final security rule on February 2003. According to this standard health providers are required to: ensure the confidentiality, integrity and availability of patients data, protect against any reasonably anticipated threads to the integrity of data, protect against accidental disclosure of the information, and ensure that the healthcare institutions employees are trained in the rules [19]. Only several of the techniques are explicitly required, as encryption when information flows over open networks and authentication using some of the techniques: password systems, two or three-way handshakes, telephone callback, and token systems. But which technique and how it should be implemented is not specified. Defining security requirements in this manner enables adoption of security measures that conform to the HIPAA security rule, but may vary from one project to the other.

Summary

There are numerous approaches on how a mobile device can be used for delivering healthcare services and every approach brings advantages and special considerations that have to be addressed. Also during development of projects that are going to be used in live healthcare systems, many requirements as usability and security must be addressed.

We believe that challenges regarding device capabilities, usability and security are the main reasons why mobile health care applications are not yet operational in large scale. There are still problems with limited capabilities in mobile devices (e.g. processing power, memory), which can affect usability of the application, and the appropriate security architecture is still not defined. The lack of standards for e-Health communication services and lack of integration between existing e-Health services and other informational services also influence acceptance of mobile devices in the healthcare sector.

In this survey we can see that there are numerous projects exploring development and deployment of healthcare services. We also see how mobile services could be useful not just for patients to whom they could improve quality of life and recovery, as well as for care providers to support them in their every day job, but also for the healthcare sector enabling fewer visits to the care provider and healthcare as a whole, because mobile applications may ultimately be able to reduce face-to-face office or hospital visits.

CONNECT Mobile project

CONNECT Mobile project has as goal development and evaluation of the CONNECT Mobile application intended to support patients who are at home between treatments and during rehabilitation. Through this application we want to provide the patients easy, secure, seamless and user-friendly access to healthcare advices and support whenever a problem arises or a health related question or concern emerges, independent of their current location and time.

Developing a mobile application for patients present great challenges due difference in user experience and mobile devices they use. To reach as many users as possible, we want the application to run on all standard mobile phones. We have selected a minimal set of the mobile Java 2 Mobile Edition (J2ME) platform for development. J2ME is the most widespread developer platform for mobile devices available on nearly all mobile phones (GSM) currently sold. The choice of the J2ME developer platform also enables creating a user-friendly and well-designed user interface that is easy to understand and manage, and support for usage of security features as encryption/decryption using an SSL connection. By placing very low requirements to the J2ME environment, and performing font handling, automatic resizing of user interface elements and adaptive navigation, we can provide the same look and feel of the service on all types of phones.

Development of the interface for CONNECT Mobile application is performed using of participatory design methods through phases: workshops with clinicians, focus groups with patients, development of user interface, expert reviews and usability testing [20]. Through this design methodology we identify patients' user requirements and factors important for successful adoption of implementation and maintenance of the CONNECT Mobile service. Developing the application that will be consistent with patient's needs and capabilities present a key issue for acceptance and usage of the application through recovery treatment.

Developing the security architecture for CONNECT Mobile project is another key challenge. Many security requirements are addressed such as authorization, encryption of data that is transferred and stored and compliance with local security laws. The proposed security solution enables: secure communication between user and server through usage of SSL connection, two phase authentication of the user through usage of secret SIM card information and user's credentials, and privacy of personal data that is stored only in the secure hospital information system and not on the terminal itself.

Conclusion

Mobile devices are widely accepted in our everyday lives. Their main characteristic, to provide access to services independent of user location and current time, enable their fast development, acceptance and popularity. In this paper we have presented a survey of projects using mobile devices for developing healthcare services. Due the numerous characteristics of mobile devices they bring different benefits for the user, and there are many different approaches for developing a healthcare service for a mobile device. Through this survey we present three approaches how mobile healthcare services can be developed according to the technology used. Because healthcare service has very high requirements regarding security and usability, we described how these requirements are addressed in projects involving mobile devices.

We see significant challenges of creating particular mobile terminals for healthcare services, and claim that using only standard features such as SMS/WAP/Voice is inadequate for advanced healthcare applications where user interaction is a key element. The CONNECT Mobile application takes a novel approach to terminal adaptation and user friendliness within a secure communication framework integrated with a live healthcare information system. We believe secure and user-friendly mobile access to healthcare services using any standard mobile phone is the key to widespread deployment of mobile healthcare applications.

References

[1] Ericsson Enterprise AB. HealthService24 eTEN-C517352, Continuous Mobile Services for Healthcare. Finall Report, 2006.

[2] Deven C, Jon S and Clive PD. The upward trend in healthcare spend. The role of mobile phones in increasing accessability and efficiency in healthcare, The Vodafone Policy Paper Series, Mar 2006: no.4: pp. 3-11.

[3] Istepanian RSH and Lacal JC. Emerging mobile communication technologies for health: Some imperative notes on m-health. Proc. 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2003: Vol.2: pp. 1414-1416.

[4] Rugge I and Behrens M. Mobile application in health care - a regional perspective. Unpublished.

[5] Wangensteen A, Lunde L, Jorstad I, and van Thanh D. A Generic Authentication System based on SIM. Proc. International Conference on Internet Surveillance and Protection ICISP '06, 2006: pp. 24.

[6] Byunggil L, and Howon K. Privacy Management for Medical Service Application Using Mobile Phone Collaborated with RFID Reader. Proc. Third International IEEE Conference on Signal-Image Technologies and Internet-Based System SITIS '07, 2007: pp. 1053-1057.

[7] Konstantas D, Jones V, and Herzog R. MobiHealth – innovative 2.5 / 3G mobile services and applications for healthcare. 11th IST Mobile and Wireless Telecommunications Summit 2002, Thessaloniki , Greece.

[8] Health Buddy from Health Hero Network Inc., see https://www.healthhero.com/

[9] Atun RA and Urganci IG. Analysis of calls to NHS direct. The role of mobile phones in increasing accessability and efficiency in healthcare, The Vodafone Policy Paper Series, Mar 2006: no.4: pp. 12-17.

[10] Antun RA, Franklin V, Greene S, Samyshkin Y, and Morris S. Use of mobile technologies to enhance control of type 1 diabetes in young people: economic evaluation. The role of mobile phones in increasing accessability and efficiency in healthcare, The Vodafone Policy Paper Series, 2006: pp. 40-46.

[11]Antun RA and Sittampalam RS. A review of the characteristics and benefits of SMS in delivering healthcare. The role of mobile phones in increasing accessibility and efficiency in healthcare, The Vodafone Policy Paper Series, 2006: pp. 18-28.

[12]Panteli N, Pitsillides B, Pitsillides A, and Samaras G. Web mobile-based applications for healthcare management, Igi Global, 2007: pp. 100-117.

[13]Rügge I and Behrens M. Mobile Applications in Health Care - A Regional Perspective. 12. Winter

Course of CATAI, Tenerife and Spain, 2004: pp. 51-56.

[14]Bielli E, Carminati F, Capra SL, Lina M, Brunelli C, and Tamburini M. A wireless health outcomes monitoring system (WHOMS): Development and field testing with cancer patients using mobile phones. BMC Medical Informatics and Decision Making, 2004: vol.4: pp. 7.

[15]Hernandez Munoz LU, Woolley SI, and Baber C. A mobile health device to help people with severe allergies. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008: pp. 8-10, 2008.

[16]Lorenz A, Mielke D, Oppermann R, and Zahl L. Personalized mobile health monitoring for elderly. Mobile HCI'07, 2007: pp. 297 – 304.

[17]Mikkonen M, Vayrynen S, Ikonen V, and Heikkila MO. User and concept studies as tools in developing mobile communication services for the elderly. Personal Ubiquitous Computing , 2002: vol.6: no.2: pp. 113-124.

[18]Pitsillides A, Samaras G, Pitsillides B, Georgiades D, Andreou P, and Christodoulou E. DITIS: Virtual collaborative teams for home helthcare. Journal of Mobile Multimedia, 2006: Vol. 2: No.1: pp. 23-36.

[19]Wimalasiri JS, Ray P, and Wilson CS. Maintaining security in an ontology driven multi-agent system for electronic health records. 6th International Workshop on Enterprise Networking and Computing in Healthcare Industry HEALTHCOM 2004: pp. 19-24.

[20]Ruland C M, Børøsund E, Varsi C. User Requirements for a Practice-integrated Nurse-administered Online Communication Service for Cancer Patients. The 10th International Congress on Nursing Informatics, Helsinki Finland, 2009. In press.

II

Designing User Friendly Mobile Application to Assist Cancer Patients in Illness Management

Jelena Mirkovic, Haakon Bryhni
Department of Informatics
University of Oslo
Oslo, Norway
jelena.mirkovic@medisin.uio.no
haakon.bryhni@nunatak.no

Cornelia M. Ruland
Center for Shared Decision Making and Nursing Research
University Hospital
Oslo, Norway
cornelia.ruland@rr-research.no

Abstract— **Mobile terminals are well suited for providing information to patients at the point of need. In the CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment) project, we have developed a mobile application, called Mobile WebChoice, as a part of a patient support tool that enables patients' access to a help and support system while they are away from hospital between treatments and during rehabilitation and recovery periods. Through our work we address research questions regarding: development of a user-friendly mobile application, user's expectations and requirements from the patient support system, and usability issues that affects acceptance of mobile applications in patients' health management process. We have used participatory design methods that included interviews and usability testing with patients and health personnel. As a result, we identified main usability requirements that must be taken in consideration when developing and adjusting patient support systems for mobile access and saw that patients find the mobile application useful and the patients are ready to accept it as an integrated part of their health management process.**

Keywords- mobile application development; health management; patient support system.

I. INTRODUCTION

Due to the increasing costs related to health and long-term care and higher demand for healthcare personnel, there is increasing need for innovative methods and new approaches in interacting with healthcare services [1]. Mobile technology can offer great advantages for access to healthcare information. Widespread acceptance of mobile phones and their ability to provide access to services independent of time and user's current location make mobile terminals well suited for timely delivery of healthcare services to healthcare providers and patients.

Also, patients are becoming more and more involved in the management of their own healthcare conditions with support and help from healthcare professionals [2]. Using new technologies they become more informed about their current conditions and care process, and can become an important participant in the process of planning and management of their own care. Mobile devices can enable patients to collect, store, and transmit clinical data to healthcare professionals and provide better and more complete insight in their health status.

This paper is organized as follows: Section II gives a brief overview of related work, Section III presents research questions we are addressing in our research work, Section IV describes research methods that are utilized together with results received through the mobile application development, Section V describes results from usability testing, Section VI presents discussion of the results and finally, Section VII gives a summary and conclusion of our research.

II. RELATED WORK

There are numerous projects that address utilization of mobile phones in healthcare management and it is shown that mobile phones can provide help for patients to understand the effects of their illness and treatment, and at the same time find a balance between seeking professional care and depending on their self-care abilities (e.g., [3][4][5]). Some researchers also describe how patients accept mobile health applications and feedback from patients regarding functionality and ease of use (e. g., [6][7][8]). Besides the research related to feasibility of mobile health applications and their potential to provide better patients' health management, we found less research addressing functionality and usability issues that have to be addressed during the development process (e.g., [9][10]). What we still found missing is research regarding more complex patient support systems, where patients are able to access the system over different terminals (mobile, PC, tablet PC). Most of the work addressing this issue in the healthcare area is describing development of mobile applications intended to be used by healthcare personnel (e.g., [11][12]). Some general guidance for developing and adapting a mobile application to a web version as [13][14][15] is present, but still we did not find the work addressing usability and mobility in the context of health support tools intended for patients use. We see that these systems are very specific, and users' needs can vary greatly from one person to other, so developing a system that is not just useful but also easy to use and adapted to users' specific needs and different terminal capabilities is very important for acceptance of the service.

III. RESEARCH QUESTIONS

As part of the CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment) project it is developed an Internet-based support system for communication and information sharing between and among patients and care providers, and patients are enabled to access the system over different terminals (tablet PCs, stationary PCs, laptops or mobile phone). Through development, adaptation and testing of the system and its components our main goal has been to identify key factors that are related to successful adoption, implementation and maintenance of this kind of tools in a real world practice. In this paper we are addressing research issues regarding development process, adaptation and integration of a mobile application in a patient support system. The main research questions that we address here are: (1) what interface requirements and adjustments are needed for the mobile application to provide patients with context-sensitive, adaptive interfaces and seamless, easy access to healthcare information independent of their current location, (2) how does previous knowledge and experience with other parts of the patient support system affect understanding and operation of the mobile application, (3) what are patients' opinions regarding mobile access to the health support systems and the application's usefulness and ease of use, (4) what are patients opinions regarding acceptance of the mobile application as one type of access to the health support system in their own health management.

IV. THE DESIGN AND IMPLEMENTATION METHODS

To address set research questions we utilized participatory design methods that included interviews and usability testing with patients and health personnel. Phases of the process are: development and evaluation of the application interface design, low fidelity usability testing with patients, development of an user interface, expert reviews and high fidelity usability testing with patients. In this section we will describe each phase in more details.

A. Previous work

Previous to our work, the support tools Choice and WebChoice are developed as part of the CONNECT project [16]. The Choice tool enables patients to report their symptoms, health problems and concerns while in the hospital, rate the degree of distress and prioritize their needs for care from health care providers. The WebChoice tool allows patients to monitor symptoms through the Internet over time, and provides access to evidence-based self-management options tailored to their reported symptoms as well as a communication area where patients can ask questions to a clinical nurse specialist and exchange experiences with other cancer patients. After development of these tools, the next step in the project was to investigate how the support system could be enhanced with mobile access, enabling use independent of time and place. It was decided that only a limited set of functionalities from the WebChoice application should be made available in the mobile application (messaging, registration of problems and an advice module) due to limitations of mobile terminal, and the first draft of design screenshots was developed.

B. Development and evaluation of the interface design

In the first step of the mobile application development we revised and adapted the first version of the application design screenshots that are developed in previous phase of project. We used general guidelines that we found in the literature (e.g., [17][18][19]) and in the same time tried to follow the recommendation given from mobile device and mobile operating system manufacturers (e.g., [20][21][22][23]).

One additional requirement that we set for our specific case is adaptation of the mobile application interface to be similar to the web version (some of the guidelines that we used are described in [13][14][15]). In this manner we adjusted the interface not only for general users but also to users with previous knowledge of other parts of the system and to provide them the feeling that they are accessing the same system through different terminals.

We adapted interface design screenshots using previously mentioned guidelines, but at the same time tried to find a good balance between general recommendations for mobile application design and specific requirements set for this type of applications. Some of the usability issues from the previous design version that we addressed and corrected are: provision of information to users regarding content on the screen (using scrollbars to give feedback about additional content that is not visible on the screen, and enabling users to always know where they are in the application through status bars and titles), consistency in name and place of commands (using just two-three standard commands per screen require us to keep consistent patterns and clear names) and text size adaptation (finding right balance between text size and amount of information on the screen to provide good readability).

C. Review of interface design by patients

When the main interface design screenshots has been created and reviewed, we organized usability testing with the low fidelity paper prototype. In the usability testing four patients participated [24]. During the test participants looked at nine interface screenshots representing different functionalities of the mobile application. They were asked about their opinions regarding the interface design (size of the text, colors, organization of element on the screen) and understanding of the interface functionalities.

Some conclusions from participants' feedback are:

1) When adapting interface from bigger screen to smaller, choosing the content that should be transferred requires cooperation with users and finding out what are their expectation from the specific system. For this type of systems we saw that all text that present description and do not give extra knowledge to users should be omitted (or transferred to a specific help page). For example, the login screen should be without introduction text and menus should contain just main command's names (without any clarifications).

 ISBN: 978-1-61208-119-9

2) Transferring extensive menus with deep structure on one screen (as in web applications) is not acceptable in the mobile application. The better solution is to make submenus, but there are still problems in connecting a few screens to correspond to the functionality of menu selection in a web application, and find the right level of granularity and amount of information to show per screen. To solve this problem, we used icons identifying the hierarchical menu level.
3) Having in mind that the amount of information per screen is very limited, it is very easy for the user to get lost in the application and do not understand what to do next. Providing users feedback regarding current place in the application help, but additional adjustments of menus and screens using familiar concepts from the web application helped the user to transfer previous user experience to the mobile application.
4) Even though content and concepts from the web application is transferred to the mobile application, in some situations it is better to adjust screens to more resemble standard mobile functionalities, like text input, menu organization and command organization. Other interface elements, such as colors and application specific icons should not be changed.
5) When adapting interface for small screens, the usage of right colors is very important. Colors on one hand could enable additional emphasis on more important interface elements, but just transferring the same colors from a web to a mobile version could result in low readability and clarity. In our example we saw that users had problems with reading text in bright color on dark background as implemented on the web version.
6) Selecting the right text size present important issue as we saw from previous steps, because there is need for a right balance between text size and amount of the text on the screen. From the users' feedback we saw that using one font size through all application is not good approach, but rather the size should be adapted depending on the screen size, resolution and amount of information on the screen.
7) Using icons and images should be very limited. If they are used just for descriptive purpose, and do not provide any other additional information to users they should be omitted (for example in menus when used in addition to the text). On the other hand in some situations it is convenient to use them to show some status or information to the user on the manner that is similar to the PC or other mobile applications (e.g. status about mail).

We saw that some of the results are in accordance with general mobile user interface development recommendations, but others are very specific for utilization in the context of the mobile applications in healthcare.

D. Development of the mobile application

For developing the mobile application we used Java Platform, Micro Edition (Java ME) [25]. The choice of the Java ME developer platform enabled us to make user-friendly and well-designed user interface adjusted for the majority of mobile terminals.

During application development we used mobile design screenshots that are developed in previous phases. Also while the mobile application was in the development phase, a new design interface was implemented for the WebChoice application; so the design of the mobile application was also adjusted to it keeping in mind previous gained knowledge about users and their specific needs. During development we made the application to dynamically change the interface according to the screen size of the device, so the main organization of the text on the pages stays the same regardless of the mobile device the application is running on. We also additionally addressed the problem of font size by making the user interface more comfortable for reading of longer texts. For example, if a patient reads text describing a self-management advice, he/she is able to change the font size, font type and orientation of the text and in this manner adjust it for better readability. This is normally not possible in a Java ME environment, which only support one font and 3 sizes. Our goal was to make the interface flexible and readable regardless of mobile phone limitations, like screen size and limited navigation possibilities. Additional adjustments are also made so the mobile application can support touch screens without a specific keyboard on the device.

We decided to develop a basic design of our application according to some general design recommendations as stated previously, but in this phase of development process we also implemented some device specific adjustments to change dynamically based on the device type. For example, in our application the right soft key command is used as a rule as back button (that is recommended in the guidelines for Nokia phones) but for writing text in input fields characters assigned to input keys are dynamically adjusted to device type.

For development of this kind of mobile application, using just standard Java ME libraries do not provide enough flexibility. To overcome this limitation, we used the Faster Imaging library [26] that enables virtualization of the mobile terminal. The program library offers improved visual display quality, improved font handling and performance for image and interface intensive applications and is designed to execute on top of all Java ME virtual machines supporting Mobile Information Device Profile (MIDP) version 2.0 and Connected Limited Device Configuration (CLDC) version 1.1 available in almost all Java-enabled phones. A key challenge for us was to provide handling of text and images on a mobile device, with minimal requirements to the terminal, and using the proposed architecture we succeeded to leverage different character fonts and provide virtual machine independent display with low processing requirements, since only very basic operations and only integer arithmetic is used. Text is represented in a highly compressed format that enable faster rendering. The readability and visual quality is preserved down to very small character size by performing "smooth-edge" technology that provides anti-aliasing with special attention to color blending, consistent view quality independent of rotation and scaling, scalable line thickness and non-isometric text handling.

E. Expert reviews

After prototype has been finished, we organized expert reviews with nurses that were involved in development and research work on other patient support tools, and are well acquainted with the Choice and WebChoice applications.

We utilized a heuristics evaluation and recruited four evaluators [27]. Guidelines that evaluators used for testing are based on the recommended heuristics for web applications [27], and we added heuristics specially addressing mobile device and mobile application characteristics found in [19][28].

The four evaluators were given the list with heuristics and short pre-evaluation session was conducted where the heuristics are explained in more details. They were asked to test the application in duration of one to two hours and note all nonconsistencies with the guidelines. After testing we organized a short debriefing session where evaluators described their experience of the process, and presented their results. Based on received feedback final corrections and adjustments were made on the application before start of a usability testing with patients.

Most of the feedback we received was regarding small interface adjustments, and more convenient organization of the content on the screen. Also, additional propositions were made to name commands more clearly and according to their specific functions and context in which they are used. Additionally, adding advanced features for the application navigation is proposed.

F. Usability testing

When we finished all previously described phases in the application development process, and addressed all usability requirements and problems that were identified we continued with a high fidelity usability testing with patients. A couple of screenshots of the mobile application that is used in the usability testing are shown in the Figure 1.

In this study we performed the usability test of two application scenarios. In the first scenario participants performed testing on just the mobile application, while in the second scenario participants performed testing first on the web application on the PC before they started testing on the mobile version. In the study participated ten patients, five for each application scenario. User group of ten patients is not large enough that represent general user population, but we think that it is large enough to get some first feedback regarding usability issues, acceptance and user needs from mobile applications used as part of the patient support tools.

The study was conducted on a Nokia 5310 phone with installed Mobile WebChoice application and access to the Internet. The test was conducted one participant at the time in an enclosed environment with minimum background noise.

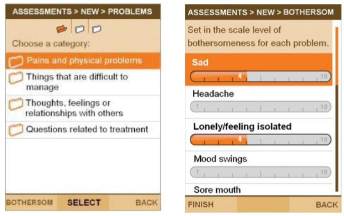
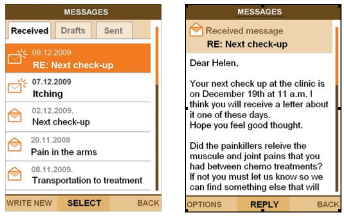
Module	Screenshots
Login and main menu	
Registration	
Messaging	

Figure 1. Screenshots of the application's modules.

1) Test Process Design and Data Collection Method

On the beginning of the test participants were briefly introduced on the objectives on the study and the CONNECT project. They were informed that they would be recorded on a video while performing tasks for later analysis. Also, they were asked to try to perform tasks on their own, based on their previous knowledge of the mobile phones and computers, and to take time as they think it is needed. Participants were asked to think out loud during the tasks, and if unavailable to progress on a given task to ask for a help, but only after trying to perform the task first on their own.

The group of participants that tested both the mobile and web version of the application first received the list of tasks to perform on the web application on a desktop PC. After performing the tasks on the web application participant continued with mobile application testing.

Prior to the mobile application testing, participants performed pre-training exercise on the mobile phone. The task list was then given to the participants. During the test, every participant has been asked to perform a total of seven tasks. The tasks were grouped in four groups, based on the main functionalities of the application. For each task the

 ISBN: 978-1-61208-119-9

time, number of errors and number of requested help were measured. Between the tasks and at the end of the testing participants were asked the set of questions to gain more subjective and qualitative feedback regarding interface design, general impressions regarding the application and it's usefulness and acceptance in their everyday health management, and answers and comments were recorded. The groups of tasks were designed as follows:

- Login to the application (task 1)
- Send the message to the nurse (task 2-3)
- Register specified problems (task 4)
- Find advices regarding previously selected and specified problems (task 5-8).

2) Targeted respondents

All participants in the study were women between 30 and 60 years old and in treatment for a breast cancer. Only one participant previously heard about the CONNECT project, and participated in previous organized usability studies. Average age of all participants was 46.5 years (average age for first group that tested just the mobile application was 49 years, and the second group that tested the mobile and the web version was 44 years). All of participants owned their mobile phone, eight owned Nokia phones, one Sony Ericsson phone and one HTC phone. According to their subjective opinions the eight participants had average previous experience with mobile phones usage and the remaining two participants had above average user expertise with a mobile phone.

V. RESULTS FROM USABILITY TESTING

In this section we present results recorded during the usability testing.

A. Quantitative results

The task completion times for both user groups are illustrated and compared in the Figure 2. We can see that for the most of the tasks completion time vary by the small values. The only higher variation in the task completion time can be observed for the task four (registration task).

In the Tables I and II are presented numbers of errors participants had while performing tasks and number of times they requested assistance while performing tasks. Here we also see the highest difference for the registration task.

TABLE I. NUMBER OF ERRORS

Task number	1	2	3	4	5	6	7	8	Sum
Mobile version	0	0	0	2	1	2	0	0	**5**
Mobile and Web version	1	0	0	0	0	1	0	0	**2**

TABLE II. NUMBER OF REQUESTED ASSISTANCE

Task number	1	2	3	4	5	6	7	8	Sum
Mobile version	3	0	2	12	1	3	0	0	**21**
Mobile and Web version	4	0	1	4	0	1	0	1	**11**

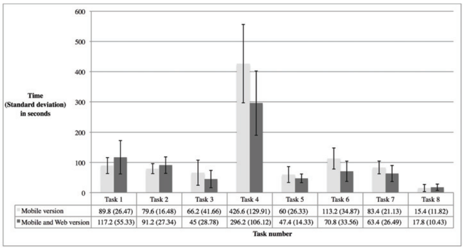


Figure 2. Task completion time for both user groups.

B. Qualitative results

Through the qualitative feedback we tried to identify main usability problems.

1) Task analysis – Login to the application and main menu

In general, participants did not have many complaints and problems regarding login functionality. Participants that owned Nokia phones managed to identify option for changing a text input type very quickly, but others requested help before completing the task. This problem was previously identified so the key for changing the text input type is assigned dynamically in the application dependent on the type of the mobile phone the application is running on. That was one of the limitations of the study because participants did not test application on their own phone, which would offer them probably more familiarity with the standard mobile phone functionalities. One participant suggested that it would be useful for her to have a dictionary option while writing a text.

All of the participants understood the main menu. Some of them commented that it is very simple, clear and easy to understand. For the six participants size of the text was good for reading, and four commented that they do not have problems reading but they recommend little bigger text to facilitate reading for them and for other potential users. All of the participants were satisfied with used colors, and just one complaint that the soft key menu is too dimmed.

In the main menu we used shortcuts (that are presented as numbers in the brackets after the menu item names) and enable more experience to move through the application more quickly. Three participants understood the meaning of numbers as shortcuts.

2) Task analysis – Send the message to the nurse

All participants understood the organization of this functionality and they were satisfied how it is working. It was very easy for them to find all the functions and perform required tasks. Two participants that tested the web application earlier stated that it is very good that the mobile version is similar to the web version. One also stated that it is very good that standard mobile phone functions are used, so she was already familiar with key functions like text input.

Just two participants have stated that they would prefer bigger letters while for others the size of the text was good for reading. Three participants had problems identifying an option for writing a new message. One complained that the soft key menu is dimmed and other suggested to make this option more visible by emphasize it. All of participant also stated that now when they know where this option is they would not have problem using it.

3) Task analysis – Register specified problems

All of the participants were satisfied how organization of the problems were implemented. One that used the web version previously stated that it is very similar to how registration is organized there, and "if one see it on the big screen it is easier to recognize and understand it on the small screen also". Two of the participants stated that they were a little confused, but if they will use this application regularly it would be easier to perform this task.

All of the participants were satisfied with the text size, and one just commented that it could be little bigger but then there would be less space for the text on the screen and that would be a bigger problem for her.

Just one participant stated that the task was little complicated for her (she used the web version previously) but the rest of them said that the task was not complicated. Also they said that they would be able to perform it again.

Three participants had problems finding the option for going to the next step in the registration process (two that used just the mobile and one that used the web version also), but this was more because they did not know and/or did not remember the name of the next step. Other participants stated that they did not have problems finding option for the next step, and one said that "this way is very similar to an usual use of mobile phones and very intuitive."

4) Task analysis – Find advice regarding previously selected and specified problems

None of the participants had major complaints and problems performing tasks in this module. All of the participants said that they think it is not difficult to perform tasks. Four of them stated that they had little problems understanding it for the first time, but still thought the tasks was not difficult to perform. All of the participants said that they would be able to perform the task again. One participant said that "it looks much like the standard options on a phone", so she did not have problems finding the right options.

In the application we implemented functionalities for changing font size and orientation of the text when there is much text on the screen, and seven participants stated that they see these options very useful and that they would use them. Two said that they personally would not use these options, but still think that they are useful for others. One said that she would not use it and she thinks it is not so important.

5) Qualitative results – application usefulness and acceptance

After testing the mobile application most of the participants were very satisfied how it is working and seven of them stated that they think the mobile application is useful and that they would use it for monitoring their health condition. One of them said that if she has a web application available she would prefer to use the web application instead, but if not she would use the mobile application because she finds it also useful. One stated that she would not use the application because it is too slow for her, but if it was faster she would probably use it. One stated that she is not sure if she would use it and that she would have to try it and see.

When asked about usefulness of the application all the participants stated that they think the application is useful. Two participants said that today they use paper and pen to note when they have some problems and questions, and afterwards use this list as a reminder during consultation with the doctor. In these situations they think this kind of patient support system would be very useful because it will help them not to forget questions for doctors and nurses. Two participants stated that they do not want to call the hospital when they have minor health related problems because they are not sure how serious the problems really are, and access to this system could provide them first guidance and feedback if they need to make a trip to the hospital. Two participants stated that they liked the fact that the mobile application is always available, because they are not often in situation to use a PC. They said that now they have more free time, so for them using the mobile application would be very convenient. One participant stated that a positive side of the application is provision of a large amount of good and quality information that could help her monitoring her condition from one day to another, and not to just focus on a current problem.

VI. Discussion

From the previous results we can see that the majority of participants are very positive regarding the mobile application as part of patient support system, and most of them think the application is very useful. After the first contact with the application most of the participants thought that if they are given the opportunity they would use it to monitor their health condition in addition to the web version. Most of the participants stated that they would prefer the web version, but they would use the mobile version if they do not have a PC with them. Also, they identified some advantages of the mobile version and found possible scenarios and situations where the mobile application could be more usable. There is also a question, if they would use the mobile application more if they were provided just mobile without web access. To find acceptance of just a mobile version, a new application should be developed that is optimized only for mobile operation.

From our usability testing we saw that users were able to use the application also when they did not have previous experience with the web application, but previous knowledge and experience help them in understanding functionalities better and performing tasks in shorter time period. Based on this, we do not recommend making a mobile application similar to a web-based application, but the interface should be familiar. We recommend to use the same colors, command names, menu items and icons/logos, but the presentation and interaction should be different, and leverage the capabilities of the mobile terminal.

 ISBN: 978-1-61208-119-9

From the qualitative feedback we gained participants comments and thoughts regarding functionality modules, and identified usability problems, additional requirements and expectations that could influence acceptance of the system. The module that had the biggest difference in quantitative measurement was the registration module and we tried to use qualitative feedback to identify the reasons for this. As we saw that there were no major usability complaints, we concluded from participants' comments and video recording that the major issue was that they did not understand the registration process and they did not read the introduction text that were given to them on the screen before the registration process started. They stated that the interface for each step is organized well, and the command for going to the next step was not hard to find, but the problem was to understand what is the next step that should be performed. This explains also difference in completion time, because participants that had performed the task before on the web version knew which options to look for going to the next step of registration. From this we saw that a more detailed description is needed in the beginning of the tasks, so the process is understood before registration is started. Additionally, when creating instructions and support documentation this module should be addressed carefully and in more detail.

We saw that the functionalities provided in the mobile application should be a subset of functionality offered by the traditional web or pc/tablet application. In this way, the application can be very simple, providing only the most important functionalities that are suitable for mobile use. One patient stated: “Basics were there. For me, as a not so frequent user of a mobile phone, it is very important to keep the application simple. Too many choices would probably make it more complicated and I would get lost.”

From the participants' feedback we saw that following traditional design guidelines for development of mobile applications is not sufficient when creating a user friendly and intuitive application. General guidelines are often in contradiction to each other (especially if they are from different mobile OS or phone manufacturers) and it is difficult to identify which guidelines are important. This is why we have proposed a selection of general guidelines, which has shown to be important to users during our patient-based testing. We suggest balance of requirements such as providing back options, consistency of command names, feedback to user where they are in the application, and organizations of menus. In addition, we have proposed new guidelines for adaptation of a general mobile application across terminals. This includes adapting size of the text dependent of amount of content of the screen; avoid the use of icons and text for additional descriptions, allowing users to change font size and orientation of the text, and the use of shortcuts. One issue that we specially addressed during development of the application was finding the right balance between size of the text on the screen and amount of information on the screen. Most of the users were satisfied with the selected text size. Some of them stated that having little bigger font would be even better, but that would affect readability of the text. From this feedback and the previous experience from the application development process we conclude that in the situation where there is large amount of text on the screen, it is better to use smaller text size and in this manner make text easier to read and understand. On the other hand, where there are just menus or small amount of information, it is better to use bigger font size.

The platform developed in the project provides unique support for adaptation to any mobile terminal, without requirements for a particular screen size. New methods for text manipulation has been developed, and as an example, we support arbitrary fonts with arbitrary size scaling in the application and the platform can adapt to most navigation methods, as for example navigation buttons, stylus, soft-keys, only numeric keys, and even touch screens in a consistent way. Thus, all patients can use their own mobile phone, and the application maintains an intuitive look and feel across terminals.

We finally observe that the mobile application is more suitable for younger people that are more acquainted with mobile technologies. One participant suggested that this application is most appropriate for the user group from 20 to 50 years. Our impression from this study where the mean age of participants was 46,5 years with average experience with mobile technology is that the application is very well accepted, easily understood and not seen as too complicated for everyday use.

VII. Conclusion and Future Work

In this paper our main goal was to show the main user's requirements, expectations, acceptance and usefulness of a patient support tool that is accessible over mobile phone in addition to a web version. For development of the mobile application we used participatory design methods where we involved patients, usability and design experts, and also health providers that are well acquainted with patients needs. We saw that the mobile application we developed has good acceptance by a group of ten breast patients that participated in our usability study. We saw that most users accept a mobile application in addition to a web or tablet application. We think this is a very important fact, because until now mobile applications are often developed as a stand alone patient support tool and all system functionalities are provided through just one application. We recommend that a mobile application should be just a part of a more complete system including other types of terminals such as web or tablet for home/hospital use, and identifying guidelines for mobile application design and functionalities represent a new area in development of patient support systems.

We see that there are certain limitations and shortcomings in our usability study that can be addressed through future work, such as performing usability testing with a larger user group with different age ranges. Valuable feedback could be also gained from potential users with special needs, for example people with vision and motoric problems. Our plan for the next stage in the project is to start a pilot study where the group of patients will be offered both the mobile and web version of the support tool, and study differences in usability, usefulness and usage patterns.

In [29] it is described results of a clinical trial that showed “less symptom distress, depression, and better self-efficacy for the patients that used Internet support system through the WebChoice application”. We have proposed a selection of design guidelines for mobile applications for health care, and how the application should be aligned to existing web and tablet applications to improve usability and flexibility. We claim that an intuitive mobile application is an important part of a health management system for patients, and may result in faster recovery and better flexibility for patients and higher efficiency of healthcare providers.

ACKNOWLEDGMENT

This work has been funded by The Research Council of Norway under Grant Verdikt 176823/S10 - Communication and Information Sharing between Patients and Their Care Providers.

REFERENCES

[1] J. Protheroe, A. Rogers, A. P. Kennedy, W. Macdonald, and V. Lee, “Promoting patient engagement with self-management support information: a qualitative meta-synthesis of processes influencing uptake”, Implementation Science 2008, vol 3(44), October 2008, doi:10.1186/1748-5908-3-44.

[2] M. E. Radina, A. C. Ginter, J. Brandt, J. Swaney, and D. R. Longo, “Breast Cancer Patients' Use of Health Information in Decision Making and Coping”, Cancer Nursing, Nobember 2010, doi: 10.1097/NCC.0b013e3181faab7c.

[3] J. Mirkovic, H. Bryhni, and C. Ruland, “Review of projects using mobile devices and mobile applications in healthcare”, Proc. Scandinavian conference on Health Informatics, 2009.

[4] M. E. Larsen, J. Rowntree, A. M. Young, S. Pearson, J. Smith, J., O. J. Gibson, et al. “Chemotherapy side-effect management using mobile phones”, Proc. Engineering in Medicine and Biology Society, 2008, pp. 5152-5155, doi: 10.1109/IEMBS.2008.4650374.

[5] J. Finkelstein and J. Wood, “Mobile eLearning Platform for Interactive Patient Education”, Proc. 2009 International Conference on Mobile, Hybrid, and On-line Learning, IEEE Computer Society (2009), pp. 23-27, doi: 10.1109/eLmL.2009.24.

[6] L. McCann, R. Maguire, M. Miller, and N. Kearney, “Patients’ perceptions and experiences of using a mobile phone-based advanced symptom management system (ASyMS) to monitor and manage chemotherapy related toxicity”, European Journal of Cancer Care, vol. 18(2), March 2009, pp. 156-164, doi: 10.1111/j.1365-2354.2008.00938.x.

[7] J. N. Stinson, G. Z. Petroz, G. Tait, B. M. Feldman, D. Streiner, P. J. McGrath, and B. J. Stevens, “e-Ouch : Usability testing of an electronic chronic pain diary for adolescents with arthritis”, The Clinical journal of pain, vol. 22(3), Mar-Apr 2006, pp. 295-305, doi: 10.1097/01.ajp.0000173371.54579.31.

[8] A. Ahtinen, E. Mattila, A. Vaatanen, L. Hynninen, J. Salminen, E. Koskinen, and K. Laine, “User experiences of mobile wellness applications in health promotion: User study of Wellness Diary, Mobile Coach and SelfRelax”, Proc. Pervasive Computing Technologies for Healthcare, 2009, pp. 1-8, doi: 10.4108/ICST.PERVASIVEHEALTH2009.6007.

[9] C. C. Tsai, G. Lee, F. Raab, G. J. Norman, T. Sohn, W. G. Griswold, and K. Patrick, “Usability and Feasibility of PmEB: A Mobile Phone Application for Monitoring Real Time Caloric Balance”, Proc. Pervasive Health Conference and Workshops 2006, Kluwer Academic Publishers (2007), pp. 173-184, doi: 10.1007/s11036-007-0014-4.

[10] E. Arsand, R. Varmedal, and G. Hartvigsen, “Usability of a Mobile Self-Help Tool for People with Diabetes: the Easy Health Diary”, Proc. Automation Science and Engineering, 2007, pp. 863-868, doi: 10.1109/COASE.2007.4341807.

[11] P. Yu and H. Yu, “Lessons learned from the practice of mobile health application development”, Proc. Computer Software and Applications Conference, 2004, pp. 58-59, doi: 10.1109/CMPSAC.2004.1342675.

[12] T. Gegg-Harrison, M. Zhang, N. Meng, Z. Sun, and P. Yang, “Porting a cancer treatment prediction to a mobile device”, Proc. Engineering in Medicine and Biology Society, 2009, pp. 6218-6221, doi: 10.1109/IEMBS.2009.5334551.

[13] H. N. Chua, S. D. Scott, Y. W. Choi, and P. Blanchfield, “Web-page adaptation framework for PC & mobile device collaboration”, Proc. Advanced Information Networking and Applications, vol.2, 2005, IEEE Computer Society (2005), pp. 727-732, doi: 10.1109/AINA.2005.348.

[14] M. Palmblad and B. Tiplady, “Electronic diaries and questionnaires: Designing user interfaces that are easy for all patients to use”, Quality of Life Research, vol. 13(7) ,2004, pp. 1199-1207, doi: 10.1023/B:QURE.0000037501.92374.e1.

[15] B. Falchuk, “Visual and interaction design themes in mobile healthcare”, Proc. MobiQuitous 2009, pp. 1-10, doi: 10.4108/ICST.MOBIQUITOUS2009.6751.

[16] C. Ruland, A. Jeneson, T. Andersen, R. Andersen, L. Slaughter, B. Schjødt-Osmo, et al, “Designing Tailored Internet Support to Assist Cancer Patients in Illness Management”, AMIA Annual Symposium. Chicago, IL, pp. 635-639, 2007.

[17] M. Jones and G. Marsden, Mobile Interaction Design. John Wiley & Sons, 2006.

[18] B. Barbara, Designing the Mobile User Experience. John Wiley & Sons, 2007.

[19] H. Sharp, Y. Rogers, and J. Preece, Interaction Design: Beyond Human-Computer Interaction. Wiley, 2007.

[20] S60 UI Style Guide, available on: http://www.forum.nokia.com/info/sw.nokia.com/id/04c58d5a-84c3-42db-83d5-486c1cf3e6b3/S60_UI_Style_Guide_v1_3_en.pdf.html, October 2010.

[21] Series 40 U Style Guide., available on: http://www.forum.nokia.com/info/sw.nokia.com/id/73e935fe-8b59-43b2-ab3e-1c5f763672db/Series_40_UI_Style_Guide.html.

[22] Mobile developing and design guidelines, available on: http://wiki.forum.nokia.com/index.php/Mobile_developing_and_design_guidelines, December 2010.

[23] Sony Ericsson UI Rulebook, available on: http://developer.sonyericsson.com/wportal/devworld/downloads/download/dw-102212-uirulebook?cc=gb&lc=en, December 2010.

[24] J. Nielsen and T. K. Landauer. “A mathematical model of the finding of usability problems”, Proc. INTERACT '93 and CHI '93 conference on Human factors in computing systems, ACM Press (1993), pp. 206-213, doi: 10.1145/169059.169166.

[25] Java Platform, Micro Edition (Java ME), available at: http://java.sun.com/javame/downloads/, December 2010.

[26] Fast, high quality imaging on any device, available at: www.fasterimging.no, December 2010.

[27] J. Nielsen, Heuristic evaluation. Usability inspection methods. John Wiley & Sons, 2004, pp. 25-62.

[28] E. Bertini, S. Gabrielli, and S. Kimani, “Appropriating and assessing heuristics for mobile computing”, Proc. Advanced visual interfaces 2006, ACM Press(2006), pp. 119-126, doi: 10.1145/1133265.1133291.

[29] C. M. Ruland, E. Borosund, and C. Varsi, “User requirements for a practice-integrated nurse-administered online communication service for cancer patients”, Studies in health technology and informatics, vol. 146 (2009), pp. 221-225, doi: 10.3233/978-1-60750-024-7-2.

III

IV