LEONARDO HORN IWAYA

A SECURITY FRAMEWORK FOR MOBILE HEALTH DATA COLLECTION

São Paulo
2014

LEONARDO HORN IWAYA

A SECURITY FRAMEWORK FOR MOBILE HEALTH DATA COLLECTION

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Mestre em Engenharia Elétrica.

São Paulo
2014

LEONARDO HORN IWAYA

A SECURITY FRAMEWORK FOR MOBILE HEALTH DATA COLLECTION

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Mestre em Engenharia Elétrica.

Área de Concentração:

Engenharia de Computação

Orientador(a):

Tereza Cristina Melo de Brito Carvalho

São Paulo
2014

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 8 de abril de 2014.

Assinatura do autor

Assinatura do orientador

FICHA CATALOGRÁFICA

Iwaya, Leonardo Horn
A security framework for mobile health data collection / L. H. Iwaya. – ed. rev. – – São Paulo, 2014.
132 p.

Dissertação (Mestrado) — Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Computação e Sistemas Digitais.

1. Computação móvel 2. Telemedicina 3. Informação (Segurança) 4. Saúde 5. Engenharia elétrica. I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Computação e Sistemas Digitais. II. t.

“A man provided with paper, pencil, and rubber, and subject to strict discipline, is in effect a universal machine.” – Alan Mathison Turing

AGRADECIMENTOS

À Profa. Dra. Tereza Cristina M. B. Carvalho, um exemplo de líder e de pessoa, ao qual eu sou grato pelo trabalho de orientação na pesquisa. Agradeço pela sua paciência, atenção e por todas as oportunidades oferecidas que me fizeram evoluir, tanto como acadêmico quanto como ser humano.

Aos professores do Departamento de Engenharia de Computação e Sistemas Digitais (PCS). Em especial, meus sinceros agradecimentos ao Prof. Dr. Marcos Antonio Simplício Junior, pela inestimável contribuição para este trabalho e na minha formação na área de segurança da informação.

Ainda, aos professores e colaboradores do Departamento de Informática do Instituto do Coração (InCor), que também prestaram enorme contribuição para consolidação desta pesquisa, a respeito do uso adequado de tecnologias em saúde pública.

À Profa. Cristina Borba pelo importante trabalho de revisão no que se refere a correta utilização da língua inglesa.

Aos companheiros e amigos do Laboratório de Arquitetura de Redes e Computadores (LARC), pelas discussões das quais pude participar e pelas críticas que enriqueceram este trabalho.

Aos que me são mais caros, agradeço aos meus familiares que me incentivaram durante toda minha vida, de forma especial para com minha formação e estudos.

Ao Centro de Inovação da Ericsson Telecomunicações S.A. (Brasil), pelo apoio financeiro, e ao Laboratório de Arquitetura de Redes e Computadores (LARC/PCS/POLI/USP), por todo suporte oferecido para viabilizar a realização desta pesquisa.

.....

To Prof. Dr. Tereza Cristina M. B. Carvalho, an example of leader and person, who I am grateful for her work as my advisor in this research. Thank you for your patience, attention and all the opportunities that made me evolve, both as a scholar and as a human being.

To the professors of the Department of Computer and Digital Systems Engineering (PCS). In particular, my sincere thanks to Prof. Dr. Marcos Antonio Simplício Junior, for his invaluable contribution to this work, and for his guidance in the area of information security.

Also, to the professors and employees of the Informatics Division at Heart Institute (InCor), who also provided enormous contribution to the consolidation of this research, regarding the appropriate use of technology in public health.

To Prof. Cristina Borba, for her important work of revision, regarding the correct use of English language.

To my colleagues and friends in the Laboratory of Computer Networks and Architecture (LARC), for the discussions that I could participate and the criticisms that have enriched this work.

For those who are most esteemed by me, I want to thank my family who have encouraged me throughout my life, and specially towards my studies and academic training.

To the Innovation Center of Ericsson Telecommunications SA (Brazil) for the financial support, and to the Laboratory of Computer Networks and Architecture (LARC/PCS/POLI/USP) for all the assistance offered that enabled this research.

RESUMO

Saúde Móvel (mHealth) pode ser definida como a prática médica e a saúde pública suportadas por tecnologias de computação móvel, como: telefones celulares, PDAs, *tablets*, sensores e outros dispositivos sem fio. Particularmente no caso dos celulares, há um aumento expressivo no número de linhas, aparelhos, e na infraestrutura de rede em países de média e baixa renda (*Low- Middle-Income Countries*, LMIC), permitindo a adoção de sistemas mHealth de maneira eficiente. Existem, hoje, vários casos de sistemas de coleta de dados voltadas à atenção primária, vigilância (em saúde) e pesquisas epidemiológicas adotados nesses países. Tais sistemas fornecem aos gestores de saúde uma informação de melhor qualidade em menor tempo, que por sua vez melhoram a capacidade de planejamento e resposta a emergências. Contudo, nota-se um relaxamento no cumprimento de requisitos de segurança nestes sistemas. Com base nisso, foi feito um levantamento de aplicações e iniciativas de pesquisa em mHealth no Brasil, no qual se constatou que um número razoável de trabalhos mencionam fracamente (13%) ou não menciona (40%) os requisitos de segurança. Este levantamento também discute sobre o estado atual das pesquisas de mHealth no Brasil, os principais tipos de aplicações, os grupos de usuários, os dispositivos utilizados e as barreiras de pesquisa identificadas. Em seguida, este trabalho apresenta o SecourHealth, um *framework* de segurança voltado ao desenvolvimento de aplicações de mhealth para coleta de dados. O SecourHealth foi projetado com base em seis requisitos principais de segurança: suportar o registro e a autenticação do usuário; tratar a desconexão e os atrasos na rede; prover o armazenamento seguro de dados prevendo possibilidades de furto ou perda dos aparelhos; fazer transmissão segura de dados entre o aparelho e o servidor; permitir o compartilhamento de dispositivos entre os usuários (e.g., agentes de saúde); e considerar opções de compromisso entre segurança, desempenho e usabilidade. O trabalho também descreve com detalhes as etapas de modelagem e desenvolvimento do *framework* - que foi integrado a uma aplicação para a plataforma Android. Finalmente, é feita uma análise do desempenho dos algoritmos criptográficos implementados, considerando o *overhead* pelo simples uso do protocolo HTTPS.

ABSTRACT

Mobile health (mHealth) can be defined as the practice of medicine and public health supported by mobile computing technologies, such as mobile phones, PDAs, tablets, sensors and other wireless devices. Particularly in the case of mobile phones, there has been a significant increase in the number of lines, equipment, and network infrastructure in Low- and Middle-Income Countries (LMIC), allowing the adoption of mHealth systems efficiently. There are now several cases of systems for data collection focused on primary care, health surveillance and epidemiological research, which were adopted in these countries. Such systems provide health care managers information with higher quality and in a shorter time, which in turn improves their ability to plan actions and respond to emergencies. However, security is not included among the main requirements of such systems. Aiming to address this issue, we developed a survey about mHealth applications and research initiatives in Brazil, which shows that a reasonable number of papers only briefly (13%) or simply do not mention (40%) their security requirements. This survey also provides a discussion about the current state-of-art of Brazilian mHealth researches, including the main types of applications, target users, devices employed and the research barriers identified. After that, we present the SecourHealth, a security framework for mHealth data collection applications. SecourHealth was designed to cope with six main security requirements: support user registration and authentication mechanisms; treat network disconnections and delays; provide a secure data storage - even in case of possible theft or loss of equipment; allow secure data exchange between the device and server; enabling device sharing between users (i.e., health workers); and allow trade-offs between security, performance and usability. This thesis also describes in detail the framework modeling and development steps showing how it was integrated into an application for the Android platform. Finally, we benchmarked the cryptographic algorithms implemented, when compared to the overhead of using HTTPS protocol.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AKE	Authentication and Key Exchange
BSF	Bootstrapping Server Function
DSS	Decision Support Systems
DTN	Delay/Disruption Tolerant Network
eHealth	electronic Health Processing
EHR	Electronic Health Records
EPR	Electronic Patient Records
EKE	Encrypted Key Exchange
CEN	*Comité Européen de Normalisation* - European Committee for Normalization
FHS	*Estratégia Saúde da Família* - Family Health Strategy
GCE	GBA Credential Engine
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HCA	Health Community Agents
HL7	Health Level Seven

HLR	Home Location Register
HSS	Home Subscriber Server
HIS	Hospital Information System
HS	Home Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IHE	Integrating the Healthcare Enterprise
InCor	*Instituto do Coração* - Heart Institute
ISO	International Organization for Standardization
JIC	Joint Initiative Council
KDF	Key Derivation Function
KMM	Key Management Mechanism
LMICs	Low- and Middle-Income Countries
MAC	Message Authentication Code
mHA	mobile Health Alliance
mHealth	mobile Health
mHDCS	mobile Health Data Collection System
MNO	Mobile Network Operator
MWSB	Mobile Web Security Bootstrap
NAF	Network Application Function
PAKE	Password Authenticated Key Exchange

PBKDF2	Password-Based Key Derivation Function version 2
PDA	Personal Digital Assistant
PHR	Personal Health Records
PGP	Pretty Good Privacy
PHC	Primary Health Care
PKI	Public-Key Infrastructure
SIAB	*Sistema de Informação da Atenção Básica* - Brazilian Information System of Primary Care
SRP	Secure Remote Password
SSL	Secure Sockets Layer
SLF	Subscriber Locator Function
SMS	Short Message Service
SDK	Software Development Kit
SDO	Standard Development Organization
SSC	Support for Subscriber Certificates
TLS	Transport Layer Security
SUS	*Sistema Único de Saúde* - Unified Health System
USP	University of São Paulo
UE	User Equipment
(U)SIM	Universal Subscriber Identity Module
USS	User Security Settings
WHO	World Health Organization

LIST OF SYMBOLS

k	key
m	message
$E_k(m)$	encryption of a message m with a key k
$E_k^{-1}(m)$	decryption of a message m with a key k
$AE_k(m)$	authenticated encryption of a message m with a key k
$AE_k^{-1}(m)$	authenticated decryption of a message m with a key k
$MAC_k(m)$	message authentication code from a message m and a key k
HM	hash function of a message m
$H_{[M]}$	concatenation and hash function of a message m
$[s]_t$	truncation of a bitstring s to t bits
i_sis	iterative counter i of a string s
ses	session ses value
's'	string s
MK	function to generate a Master Key MK
KDF	key derivation function
K_{nofs}	key with no forward secrecy
K_{wfs}	key with weak forward secrecy
K_{sfs}	key with strong forward secrecy
$tlenx$	length size of a bitstring x

1 INTRODUCTION

The concept of mobile Health (mHealth) refers to the intersection of mobile computing technology with medical sensors and communication devices, creating solutions that support and improve health care (ISTEPANIAN; JOVANOV; ZHANG, 2004). This concept is also related to eHealth (electronic Health processing), but while the latter is more focused on fixed computing facilities (e.g., desktop computers), the former aims to explore more intensively the advances in wireless communication, ubiquitous computing and "wearable" device technologies (TACHAKRA et al., 2003). However, as defined in (GOE, 2011a) the mHealth could be considered a subset of the eHealth technology.

Several socioeconomic factors have contributed to increase the interest in the mHealth area. Examples include the wider availability of mobile devices with high computing capabilities, the growth in coverage of mobile cellular networks (ITU, 2010; ITU, 2011) and the need to actively bring adequate health care and support for people wherever they may be (GOE, 2011a; CONSULTING, 2009). Ultimately, the world has reached a point, in which more people have access to mobile phones than to proper sanitation (i.e., toilets or latrines) and clean water (WATER.ORG, 2013).

This attention around the mHealth area is spread all around the globe, which has recently led the World Health Organization (WHO) to develop surveys and reports focused specifically on such solutions (GOE, 2011a; GOE, 2011b; J. OSS-

MAN, 2010). Applications surveyed include mobile telemedicine, decision support systems, solutions for raising treatment compliance and awareness, Electronic Patient Records (EPR), data collection systems for enabling health surveys and surveillance, to cite a few. Among the conclusions drawn from such studies is the fact that, in the future and after an adequate evaluation, mHealth solutions are expected to be integrated into and improve existing country-wide health strategies (GOE, 2011a; CONSULTING, 2009).

The deployment of mHealth solutions is particularly promising in emerging countries, in which health authorities can take advantage of the flourishing mobile market to bring adequate health care to unserved or underserved communities (IWAYA et al., 2013). Indeed, specialized applications for health surveys and surveillance play a crucial role in such regions, providing a rich repository for decision making systems in the field of public health (GOE, 2011a; CAMBRIDGE; MOBILE, 2011; HERTZMAN; MEAGHER; MCGRAIL, 2012). Applications in this category typically involve remote data collection of Primary Health Care [1] (PHC) indicators, referred to family-related data, sanitary conditions, identification of common diseases in a given region, or from people tracking with chronic conditions/diseases. The data can be collected, for example, at health units located within the target communities or during visits to the patients' homes. This process is usually carried out by health teams that include medical personnel (e.g., physicians and nurses) and/or health agents responsible for specific regions (Sá et al., 2012). The data collected is then used by health authorities, allowing them to take effective actions based on more accurate information about the health conditions in the area surveyed. Mobile data collection systems, instead

[1] The primary health care (PHC), also called primary care (in Portugal) and basic care (Government of Brazil), was defined by the World Health Organization in 1978 (WHO, 1978) as: *"essential health care based on practical, scientifically sound and socially acceptable methods and technology, made universally accessible to individuals and families in the community through their full participation and at a cost that the community and country can afford to maintain at every stage of their development in the spirit of self-reliance and self-determination"*.

of paper-based forms, can avoid wrong interpretation due to misunderstandings related to hand writing; allow quick data validation and consolidation; and faster decision-making (YU et al., 2009; SHAO, 2012).

1.1 Motivation

Despite its potential for effectively improving health and wellness, mHealth still faces many challenges for its widespread adoption. One important concern refers to security, even though medical data is usually subject to a very strict legislation aiming to prevent unauthorized use or disclosure. However, many mHealth proposals do not employ robust security solutions to comply with such laws, hindering their ability to become real deployments (NORRIS; STOCKDALE; SHARMA, 2009; PATRICK et al., 2008). Such concern is reflected in studies about security and privacy properties of nation-wide electronic health care systems proposed in countries such as Germany (SUNYAEV; LEIMEISTER; KRCMAR, 2010) and Canada (INFOWAY, 2008). It also appears in recent reports from organizations such as WHO (World Health Organization) (GOE, 2011a) and the mHealth Alliance (J. OSSMAN, 2010), which point out data security and citizen privacy as issues that require more attention in order to ensure the success of mHealth initiatives.

Another important issue is that, while developed countries can usually benefit from a nearly-ubiquitous mobile infrastructure, the lack of such wide coverage in developing countries becomes an important constraint for the adoption of such technologies in practice. Consequently, data collection solutions employed in remote areas need to be delay-tolerant (at the application level) and employ techniques for locally storing acquired data in a secure manner. In addition, it is necessary to protect the patients' data and privacy even when devices are shared by different users or if they are stolen while still carrying some data (KAPLAN, 2006).

Still, security is not among the main discussion topics in most reports focused on mhealth-related projects around the world (GOE, 2011a) or in specific countries such as India (GANAPATHY; RAVINDRA, 2008). Indeed, except for a few exceptions, such as the mHealth report from China (CAMBRIDGE; MOBILE, 2011), security is not detailed or is addressed as a high-level requirement (e.g., security, privacy, access control). These reports (GOE, 2011a; GANAPATHY; RAVINDRA, 2008; CAMBRIDGE; MOBILE, 2011) drive us on a similar survey of Brazilian initiatives in mHealth (IWAYA et al., 2013); and, since security is always a matter of concern in medical systems, it has motivated us to stress its analysis during literature review. Thereafter, we identified that the development of security frameworks for mHealth applications was a research gap worthy working.

1.2 Objectives

This thesis devises a security framework designed for a subcategory of mHealth applications, the so-called data collection (also known as data gathering) applications. In this context, the following main goal can be defined for the purpose of this research:

- To conceive a framework that complies with the security requirements of mHealth Data Collection Systems (mHDCS) and related performance and usability trade-offs in constrained-resource devices.

This main goal can be detailed into other more specific research milestones:

1. To review the mHealth literature and research projects around the globe, aiming to assess the state-of-the-art of security solutions focused on this field.
2. To review the Brazilian research efforts and to analyze the most prominent application categories, deployed devices, users, and how security is tackled.

3. To make an analysis of security requirements and features for the specific subcategory of data collection applications, as well as the related work on the field.

4. To specify a security framework complying with the elicited requirements and their possible trade-offs with performance and usability.

5. To model and to implement the proposed framework.

6. To integrate the software framework in a proof-of-concept mHealth application for data collection.

7. To benchmark the framework performance and to compare it with similar-purpose technologies.

1.3 Method

This research can be categorized as an applied research, based on theoretical analysis and practical application of science. Initially, the literature review adopts a method of selective choice of technical papers, reports and books related to mHealth, health standards, information security and patient data privacy. This preliminary study supports the identification of security gaps in mHealth applications, which also led us to write a survey on mHealth research initiatives in Brazil. After that, a subsequent analysis of the subcategory of mHDCS was performed, so as to identify and then to analyze the related work.

This preliminary study assists the requirement analysis and the security framework specification for mHDCS, called SecourHealth. Therefore, the SecourHealth's API was implemented and integrated into GeoHealth (Sá et al., 2012). GeoHealth is an existing mHDCS developed by InCor and deployed west region of Sao paulo, used to survey underserved and/or unserved families in order

to support primary health care programs. In the last stage of the implementation, the security features were tested and benchmarked in order to demonstrate the framework feasibility.

1.4 Contribution

This research provides a double contribution. First, a related survey on the mHealth field was written and published (in (IWAYA et al., 2013)), identifying the mHealth projects in Brazil and research drivers, their health application focus, types of devices used, security features and so on. Second, the SecourHealth[2] framework for mHDCS is proposed and its software models are detailed; the framework implementation is fully described and integrated into a real application.

It is also worth noticing that the research has led to two patent applications (not yet published), one related to the security mechanisms provided by SecourHealth and the other related to the Generic Bootstrapping Architecture (see Appendix A).

1.5 Research Context

This master thesis was made within the research project named Personalized mobile health solutions for Brazil - from April 2011 to July 2013. The project goal was designing mobile solutions applied to the area of health care, with research activities focused on mobile technologies, patient data privacy and security. The mHealth project was a partnership involving Ericsson Research (Sweden), the Heart Institute (InCor), and the Laboratory of Computer Networks and Architecture (LARC/EPUSP) supported by the Innovation Centre, Ericsson Telecomunicações S.A. (Brazil).

[2]The word *secour* comes from the French language and means “to succor”, “great help” or “rescue”.

1.6 Thesis organization

This thesis is organized as follows:

- Chapter 2 presents an overview of the mHealth area around the globe and a further study about the Brazilian initiatives;
- Chapter 3 discusses the security background and in Chapter 4 the framework requirements;
- Chapter 5 describes the SecourHealth framework;
- Chapter 6 details the SecourHealth implementation and integration within the GeoHealth data collection system;
- finally, Chapter 7 presents the main conclusion of the research in terms of its outcomes, publications and future works.

2 MOBILE TECHNOLOGY FOR HEALTH CARE

The mobile health (mHealth) technology can be defined as the integration of mobile computing, medical sensors, and portable devices to ensure health care (ISTEPANIAN; JOVANOV; ZHANG, 2004). Even though mHealth is closely related to the concept of eHealth (electronic process in health), which is more focused on desktop computers, mHealth aims to explore more intensively the advances in wireless communication, ubiquitous computing and "wearable" device technologies in the health area (TACHAKRA et al., 2003; ABAJO et al., 2011). This technology is particularly promising for emerging countries (YU et al., 2009; CHEN; HSIAO, 2012), in which health authorities can take advantage of the flourishing mobile market to bring adequate health care not only to aging people, but also to un-served or under-served communities (CHENG et al., 2011). In such regions, mHealth can effectively improve basic care and help to fight against endemic and epidemic diseases not so often encountered in developed countries (KAPLAN, 2006). The remainder of this Chapter presents the global and Brazilian perspectives of mobile health care, showing research initiatives and giving some insights for further studies.

2.1 Overview of Mobile Health

The growing importance of mHealth worldwide has led to a considerable effort by official health organizations as regards classifying and categorizing such

solutions. Since 2009, the World Health Organization (WHO) has published annual reports covering initiatives in eHealth and mHealth (CONSULTING, 2009; WHO, 2009; GOE, 2011b; GOE, 2011a). The mHealth Alliance (mHA)[1], hosted by the United Nations Foundation, is another institution that aims to maximize the impact of mobile health, especially in emerging economies, by ensuring interoperability and promoting open-standards. Recently, mHA launched the website Health Unbound (HUB)[2], an interactive network and on-line knowledge resource center for the mHealth community (HUB, 2013). Even though these initiatives are useful for giving an overall perspective of the mHealth area, they are still quite recent and do not yet provide a comprehensive analysis of mHealth solutions being used in each country.

Deeper analysis focused on emerging countries have been developed in (GANAPATHY; RAVINDRA, 2008), (CAMBRIDGE; MOBILE, 2011) and (IWAYA et al., 2013). The first describes eHealth and mHealth projects developed in India, trying to predict the impacts of these technologies and how they can improve the health systems in emerging countries. The second evaluates several mHealth projects in China, trying to understand barriers and opportunities for such solutions, and presents a work performed by a partnership between Cambridge University and China Mobile. The third identifies research opportunities, limitations and trends in Brazilian mHealth and provides an in-depth analysis of relevant aspects of current solutions (e.g., features, providers, goals, target areas, and maturity of the projects). The latter work is a partial contribution of this research, detailed in Section 2.3.

The researches and reports above consistently show that higher-income countries (e.g., United States or Europe) currently show more eHealth and mHealth activity than lower-income countries do (e.g., in Africa and Latin America). Nonetheless, in both cases, mHealth is more commonly incorporated

[1] http://www.mhealthalliance.org/
[2] http://www.healthunbound.org/

into processes and services which historically use voice communication through conventional telephone networks. Indeed, according to a survey made by the World Health Organization (GOE, 2011a) among government entities, which is summarized in Figure 1, the prevailing classes of mHealth initiatives today correspond to health call centers/health-care telephone help lines (59%), emergency toll-free telephone services (55%), emergencies (54%), and mobile telemedicine (49%); conversely, solutions that require more complex capabilities and infrastructure in order to take full advantage of mHealth are reported as the least common initiatives, which is the case of health surveys (26%), surveillance (26%), awareness raising (23%), and decision support systems (19%). However, as mobile devices become cheaper and more powerful (i.e., more processing power, memory availability and connectivity of the mobile devices to the Internet) the initiatives regarding *patient monitoring* to *decision support systems* (see Figure 1) are expected to increase in the near future.

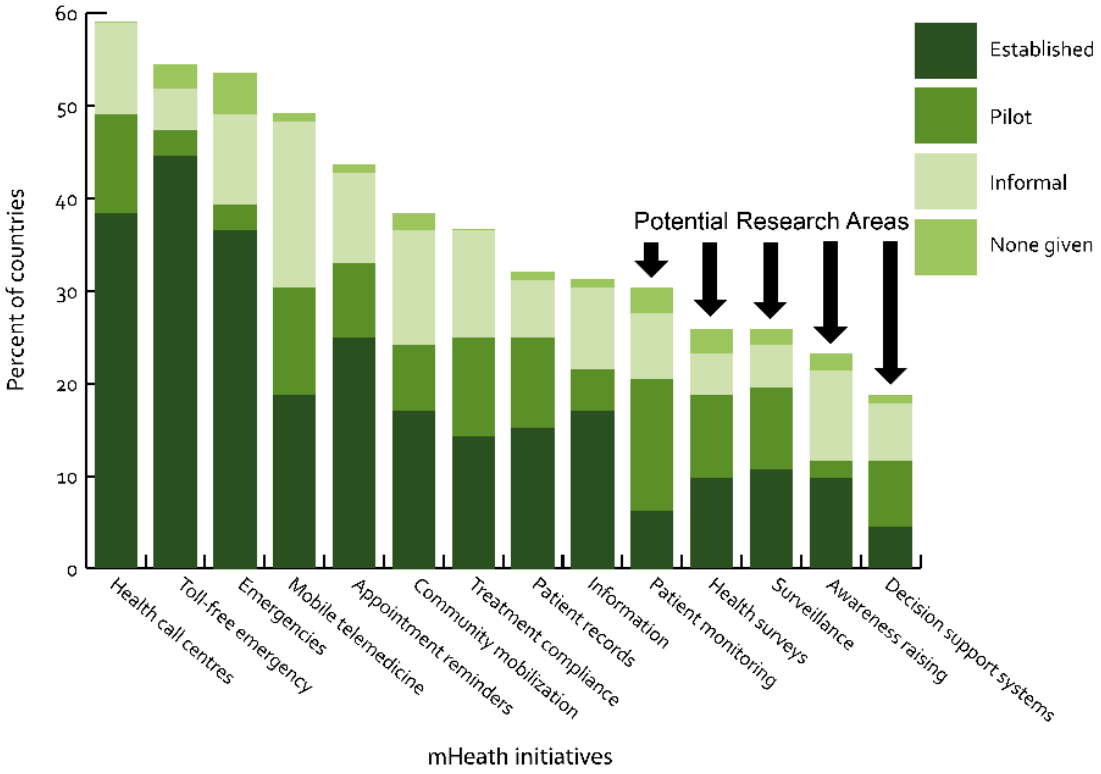


Figure 1: Adoption of mHealth initiatives and phases of implementation, globally. Adapted from (GOE, 2011a).

Despite its potential for effectively improving health and wellness, the mHealth area still faces many challenges. One concern refers to security: even though the handling of medical data is covered by a very strict legislation in most countries, many mHealth proposals do not employ robust-enough security solutions for coping with such laws, hindering their ability to become real deployments (CHAKRAVORTY, 2006; NORRIS; STOCKDALE; SHARMA, 2009; PATRICK et al., 2008). Another relevant issue, as emphasized by the World Health Organization (WHO) (GOE, 2011a) and (J. OSSMAN, 2010), is that the dominant approach of mHealth today consists in isolated, small-scale pilot projects that address specific issues of information access and sharing. The result of the lack of collaboration among these different initiatives is that many of existing pilot projects are unable to evolve into country-wide solutions. At the same time, they do not adopt globally accepted standards or interoperable technologies (PAYNE, 2013), making future integrations more difficult or even impossible. In addition, while developed countries can usually benefit from a nearly-ubiquitous mobile infrastructure, the lack of such wide coverage in emerging countries leads to further challenges. For example, patient monitoring solutions deployed in remote areas need to be delay-tolerant and, usually, must employ techniques for locally relay and/or store acquired data in a secure manner.

2.2 Key Research Areas in mHealth

The mHealth field can be subdivided into several application/system categories. However, there is no consensus in the literature on how to classify mHealth initiatives and key research areas. Here we follow the classification proposed by WHO (J. OSSMAN, 2010), which shares many characteristics with the terminology employed in many other relevant mHealth-oriented reports (WHO, 2009; CONSULTING, 2009; GOE, 2011a; CAMBRIDGE; MOBILE, 2011). This taxonomy

is described below:

A. *Health call centers/Health care telephone help line*: delivery of triage services and health care advices by trained professionals, by means of telephones. Such initiatives are commonly used to manage national emergencies (e.g., epidemic outbreaks).

B. *Emergency toll-free telephone services*: often used for quick access to health professionals or staff trained to provide guidance during medical emergencies. Telephony services are used to contact a health call center and/or emergency toll-free number (e.g., 911 in the United States or 192 SAMU in Brazil).

C. *Public health emergencies*: can be defined as the use of mobile devices to respond to emergency and disaster situations, such as natural disasters and disease outbreaks.

D. *Mobile telemedicine*: can be defined as the use of a mobile device functions (e.g., voice, text, data, imaging, or video) for different situations, such as communication between health professionals for consultation about patients or treatment of chronic patients living at home. The goal of such projects is usually to overcome human resource shortages in the health sector, facilitating access to treatment and/or specialized care, as well as reducing unnecessary referrals.

E. *Appointment reminders*: comprise services that rely on voice or SMS (Short Message Service) messages sent to patients, e.g., for scheduling consultations, delivering treatment results, or broadcasting immunization reminders.

F. *Community mobilization & health promotion*: defined as the use of text messaging for health promotion or alerting target groups of health campaigns.

Such applications can be used, for example, to increase participation in immunization campaigns or to promote voluntary counseling and human immunodeficiency virus (HIV) screening.

G. *Treatment compliance*: can be described as the delivery of reminder messages, by voice or SMS, aiming to improve treatment compliance, disease eradication, and overcoming challenges such as resistance to taking the required medicine. It is commonly applied to support patients suffering from chronic diseases such as diabetes, HIV/AIDS, and tuberculosis (TB).

H. *Patient records*: the use of mobile devices to support the treatment of patients, including collecting and displaying patient records. This class of mHealth applications enables access to Electronic Health Records (EHR) at the point-of-care using mobile technologies.

I. *Information initiatives*: comprises services that provide access to health science publications or databases at the point-of-care (i.e., bedsite or near of the patient site), by means of portable devices.

J. *Patient monitoring*: defined as using technology to manage, monitor, and remotely treat patient illness (e.g., patients suffering from diabetes or cardiac conditions). Remote sensors installed in households or imaging devices linked to mobile phones are often used to facilitate data transmission to the health service provider. This can reduce the need for visits to a health center for regular check-ups, as well as inform emergency-response teams in case of necessity.

K. *Health surveys*: consist in the use of mobile devices for collecting and reporting health-related data.

L. *Surveillance*: defined as the use of mobile devices for inputting and transmitting data that will be used by surveillance programs to track diseases. This area has

a large overlap with Health Surveys initiatives and, thus, both are presented together in this thesis.

M. *Awareness raising*: includes the use of health information products, games, or quiz programs to educate people on relevant health topics such as HIV/AIDS. These programs are commonly available for download onto mobile phones or as a series of text messages that tells a story containing health-related elements.

N. *Decision support systems*: defined as software algorithms that help health providers to make their clinical diagnoses at point-of-care or health managers to take actions based on data gathered from health surveys. For example, they can provide advice based on a combination of a patient's medical history (e.g., prescribed drugs and alleged symptoms) and the data provided by sensors monitoring patient's vital signs. Mobile devices are used to input the patient's data and to receive information from the system.

This classification is quite comprehensive and constitutes an interesting basis for discussion. Nonetheless, some of them are quite well established (e.g., A, B, C, D) in most countries and, thus, are not currently theme of technological researches. This can be observed in Figure 2, which presents the development stages of mHealth initiatives in the Americas. For example, health call centers and emergency toll-free solutions (i.e., A and B) are part of the basic infrastructure provided by Unified Health System (*Sistema Único de Saúde* – SUS) and private health institutions in Brazil, and thus is not a subject of research in the mHealth area. Therefore, herein we focused on the categories highlighted in Figure 2 as the less well-established in America, namely: health surveys & surveillance, patient records, patient monitoring, decision support systems, treatment compliance and awareness raising.

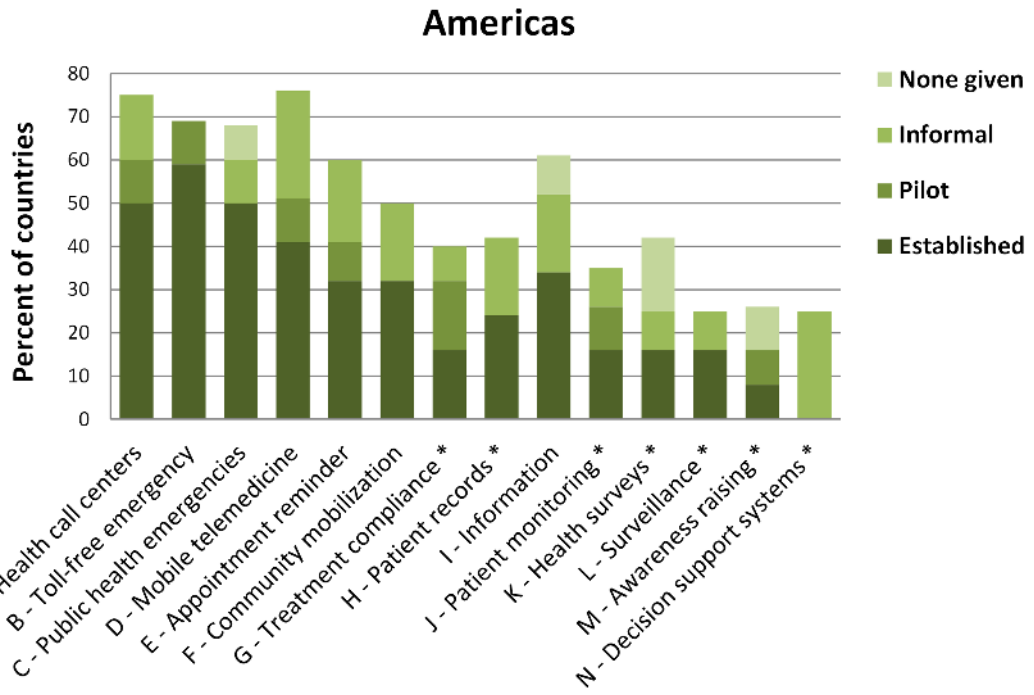


Figure 2: Adoption of mHealth initiatives and their implementation stages in America (adapted from (GOE, 2011a)). Areas evaluated in this survey are marked with a $*$.

It is noteworthy however that in such a continuously evolving field, some solutions may actually include features that cut across different mHealth research areas - e.g., data collection systems that supports epidemic outbreak control and tracking of inhabitants health conditions. For this reason, in Section 2.3, we try to (1) identify common characteristics and tendencies shown by the surveyed solutions and (2) highlight some of the main features of each solution, allowing a better understanding of its purpose and complexity.

2.3 Mobile Health in Brazil

Aiming to consolidate the view about the Brazilian state-of-art research on mHealth, our preliminary work was to conduct a survey on this subject, resulting in the publication of (IWAYA et al., 2013). This paper ended up being quite long; as a consequence, it is not fully reproduced in this chapter, which focuses only on its

main findings.

2.3.1 Health Care in Brazil

The Brazilian health care system consists of both public and private entities (DATASUS, 2011). The private health care system comprises the private institutions that do not belong to the Unified Health System; when using the private system, patients are responsible for their own medical bills. In comparison, the public system provides free universal health coverage to all Brazilians by means of the SUS program. As result of the government's far-reaching and free health coverage, around 80% of the population relies exclusively on SUS and the remainder uses the "supplemental" medical care system provided by private institutions (DATASUS, 2011). As expected, however, this discrepancy is less accentuated in wealthier regions of the country such as the State of São Paulo, in which approximately 40% of the population has some private health coverage (DATASUS, 2011).

After the implementation of SUS in 1990, two main governmental policies were adopted as part of this program (BARROS; BERTOLDI, 2008): the first is *decentralization*, reducing the need of displacing patients over long distances for receiving basic care; the second is the *focus on primary health care*, which led to several initiatives, among which the Family Health Strategy (FHS) that has an increasing importance since its creation in 1994. The FHS program focuses on disease prevention rather than only on its treatment, and was conceived to bring health care closer to the population, which is accomplished by means of regular visits by the health agents to the families (BERTOLDI et al., 2009). This work is performed by Primary Care Teams responsible for permanent and systematic follow-up of a given number of families residing in a delimited area covered by a regional health unit. Each team is formed by medical personnel (a general practitioner, a nurse, and an auxiliary nurse) and by four Health Community Agents (HCAs). An interesting characteristic

of this structure is that the basic requirement for becoming a HCA is to reside in the area to be covered by the Primary Care Team, enabling easy communication with the local community.

During their visits, the Primary Care Teams gather data related to many aspects of the families' health, such as house type, sanitation conditions, number of family members and information about them, presence of chronic diseases or pregnancy, vaccination status, etc. All data are collected using standardized forms, anonymized and then consolidated in the Brazilian Information System of Primary Care (SIAB) database. This and other health-related databases (e.g., SINAN, which is focused on epidemics) can be freely accessed over the Internet by every citizen and are commonly used by health managers for planning their own health initiatives.

2.3.2 mHealth Research Initiatives in Brazil

In recent years, the fast expansion of mobile coverage in Brazil created a rich environment for the development of mHealth projects. In what follows, we succinctly put our considerations about the initiatives developed and published by different institutions (including universities, companies, hospitals, government agencies, or partnerships between them).

2.3.2.1 Health surveys & surveillance

Most applications in Brazil belonging to this category focus on primary care, both in urban and remote regions of the country. Even though many of these projects are quite general in terms of target population, some of them were developed for specific groups such as children (COSTA; SIGULEM, 2004; COSTA et al., 2010), or for specific health conditions, such as oral hygiene (BREGA et al., 2008), dengue fever(JORGE; ZIVIANI; SALLES, 2009; NOKIA, 2013) or heart diseases (JONES

et al., 2011; FOUNDATION, 2011).

Often, the health surveys developed in the country are directly or indirectly associated to the Family Health Program, meaning that their application scenario considers the existence of HCAs visiting families in different areas. This is the case of the solutions discussed in (CAVICCHIOLI-NETO et al., 2006; JORGE; ZIVIANI; SALLES, 2009; DANTAS; CAVALCANTE; FILHO, 2009; PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010; FROTA et al., 2011; NOKIA, 2013; PRSYSTEMS, 2011; Sá et al., 2012). One common improvement introduced by these applications is the construction of standardized e-forms running on mobile devices, replacing the paper-based forms (standardized by SUS) normally used by the HCAs in their periodic visits. Such tools accelerate data acquisition while reducing input and transcription errors, leading to higher consistency and improved quality of the information provided to health professionals. They also enable more effective response to disease outbreaks, since consolidated information becomes available to the responsible authorities in much shorter periods, accelerating the decision-making process. In other cases, the solution goal is to collect supplementary data not originally available from the standard SIAB forms, such as children-related information (COSTA; SIGULEM, 2004; COSTA et al., 2010) or use of medications and medicinal plants (FACHEL et al., 2011). There are also projects that aim to improve the data analysis process, proposing the use of auxiliary tools such as expert systems (PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010; FROTA et al., 2011) or visualization of geo-referenced data (PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010; Sá et al., 2012).

In all cases, the data collected is sent to a database managed by the responsible health care units. This can be done remotely (e.g., using a 3G connection) or using local area communication capabilities inside these units (e.g., cradle communication, Bluetooth or WLAN). However, since there are large

disparities between the communication infrastructure available throughout the country, these solutions commonly support both data delivery methods.

When not associated to the Family Health program, these solutions tend to focus on the physicians in the health units, helping in the medical diagnosis or providing means of access to electronic records (BULCAO-NETO et al., 2008; FREITAS; CAMACHO-GUERRERO; MACEDO, 2008; BREGA et al., 2008; JONES et al., 2011; FOUNDATION, 2011). The goal of such applications is to facilitate and to accelerate the process of collecting relevant information from patients. At the same time, they allow physicians to update and to access their patients' records in the point of care. For example, they provide mechanisms for inputting treatment prescriptions or adding annotations regarding a specific image or video. In addition, these solutions commonly have auxiliary tools such as built-in communication functionalities that allow health professionals to exchange messages with their colleagues (e.g., for asking a second opinion) (BULCAO-NETO et al., 2008; FREITAS; CAMACHO-GUERRERO; MACEDO, 2008; JONES et al., 2011).

Ultimately, although data security is a critical concern in many of those initiatives (especially in the case of remote communications), approximately half of the surveyed projects (COSTA; SIGULEM, 2004; COSTA et al., 2010; JORGE; ZIVIANI; SALLES, 2009; PIMENTEL; SILVA; CONCEICAO, 2010; FROTA et al., 2011; CONCEICAO; PIMENTEL; SILVA, 2010; JONES et al., 2011; PRSYSTEMS, 2011; Sá et al., 2012) implement some mechanism for user authentication and secure data transmission, but such concerns are not even mentioned in the remaining initiatives (CAVICCHIOLI-NETO et al., 2006; BULCAO-NETO et al., 2008; FREITAS; CAMACHO-GUERRERO; MACEDO, 2008; BREGA et al., 2008; DANTAS; CAVALCANTE; FILHO, 2009; FACHEL et al., 2011; NOKIA, 2013; FOUNDATION, 2011).

2.3.2.2 Patient records

Most pioneer projects in this area considered the use of mobile devices by physicians inside the hospitals. Some solutions simply provide physicians with access to their patients' medical history using mobile devices (MURAKAMI et al., 2004; MEZAROBA; MENEGON; NICOLEIT, 2008; ORTIS, 2009), while other initiatives also allow the acquisition of medical information at the point of care (MORAES; PISA; LOPES, 2004; BARBOSA et al., 2006; CRISPIM-JR.; FERNANDES, 2006; MARTHA et al., 2006).

A more recent trend followed in (DUARTE et al., 2010; CORREIA, 2011; VIGOLO; FADEL; BASTOS, 2008; TECHNOLOGIES, 2009b; TECHNOLOGIES, 2009a; HOSPITAL, 2009) consists of solutions focused on empowering health professionals in their home care visits. Usually, they aim to replace traditional paper-based forms, increasing responsiveness, centralizing information, and avoiding multiple registers or poorly filled information. These goals are repeatedly shared with many of the aforementioned *health surveys & surveillance applications*. In addition, such initiatives also provide tools that allow physicians to access relevant information from health units' databases (e.g., patients' records) before starting a home care session. Some applications go beyond, improving the amount of information about the patient that can be acquired (e.g., including pictures and video) and allowing communication between physicians and health institutions (e.g., for obtaining information about the availability of some medicine in a health unit) (DUARTE et al., 2010; CORREIA, 2011).

It is interesting to notice that security is recognized as an important concern in most of the projects surveyed in this category. Most of them are especially concerned with authentication and access control mechanisms (MARTHA et al., 2006; VIGOLO; FADEL; BASTOS, 2008), while some also include the protection of

data communication (BARBOSA et al., 2006; DUARTE et al., 2010; CORREIA, 2011; MEZAROBA; MENEGON; NICOLEIT, 2008; ORTIS, 2009; TECHNOLOGIES, 2009b; TECHNOLOGIES, 2009a; HOSPITAL, 2009). Even when such security features are not actually implemented, their deployment is usually considered an important addition to future versions of the prototypes provided (MURAKAMI et al., 2004; MORAES; PISA; LOPES, 2004). This occurs because this application frequently extends hospital EHR and PHR information systems, quite well established and standardized due to country regulations.

Finally, almost all the surveyed projects try to be generic in terms of the health conditions covered. The exception is (VIGOLO; FADEL; BASTOS, 2008), which focuses on patients suffering from hanseniasis.

2.3.2.3 Patient monitoring

From the survey, patient monitoring solutions can be distinguished in three different classes. This classification depends mainly on who is the owner of the devices and which is the target deployment scenario, i.e.,:

- In a first scenario, patients at home use their own mobile devices for gathering health-related data, either manually or automatically (using sensors), and then send this information to health institutions (CASTRO et al., 2004; CRUZ; BARROS, 2005; ANDREAO; FILHO; CALVI, 2006; MACHADO et al., 2011; PORTOCARRERO et al., 2010).

- A second scenario comprises the use of mobile devices on the bedside, forming body area networks with various sensors that capture real-time data of patients. (MURAKAMI et al., 2006; ANDREAO; FILHO; CALVI, 2006; GUTIERREZ et al., 2008b; ROLIM et al., 2010; SPARENBERG; KALIL; PORTAL, 2010; LACERDA et al., 2010).

- Likewise, in a third scenario, a similar architecture of bedside devices is re-arranged inside the ambulances, allowing health care workers from remote locations to exchange information with a health centre while a patient is being moved (ANDREAO; FILHO; CALVI, 2006; CORREA et al., 2011; SANTOS et al., 2009).

Many of the solutions in this category present a considerable overlap with the area of mobile telemedicine[3], since they cover not only the (intense) data transmission of vital signs from remote locations, but also allow paramedics to ask for specialized support when analyzing this data. This is the case, for example, of solutions in which patients suffering a heart attack are monitored on their way to the hospital (CORREA et al., 2011; SANTOS et al., 2009), or when the triage of emergency patients leverages on the second opinion provided by specialized centers (CRUZ; BARROS, 2005; LACERDA et al., 2010; SPARENBERG; KALIL; PORTAL, 2010).

Notice that, unlike the projects in the previous categories, most projects for patient monitoring are focused on a specific type of health issue, such as cardiac conditions (CRUZ; BARROS, 2005; MURAKAMI et al., 2006; ANDREAO; FILHO; CALVI, 2006; GUTIERREZ et al., 2008b; SPARENBERG; KALIL; PORTAL, 2010; LACERDA et al., 2010; CORREA et al., 2011), mental disorders (CASTRO et al., 2004) and the analysis of physical activities (PORTOCARRERO et al., 2010). Among the solution surveyed, only three (SANTOS et al., 2009; ROLIM et al., 2010; MACHADO et al., 2011) are meant for general health conditions. This can probably be explained by the fact that not all diseases ask for constant monitoring of patients, but, when that is the case, they also require a quite specialized system for data treatment and visualization. The large number of solutions focused on cardiovascular diseases, on the contrary, is explained by the fact that this is one of the most serious health issues round the

[3]Employ telecommunications technology for health care services, as by accessing remote databases, linking clinics or physician's offices to referred hospitals, or transmitting medical data for examination at another site (ASSOCIATION, 2012).

world and also in Brazil (WHO, 2005; ISHITANI et al., 2006), motivating initiatives in this specific area.

One important concern shared by many of the surveyed projects (e.g., (CRUZ; BARROS, 2005; LACERDA et al., 2010; SPARENBERG; KALIL; PORTAL, 2010; CORREA et al., 2011)) is the need of allowing communication between physicians in different institutions (e.g., Basic Health Units and Specialized Hospitals). The goal in this case is to allow specialists to delivery accurate diagnosis to generalist health physicians in the numerous non-specialized centers over the country. However, a challenge faced by many remote monitoring projects is the deficient communication infrastructure available in many regions of Brazil. This may not be a serious issue for deployments in metropolitan cities (MURAKAMI et al., 2006), but it is certainly an important concern when remote and poor areas are involved, as stressed in (LACERDA et al., 2010).

Finally, patient monitoring systems process a large amount of medical data, implying the observance of security requirements. For this reason, aspects such as communication encryption and user authentication are implemented in (GUTIERREZ et al., 2008b; SANTOS et al., 2009; CORREA et al., 2011), while in (CASTRO et al., 2004; ANDREAO; FILHO; CALVI, 2006) the authors explicitly considered authentication. However, more than half of the surveyed projects falling into this category, namely (CRUZ; BARROS, 2005; MURAKAMI et al., 2006; MACHADO et al., 2011; PORTOCARRERO et al., 2010; LACERDA et al., 2010; SPARENBERG; KALIL; PORTAL, 2010), do not even mention security among its requirements, while (ROLIM et al., 2010) discusses the need of security but does not implement the mechanisms required for providing it.

2.3.2.4 Decision support systems

The Decision Support Systems (DSS) area is closely related to data collection technologies and databases, as they deal with a large amount of data collected, aiming to extract relevant information for decision-making. Therefore, the deployment of such solutions in Brazil can greatly benefit from the large amount of data available in the SUS databases (e.g., the SIAB database). Indeed, there are a number of DSS-oriented *electronic-Health* studies in the country that employ such databases for health planning and analysis of the behavior of some diseases (e.g., (TRINDADE, 2005; MATTOS, 2003)). However, in our studies we were able to identify only two *mHealth* projects focusing on the SUS databases: the Colibri (PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010) and the LISA (FROTA et al., 2011) projects, already discussed in section 2.3.2.1, which provide platforms for data collection and processing as well as the treatment of this information by expert systems. In addition to these projects, there are also the research initiatives developed by Brazilian universities described in (JOSÉ et al., 2005) and (MENEZES-JR. et al., 2011). The first consists of an expert system for helping in the anamnesis process, while the second presents a DSS system for the diagnosis of asthma symptoms.

This reduced number of solutions is in accordance with WHO analysis (J. OSSMAN, 2010) depicted in Figure 2, which shows that DSS is the least explored area in America and most initiatives are in the form of pilot and informal projects. Therefore, this field displays a wide and yet largely unexplored potential for research and development of mHealth initiatives in Brazil. Such solutions should allow health managers to make a more efficient use of the information available, avoiding existing deficiencies such as lack of integration between systems, low strategic alignment and commitment by health managers, data unreliability and difficulty in its utilization for decision-making at the local level (SILVA; LAPREGA,

2005; MENDONCA; MACADAR, 2008).

Concerning security, secure data transmission and user authentication are the mechanisms more commonly deployed (PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010) or at least discussed (MENEZES-JR. et al., 2011) in such solutions. It is not, however, among the concerns mentioned in (JOSÉ et al., 2005).

2.3.2.5 Treatment compliance

Medical studies show that many HIV/AIDS patients in Brazil have learned to use their mobile phones' alarm functionality for improving treatment adherence on their own (KOURROUSKI; LIMA, 2009). However, this self-motivated approach is unlikely to work with patients suffering from mental disorders such as schizophrenia, a disease with high non-compliance rate (i.e., people give up or do not do the treatment correctly) in the country (ROSA; MARCOLIN; ELKIS, 2005). Nevertheless, our analysis revealed only two formal research initiatives in this category: one of them focuses on asthma treatment (CHATKIN et al., 2006) and the another is oriented toward general diseases requiring frequent medication (NARDON, 2006).

The positive results obtained in such projects indicate that there is still plenty of room for new initiatives in this area. In this context, and as discussed by WHO in (J. OSSMAN, 2010), SMS and other low-cost initiatives not requiring advanced mobile devices can be considered the most effective approaches for treating chronic health conditions (e.g., diabetes, HIV/AIDS, schizophrenia, and tuberculosis) and increasing attendance of health-promoting programs (e.g., immunization, smoking cessation and health awareness).

Security concerns were not discussed in any of these initiatives, but evidently the minimum security requirements (e.g., data privacy) are necessary in real

deployments for ensuring at least adherence to regulations.

2.3.2.6 Awareness raising

In Brazil, **eHealth** initiatives for awareness raising can be found in the form of serious games. Examples include the desktop-based applications Sherlock Dengue (HOUNSELL; MIRANDA; KEMCZINSKI, 2010), Zig-AIDS (MONTEIRO; REBELLO; SCHALL, 2012) and the odontology game described in (MORAIS; MACHADO; VALENCA, 2010), which focus on education about dengue fever, HIV/AIDS and dental hygiene, respectively. Even though such initiatives indicate the interest in the area, we were unable to identify any mHealth research project falling into this category. Nonetheless, since this trend is still quite recent in Brazil, it is reasonable to envision the adaptation of such initiatives to mobile scenarios, as well as new developments leveraging on the rapid expansion of mobile devices in the country.

2.3.3 Summary

Table 1 summarizes this section, relating the mHealth solutions surveyed with their respective areas. The table shows five mHealth categories mentioned in the WHO taxonomy (J. OSSMAN, 2010), which were identified as the potential research areas in the preliminary survey (IWAYA et al., 2013); although, unexpectedly, for the awareness raising category, no Brazilian mHealth initiative was found.

2.3.4 Analysis and Discussions

The analysis of the solutions surveyed shows that most of them can be classified as Health Survey & Surveillance, Patient Records or Patient Monitoring systems, while solutions classified as Decision Support Systems, Treatment Compliance and Awareness Raising are considerably less expressive in number. This is depicted in Figure 3. When we compare the results obtained in our survey

Table 1: Summary of mHealth solutions surveyed.

Research Area	**References**
Health surveys & surveillance	(COSTA; SIGULEM, 2004; COSTA et al., 2010; CAVICCHIOLI-NETO et al., 2006; BULCAO-NETO et al., 2008; FREITAS; CAMACHO-GUERRERO; MACEDO, 2008; BREGA et al., 2008; DANTAS; CAVALCANTE; FILHO, 2009; JORGE; ZIVIANI; SALLES, 2009; PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010; FROTA et al., 2011; FACHEL et al., 2011; JONES et al., 2011; NOKIA, 2013; FOUNDATION, 2011; PRSYSTEMS, 2011; Sá et al., 2012)
Patient records	(MURAKAMI et al., 2004; MORAES; PISA; LOPES, 2004; BARBOSA et al., 2006; CRISPIM-JR.; FERNANDES, 2006; MARTHA et al., 2006; MEZAROBA; MENEGON; NICOLEIT, 2008; VIGOLO; FADEL; BASTOS, 2008; ORTIS, 2009; TECHNOLOGIES, 2009b; TECHNOLOGIES, 2009a; HOSPITAL, 2009; DUARTE et al., 2010; CORREIA, 2011)
Patient monitoring	(CASTRO et al., 2004; CRUZ; BARROS, 2005; MURAKAMI et al., 2006; ANDREAO; FILHO; CALVI, 2006; SANTOS et al., 2009; PORTOCARRERO et al., 2010; ROLIM et al., 2010; SPARENBERG; KALIL; PORTAL, 2010; GUTIERREZ et al., 2008b; LACERDA et al., 2010; MACHADO et al., 2011; CORREA et al., 2011)
Decision support systems	(JOSÉ et al., 2005; PIMENTEL; SILVA; CONCEICAO, 2010; CONCEICAO; PIMENTEL; SILVA, 2010; FROTA et al., 2011; MENEZES-JR. et al., 2011)
Treatment compliance	(NARDON, 2006; CHATKIN et al., 2006)
Awareness raising	–

with those described by WHO in their survey in America (J. OSSMAN, 2010), we can observe that solutions for Health Survey & Surveillance, Patient Records and Patient Monitoring are indeed expected to be quite representative, while Decision Support Systems are not surprisingly much less expressive. On the other hand, the low number of Treatment Compliance initiatives in Brazil is somewhat unusual when compared with the rest of the continent, appearing as an interesting opportunity for new studies/research projects. A similar observation applies to solutions for awareness raising, which, albeit not numerous, are still present in America but explored in Brazil mainly in the form of eHealth initiatives.

The maturity of the projects in each category is depicted in Figure 4, which groups the solutions according to their status (deployed or not deployed). This figure shows the most deployed solutions, although in many cases they only resulted in testing prototypes rather than being incorporated as established solutions. Nevertheless, the fact that some recent projects became commercial

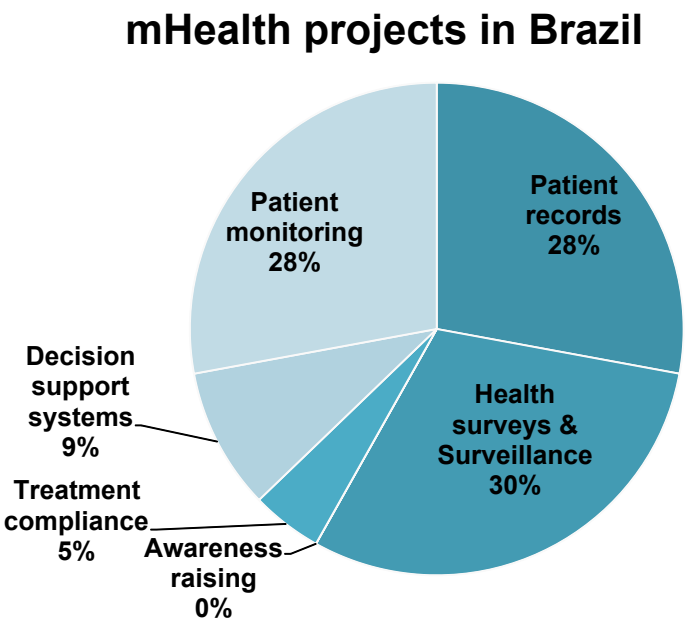


Figure 3: Percentage of mHealth research areas in Brazil.

products (e.g., (TECHNOLOGIES, 2009b; TECHNOLOGIES, 2009a; HOSPITAL, 2009; PRSYSTEMS, 2011)) or were indeed adopted by public or private health institutions (e.g., (CORREA et al., 2011; FOUNDATION, 2011)) are good indicators of the growing acceptance of such solutions in the country.

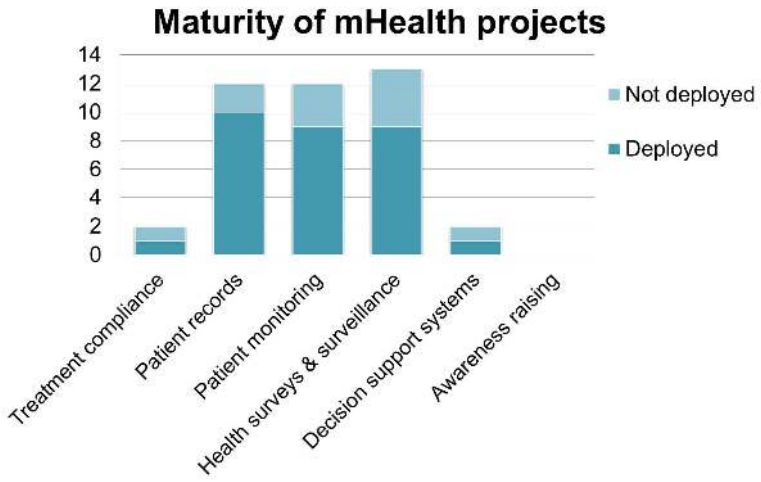


Figure 4: Maturity of mHealth research initiatives in Brazil.

Despite the involvement of private companies, most of the research in the area is still developed in partnerships with universities: as depicted in Figure 5,

there is one or more universities involved in approximately 79% of the 42 projects surveyed. This scenario might continue at least until mHealth services become more feasible as a source of profit for private companies. Until then, the task of bringing new discoveries and innovation into the field is likely to be left to the academia, especially considering that the latter is usually more capable of receiving research funding from the most interested entity in this scenario: the public sector. Indeed, even though public health agencies are also important providers of mHealth solutions in the country, this participation is mainly indirect, consisting of projects developed in cooperation with universities. The expected expansion of the mHealth consumer market and the emergence of new opportunities led by such pioneer researches should change this scenario, resulting in a larger presence of the private sector and the development of specific subvention programs for eHealth and mHealth research initiatives.

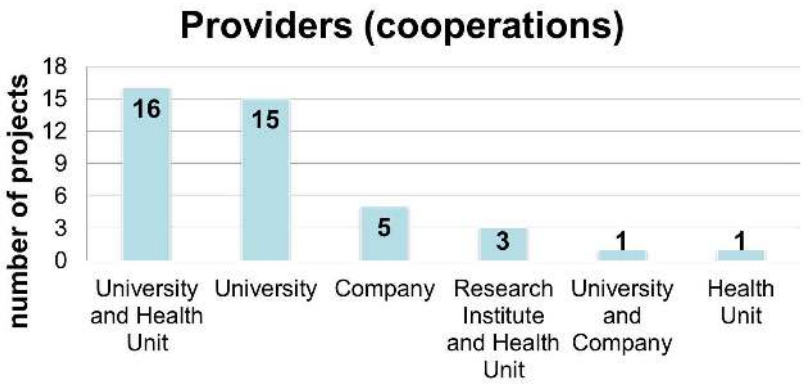


Figure 5: Providers of mHealth solutions in Brazil and cooperation among them.

Finally, as shown in Figure 6, security is not mentioned in many of the solutions surveyed. There are at least two possible explanations for this: (1) either the authors decided not to deal with security requirements in their pilot prototypes or (2) those features were simply omitted from the solution description so that the authors could focus on the description of the technology and benefits involved rather than on non-functional requirements. In any case, in order to cope with laws concerning patient's privacy, the implementation of robust security mechanisms is mandatory

for any system that handles medical data and must thus be fully considered when mHealth solutions are deployed in the field.

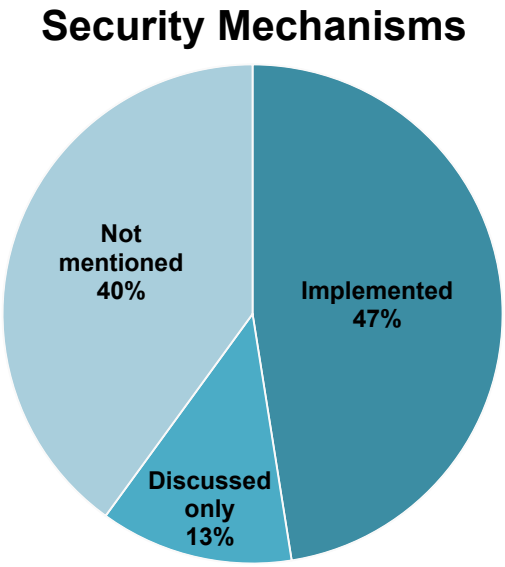


Figure 6: Deployment of security mechanisms in the solutions surveyed.

2.4 Chapter Considerations

Among the areas surveyed, those that display larger opportunities of innovation given the small number of existing projects are Decision Support Systems, Treatment Compliance and Awareness Raising; in comparison, Health Survey & Surveillance, Patient Records or Patient Monitoring are quite saturated with solutions, some of them having overlapping goals and features. Another trend worth exploring is the development of security mechanisms that support a large variety of applications while complying to health regulations. The services required include data privacy and authentication, access control policies, securing communications between devices and servers, among others. This interest comes from the fact that, even though some of the solutions surveyed do implement security services, they do not follow the same guidelines or adopt the same standards. Therefore, it is difficult to predict how serious the interoperability

problems resulting from their integration would be in a country-wide solution.

One of the main limitations of the mHealth initiatives in the country refers to the lack of cooperation between solution providers and the small participation of the industry in the area. As a result, research is mainly lead by universities (commonly with government funding). This scenario ends up leading to interoperability issues and hindering the development of nation-wide solutions. Some essential aspects to overcome this situation include: the decision making from health managers and/or medical staff to adopt valuable mHealth solutions; the development of partnerships between the institutions to successfully deploy mHealth projects; and a coordinated investment both from the public and private sectors in strategic areas.

Finally, one particularity of Brazil of especial interest for the mHealth area is the widespread presence of HCAs throughout the country, forming a powerful human infrastructure. Many initiatives can (and some actually do) benefit from those agents' visits to patients, especially solutions focused on preventive programs and control of conditions with long duration and generally slow progression. At the same time, in areas covered by the Family Health Program, empowering those agents with mobile equipment is much more cost-effective than distributing devices to all patients, while a similar level of ubiquity can be obtained. Therefore, the presence of these agents can be seen as an interesting approach for solving some of the issues typically faced by mHealth in emerging countries, such as lack of investment in technology and deficient communication infrastructures.

3 SECURITY MECHANISMS FOR MHEALTH

This chapter reviews cryptographic mechanisms and algorithms that can be used to design a security framework for mHDCS. In Chapter 4 further describes the framework requirements, but in brief, a Key Management Mechanism (KMM) should be devised in order to provide Authentication and Key Exchange (AKE) between parties (user's mobile and application server). In the case o mHDCS, the authentication protocols and key derivation schemes usually rely on symmetric cryptography, using passwords. These protocols should also give support for online and offline user authentication. Other mechanisms should cope with confidentiality of stored and in-transit data, by means of encryption schemes for secure storage and transmission. Therefore, the mechanisms here described will be then deployed to form the framework building blocks, specified in Chapter 5. The security background herein presented, thus, firmly grounds the design and implementation stages for the next chapters.

3.1 Authentication and Authenticated Key Exchange

User authentication is one of the most vital elements in modern computer security. Even though there are authentication mechanisms based on biometric devices ("what the user is") or physical devices such as smart cards ("what the user has"), the most widespread strategy still lies in secret passwords ("what the user

knows") (POINTCHEVAL; ZIMMER, 2008). This happens because password-based authentication remains as the most well-known, simplest, cost effective and efficient method of maintaining a *shared secret* between a user and a computer system. Right or wrong, these advantages in practice tend to out shadow the disadvantages related to the problems of choosing strong, yet easy-to-remember passwords. Thus, it is likely that we will see passwords being used for quite some time into the future (ROEDER, 2013).

The most useful password-based systems normally employ Key Derivation Functions (KDFs), cryptographic algorithms that allow the generation of a pseudorandom string of bits from the password itself (SCHNEIER, 1996, sec. 2.4). Typically, the output of a key derivation function is employed in one of two manners: it can be locally stored in the form of a "token" for future verifications of the password or it can be used as the secret key for data encryption and/or authentication. Whichever the case, such solutions internally employ a one-way (e.g., hash) function, so that recovering the password from the key derivation output is computationally infeasible (DIFFIE; OORSCHOT; WIENER, 1992). Nonetheless, an attacker can still use the so-called dictionary attacks (SCHNEIER, 1996, sec. 8.1), in which he/she tests many different passwords until a match is found. Key derivation functions usually rely on two basic strategies for preventing such brute-force attacks. The first is to purposely raise the cost of every password guess in terms of computational resources such as processing time and/or memory usage. The second is to take as input not only the user-memorisable password, but also a sequence of random bits known as *salt* [1] (SCHNEIER, 1996, sec. 3.2). The presence of such random variable thwarts several attacks based on pre-build tables of common passwords, i.e., the attacker is forced to create a new table from scratch for every different *salt*. The *salt* can, thus, be seen as an index into a large set of

[1] **Salt** is a random string that is concatenated with passwords before being operated on by the one-way function.

possible keys derived from the password, and need not be memorized by the user or kept secret.

3.2 Password-based remote authentication and key exchange

In principle, KDFs could be used for data delivery: if the local and remote systems share the same password, they could exchange data by revealing to each other the *salt* employed for generating the key that protects such data. However, since this would allow attackers to use the same *salt* in an offline dictionary attack, KDFs are usually employed only for local data storage, establishing a secure channel between the human user and the local system.

Data delivery to remote locations usually employs Password Authenticated Key Exchange (PAKE) protocols. Such schemes allow two or more parties who share a password to authenticate each other and create a secure channel for protecting their communications (for example, (BELLOVIN; MERRITT, 1992; BELLARE; POINTCHEVAL; ROGAWAY, 2000)). In order to be considered secure, PAKE solutions must ensure that an unauthorized party (one who controls the communication channel but has no access to the password) is unable to learn the resulting key and is, as much as possible, unable to guess the password using offline brute force attacks.

In other words, the Secure Remote Password (SRP) project group (PROJECT, 2013) emphasizes that this class of protocols should be devised considering that:

- Attackers have complete knowledge of the protocol.
- Attackers have access to a large dictionary of commonly used passwords.
- Attackers can eavesdrop on all communications between client and server.

- Attackers can intercept, modify, and forge arbitrary messages between client and server.
- A mutually trusted third party is not available.

Looking briefly into the history of PAKE protocols, the Encrypted Key Exchange (EKE) (BELLOVIN; MERRITT, 1992) was probably the first successful proposal. Although several of the published methods were flawed, the surviving and enhanced forms of EKE effectively amplify the security of a shared password and turn it into a shared key, which can then be used for message encryption and/or authentication. Other provably-secure PAKE include the schemes described in (BOYKO; MACKENZIE; PATEL, 2000) (which uses the standard model[2]) and in (BELLARE; ROGAWAY, 1993)(which uses the random oracle model[3]). These EKE inspired proposals are now also called EKE family of protocols.

3.3 Forward security/secrecy

The security of computer systems commonly depends on meeting the condition that attackers cannot gain access to its underlying secret (ITKIS, 2004). In practice, however, ensuring that this condition is met is a difficult challenge. In addition, most strategies employed for hindering the exposure of the secret keys end-up raising the solution cost, and may not be adequate for use in all scenarios. Examples include the use of special devices (e.g., smart-cards) and *multiple factor mechanisms* (e.g., regular passwords combined with smart-cards and/or biometric

[2]Cryptographic systems are commonly based on complexity assumptions, such as the factorization problem, that can not be solved in polynomial time. This constructions that can be proven secure using only mathematical complexity assumptions are said to be secure in the standard model.

[3]A random oracle is a mathematical abstraction that *"provides a bridge between cryptographic theory and cryptographic practice"* (BELLARE; ROGAWAY, 1993), typically used when the cryptographic hash functions in the method cannot be proven to possess the mathematical properties required by the proof. A system that is proven secure when every hash function is replaced by a random oracle is described as being secure in the random oracle model, as opposed to secure in the standard model.

readings)(POINTCHEVAL; ZIMMER, 2008). Therefore, assuming that a sufficiently motivated adversary may succeed in exposing the system secrets (e.g., by stealing and directly accessing the devices' storage unit), it is important to explicitly deal with such events and elaborate strategies for minimizing potential damages.

One interesting approach for the above issue is to build (password-based) protocols having the so-called perfect forward security (also called forward secrecy) property (DIFFIE; OORSCHOT; WIENER, 1992). In the case of PAKE schemes, this property can be translated as follows: if the long-term secret information (e.g., the password) is revealed to an attacker, this information cannot be used to obtain ephemeral keys from past communications, effectively protecting all information previously exchanged (SUN; YEH, 2006). In other words, if the parties participating in the protocol share a long-term secret S and run the protocol r times before S is discovered by an attacker, that attacker is unable to determine the set of ephemeral keys $K_1, \ldots, K_r$ generated prior to this disclosure of S; only the subsequent keys $K_r + i$ where $(i > 0)$ generated using the same S can be compromised by that attacker. This concept is an integrating part of many modern security solutions, including pseudo-random generators, digital signatures and public key encryption (ITKIS, 2004). It is usually employed for securing data channels between communicating parties during a limited/temporal interaction. Nonetheless, it is also possible to employ the forward secrecy concept for securing data storage, avoiding the encryption of large quantities of data with a single secret key (e.g., as done in OpenPGP's (BROWN; BACK; LAURIE, 2001) e-mail encryption (SUN; HSIEH; HWANG, 2005)). Whichever the case, the main drawback of applying forward secrecy is that such strategy incurs additional operations and, most likely, a more complex key management/evolving scheme.

3.4 Device Authentication with GAA/GBA

PAKE mechanisms are useful to achieve mutual authentication between parties (e.g., server and users) upon a previously agreed secret. However, they do not provide any type of *device authentication*, meaning that (1) legitimate users can perform the protocol from any (possibly misconfigured) equipment, and (2) attackers can use any device to establish a connection with the server and try to deliver (likely rubbish) data. This problem has been addressed by Mobile Network Operators (MNO) to authenticate mobile phone lines. Further, in 2005 the 3rd Generation Partnership Project (3GPP)[4] released the Generic Authentication Architecture (GAA) specification, with which MNOs can provide authentication as a service (LAITINEN et al., 2005)

The GAA permits two types of authentication mechanisms, one based upon shared secrets between entities and another based on (public, private) key pairs and digital certificates (ETSI, 2005), for loading key material into the (U)SIM[5] card. The former is called Generic Bootstrapping Architecture (GBA), a mechanism to issue shared secrets between Network Application Function (NAF) and User Equipment (UE). The latter is named Support for Subscriber Certificates (SSC) based on a Public-Key Infrastructure (PKI), so that the UE needs to issue a certificate through the PKI portal (e.g., own a valid SIM Card), before being able to authenticate itself with other NAF. Both mechanisms were devised in order to offer authentication as a service for web applications in general, thus either GBA or SSC may also use HTTPS communication channels during the key issuing phases.

The GAA/GBA is particularly useful for mobile applications (SHANMUGAM et al., 2006; DOMINICINI, 2012), offering a strong user authentication scheme (lighter

[4] **3GPP** is a cooperative effort of telecommunications standard development organizations that develops technical specifications for 3G networks

[5] Universal Subscriber Identity Module (U)SIM, introduced for UMTS cellular networks and 3G technologies.

than GAA/SSC) with the device authentication feature (HOLTMANNS et al., 2008). More precisely, security-sensitive code can be kept inside the (U)SIM card as aforementioned, thus reducing the system exposure to malicious software. Also, GAA/GBA can be used to authenticate the client's device as soon as a connection with the server is established, limiting the action of attackers. This latter process may be employed prior to any content delivery, and would then consist in the following steps:

1. The Client perceives the presence of a 3G connection and connects with the Server via an HTTPS channel, thus allowing the client to authenticate the Server.
2. The Client runs the GAA/GBA protocol for establishing a common key Ks_NAF with the Server.
3. Client and Server run a challenge-response protocol in order to confirm that both have the same Ks_NAF, thus authenticating the client inside the established HTTPS channel.
4. If the authentication is successful, the Client sends authenticated data; otherwise, the Server terminates the connection.

The GAA/GBA thus provides the following advantages when compared to the basic scenario in which this device authentication process is absent:

- Stronger security: data delivery process involves double authentication (user via password and device via GAA/GBA).
- Device filtering: only registered devices are able to send data toward the server. As a result, attackers trying to exhaust the server's resources by sending a large amount of rubbish data toward it will have to previously

perform a successful GAA/GBA authentication. Otherwise, the Server will close the HTTPS session and discard the data provided without further consideration. Comparatively, in the basic scenario the server would likely verify that at least a few messages are unauthentic before concluding that the device owner is actually a malicious entity. Therefore, GAA/GBA improves the server availability and resilience against some types of denial-of-service attacks.

- Data confidentiality towards network operator: the Mobile Network Provider does not gain access to the data transmitted since it is protected by information shared only by the user and the server, i.e., the user password. Therefore, it is very unlikely that this process violates any of the (usually strict) laws concerning access to medical data.

- Transparency: the whole process is completely transparent to users, there is thus no perceptible difference between the GAA/GBA-empowered and the basic cases from their point of view.

We note that the only reason why the procedure above employs HTTPS for server-side authentication and data encryption is to provide compatibility with the protocols previously described. Nonetheless, if compatibility is not required, GAA/GBA usage procedure can also be employed to provide both services, without the need of HTTPS or certificates.

3.5 Secure Data Storage

At the time user and server agree on a common *master key*, e.g., by means of a PAKE protocol, this key can be used to protect the data stored in the mobile phone. This secure storage mechanism should encrypt all the sensitive information that will reside in the mobile storage (e.g., configuration files, user's data) and the in-flight

data (e.g., data gathered) that is temporarily stored in the mobile before being sent to the server. This mechanism shall use sufficiently lightweight encryption algorithms concerning to the mobile computing power limitations and available memory.

Hence, encryption assures data confidentiality in such a way that eavesdroppers cannot read it, even if the authorized parties can. However, as pointed out by (SNIA, 2009), encryption carries the risk of making data unavailable due to data transformation, or if anything goes wrong with the key management process. In other words, the key management process becomes more complex since at least on the server-side its necessary to store partial values to rebuild users' keys in order to decrypt and to consolidate data received.

3.6 Chapter Considerations

This chapter discussed four concepts and mechanisms that underpins a security framework for mHDCS, namely they are: authentication and key exchange (based on password or not); forward secrecy in key generation; device authentication based on GAA/GBA; and secure data storage. Security components alone, however, still not cover all the mHDCS framework functionalities: some of them related to the system usability and other related to network and communication functions. Chapter 4 fully describes these other inherent requirements of mHDCS.

It is also worthy noting that the mechanisms here described were explained in order to conceptualize them, but not to detail specific algorithms and parameters. Nonetheless, these algorithms used in our proposal are them detailed in Chapter 6, that describes the SecourHealth implementation.

4 SECURITY REQUIREMENTS FOR MHEALTH

In this chapter, we review the security requirements for designing a mHealth Data Collection Systems (mHDCS), as well as standards and usability factors. This class of application has many issues to be accounted, but in our proposal the networking and security requirements are emphasized. In short, developers of mHDCS should foresee the connectivity problems inherent to mobile networks (e.g., 3G), and thus design the application to deal with it transparently. Security mechanisms are also fundamental and they should ensure patient's data privacy since the data is (temporarily) stored, sent through the Mobile Network Operator (MNO), and reaches the server. Therefore, the security background described in Chapter 3 and requirement analysis hereafter detailed should ground the design and implementation stages presented in Chapters 5 and 6.

4.1 General Issues in mHealth

Despite the growing adoption of mobile computing in health care, there are major complaints about smartphones/PDAs and barriers to their use. In general, a list of typical issues for these handheld computers includes, but is not limited to (GUTIERREZ et al., 2008a):

- **Personal factors**, such as large fingers for small buttons, poor eyesight (inability to read the small fonts), memory problem (users forget to carry the device), discomfort with the device and dependency or over-reliance on the

device (PATRICK et al., 2008).

- **Data entry** is difficult, since common mechanisms based on capacitive pen are unintuitive and not easy to use (LU et al., 2005; MCALEARNEY; SCHWEIKHART; MEDOW, 2004) (specially for filling forms).

- **Physical problems**, such as size, weight, constrained battery life and small screen (devices should be smaller and lighter but should have the screen as large as possible (LU et al., 2005; MCALEARNEY; SCHWEIKHART; MEDOW, 2004)).

- **Low robustness**, the user limits the device utilization because he/she is afraid of breaking it (LU et al., 2005; MCALEARNEY; SCHWEIKHART; MEDOW, 2004).

- **Security** features are mandatory to ensure patient's data privacy (LIND et al., 2002; CHAKRAVORTY, 2006; NORRIS; STOCKDALE; SHARMA, 2009).

- **Networking** and broadband wireless access is needed for reliable and faster communication among parties (PATRICK et al., 2008).

- **Compliance and standards**, the design of equipment and applications must comply with the health legislations and standards, which differ from country to country (PAYNE, 2013).

- **Communication cost**, the energy consumption related to the communication done by wireless devices for continuous monitoring, data gathering and data (re-)transmission (e.g., 3G communication), and thus, associated to the equipment's battery life-time.

4.2 Standards and Systems Compliance for mHealth

The (lack of) standardization of eHealth/mHealth systems is a major problem for low- and middle-income countries (LMICs). As a result, the promise of a full interconnected and interoperable health system that provides the right information to the right place at the right time is still far from being a reality. However, as reported by the Mobile Health Alliance (mHA) in (PAYNE, 2013), several Standard Development Organizations (SDOs) have made significant progress for the future of health informatics standards. The most important SDOs considered by (PAYNE, 2013) are:

- ISO Technical Committee 215 (ISO/TC 215);
- Health Level 7 International (HL7);
- European Committee for Normalization (CEN) TC 251; GS-1;
- International Health Terminology Standardization Organization (IHTSDO);
- Clinical Data Interchange Standards Consortium (CDISC);
- Integrating the Healthcare Enterprise (IHE).

These SDOs comprise the Joint Initiative Council (JIC), which aims to harmonize the activities through joint publication of standards and to mediate forums for resolving conflicts. In addition to the JIC, another option is the standardized Health Insurance Portability and Accountability Act of 1996 (HIPAA), which can be a strong starting point to design eHealth/mHealth applications. For instance, HIPAA suggests using Advanced Encryption Standard (AES) for encryption, Virtual Private Network (VPN) for Internet transmissions, and data transfer over the Internet secured by Transport Layer Security (TLS) (AMA, 2013).

In Brazil, the Federal Council of Medicine adopts similar security standards. The Certification Manual for Electronic Health Record Systems (SILVEIRA et al., 2009) presents the Brazilian requirements for managing medical data, which is strongly based on the ISO/TC 215 standards.

The definition of mHealth standards is crucial to improve interoperability, thus facilitating system's design and implementation. Furthermore, it enables Health Information Systems (HIS) to work together within and across organizational boundaries to advance the effective delivery of health care (PAYNE, 2013). Currently, efforts have been made to standardize interfaces, semantics, processes and institutional attributes in HIS (WOZAK et al., 2008). However, security it is still considered as an add-on at the network and application layers (WOZAK et al., 2008). In the work (LUXTON; KAYL; MISHKIND, 2012), the authors encourage discussions on data security to assure privacy, to allow interoperability, and to maximize the full capabilities of mobile devices in health care. In short, they suggested removing the responsibility of data encryption and security from the mobile platform (i.e., data does not remain into the mobile); or to create a secure mobile framework; to develop a secure mobile version of an operating system for use within the medical community; or any hybrid approach of these methods.

It is worth noting that SDO's such as ISO/TC 215, HL7 and CEN made some progress on releasing standards for security in medical data (ISO, 2013; CEN, 2008; HL7, 2013), as well as HIPAA. Their work was, however, mainly focused on traditional HIS (e.g., Electronic Health Records (EHR) and Personal Health Records (PHR)). Therefore, the more inherent issues of mHealth applications had not yet been addressed, such as: 3G/4G connectivity, challenged networks scenarios, mobility and lightweight security mechanisms for constrained devices.

4.3 Data Collection - Requirements and Assumptions

Data collection systems are mainly used as a tool for gathering primary health care information and tracking existing diseases, driving health promotion initiatives in the affected communities (GOE, 2011a). Figure 7 illustrates such systems, showing a generic architecture in which the paper forms traditionally employed for data collection are replaced by a mobile device and the latter communication capabilities allow data to be delivered faster and more reliably. In this scenario, health care workers act as data collection agents, being responsible for visiting families in their houses and for acquiring health-related information. During those visits, the agents fill out electronic forms containing several questions designed for this specific purpose and load them into the mobile device. Partially filled forms (i.e., forms lacking mandatory information) are stored in the device storage and, after consolidation, are delivered to the server (e.g., via 3G or Wi-Fi) together with the corresponding family location. The server stores all the data received in a database, which can then be accessed and analyzed using a health management system.

Figure 7: Remote data collection scenario.

Since data collection systems deal with sensitive information, both stored

and in-transit data must be protected from unauthorized access or modification. Otherwise, there may be security breaches such as illegal disclosure to health insurance or pharmaceutical companies, or simply to someone who steals a mobile device and can decide to publish socially-sensitive health conditions (e.g., AIDS or teenage pregnancy) on the Internet. Such events are likely to affect people's trust in the application and discourage their participation in health programs involving such systems (HODGE, 2003), or even lead to lawsuits against those responsible for such programs. Therefore, to ensure the scalability and longevity of such programs, proactive security measures should be taken. There are, however, several constraints that must be taken into account by any security framework targeted at mobile data collection applications, especially when considering large-scale but low budget projects usually found in developing countries.

In short the requirements addressed in this chapter are within six main requirement groups:

1. Tolerance to delays and lack of connectivity;
2. Protection against device theft or loss;
3. Secure data exchange between mobile device and server
4. Lightweight and low cost solution;
5. Device sharing among health agents;
6. Usability for computational literate users.

In what follows, the requirements involved in the design of the proposed SecourHealth framework are discussed in detail.

4.3.1 Tolerance to delays and lack of connectivity

Many data collection systems are deployed in remote locations where network access is not continuously available, meaning that frequent disconnections are expected to occur between the mobile device and the server (FACHEL et al., 2011; GEJIBO et al., 2012; Sá et al., 2012). Consequently, the mobile device should be able to authenticate the user in an offline manner and also employ mechanisms for temporarily storing acquired data in a secure manner, using encryption. Even though an entirely offline mode of operation should be allowed, if the data needs to be delivered quickly the mobile device should be capable of doing so as soon as a communication channel is detected and without intervention from the user, allowing a reasonably fast data upload process even in regions with intermittent connectivity.

4.3.2 Protection against device theft or loss

The mechanisms employed for temporary data storage should also provide protection against unauthorized access or modification. Ideally, this protection should remain active even if the mobile device in which the data is stored is stolen while the user's session is still active (i.e., the user is still "logged in" to the device) and the device volatile memory is accessed. In other words, the security solution should enable some level of forward secrecy, preventing attackers from using the information available on the device memory to access locally stored data not yet delivered. On the other hand, imposing forward secrecy may not be suitable for all situations, since it may be necessary to allow agents to recover the information from previously saved forms, e.g., because they were only partially filled or contained incorrect data. Therefore, the security framework should be flexible enough to support different forward secrecy configurations in accordance with the country regulations.

4.3.3 Secure data exchange between mobile device and server

In order to protect in-transit information, all data must be properly encrypted before transmission to/from the server. In addition, the security solution should provide the server with means to verify if the data received was actually generated by a legitimate user, thus preventing unauthorized entities from injecting (possibly fake) information into the system database.

Note that conventional mechanisms for establishing secure connections (e.g., TLS/SSL) may not be the best alternative for data delivery in such applications (MANCINI et al., 2011), especially in scenarios where the communication infrastructure is far from ubiquitous and the devices employed have low computational power. This happens because the data temporarily stored in the device already needs to be encrypted (as discussed in Section 4.3.2) and, thus, adding an extra security layer for protecting its delivery can be seen as an excessive overhead.

Aiming to create a solution that does not depend on secure communication tunnels for data delivery, our approach is to independently authenticate every piece of data that travels from and to the mobile device. Specifically, and as further discussed in Chapter 5, the protocol itself has no strict need for creating and authenticating a session before the data is delivered.

4.3.4 Lightweight and low cost solution

Low-budget projects, especially in developing countries, may impose restrictions on the computational capabilities of the mobile devices employed for collecting data, including limitations on processing power and available memory. Therefore, the security framework should rely as much as possible on lightweight cryptographic mechanisms such as those based on symmetric keys during its

operation - as opposed to more onerous public-key cryptosystems (e.g., RSA, TLS), yet an exception would be elliptic curve techniques. Moreover, the security mechanisms deployed should not depend on hardware capabilities not usually available in commercial mobile devices (e.g., the data should be protected even in the absence of a tamper-proof module), although it should be able to take advantage of such capabilities if they are available.

4.3.5 Device sharing among health agents

Budget limitations or practical reasons may lead to a scenario in which the mobile devices are shared by multiple agents. In order to cope with this constraint, the security solution should allow registered users to access the system from any device in which the data collection application is installed. In other words, users should be able to share devices in a straightforward and transparent manner while preventing privacy and access control issues that might arise from the fact that a same device may carry data from different health care workers.

4.3.6 Usability for computational literate users

In many deployments, the staff responsible for data collection may include people with little education background and/or little experience with computers (SHAO, 2012). Even though this can be overcome with intense training, frustrating experiences may become an extra barrier for the system's wide acceptance. This is one of the main reasons why many projects aiming to replace paper forms by electronic ones try to take into account the procedures these professionals are already used to follow, hopefully facilitating migration to the new system (CORREIA; KON; KON, 2008). Therefore, despite the need of strong security mechanisms when collecting data using digital forms, it is important to keep in mind that they must not impair the system usability. For example, although using some type of credential

(e.g., username and password) for user authentication is nearly unavoidable, users should not have to provide their credentials repeatedly or memorize multiple credentials. In addition, after the data acquired is consolidated, its delivery, encryption/decryption and authentication/verification should be automatically and transparently performed, without the need of manual intervention by the user.

4.3.7 Summary of requirement analysis

Aiming to facilitate references and comparison, Table 2 presents requirements discussed for mHDCS. The requirements are distributed in Groups (G) and identified with Requirement Numbers (RN). Also, one or more type(s) are associated to each requirement. The types include categories of: Security (S) for data privacy, confidentiality and networking; Usability (U) that considers users' profile to cope with personal factors and computer illiteracy; Lightweight (L), related to memory and computation consumption; and Functional (F) requirements that explicitly provide an application function to the end user.

Most of these requirements are in the Security or Usability types because its is the focus of the proposed framework. In other words, the framework provides mostly security features that are transparent to the health workers perspective, so that considered as non-functional requirements. The requirements 1-1, 4-2, and 4-3, for authentication and device sharing were although marked in Functional and Security types. That is because these items can extend the mHDCS functionalities while also can provide a desirable security feature.

4.4 Chapter Considerations

This chapter presents the requirement analysis of SecourHealth. The design of this security framework for mHDCS should observe the legislation/standard,

Table 2: Summary of SecourHealth requirement analysis

RN	Details and justification	S	U	L	F
G1 - Tolerance to delays and lack of connectivity					
1-1	Device should be able to authenticate in an offline manner	✔	✔		✔
1-2	Application should employ mechanisms for temporarily storing acquired data in a secure manner		✔		
1-3	Device should be capable of delivering the acquired data as soon as a communication channel is detected (without user's intervention)		✔		
1-4	Application should allow data upload process even in regions with intermittent connectivity		✔		
G2 - Protection against device theft or loss					
2-1	Mechanism for temporary data storage should provide protection against unauthorized access or modification	✔			
2-2	Mechanisms should protect stored data, even if the mobile device is stolen/lost, has a user's session active	✔			
2-3	Application should prevent attackers from using (key material) information available in the device memory	✔			
2-4	Application should reduce the amount of data exposure by the breakage of encryption keys (forward secrecy)	✔			
2-5	Data storage should allow the use of key with different levels of forward secrecy	✔	✔		
G3 - Secure data exchange between mobile devices and server					
3-1	Application should rely as much as possible on lightweight cryptographic mechanisms		✔	✔	
3-2	Data should be protected even in the absence of tamper-proof module	✔	✔		
G4 - Device sharing					
4-1	Device sharing should be allowed among multiple agents owing to budget and practical reasons		✔		✔
4-2	Mechanisms should allow registered users to access the system from any device with the mHDCS	✔	✔		
4-3	Users should be able to share devices in a straightforward and transparent manner		✔		✔
4-4	Device sharing should not impact proper data privacy and access control	✔			
G5 - Usability					
5-1	Staff and agents may include people with little education and experience with computers		✔		
5-2	Security mechanisms should not impair usability		✔		
5-3	User should not provide their credentials repeatedly	✔	✔		
5-4	User should not memorize multiple credentials	✔	✔		

data security, and networking issues. As reviewed in Section 4.2, the SDO's (e.g., HIPAA, ISO, CEN and HL7) are responsible for publishing standards on medical data management and medical terminology. Additionally, these SDOs had already created security work groups and released specific standards on medical data security to facilitate interoperability among HIS (mainly hospital's EHR). Such standards serve as an initial working basis, once they recommend the employment of security mechanisms such as AES for data encryption, VPN tunnels for site-to-site communication, and application communication enforced with TLS protocol (e.g., HTTPS). However, once these standards were not aimed to tackle mHealth issues, Section 4.3 stressed the prominent requirements for mHDCS.

The requirement analysis is grounded on the literature review of mHDCS, comprising projects developed around the globe (CONSULTING, 2009; SHAO, 2012) and in Brazil (IWAYA et al., 2013). The main requirements include: tolerance to delays and lack of connectivity; protection against theft and loss; secure data exchange; lightweight and low-cost mechanisms; device sharing; and usability. In that way, in Chapter 5 conceives the security framework for mHDCS, addressing the mechanisms presented in Chapter 3 to meet the requirements here discussed.

5 SECURITY FRAMEWORK FOR MHEALTH DATA COLLECTION

This chapter describes the SecourHealth framework and its basic building blocks employed to fulfill the requirements outlined in Section 4.3. Before we proceed, however, we believe that an explanation about the solution name should be given: the word *secours* from French means “succor”, “great help” or “rescue”, and slightly sounds like the English word *secure*. This name was chosen because the intention of SecourHealth is to provide a secure framework for mHDCS, bringing some help and relief to its developers and users.

The SecourHealth framework comprises a set of security mechanisms for mHDCS. It specifies the user authentication procedures (both online and offline), based on a symmetric protocol based on a PAKE. The key agreement protocol allows the framework to derive a set of keys with different purposes, and with different security levels and forward secrecy properties. Likewise, SecourHealth permits three different models of data exchange among client device and server. Lastly, the mechanisms for device authentication based on the GAA/GBA is proposed, that uses the Mobile Network Operator (MNO) to authenticate mobile phones. Figure 8 presents an overview of SecourHealth building blocks, further explained in the following.

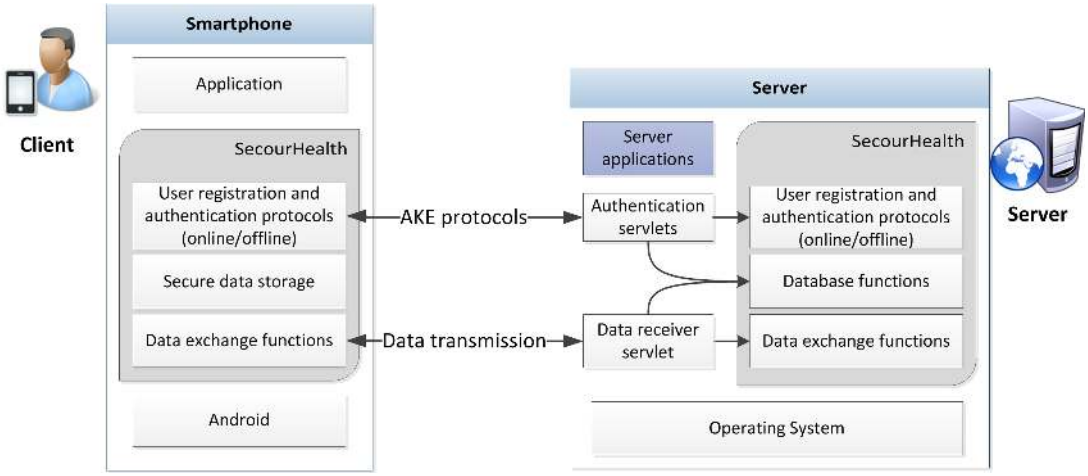


Figure 8: Overview of basic building blocks of SecourHealth.

5.1 Preliminaries and notation

Along the discussion, we assume that the user's credentials for accessing the system consist of a username (henceforth denoted usr) and a password (henceforth denoted pwd), provided to legitimate users at the system managers' discretion. Typically, usr is provided by the system, while pwd is chosen by the user and must have a minimum length, enforced upon the user's enrollment in the system. The SecourHealth framework does not impose any specific limitation on how this is done, however, as long as the server keeps a list o valid (usr, pwd) pairs.

The following notation is employed in the remainder of this document. We use $E_K(M)$ and $E_K^{-1}(M)$ for representing, respectively, encryption and decryption of message M under key K. Similarly, we denote by $AE_K(M)$ and $AE_K^{-1}(M)$ the authenticated-encryption and authenticated-decryption (i.e., the processes combining encryption/authentication and decryption/verification (BLACK, 2005)) of message M under key K. The authentication tag generated by a Message Authentication Code (MAC) for a message M under key K is denoted as $MAC_K(M)$.

We denote by $H(M)$ the application of a hash function on message M, and by $H^n(M)$ the iterative application of the hash function on M, n times (note that

$H^0(M) = M$). We also write $H_{[s]}(M)$ to denote the application of the hash function on M after it is prepended with an arbitrary bitstring s (i.e., $H_{[s]}(M) = H(s \,||\, M)$); hence, $H^n_{[s]}(M)$ indicates that s is prepended to the input of the hash function before each of its n applications.

We write $|a|$ for indicating the length, in bits, of string a and $a \,||\, b$ for the concatenation of strings a and b. Constant strings of characters are written between single quotes (e.g., '$string$'). Finally, $[s]_t$ denotes the truncation of bitstring s to t bits, which is done by taking the leftmost t bits of s.

5.2 User Registration

The registration process must be performed whenever a user accesses a mobile device for the first time. Since the device has no information for authenticating the new user, this process requires connectivity to the server, which will be responsible for this first authentication. The successful completion of the registration protocol generates the information required for future, offline authentications.

Without loss of generality, in the protocol description we assume that the server keeps the user's password pwd in its database. We notice, however, that since security good practices dictate that passwords should not be stored in plaintext, in real implementations pwd may actually refer to some information derived from the user's password (e.g., its hash) rather than the password itself.

The complete registration mechanism consists in the challenge-response protocol illustrated in Figure 9 and described as follows:

1. The mobile application generates a random $salt$ value, which is combined with the user-provided password by means of a key derivation function (KDF). The result is the master key $MK = KDF(salt \,||\, pwd)$. The password itself

can then be erased from the device memory, since the registration process does not depend on its value from this point on. There is no restriction on the exact KDF function adopted for this process. A common approach is to employ the Password-Based Key Derivation Function version 2 (PBKDF2) as defined in the PKCS#5 specification (KALISKI, 2000), or more recent solutions such as scrypt (PERCIVAL, 2009) or Lyra (ALMEIDA et al., 2014). The goal of such algorithms is to ensure higher security against brute-force attacks (also known as dictionary attacks) that explore the low entropy of human-memorisable passwords: the random $salt$ thwarts the application of pre-built tables of common passwords, i.e., the attacker is likely to be forced to create a new table from scratch for every different $salt$ value; in addition, the speed of the derivation process is configurable (e.g., in PBKDF2, by the repeated application of a hash function), so that it is possible to raise the computational cost of such attacks whereas the delay perceived by a human user can remain negligible (e.g., around 1 second).

2. The mobile application then establishes a secure connection with the server, authenticating that server and protecting the communication against eavesdropping from this point on. In order to do so, standard security mechanisms such as Secure Sockets Layer (TLS/SSL) or the Generic Bootstrapping Architecture (GBA) (3GPP, 2006; HOLTMANNS et al., 2008) can be employed. Under the protection of this tunnel, the mobile application sends the user identification usr together with the random $salt$ generated in step 1.

3. The server computes the master key MK using the user's password and creates a random $seed$ value. The value of $seed$ plays an important role in providing forward secrecy to locally stored data, as further discussed in Section 5.4, but during the registration it is used simply for creating a

challenge message.

4. The server issues a challenge to the mobile application: it encrypts the random $seed$ using the master key MK computed in the previous step, so that only a user who can compute the same MK is able to recover the correct $seed$.

5. The mobile application uses MK computed in step 1 for decrypting the value of $seed$. Then, it computes a shared key K_0 as $K_0 = H_{[seed]}(MK) = H(seed \,||\, MK)$. As further discussed in Section 5.4, this key will be used for providing (strong) forward secrecy to data locally stored in the mobile device. At this point, however, it is used simply for computing the response to the server's challenge as $MAC_{K_0}(\text{`}user\_ok\text{'} \,||\, usr \,||\, salt \,||\, seed)$, which corresponds to the authentication tag of all previously exchanged variables together with a constant string.

6. The response, which is the authentication tag is sent to the server.

7. The server computes the same K_0 as the mobile application and verifies if the response provided by the latter is valid, which implies that the mobile device was able to recover the value of $seed$ using the password input by the user. In case of success, the server stores $salt$, $seed$ and MK, which are associated with the corresponding user and identify him/her in the registered device. These are associated with the corresponding user and identify him/her in the registered device, the identification of which can also be stored for avoiding double registrations. The server also creates a positive assertion of the form $MAC_{K_0}(\text{`}serv\_ok\text{'} \,||\, usr \,||\, salt \,||\, seed)$.

8. The assertion generated in the previous step is sent to the mobile application.

9. The mobile application verifies the assertion received using K_0 and the value of the $seed$ computed in step 5. If the verification is successful,

this means that the user entered a legitimate password, which was not certain until this point. In this case, the application locally stores (1) the value of the $salt$ used during the protocol and (2) an authentication token $Auth = [MAC_{MK}(\text{`}auth\text{'})]_{tsize}$, which indicates that the user is registered in this mobile device and allows him/her to perform offline authentications afterward. Notice that the token is truncated to the system-defined parameter $tsize$, something that is further discussed in section 5.4.

Thereafter, the server can unregister any user simply by removing the entries for his/her username usr from its database.

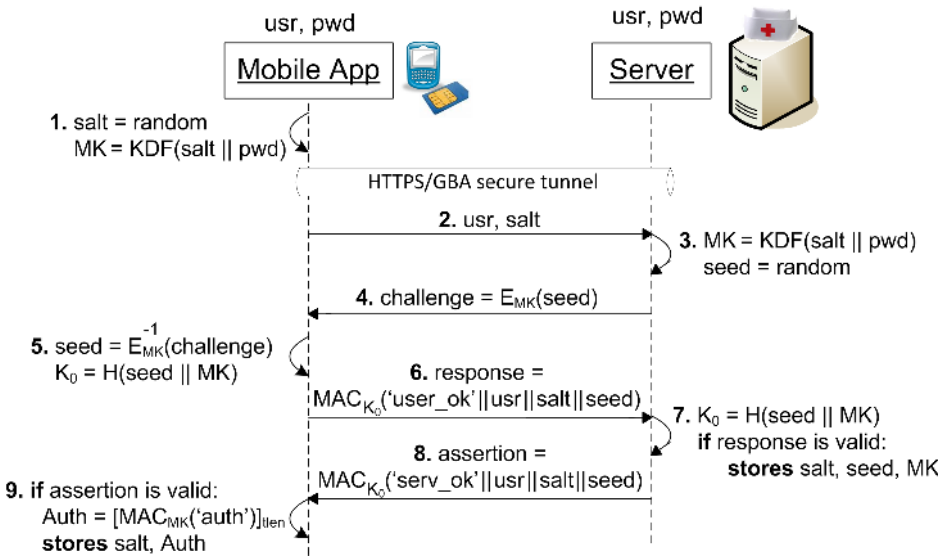


Figure 9: User registration process (online).

5.3 Offline User Authentication

Users can employ their credentials to access the system from any device in which they have previously registered, even in case of lack of connectivity. After usr and pwd are provided by the user, the application employs the locally stored $salt$ for computing the master key MK as described in Section 5.2, i.e., $MK = KDF(salt \,||\, pwd)$. This key is then used for generating a verification token

$verif = MAC_{MK}(\text{'}auth\text{'})$, which is compared with the authentication token $Auth$ locally stored. If $[verif]_{tsize}$ matches the value of $Auth$, the user is authenticated and can access the application. This process is illustrated in Figure 10.

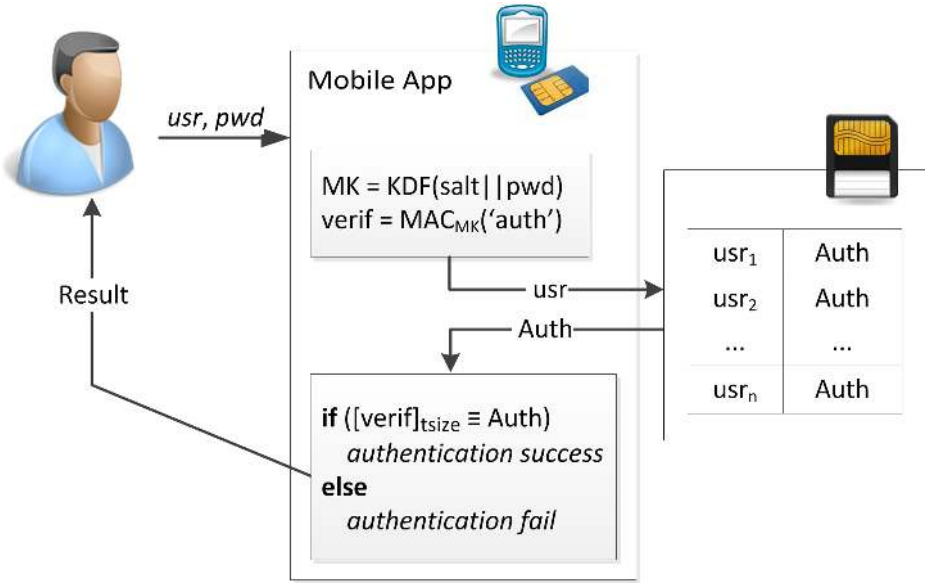


Figure 10: User authentication process (offline).

Note that a wrong password will be accepted in this offline verification process with probability 2^{-tlen}. Accepting the wrong password in this local authentication is not an issue from a security point of view, since the master key MK generated from such password will be invalid with overwhelming probability and, thus, will not be useful for creating or correctly decrypting any valid data afterward. The goal of this local authentication is, thus, simply to give legitimate users a guarantee that they are employing the correct keys while saving data, since otherwise that data will become unrecoverable. Therefore, $tlen$ should be large enough so that, in practice, a mistaken password never goes unnoticed by a legitimate user; on the other hand, a small $tlen$ gives less information for attackers trying to match a guessed password to the stored value of $Auth$, since the probability of filtering wrong guesses will be only 2^{-tlen}. If the users of the system employ alphanumeric passwords, which typically display approximately 40 bits of entropy on average (FLORENCIO; HERLEY, 2007), a reasonable approach is to adopt $tlen = 20$. This leads to a one in a million

chance of accepting the wrong password while still forcing a brute-force attack to test approximately 2^{20} unfiltered password guesses against something other than $Auth$. Since the security provided by this approach depends on how the master key MK generated from it is used in the system, we postpone the discussion on this password-guessing matter to Section 5.4.4

5.4 Secure Data Storage

After the authentication process is completed and the master key MK is computed from the user's password, SecourHealth generates keys that are used by an authenticated encryption algorithm $AE()$ for protecting each form saved. The system can generate three types of keys, as described as follows. After such keys are generated, the master key MK is immediately wiped out of the device memory.

5.4.1 No forward secrecy ($K_{\mathbf{nofs}}$)

The K_{nofs} key is computed directly from the master key MK as $K_{\text{nofs}} = H(0 \,||\, MK)$ and is kept unchanged in the device volatile memory until the application is closed[1]. This key should be used for protecting forms that need to be easily recoverable during a session and that require no forward secrecy: its continuous availability in memory allows a user to promptly decrypt K_{nofs}-protected forms without re-entering his/her password, but, for the same reason, this key is revealed to attackers who are able to access the device memory (e.g., by stealing the device while the application is still open). K_{nofs} should be useful, for example, in applications that allow users to save any number of partially filled forms and come back to them later during the same session. If forms protected with this key are delivered to the server, the latter can easily process them by computing the same $K_{\text{nofs}} = H(0 \,||\, MK)$ from the user's

[1] It is worth noting that the mechanisms suggested for key management and data encryption do not cope with scenarios when the application crashes due to Operating System failures. These failures would cause the loss of unsaved forms and encryption keys, requiring re-authentication.

master key. In addition, K_{nofs} is also employed for protecting data received from the server (see Section 5.5) and in the encryption of the K_{sfs} key (see Section 5.4.3).

5.4.2 Weak forward secrecy (K_{wfs})

The K_{wfs} key provides weak forward secrecy, in the sense that an attacker who accesses the device volatile memory while the application is still running is unable to decrypt any K_{wfs}-protected form, but it does not protect data against attackers who discover the user's password. This key is computed at the start of the user's session as $K_{\text{wfs}} = H_{[ses]}(MK) = H(ses \,||\, MK)$, where MK is the master key and $ses \neq 0$ is a session number renewed every session (i.e., whenever a user re-authenticates him/herself). Right after a form is encrypted and authenticated using K_{wfs}, this key is replaced by the result of hashing it with ses once again, i.e., the system makes $K_{\text{wfs}} = H_{[ses]}(K_{\text{wfs}}) = H(ses \,||\, MK)$. In other words, the i_w-th saved form will actually be protected using $K_{\text{wfs}}^{ses,i_w} = H_{[ses]}^{i_w}(MK)$, each form being paired with its corresponding value of ses and i_w in order to allow its subsequent decryption and authenticity verification. As a result, the device volatile memory never holds the key required for decrypting a form protected by K_{wfs}^{ses,i_w}, but only the next, still unused, $K_{\text{wfs}}^{ses,i_w+1}$ key. This type of key should be useful for protecting consolidated forms that might require modification later, but not too often: given the values of ses and i_w, the user can access the corresponding form simply by providing his/her password once again, which allows the system to compute K_{wfs}^{ses,i_w} from the resulting master key. The server follows an analogous process in order to recover the contents of forms protected in this manner.

5.4.3 Strong forward secrecy (K_{sfs})

The K_{sfs} key provides strong forward secrecy, meaning that attackers are unable to decrypt any K_{sfs}-protected form even if they discover the corresponding

password or access the device volatile memory while the application is still open. The reason is that this key is computed as $K_{\text{sfs}} = K_0 = H(seed \,||\, MK)$ right after the completion of the registration process and, analogous to K_{wfs}, replaced by its hash value after being used to protect a form; in other words, the i_s-th saved form is encrypted using $K_{\text{sfs}}^{i_s} = H^{i_s}(seed \,||\, MK)$. Since the mobile device does not store the random $seed$, its value cannot be recovered using locally stored information, even if the password is known. This property also leads to the need of storing the next available K_{sfs} in the device non-volatile memory after usage since, unlike K_{wfs}, this key cannot be recomputed otherwise. In SecourHealth, after the i_s-th form is encrypted, $K_{\text{sfs}}^{i_s+1}$ is first encrypted with K_{nofs} and then stored, which allows users to recover their next, still unused value of K_{sfs} while preventing any other user sharing the device from doing the same. The improved security provided by K_{sfs} is counterbalanced by the user's inability to modify the data after it is saved with this key, since the only entity that is able to decrypt and to verify forms protected in this manner is the server itself. In order to do so, the server needs to be provided with (1) the value of the $salt$ used for the corresponding user's registration, which identifies the value of $seed$ and allows the computation of K_0, and (2) the value of i_s corresponding to each form, which determines how many times K_0 must be hashed for obtaining the correct $K_{\text{sfs}}^{i_s}$.

It is important to notice that attackers who discover the user's password can violate the forward secrecy property of K_{sfs} if they are able to recover the server's $challenge$ (see step 4 of the registration protocol), whose decryption with the corresponding master key recovers the value of $seed$. Considering that this message is protected by a secure tunnel, however, doing so requires the attacker to break the tunnel underlying protocol, which should be infeasible against technologies such as TLS, or compromise the server itself (who knows the value of $seed$), in which case the data would not be secure anyway. Nonetheless, if the

attacker is somehow able to trick the user into creating a tunnel with him/herself rather than with the legitimate server, a man-in-middle attack can be perpetrated and the security of the protocol is lost. Namely, the attacker can relay all messages between the user and the server, and then perform an offline dictionary attack on the keys established between them: the attacker can compute a candidate MK' from $salt$ and a guessed pwd, compute $seed'$ and K'_0 from $challenge$ and MK' and then verify the guess by matching the user-provided $response$ with $response' = MAC_{K'_0}(\text{`}user\_ok\text{'} \,||\, usr \,||\, salt \,||\, seed')$. Avoiding such issue in the web may be a difficult challenge, since many users tend to ignore warnings about certificate errors when accessing websites (SUNSHINE et al., 2009; ENGLER et al., 2009) and may end-up connecting to a fake server. Nevertheless, such a threat should be more easily avoidable in the (presumably more controlled) scenario of data collection solutions, in which the application itself can utterly prevent users from making unsafe connections.

5.4.4 Key generation and usage – summary

A good password-based scheme should prevent attackers from easily performing offline dictionary attacks, which are much harder to detect than online attacks. This is the main motivation of proposals that employ different passwords for different purposes, such as authentication toward the server and toward the devices (e.g., as proposed in (MANCINI et al., 2011)): in such cases, it is easier to force the attacker to contact the server when trying to verify the password shared only with this entity. This approach, however, impairs the system usability, and may even create a false sense of security since users may feel compelled to choose similar (if not identical) passwords for different uses.

The approach adopted in SecourHealth requires a single password while still providing protection against offline attacks, at least if the strong forward secrecy

approach is adopted. Specifically, in order to determine if a guessed password is correct, the attacker would have to (1) run the registration protocol described in Section 5.2 and verify if a positive assertion is received, or (2) check if the resulting MK can be used to verify the authentication tag of some locally stored, legitimate data. This first case is analogous to an online dictionary attack and can be easily detected by the server, which can act accordingly. For example, the server could notify the user and limit the rate of registration attempts with the corresponding usr for an arbitrarily large period of time, possibly also holding as suspicious the data provided by that user until further analysis. The second case can be performed offline, but only if there is some locally stored form not protected by the *strong* forward secrecy mechanism described in section 5.4.3. In other words, since the (guessed) master key alone cannot be used to compute any previous K_{sfs}, forms protected with this key are useless in offline attacks. In comparison, the weak forward secrecy mechanism provides a trade-off between security and usability, since it allows a legitimate user to recover a form from the device memory (e.g., in case it was wrongly filled) but provides less protection against dictionary attacks. Table 3 summarizes this discussion, showing the security and capability properties of each key type provided by SecourHealth.

Figure 11 shows the data structures employed by SecourHealth, i.e., the keys that remain in RAM and the data structures stored in the non-volatile (e.g., flash) memory device. The data flow of the key generation process is summarized in Figure 12, showing which actions take place after a successful registration and after the completion of the offline authentication. Obviously, depending on the application specific requirements, only a subset of the discussed keys needs to be actually created and used. For instance, in a scenario in which consolidated forms are not expected to be modified, but rather replaced by new ones, K_{sfs} might be used for protecting all forms to be delivered to the server; meanwhile, K_{nofs} could be

Table 3: Properties of the different keys provided by SecourHealth

Property		K_{nofs}	K_{wfs}	K_{sfs}
Security	Data secrecy if attackers access volatile memory, but do not discover password	No	Yes	Yes
	Data secrecy if attackers access volatile memory and discover password	No	No	Yes
	Prevents offline dictionary attacks if local data is not stolen	Yes	Yes	Yes
	Prevents offline dictionary attacks even if local data is stolen	No	No	Yes
	Prevents online dictionary attacks	No	No	No
Capability	Knowledge of password (by attacker or legitimate user) allows recovery of stored data	Yes	Yes	No
	Allows data to be recovered without requiring user to input password	Yes	No	No
	Protected data can be sent to server at any time, without user intervention	Yes	Yes	Yes

used only for auxiliary processes (e.g., encrypting K_{sfs}) and for encrypting partially filled forms, but not for their authentication, since they will never leave the mobile device. In this setting, offline dictionary attacks would become much harder to succeed due to the lack of locally available information for filtering wrong guesses. On the other extreme, when modifications to consolidated forms are frequent, it might be necessary to employ K_{nofs} in the protection of all forms for the sake of usability.

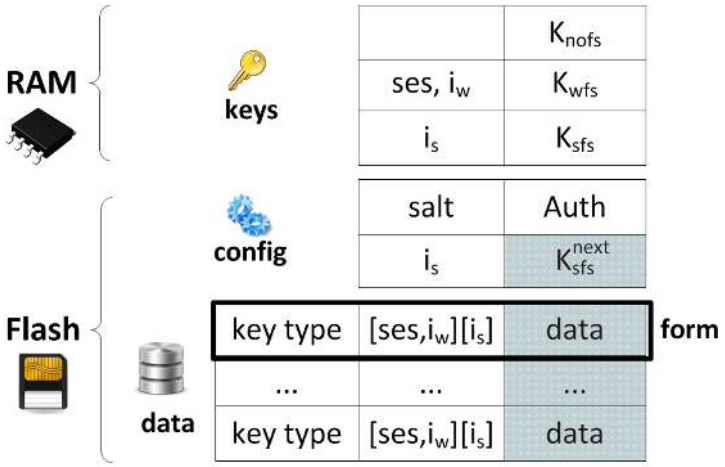


Figure 11: Memory organization in SecourHealth. Shaded fields indicate that the data is encrypted.

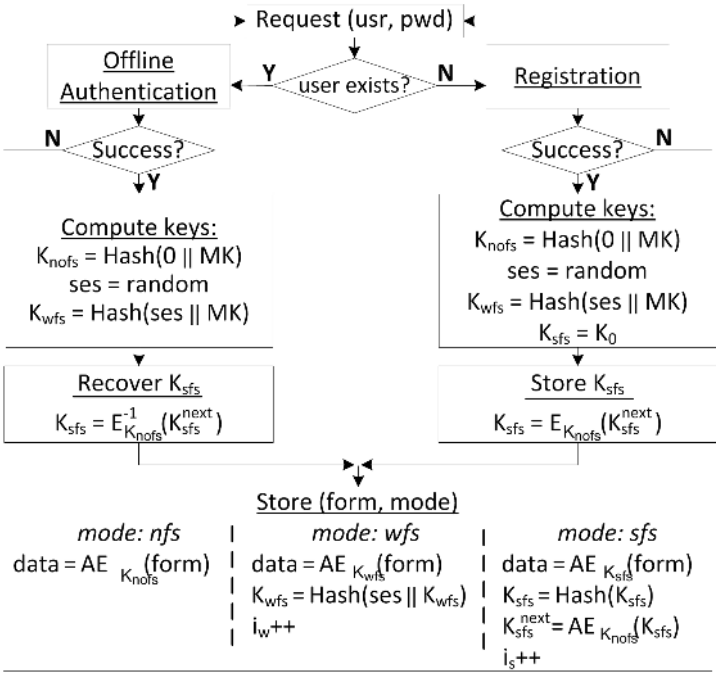


Figure 12: Generation and usage of the different keys in SecourHealth.

5.5 Data exchange with server

Figure 13 depicts the processes employed when the mobile device communicates with the server for sending or retrieving data. As discussed in Section 5.4, forms that are ready to be handed over to the server are authenticated when placed in the mobile device local memory. Therefore, they can be delivered as soon as a communication channel is detected, without requiring the user's intervention. The server will then be able to compute the required keys for decrypting and verifying the authenticity of the data received. This is done using information defined upon the user's registration (e.g., the master password), which can be appended to the forms (e.g., the value of i_s when K_{sfs} is employed). After a form is received and verified, the server must send a confirmation to the mobile device, which may then remove the corresponding data from its local memory. If this data delivery process is not performed inside a secure tunnel, the confirmation must be authenticated in order to prevent an attacker from sending a fake upload

report to the mobile device; it should also contain a timestamp ts in order to identify the request and to avoid replay attacks. As illustrated in Figure 13, in SecourHealth the upload report is protected using K_{nofs}, which allows the device to transparently verify its authenticity.

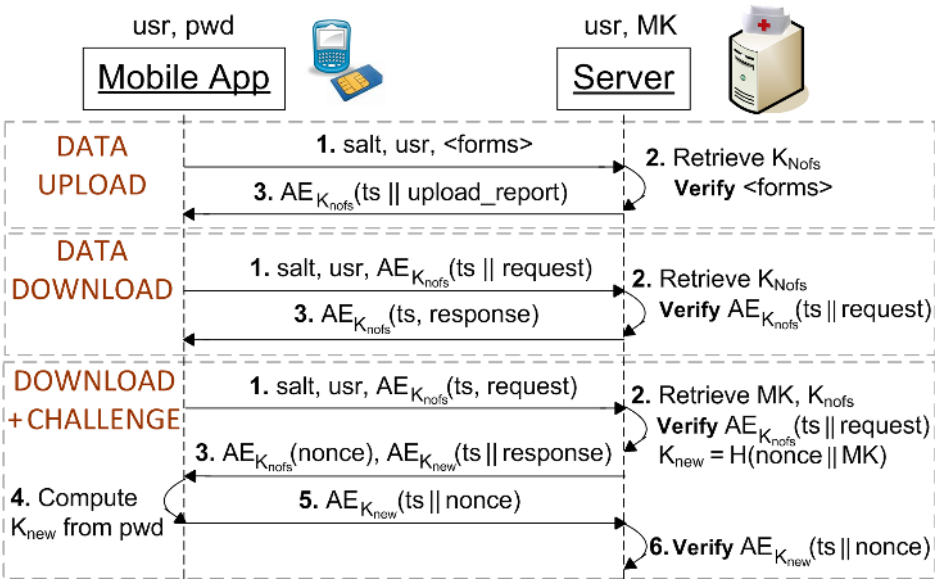


Figure 13: Data exchange between mobile device and server (upload and download). All requests to the server involve a timestamp ts that identifies the request and prevents replay attacks.

Some applications also involve the reception of data from the server, such as when existing information about a family needs to be updated. In such cases, the user must send an authenticated request to the server, which will answer according to the corresponding user's access rights. The basic protocol for doing so is similar to the one employed for data delivery: both the request and the response are accompanied by a timestamp ts and both are protected by K_{nofs}. Once again, this approach provides improved usability, since users do not need to re-enter their passwords for each request. This also allows attackers who gain access to the device while a session is still active, to inconspicuously download data from the server posing as the legitimate user. This can be avoided if, after verifying the authenticity of a request, the server issues a challenge together with

the requested data: instead of using K_{nofs}, the server derives the key K_{new} from a random *nonce* and the master key MK, which obliges the user to input his/her password in order to decrypt the data and to respond to the challenge. If the response provided is correct, the server may fall back to the simpler process in which no challenge is issued; on the other hand, if the server detects that a large number of challenges are incorrectly answered (or, simply remain unanswered), it might, for example: emit an alert to the user or manager; limit the request rate for that account; or, in an extreme case, cancel the user's registration to that device, forcing a new run of the registration protocol. The frequency in which the server should issue challenges rather than directly answering to the user's requests should be configured according to the desired security-usability trade-off of the target application. In fact, this optional mechanism might even be made unnecessary if the application itself has some type of "lock-down" mechanism that prevents it from remaining open for too long.

5.6 Improving Authentication with GAA/GBA

GAA (Generic Authentication Architecture) and GBA (Generic Bootstrapping Architecture) technologies can be used in this scenario as a complementary tool, reinforcing security in the mechanisms described. Nonetheless, since the deployment of GBA depends on hardware capabilities not necessarily available on all deployment scenarios, we describe the GBA-based solution in this separate section rather than integrated with the password-based approach described in Section 3. Specifically, we discuss how GBA can be used in the authentication of registered devices toward the service administrator (usually the hospital, which acts as the Network Application function (NAF) in the GAA/GBA architecture) and/or to strengthen the solution key management processes. We emphasize that those usages are independent from each other, and can, thus, be applied either

jointly or separately. In addition to the mechanisms described, GAA/GBA offers at least one interesting feature: the SIM card itself may be used to store and to run security-sensitive code (e.g., keys, encryption algorithms, etc.), creating a safer environment where this code is isolated from (malicious) software running on the client device. Moreover, GAA/GBA create new business opportunities for Mobile Network Operators (MNOs), which on the one hand can be an interesting source of revenue for MNOs and on the other hand can motivate the further adoption of such systems (assuming the MNO will be willing to promote its wide usage).

5.6.1 Device Authentication

The protocol described in Section 5.2 (Figure 9) provides both server authentication (by means of an HTTPS connection with server-side certificates) and user authentication (by means of a challenge response mechanism built upon the user registered password). However, it does not provide any type of device authentication, meaning that (1) legitimate users can perform the protocol from any (possibly misconfigured) equipment, and (2) attackers can use any device to establish a connection with the server and try to deliver (likely rubbish) data.

In a scenario in which GAA/GBA SIM cards are available, this technology can be used to address both issues. More precisely, security-sensitive code can be kept inside the SIM card as aforementioned, thus reducing the system exposure to malicious software. In addition, GAA/GBA can be used to authenticate the client's device as soon as a connection with the server is established, limiting the action of attackers. The latter process may be employed prior to content delivery (described in Section 5.4), and would then consist in the following steps:

1. The Client perceives the presence of a 3G connection and connects with the Server via an HTTPS channel, thus allowing the client to authenticate the Server.

2. The Client runs the GAA/GBA protocol for establishing a common key Ks_NAF with the Server.

3. Client and Server run a challenge-response protocol in order to confirm that both have the same Ks_NAF , thus authenticating the client inside the established HTTPS channel.

4. If the authentication is successful, the Client sends authenticated data as described in Section 5.4; otherwise, the Server terminates the connection.

In this manner, GAA/GBA provides the following advantages when compared to the basic scenario in which this device authentication process is absent:

- Stronger security: data delivery process involves double authentication (user via password and device via GAA/GBA).

- Device filtering: only registered devices are able to send data toward the server. As a result, attackers trying to exhaust the server resources by sending a large amount of rubbish data toward it will have to previously perform a successful GAA/GBA authentication. Otherwise, the server will close the HTTPS session and discard the data provided without further consideration. In the basic scenario the server would likely verify that at least a few messages are unauthentic before concluding that the device owner is actually a malicious entity. Therefore, GAA/GBA improves the server availability and resilience against some types of denial-of-service attacks.

- Data confidentiality towards network operator: the Mobile Network Provider does not gain access to the data transmitted since it is protected by information shared between user and server, i.e., the user password. Therefore, this process is very unlikely to violate any of the (usually strict) laws concerning access to medical data.

- Transparency: the whole process is completely transparent to the users, there being no perceptible difference between the GAA/GBA-empowered and the basic cases from the users' point of view.

We note that the only reason for employing HTTPS for server-side authentication and data encryption is to provide compatibility with the protocols previously described. Nonetheless, if compatibility is not required, GAA/GBA usage procedure can also be employed to provide both services (see Figure 25 in Appendix A for further details), without the need of HTTPS or certificates.

5.7 Framework Considerations

SecourHealth is designed as a flexible solution for securing mHDCS, including lightweight security mechanisms that are useful in different application scenarios. In summary, the proposed framework addresses the requirements described in section 4.3 as follows:

- Tolerance to delays and lack of connectivity: SecourHealth allows users to authenticate themselves in any device in which they have previously registered and then operate in a completely offline mode if required. Even though the registration itself requires connectivity, it must be performed only once per device, and this could be done before the users go to the field. After the data is collected, the forms are protected using one of the keys described in section 5.4, and can be delivered to the server as soon as a communication channel becomes available without the need of a direct intervention from the user.

- Protection against device theft or loss: SecourHealth supports data protection mechanisms with distinct security characteristics, allowing each

application to adopt the required level of security against the capture of devices by attackers. The password itself is never left in memory, but used to derive different keys: K_{nofs}, K_{wfs}, and K_{sfs}. Specifically, if only K_{sfs} is employed for protecting locally stored forms, attackers are unable to use them in offline dictionary attacks or to recover their contents after somehow discovering the password; K_{wfs} and K_{nofs} are less secure in principle, but lead to better usability as they allow users to decrypt and to modify stored forms if necessary. Finally, as discussed in section 5.5, SecourHealth includes mechanisms that limit the attackers' ability to retrieve information from the server even after stealing a device in which a legitimate user's session is still active.

- Secure data exchange between mobile device and server: All data exchanged between server and mobile device is encrypted and authenticated, even in the absence of an underlying secure connection.

- Lightweight and low-cost solution: SecourHealth does not require any specific hardware and relies basically on lightweight cryptographic mechanisms, its (potentially) most expensive operation being establishing a secure tunnel during registration. Moreover, the protocols employed were designed to minimize the number of messages exchanged between server and mobile device: the most common operations (uploading/downloading data to/from the server) involve only one message from each side of the communication, while all other operations (registration and challenge issuing) involve at most two messages from each side.

- Device sharing: The proposed mechanism allows legitimate users to register from any SecourHealth-enabled device while preventing users from accessing each other's data in shared devices.

- Usability: SecourHealth allows users to access the system with a single credential. Moreover, it supports many configurable security-usability trade-offs. For example, the system can be configured to request the user's credential only once per session or, if desired, once again whenever a more sensitive operations is performed (e.g., accessing a locally stored form or downloading data from the server). Finally, data can be exchanged with the server without the user's direct intervention, allowing data to be quickly delivered whenever a communication channel is detected.

5.8 Related Work

There are many frameworks in the literature for enabling generic data collection using mobile devices (for a survey, see (SHAO, 2012)), and that can also be used by health applications. Despite their interest from a standardization point of view, the design of such solutions usually provide only basic security features, if any. For example, standards such as Open Data Kit (ODK) (ANOKWA et al., 2009) and openXdata[2] provide support to HTTPS and session authentication by means of username and password, while more advanced features such as secure storage and forward secrecy are not mentioned in their specifications. This reduced concern with security is somewhat understandable, since their focus is the data standards and the practical features rather than how to protect the collected data. However, in scenarios that handle highly security-sensitive data such as medical information, an additional security layer becomes essential. Nonetheless, it is an unfortunate fact that strong security mechanism do not appear as one of the main concerns in many mHDCS, such as GeoHealth (Sá et al., 2012), Epihandy (BAGYENDA et al., 2009), Borboleta (CORREIA; KON; KON, 2008), and Mobile Health Data Kit (MHDK) (SHAO, 2012), to cite a few recent works. Actually, in our literature

[2]openXdata: http://www.openxdata.org/

review of mobile data collection applications (both in the field of mobile health and more general scenarios), we were unable to find any solution displaying the flexible combination of forward secrecy levels provided by SecourHealth.

Despite not being a majority, some interesting proposals for providing user/device authentication and data confidentiality in the context of mHeatlh applications do exist. Many of them focus on adding robust security mechanisms to Electronic Patient Record (EPR) systems, considering scenarios in which data is exchanged inside a hospital or between health facilities. Examples include (HUP-PERICH et al., 2012), which focus on allowing patients to asynchronously authorize a health professional to access their (encrypted) EPR data, and (SHANMUGAM et al., 2006), which discusses how users could access their medical records from their homes using the Generic Bootstrapping Architecture (GBA). There are also proposals for securely transferring medical information from/to the point of care (MIRKOVIC; BRYHNI; RULAND, 2011), applying (offline) access control policies to the patients' data (AKINYELE et al., 2011), and establishing authentication models suitable for health applications (SAX; KOHANE; MANDL, 2005). Even though such solutions share some features with the proposed SecourHealth framework, they usually focus on EPR security issues such as access control policies and securing in-transit data, not coping with many of the specific security requirements of data collection systems (e.g., secure storage in scenarios with lack of connectivity).

Mechanisms for secure storage and end-to-end encryption appear in mHDCS such as PopData (HERTZMAN; MEAGHER; MCGRAIL, 2012). However, one of the few thorough solutions in the literature that focus specifically on securing the whole mHDCS process is the protocol proposed in (MANCINI et al., 2011), which, together with the secure storage mechanism described in (GEJIBO et al., 2012), forms an extension of the openXdata standard. The combined solution includes essential security features such as mutual authentication between user and server,

encryption of stored data, and secure data delivery. Important requirements such as allowing devices to be shared and offline authentication of users are fully taken into account. Nevertheless, forward secrecy is not among the mechanisms provided, allowing attackers with physical access to the device to also access the stored data.

Moreover, the protocol specification from (MANCINI et al., 2011) includes some apparently unnecessary operations. Namely, its registration process requires user and server to share not only a username and password, but also a secret key $Secret$. This secret key is not directly used for data encryption or mutual authentication, as could be expected, but rather employed for validating the server public key upon the registration of the user in a new device. The public key is then used for encrypting a new symmetric key every time some data needs to be downloaded from the server or uploaded to it. This profusion of keys not only makes the protocol more complicated, but also defeats one of the main purposes of asymmetric encryption: allowing two entities to communicate securely without the need of any pre-shared information. The use using public key encryption in this case, besides making the protocol more computationally expensive, prevents attackers from tricking the device into communication with the wrong server. However, challenge-responses involving $Secret$ rather than the public key would have the same effect at lower cost: if $Secret$ is unknown by the attacker, he/she will be equally unable to answer challenges based on public or secret keys; otherwise, if $Secret$ is known, the attacker can use it to validate his/her own public key rather than that of the server and answer both types of challenges. This computational cost should be especially noticed if, as proposed by the authors, the RSA algorithm is used with 128- and 256-bit security levels: in this case, RSA would take respectively 3072- and 15360-bit keys, which may be overkilling in resource constrained devices.

SecourHealth (presented in Chapter 5) not only adds forward secrecy to stored data, but also avoids the above issues altogether by almost removing the need for asymmetric cryptography, using shared-key challenges for authentication whenever necessary. It also can leverage on mechanisms for establishing secure channels already employed in some applications, which could remove any need for especial-purpose public-key encryption protocols. Examples include the Generic Bootstrapping Architecture (GBA) (3GPP, 2006; HOLTMANNS et al., 2008), a very lightweight authentication mechanism for mobile networks, and HTTPS, which is more costly but remains widely supported and adopted by mHealth solutions, including GeoHealth (Sá et al., 2012) and solutions based on the OpenRosa specification[3].

5.9 Chapter Considerations

In this chapter we presented the SecourHealth framework, a security solution that complies with the security requirements presented in Section 4.3. As such, it prevents the disclosure of patient's data to unauthorized parties and also injection of fake information into the data collection system. In this context, the security framework proposed ensures a high level of data confidentiality even in the case of device theft, allows user and data authentication towards the server, and enables swift delivery of (authenticated) data whenever a 3G connection becomes available. At the same time, the architecture proposed is very efficient, making use of lightweight and standardized security primitives in its construction. Finally, it allows integration with the GAA/GBA framework, which further improves security in a highly transparent manner while providing new business opportunities for network operators through authentication as a service mechanism.

The work proposed by (MANCINI et al., 2011) devises a worthy and interesting

[3]http://www.openrosa.org/

security framework. Also, to the best of our knowledge, they were one of only that properly addressed the requirements for a mHDCS, considering the LMIC scenario. However, their proposal did not foresee all the requirements presented in Section 4.3. SecourHealth offers stronger mechanisms of authentication with forward secrecy, data storage and delay-tolerant data transmission in the application layer. The solution also allows an entirely offline operation mode, after just one successful online user registration.

6 SECOURHEALTH IMPLEMENTATION AND TESTS

In order to assess the behavior of the SecourHealth framework in a real environment, we integrated the mechanisms proposed into the GeoHealth (Sá et al., 2012), which runs over an Android platform. This application was developed by InCor as a partial cooperation with Medicine Faculty of the University of Sao Paulo (FMUSP), within the West Region Project. Currently, its being used in the city of São Paulo as part of a governmental initiative for health data collection called Family Health Strategy (FHS). The FHS involves teams of data collection agents responsible for assisting families in a well-defined geographical area, surveying several primary care conditions and promoting actions such as prevention, recovery, and rehabilitation. These health agents deploys smartphones for this data collection and partially filled forms are stored in the device local memory (i.e., SD Card) so that they can be filled later by the agents. After consolidation, such forms are put in a first-in-first-out queue and sent as soon as possible to the server. All the data collected is geo-referenced, providing health managers with a clear view of the population's conditions in the regions surveyed.

6.1 GeoHealth and SecourHealth Integration

The original GeoHealth architecture uses passwords for protecting the access to the application. More precisely, before accessing the application, the user needs to send a password to the server to be validated and, in case of success, the

password is stored in the mobile device memory. HTTPS is used for securing all communications with the server, including the password registration and data delivery. Under the protection of such tunnel, the data itself is not otherwise encrypted or authenticated. Even though this approach does not incur in any serious security issue for in-transit data, it leads to some undesirable overhead due to the repeated establishment of TLS/SSL sessions, and it requires the password to remain in memory all the time. Moreover, no security mechanism is employed for protecting the information kept in the mobile device memory while no communication channel is available.

The SecourHealth-empowered GeoHealth system overcomes these issues in the following manner.

- User registration: Even though the registration of a new user still employs HTTPS, the password is not sent in clear through this tunnel but becomes part of the challenge-response protocol described in section 5.2. When compared to the "plain" GeoHealth version, this process adds some extra overhead (the protocol described in Section 5.2) before users are able to use a new device. Nevertheless, since this needs to be done only once and the whole process is very similar to the regular password registration, the burden introduced is not significant in practice (consists in a challenge-response instead of a HTTPS request, and the creation of a configuration file with the $Auth$ tag for offline authentication).

- Secure storage: Partially filled forms are encrypted (but not authenticated) using K_{nofs}, because they need to be repeatedly accessed by the agents and are not delivered until consolidated. Consolidated forms are not expected to be changed since they are likely to be sent to the server automatically soon after being saved. Therefore, the system uses K_{sfs} for encrypting and authenticating them. K_{wfs} is not used in the system and, thus, it is not

generated.

- Data exchange: Data exchange with the server is performed without the prior establishment of an HTTPS channel, accelerating the delivery of consolidated forms. Downloading data from the server normally does not involve challenges issued by the server. The reason is that the policy adopted in GeoHealth when users request some data is already quite strict: the server has a list of families to be visited by each agent and usually prevents access to information not belonging to such families. Challenge issuing is thus limited to when an agent requests information about the number of families well above the average in the same day or in exceptional cases (e.g., unplanned emergency visits to families not assigned to the requesting agent). Namely, for the current average of six families visited per agent per day, a challenge would be issued when the agent requests information about the 10-th family in less than 24 hours.

6.1.1 Platform characteristics

The platform used in the resulting integrated system is the Motorola Milestone 2, a reasonably high-end mobile device equipped with a 1 GHz processor, 8 GiB internal flash memory, 512 MiB of RAM, 3G connection and a 5MP camera[1]. The implementation was done in Java using the Android Software Development Kit (SDK), which provides a set of API libraries to build and to test applications for the Android Gingerbread (version 2.3 API level 9). The cryptographic algorithms employed were all taken from Spongy Castle[2], an Android repack of the Bouncy Castle Java cryptography API[3]. Lastly, communications with the server are performed using a 3G connection with a nominal speed of 300 kilobits per second

[1] Motorola Milestone 2 details: http://pdadb.net/index.php?m=specs&id=2570&view=1&c=motorola_milestone_2_a953

[2] Spongy Castle: http://rtyley.github.io/spongycastle/

[3] Bouncy Castle: http://www.bouncycastle.org/java.html

(kbps).

6.1.2 Mobile configuration

SecourHealth was adapted and integrated within the GeoHealth application, but there are some vulnerabilities related to the platform/application settings that are out of the scope. For instance, the execution of malicious application inside the mobile (e.g., key loggers, or malware) cannot be tackled. Therefore, we assume that the mobiles should be preconfigured by the mHDCS administrators, and only the necessary applications should be installed. Unnecessary applications can be removed or blocked to avoid misuse of resources. The HCA should be not allowed to download and install applications in the mobile. Also, there are already locking applications that can help administrators to precofigure the mobile in Android Kiosk Mode, which blocks all applications excepting the ones that the user would need. In summary, we presuppose that the mobiles are well configured before utilization.

6.1.3 Cryptographic algorithms and APIs

The cryptographic algorithms used in the implementation are the following. We adopt PBKDF2 (KALISKI, 2000) as a key-derivation function for computing the master key from the password, using adequate parameters so that the total derivation time remains around 1 second. The underlying hash algorithm for PBKDF2 and other processes is SHA-256 (NIST, 2012). Message authentication is performed using HMAC-SHA256 (NIST, 2002), while authenticated encryption is performed with EAX (BELLARE; ROGAWAY; WAGNER, 2004). The underlying block cipher for all algorithms is the Advanced Encryption Standard (AES), observing the NIST recommendations (NIST, 2001).

This body of algorithms is essential for SecourHealth and can be implemented

using the: Javax.Crypto[4] and Bouncy Castle cryptographic APIs. However, a developer may adopt equally strong implementations (e.g., using other cryptographic APIs) as necessary, and adapt (if needed) the software models hereafter described (e.g., other programming language or paradigm).

6.1.4 Software Models for Authentication and Storage

The SecourHealth software package implemented in Java can be specified by means of software models using the object-oriented programming paradigm. The class diagram in Figure 14 defines other packages that make up the framework (i.e., *java.io*, *java.util*, *javax.Crypto* and Bouncy (Spongy) Castle Crypto API). Also, it defines three classes, which SecourHealth is built on, namely: *KeyManager*, *SecurityFunctions* and *SenderServicePool*.

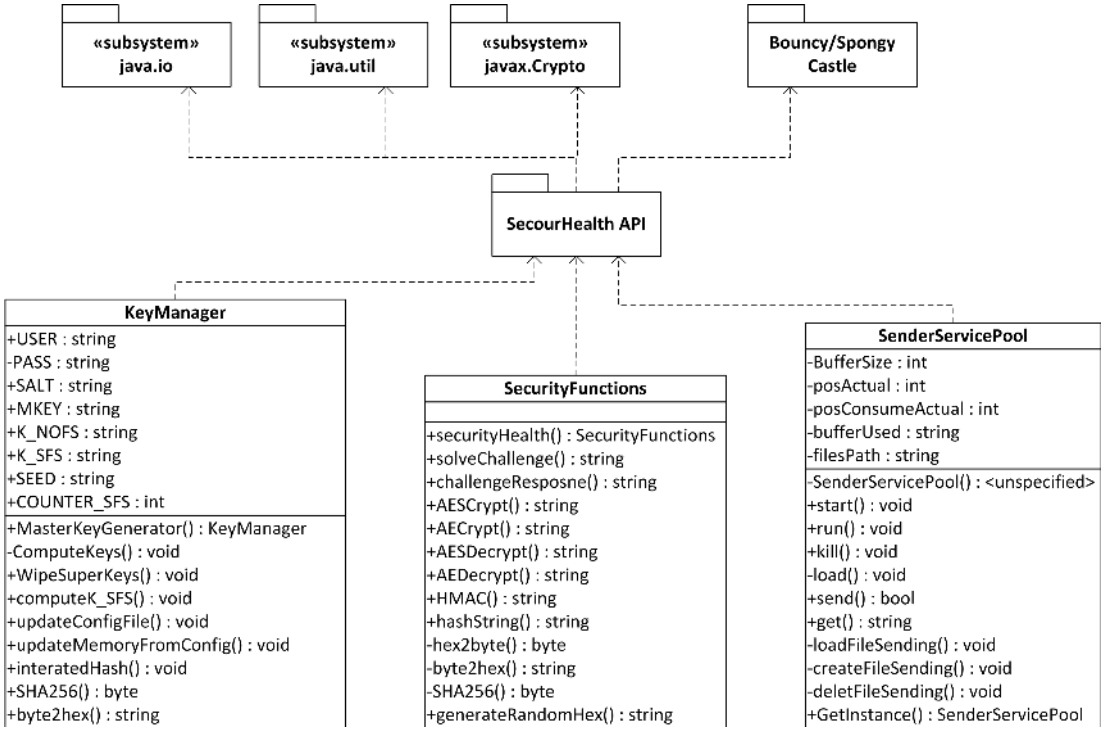


Figure 14: SecourHealth class diagram for a mobile application.

The *KeyManager* is responsible for computing the symmetric KDF algorithms.

[4]Javax Crypto (Android): http://docs.eoeandroid.com/reference/javax/crypto/spec/package-summary.html

This class implements the PBKDFv2 to generate MK and computes other system keys (i.e., K_{nofs}, K_{wfs}, and K_{sfs}). KeyManager also provides functions for SHA-256 hash standard and manages the keys allocated in memory and at the configuration files. The *SecurityFunctions* package implements security mechanisms such as authentication (HMAC), encryption (i.e., AES/CBC/PKCS5Padding), authenticated encryption (i.e., AES/EAX/NoPadding), and other utility functions. The *SenderServicePool* handles the circular buffer used to store consolidated forms ready for sending. It is a singleton class instantiated after the user's login, running as a parallel application thread that checks network connectivity in order to send the forms to the server.

Aiming to further describe the class relationships, the sequence diagrams in Figures 15 and 16 show the authentication and form submission procedures. These diagrams were used to specify the sequence of instructions that should be executed on the mobile-side. On the server-side, we work with servlets[5] (e.g., **save**.geohealth.br and **login**.geohealth.br). The servlet has to act as an *AppController*, calling all the SecourHealth functions using the same approach. Besides, on the server-side, the *SenderServicePool* can be suppressed.

6.1.5 Pilot application

Figure 17 shows some screen shots of the client application authentication process, which is the same for both registration (i.e., first-time usage) and any posterior offline authentications. If this process is successful, the user does not need to re-enter his/her password until the application is closed, unless the server issues a challenge as previously discussed.

After the data is collected, the corresponding forms are all stored in the mobile

[5]Servlet is a small, server-resident program that typically runs automatically in response to user input.

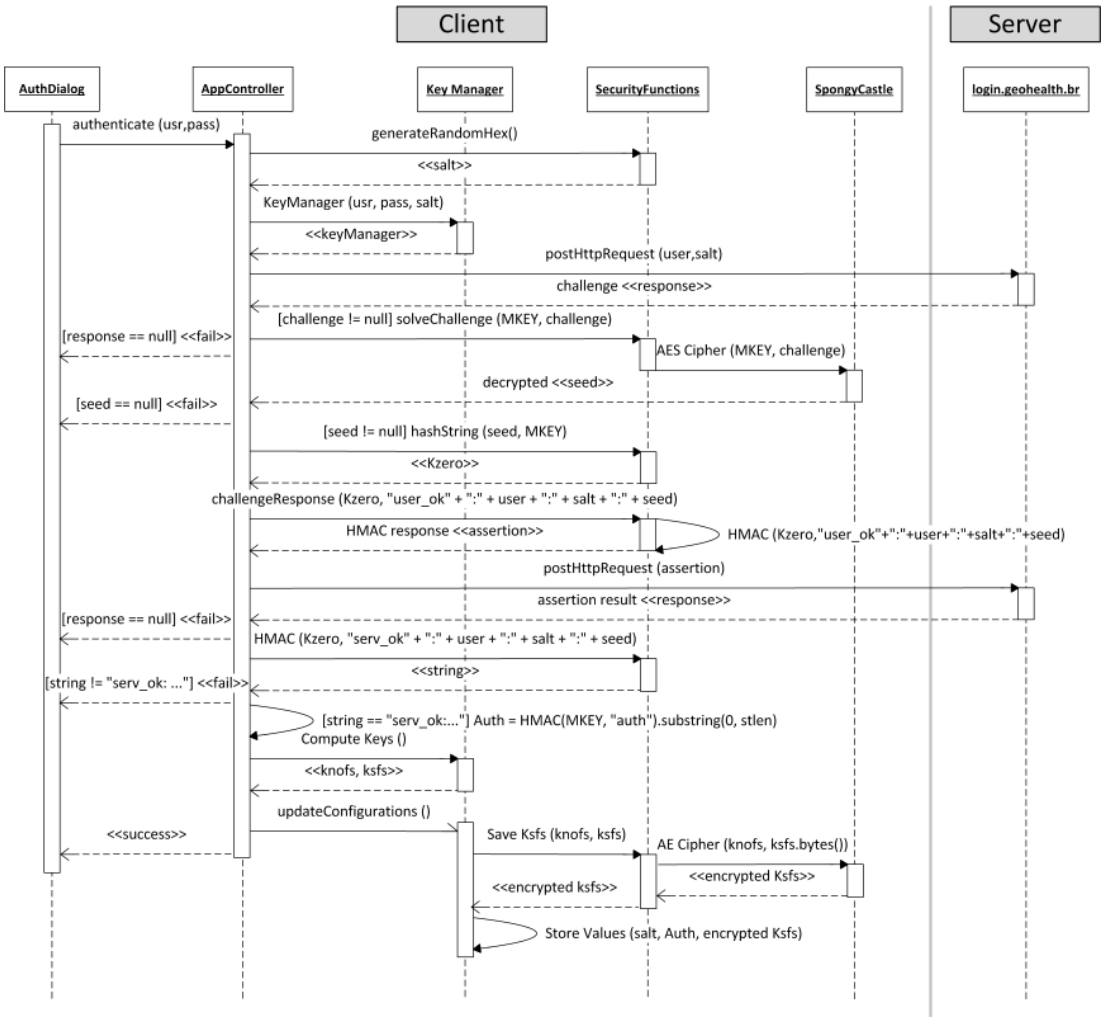


Figure 15: Authentication sequence diagram on the client side.

phone internal memory in XML format, as illustrated in Figure 18: (1) partially filled forms are encrypted with K_{nofs} and placed inside the *tmpFiles* folder; (2) when the form is filled and ready to be sent, it is authenticated and encrypted with the current value of K_{sfs}, and then stored as a new *buffer**N*** file inside a *buffer* folder. Whenever there are forms in this latter folder, the application will periodically search for 3G connectivity until all forms are successfully delivered to the server and overwritten from the device's memory.

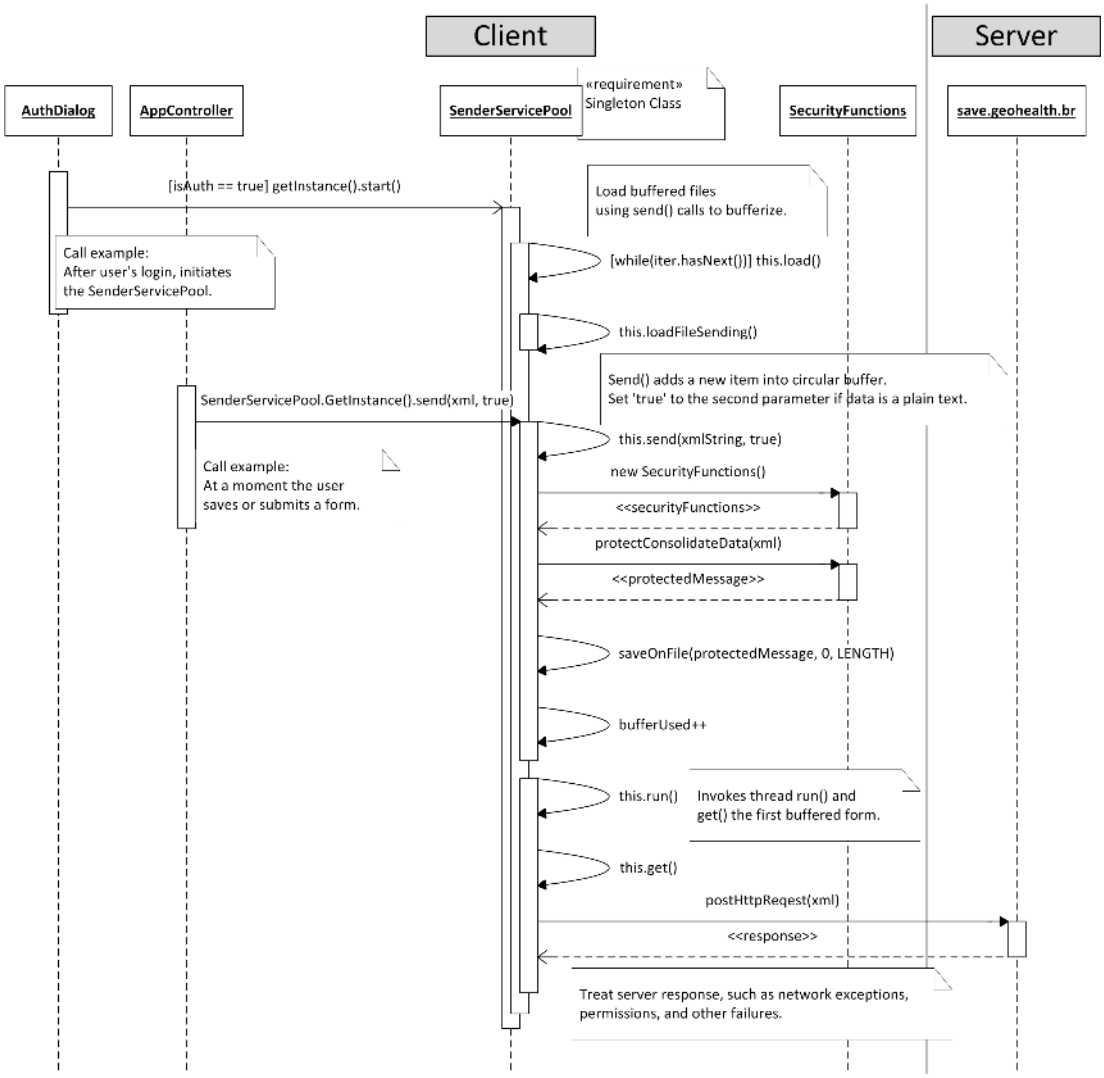


Figure 16: Form sender and storage control.

6.1.6 Benchmark results

Table 4 presents the benchmarks for the user registration protocol on the client side, following the same enumeration used in Figure 9. The purpose of this benchmark is: (a) to evaluate the impact of cryptographic algorithms and time elapsed to perform a user registration; and, (b) to evaluate the behavior of HTTPS versus HTTP, and analyze the additional overhead imposed by the TLS/SSL protocol. For this test, each result in Table 4 corresponds to the average of 20 executions of the same operation. In step 1.b of the registration protocol, the generation of MK was designed to take 1 second of processing time,

(a) (b) (c)

Figure 17: User authentication interface.

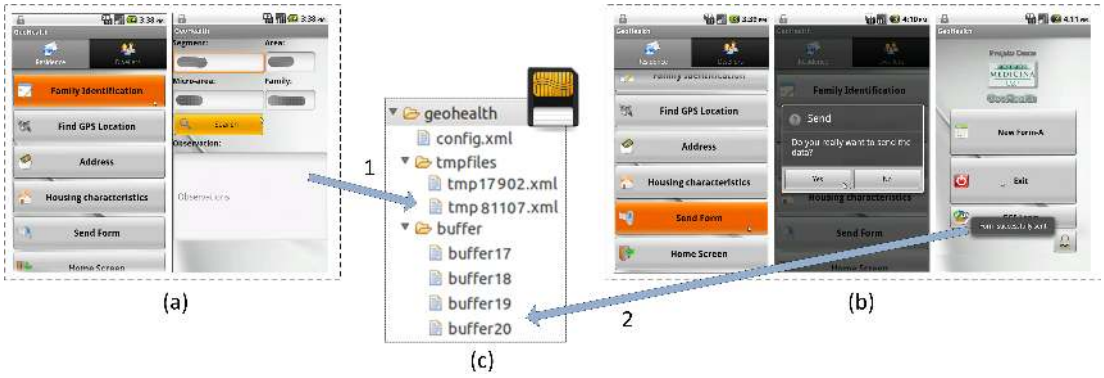


Figure 18: Temporary storage of partially and consolidated forms. (a) Partially filled form. (b) Filled form ready to be delivered. (c) SD Card with stored files.

which led to 3600 iterative applications of the hash function. For operations that involve data communication – namely, steps 2 and 6, – failures due to signal losses were ignored aiming to allow the evaluation of the overhead introduced by the cryptographic algorithms only. In addition, for minimizing such failures, the tests were performed in a metropolitan area of São Paulo with good 3G coverage/availability.

6.1.6.1 HTTPS versus HTTP deployment

From Table 4, we can evaluate the overhead introduced by HTTPS by comparing the costs of step 2, which includes the establishment of a TLS/SSL tunnel, and step 6.b, which does not. Also, the HTTP *request-response* method for message exchange in steps 2 and 6.b generates 180 and 308 bytes of data traffic (using a usr and pwd with 9 characters each). The result is that this overhead ranges from approximately 0.5 to 2.9 seconds. Even though this overhead is low in practice, repeating the same experiments in a scenario with a weak 3G signal reveals that the number of connection failures due to timeout, when one attempts to establish an HTTPS connection before sending data, is considerably higher than the case when the data is sent without the establishment of a secure tunnel. Namely, the experiments showed that an HTTPS connection fails around 20% more often than an HTTP connection in such limited connectivity scenarios. Even though this is unlikely to be a critical issue, such observation confirms the interest of avoiding the repeated establishment of HTTPS tunnels for data delivery to the server, which are unnecessary in the data delivery mechanisms of the SecourHealth framework.

N.	Operation	Avg. (ms)	Num. Bytes (sent/received)	Comment
1.a	$salt = random$	3.1 ± 0.8		
1.b	$MK = KDF(salt \,\|\|\, pwd)$	1012.1 ± 12.9		3600 hashes
2	Auth. request: $(usr, salt)$	3266.3 ± 748.8	84 / 96	3G (good)
5.a	$seed = E^{-1}_{MK}(challenge)$	173.8 ± 37.7		
5.b	$K_0 = H(seed \,\|\|\, MK)$	22.0 ± 5.1		
6.a	$resp = MAC_{K_0}(\text{`}user\_ok\text{'}...)$	58.9 ± 15.2		
6.b	Send to server: $resp$	1552.7 ± 413.1	244 / 64	3G (good)
9	Check $MAC_{K_0}(\text{`}serv\_ok\text{'}...)$	47.0 ± 11.0		

Table 4: Benchmark of the registration process.

6.1.6.2 Secure Storage Mechanisms

We also evaluated the time consumed by the secure storage mechanisms employed by SecourHealth, namely: the authenticated-encryption of data, local storage of the result, and derivation of a new K_{sfs} after its usage. Table 5 shows the benchmarks for two types of data: a typical form (≈ 3 KB) and a photo (≈ 150 KB). This table shows that the K_{sfs} derivation does not introduce a significant burden to the whole process.

On the contrary, the authenticated-encryption mechanism imposes a considerable cost for the storage of reasonably large files. However, since it can be performed in the background, it should not be noticeable by the user.

Operation	**Form ($\approx$ 3 KB) Average (ms)**	**Photo ($\approx$ 150 KB) Average (ms)**
Derive K_{sfs}	1.3 ± 0.3	
Authenticated-encryption	45.0 ± 27.3	3125.0 ± 274.7
Store result in SDCard	6.04 ± 0.4	117.8 ± 11.1

Table 5: Benchmark of the secure storage mechanisms employed in SecourHealth.

6.2 Implementing SecourHealth with GAA/GBA

Due to the reduced support for GBA provided by existing Mobile Network Operators, a real implementation of SecourHealth with GBA still cannot be deployed in practice. Accordingly, we firstly designed and developed the SecourHealth without the GBA functions, and integrated it into GeoHealth. Then, as a proof of concept, we added the GBA to scheme proposed by using the Mobile Web Security Bootstrap API[6] (MWSB), presented in Figure 19, after some small adaptation for Android. MWSB is provided by Ericsson Labs (Ericsson Labs, 2012) and has been implemented following the 3rd Generation

[6]MWSB API documentation: https://labs.ericsson.com/apis/key-management-service

Partnership Project (3GPP) standard TS 33.220 GBA. However, in this model, the GBA client (i.e., mobile phone) uses a software based *SIM card (called GBA Credential Engine (GCE)). The GCE is a piece of software from the Ericsson Labs Identity Management that partially simulates SIM Card functionalities. It can be used for improving security when a physical SIM is unavailable or for testing purposes. Additionally, it is necessary to request two API keys: one for Network Application Function (NAF) server (e.g., the GeoHealth server); and another for User Equipment (UE) (i.e., the SIM card information used by GCE). The server side of the MWSB enabler consists of two nodes: Bootstrapping Server Function (BSF) and Home Subscriber Server (HSS). These two servers are hosted by Ericsson Labs.

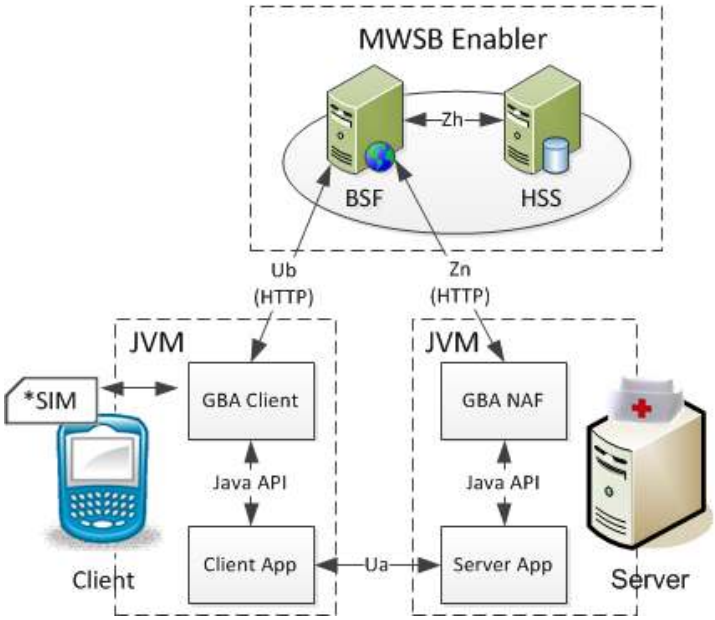
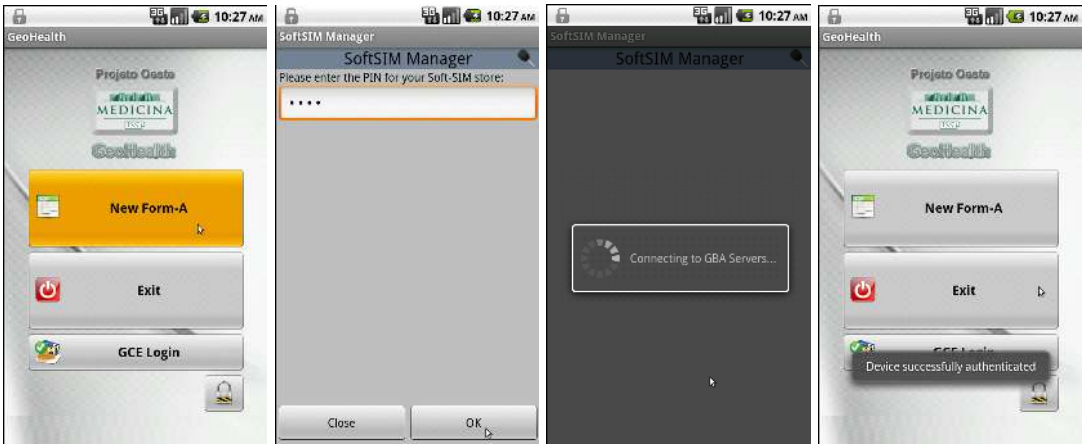


Figure 19: MWSB enabler architecture (Adapted from (Ericsson Labs, 2012)).

To implement the algorithm described in Section 5.2 for generating the master key K, we use the PBKDF2 with the pseudo random function SHA-256. The ephemeral keys K_{nofs} and K_{sfs} were also iteratively computed by the same SHA-256 hash mechanism. In the same way, we adopted the aforementioned HMAC-SHA256 to verify both the data integrity and the authenticity of the messages and forms sent. However, from the user's perspective, the entire

process occurs transparently. In Figure 20, the compliant GBA authentication is presented, so that the user firstly uses the GCE application for device authentication then he/she does the “common login” in with username and password.



(a) User clicks for authentication. (b) Launch GBA login, using PIN code. (c) UE and NAF should run GBA. (d) Device allowed for “common login”.

Figure 20: Device authentication trough GBA.

The GCE specification is part of the Identity Management Framework, hosted at Ericsson Labs[7]. There, they provide the KMS API[8], which relies on the Mobile Web Security Bootstrap API for bootstrapping, as well as the complete documentation about the GCE and MWSB and with exemplary source code for Java web applications. It is worth mentioning that developers and researchers should register in the site and create an account, before gaining access to more detailed files and resources.

6.3 Chapter Considerations

This chapter presents the results of testing the prototype developed to validate SecourHealth. The first version of SecourHealth is already running into GeoHealth,

[7]https://idm.labs.ericsson.net/portal/welcome.do
[8]https://idm.labs.ericsson.net/portal/simHelp.do

that is currently being used by 180 HCA in health units in the west region of Sao Paulo under InCor's coordination. SecourHealth meets the requirements given in Chapter 4, and can replace SSL approaches without any losses, but in fact decreasing the security overhead. Moreover, we also described how to extend SecourHealth to support device authentication based on GAA/GBA protocols, which proves to be useful to avoid DoS attacks and for device filtering. The GBA framework also bears the requirement of device authentication without any loss of confidentiality, since the MNO will be not able to eavesdrop the medical data transmitted between mobile and server.

SecourHealth also aims to tackle with the interoperability issues related to security, already discussed in the literature (WHO, 2009; GOE, 2011a; LIND et al., 2002). By adopting a framework-based strategy, we intended to facilitate the integration of security mechanisms within other mHDCS. Also, although we have implemented the SecourHealth for Android, the software models remains the same and can be adapted for other platforms (e.g., iOS or BlackBerry) and its programming languages.

7 FINAL CONSIDERATIONS

Mobile phones provided new ways to delivery and support health care (ABAJO et al., 2011). As a consequence, the mHealth applications have been largely deployed around the globe in a multitude of health programs (WHO, 2009; SHAO, 2012), in which we understand that medical data security is crucial. However, this concern was not properly tackled, either in internationals (J. OSSMAN, 2010; GOE, 2011a) or in Brazilian (IWAYA et al., 2013) researches. In that way, our research aims to contribute to the development of security solutions for mHealth. Specifically, conceiving a security framework for mHDCS, that can be adopted in multitude of health programs based on data gathering (WHO, 2009).

7.1 Results and Contributions

This research provides two main contributions: one is the in-depth survey of mHealth initiatives in Brazil; the second is the full specification of SecourHealth. The survey shows some results that might be of interest of both medical and developer communities. The survey highlights the important role that mHealth is taking in our public and private health services - and the lack of more robust applications (not only security flaws, but also interoperability and go-to-market issues). It also shows that Brazil has an exceptional HCA (Health Community Agents) workforce, spread across the country through the FHS (Family Health Strategy), a government program that should more frequently be a target of

researches.

In the security field, this research achieved two main results. First, SecourHealth framework meets the requirements specified in Chapter 4, and can replace SSL approaches decreasing the security overhead. The framework can be also extended to support GAA/GBA protocols, providing device authentication through the MNO, which is useful to avoid DoS attacks and for device filtering. Second, SecourHealth aims to tackle interoperability problems addressed in the literature (WHO, 2009; GOE, 2011a; LIND et al., 2002). By adopting a framework-based strategy, we intended to facilitate its integration within other applications. Despite our proof-of-concept being in Android, the software modeling remains the same, and it can be easily adapted to other programming languages.

The SecourHealth is integrated into GeoHealth since November 2012, being used by 180 HCA in six health units, in the west region of Sao Paulo. The amount of data generated demanded a scalable software implementation, as well as the number of HCA demanded to SecourHealth a special attention to not impair the system usability. Currently, the HCA have monthly accompanied almost one hundred thousand inhabitants, which is about twenty five thousand families.

Lastly, according to the analysis made by the reviewers of this thesis and related publications, the SecourHealth also provides an indirect contribution. The framework can be partially or totally employed for other application for data gathering that may have nothing to do with health care. The framework modules can be also used independently, e.g., use just the authentication protocols, or just the key derivation scheme for secure storage. However, due to the research time constraints, we were not able to perform a further investigation on this matter. Moreover, the SecourHealth was thoroughly designed to cope with the mHDCS scenarios, and thus, it is more probable that the framework will require modifications if employed for other generic data collection solutions.

7.2 Research Benchmark Limitation

Throughout the SecourHealth's specification and investigation about security in mHealth arena, was identified a limited number of related works. As far as we know, the work of (GEJIBO et al., 2012) is the only that fully specifies a security solutions for mHDCS. Although, they do not provide implementation results and benchmarks. This lack of references prevented a broader comparison of the security mechanisms implemented by SecourHealth. However, the SecourHealth implementation was compared with the HTTPS implementation over SSL/TLS protocol, which was often employed in other mHDCS.

7.3 Publications

The following publications and patents were the direct or indirect results of the research effort discussed in the master's thesis:

Paper published

- L.H. Iwaya, M.A.L. Gomes, M.A. Simplício, T.C.M.B. Carvalho, C.K. Dominicini, R.R.M. Sakuragui, M.S. Rebelo, M.A. Gutierrez, M. Näslund, P. Håkansson, **Mobile health in emerging countries: A survey of research initiatives in Brazil**, International Journal of Medical Informatics, Volume 82, Issue 5, May 2013, Pages 283-298, ISSN 1386-5056.

Papers in progress

- M.A. Simplicio, L.H. Iwaya, T.C. M. B. Carvalho, M. Näslund, **SecourHealth: a delay-tolerant security framework for mobile health data collection**. Submitted to: IEEE Journal of Biomedical and Health Informatics (July 2013).

- J.H.G. Sá, M.S. Rebelo, M.A. Gutierrez, A. Brentani, S. Grisi, M.A. Simplicio,

L.H. Iwaya, T.C.M.B. Carvalho, M.Näslund, P. Håkansson, **GeoHealth: A Georeferenced System for Secure Data Collection and Analysis in Primary Care**. To be submitted to: International Journal of Medical Informatics.

Patent application

- M. Näslund, M.A. Simplício, T.C.M.B. Carvalho, C.K. Dominicini, L.H. Iwaya, P. Håkansson. **GAA/GBA for Two Factor Authenticated Key Agreement** (December 2012). Reference number: P38439 WO1.
- M. Näslund, M.A. Simplício, T.C.M.B. Carvalho, L.H. Iwaya, L. Magnusson. **Password-based secure storage and delivery with configurable forward secrecy** (July 2013). Reference number: P40269 WO1.

7.4 Future Works

As future work, we intend to address one of the main challenges faced by mHealth solutions together with security: standardization. Namely, we plan to consider the integration of the mechanisms proposed in SecourHealth into standard frameworks for data collection, such as those following the OpenRosa specification. Another potential use of SecourHealth is as an integral part of other typical mHealth applications that rely on mobile devices for exchanging data with a server. One example are remote monitoring systems, in which a set of sensors continuously supervise a patient's health conditions at his/her home, periodically delivering the data acquired to a server using a mobile device as gateway.

It is worth noting that SecourHealth was implemented over a PAKE protocol due to its triviality. Nonetheless, both for mobile phones and sensors, developers can address the Elliptic Curve Cryptography (ECC) to use lightweight public-key schemes. Also, in the context of sensor network security, the ECC becomes more

interesting (SETHI, 2012). Therefore, SecourHealth can be also improved to use ECC in the AKE protocols.

In general, SecourHealth might be useful for other applications that have similar requirements of periodic data transmission and storage. Also, there are other categories of mHealth applications that need security appliances. For instance, Dominicini (DOMINICINI, 2012) proposed a user-centric approach for sharing data using the Web, which allows patients to share their medical records among trusted institutions from their mobile phones. Another example proposed by Pereira et al (PEREIRA et al., 2013), which implements a solution that guarantees security and integrity in the transmission of SMS messages. The SMS technology is simple but extremely effective for tracking treatment compliance, quite important for diseases such as HIV/AIDS and tuberculosis.

Nevertheless, whereas mobile computing is converging to smaller devices, body area networks and sensors, the usage of “mobile phones” maybe overtaken by the concept of ubiquitous health care (VISWANATHAN; CHEN; POMPILI, 2012). The integration of mHealth services (e.g., data collection + surveillance + remote monitoring) and this new “uHealth” concept brings new security requirements. Likewise, future works in this area would also combine the security enforcements already proposed in order to integrate security mechanisms in a sole framework, which can be interesting at the standardization perspective.

REFERENCES

3GPP. *TS 33.220 – Generic Authentication Architecture (GAA)*. [S.l.], June 2006.

3GPP. *TS 24.109 – Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details*. [S.l.], December 2008.

3GPP. *TS 29.109 – Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*. [S.l.], March 2010.

ABAJO, B.; RODRIGUES, J.; SALCINES, E.; FERNANDEZ, J.; CORONADO, M.; LOZANO, C. m-health y t-health. la evolucicion natural del e-health. In: *RevistaeSalud.com*. [S.l.: s.n.], 2011. v. 7, n. 25. ISSN 1698-7969.

AKINYELE, J. A.; PAGANO, M. W.; GREEN, M. D.; LEHMANN, C. U.; PETERSON, Z. N.; RUBIN, A. D. Securing electronic medical records using attribute-based encryption on mobile devices. In: *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. New York, NY, USA: ACM, 2011. (SPSM '11), p. 75–86. ISBN 978-1-4503-1000-0. Disponível em: <http://doi.acm.org/10.1145/2046614.2046628>.

ALMEIDA, L.; ANDRADE, E.; BARRETO, P.; SIMPLICIO, M. Lyra: Password-based key derivation with tunable memory and processing costs. *Journal of Cryptographic Engineering (to appear)*, 2014. See also www.lyra-kdf.net/.

AMA. *HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information*. 2013. Http://www.ama-assn.org/resources/doc/washington/hipaa-phi-encryption.pdf.

ANDREAO, R.; FILHO, J. P.; CALVI, C. TeleCardio: Telecardiologia a serviço de pacientes hospitalizados em domicílio. In: *X Congresso Brasileiro de Informática em Saúde (CBIS 2006)*. [S.l.: s.n.], 2006. p. 1267–1272.

ANOKWA, Y.; HARTUNG, C.; BRUNETTE, W.; BORRIELLO, G.; LERER, A. Open source data collection in the developing world. *Computer*, v. 42, n. 10, p. 97–99, 2009. ISSN 0018-9162. See also www.http://opendatakit.org/.

ASSOCIATION, A. A. T. *Telemedicine/Telehealth Terminology*. 2012. Http://www.americantelemed.org/files/public/abouttelemedicine/Terminology.pdf.

BAGYENDA, P. A.; KAYIWA, D.; TUMWEBAZE, C.; FRANK, N.; MARK, M. A mobile data collection tool – Epihandy. *Special topics in computing and ICT research*, Fountain publishers, v. 5, p. 327–332, 2009.

BARBOSA, J. M.; BARBOSA, T. M. G. de A.; FERREIRA, J. O.; SILVA-NETO, O. C. da; SILVA, S. da; SENE-JR., I. G.; BARBOSA, J. R. G. Projeto HealthTools: Um sistema para monitoramento da saúde e da qualidade de vida das pessoas por meio da tecnologia Java. In: *Anais do XXVI Congresso da SBC*. [S.l.: s.n.], 2006. v. 26, p. 301–315.

BARROS, A.; BERTOLDI, A. Out-of-pocket health expenditure in a population covered by the Family Health Program in Brazil. *International Journal of Epidemiology*, v. 37, p. 758–765, 2008.

BELLARE, M.; POINTCHEVAL, D.; ROGAWAY, P. Authenticated key exchange secure against dictionary attacks. In: PRENEEL, B. (Ed.). *Advances in Cryptology EUROCRYPT 2000*. Springer Berlin Heidelberg, 2000, (Lecture Notes in Computer Science, v. 1807). p. 139–155. ISBN 978-3-540-67517-4. Disponível em: <http://dx.doi.org/10.1007/3-540-45539-6_11>.

BELLARE, M.; ROGAWAY, P. Random oracles are practical: A paradigm for designing efficient protocols. In: *First ACM Conference on Computer and Communications Security (CCS)*. [S.l.: s.n.], 1993. p. 62–73.

BELLARE, M.; ROGAWAY, P.; WAGNER, D. The EAX mode of operation: A two-pass authenticated-encryption scheme optimized for simplicity and efficiency. In: *Fast Software Encryption - FSE'04*. [S.l.: s.n.], 2004. p. 389–407. http://www.cs.ucdavis.edu/~rogaway/papers/eax.pdf.

BELLOVIN, S.; MERRITT, M. Encrypted key exchange: password-based protocols secure against dictionary attacks. In: *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*. [S.l.: s.n.], 1992. p. 72–84.

BERTOLDI, A.; BARROS, A.; WAGNERD, A.; ROSS-DEGNAND, D.; HALLAL, P. Medicine access and utilization in a population covered by primary health care in Brazil. *Health Policy*, v. 89, p. 295–302, 2009.

BLACK, J. Authenticated encryption. In: ____. Berlin, Germany: Springer, 2005. ISBN 978-0-387-23473-1.

BOYKO, V.; MACKENZIE, P.; PATEL, S. Provably secure password-authenticated key exchange using diffie-hellman. In: *Proceedings of the 19th international conference on Theory and application of cryptographic techniques*. Berlin, Heidelberg: Springer-Verlag, 2000. (EUROCRYPT'00), p. 156–171. ISBN 3-540-67517-5. Disponível em: <http://dl.acm.org/citation.cfm?id=1756169-.1756186>.

BREGA, J. R. F.; LAURIS, J. R. P.; MOREIRA, P. R. C.; PEREIRA, R. C. Levantamento epidemiológico em saúde bucal utilizando ferramentas móveis. In: *XI Congresso Brasileiro de Informática em Saúde (CBIS'2008)*. [S.l.: s.n.], 2008.

BROWN, I.; BACK, A.; LAURIE, B. *Forward Secrecy Extensions for OpenPGP*. [S.l.], 2001. Disponível em: <http://tools.ietf.org/html/draft-brown-pgp-pfs-01>.

BULCAO-NETO, R. F.; SANKARANKUTTY, A. K.; MACEDO, A. A.; AZEVEDO-MARQUES, P.; WICHERT-ANA, L.; CAMACHO-GUERRERO, J. Supporting ethnographic studies of ubiquitous computing in the medical grand round experience. In: *Proceedings of the 2008 ACM symposium on Applied computing*. New York, NY, USA: ACM, 2008. (SAC'08), p. 1642–1646. ISBN 978-1-59593-753-7.

CAMBRIDGE, U. of; MOBILE, C. *Mobile Communications for Medical Care - a study of current and future health care and health promotion applications, and their use in China and elsewhere*. [S.l.], 2011.

CASTRO, L. S. S.; BRANISSO, H. J. P.; FIGUEIREDO, E. C.; NASCIMENTO, F. A. O.; ROCHA, A. F.; CARVALHO, H. S. HandMed: Um sistema móvel integrado para captura automática de sintomas. In: *IX Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2004. v. 9, p. p.1–6.

CAVICCHIOLI-NETO, V.; GAGLIARDI, H. F.; FURLAN, L. B.; REQUENA, D. B.; BOUSQUAT, A. E. M.; PISA, I. T.; ALVES, D. Uma arquitetura computacional móvel para avaliar a qualidade do sistema público de saúde na região metropolitana de são paulo. In: *X Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2006. v. 10, p. p.1–6.

CEN. *Health informatics - Electronic health record communication - Part 4: Security*. [S.l.], 2008.

CHAKRAVORTY, R. A programmable service architecture for mobile medical care. In: *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*. [S.l.: s.n.], 2006. p. 531–536. ISBN 0-7695-2520-2.

CHATKIN, J. M.; BLANCO, D. C.; SCAGLIA, N.; WAGNER, M. B.; FRITSCHER, C. C. Impact of a low-cost and simple intervention in enhancing treatment adherence in a Brazilian asthma sample. *Journal of Asthma*, v. 43, n. 4, p. 263–266, 2006.

CHEN, R.-F.; HSIAO, J.-L. An investigation on physicians' acceptance of hospital information systems: A case study. *International Journal of Medical Informatics*, v. 81, n. 12, p. 810–820, 2012. ISSN 1386-5056.

CHENG, K. G.; ERNESTO, F.; OVALLE-BAHAMóN, R. E.; TRUONG, K. N. Barriers to acceptance of personal digital assistants for hiv/aids data collection in angola. *International Journal of Medical Informatics*, v. 80, n. 8, p. 579–585, 2011. ISSN 1386-5056. <ce:title>Special Issue: Supporting Collaboration in Healthcare Settings: The Role of Informatics</ce:title>.

CONCEICAO, A. F.; PIMENTEL, T. R. G.; SILVA, E. M. Serviço para coleta móvel e processamento de dados provenientes do programa de saúde da família (PSF). In: *1st Brazilian Symposium on Services Science*. [S.l.: s.n.], 2010.

CONSULTING, V. W. *MHealth for Development: The Opportunity of Mobile Technology for Health care in the Developing World*. Washington, D.C. and Berkshire, UK, 2009.

CORREA, B.; GONçALVES, B.; TEIXEIRA, I.; GOMES, A.; ZIVIANI, A. AToMS: A ubiquitous teleconsultation system for supporting AMI patients with prehospital thrombolysis. *International Journal of Telemedicine and Applications*, 2011.

CORREIA, R. *Borboleta: um sistema de telesaúde para auxílio à atenção primária domiciliar*. Dissertação (Mestrado) — University of Sao Paulo, 2011.

CORREIA, R.; KON, F.; KON, R. Borboleta: a mobile telehealth system for primary homecare. In: *Proceedings of the 2008 ACM symposium on Applied computing*. New York, NY, USA: ACM, 2008. (SAC '08), p. 1343–1347. ISBN 978-1-59593-753-7. Disponível em: <http://doi.acm.org/10.1145/1363686-.1363998>.

COSTA, C. L. de B.; PINTO, V. C.; CARDOSO, O. L.; BABA, M. M.; PISA, I. T.; PALMA, D.; SIGULEM, D. BabyCare: apoio à decisão na atenção primária materno-infantil com computadores de mão. In: *Ciência & saúde coletiva*. [S.l.: s.n.], 2010. v. 15, n. 2, p. 3191–3198. ISSN 1413-8123.

COSTA, C. L. de B.; SIGULEM, D. Coleta, armazenamento e apoio à decisão na atenção primária infantil. In: *IX Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2004. v. 9, p. 1–4.

CRISPIM-JR., C. F.; FERNANDES, A. M. R. Uma solução em software livre para PEP na área da computação móvel. In: *II Congresso Sul Catarinense de Computação*. [S.l.: s.n.], 2006. v. 2, p. p.1–8.

CRUZ, D.; BARROS, E. Vital signs remote management system for PDAs. In: *Euromicro conference on Digital System Design*. [S.l.: s.n.], 2005. v. 8, p. 170–173.

DANTAS, C. N.; CAVALCANTE, T. J. M. M.; FILHO, A. M. P. P. Projeto-piloto - sistema de informação da atenção básica (SIAB) móvel: Articulando saberes. In: *Seminário Nacional de Diretrizes para Enfermagem na Atenção Básica em Saúde*. [S.l.: s.n.], 2009. v. 2, p. 449–452.

DATASUS. *DataSUS (Unified Health System's Database)*. 2011. Http://www2.datasus.gov.br/DATASUS/index.php.

DIFFIE, W.; OORSCHOT, P. C. V.; WIENER, M. J. Authentication and authenticated key exchanges. *Des. Codes Cryptography*, Kluwer Academic Publishers, Norwell, MA, USA, v. 2, n. 2, p. 107–125, jun. 1992. ISSN 0925-1022. Disponível em: <http://dx.doi.org/10.1007/BF00124891>.

DOMINICINI, C. K. *Uma abordagem centrada no usuário para compartilhamento e gerenciamento de dados entre aplicações web*. Dissertação (Mestrado) — Escola Politécnica, Universidade de São Paulo, 2012.

DUARTE, G.; CORREIA, R.; LEAL, P.; DOMINGUES, H.; KON, F.; KON, R.; FERREIRA, J. Borboleta and SaguiSaúde – open source mobile telehealth for public home healthcare. In: *Proceedings of the 8th International eHealth, Telemedicine and Health ICT Forum (Med-e-Tel)*. [S.l.: s.n.], 2010.

ENGLER, J.; KARLOF, C.; SHI, E.; SONG, D. PAKE-based web authentication: the good, the bad and the hurdles. In: *IEEE Web 2.0 Security and Privacy Workshop*. [S.l.: s.n.], 2009. p. 1–9. http://webblaze.cs.berkeley.edu/2009/pake/IsItToLateForPAKE.pdf.

Ericsson Labs. *In the Labs, Ericsson Labs*. 2012. Https://labs.ericsson.com/.

ETSI. *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description(3GPP TR 33.919 version 6.2.0 Release 6)*. [S.l.], 2005.

FACHEL, F. N. S.; CARDOSO, R. B.; SANTOS, M. A.; RUSSOMANO, T. Telepharmacy: Pharmaceutical care in remote areas of the Brazilian Amazon rain forest. In: *The International eHealth, Telemedicine and Health ICT Forum for Educational, Networking and Business*. [S.l.: s.n.], 2011. p. 648–651.

FLORENCIO, D.; HERLEY, C. A large scale study of web password habits. In: *Proc. of the 16th international conference on World Wide Web*. Alberta, Canada: [s.n.], 2007. p. 657–666.

FOUNDATION, A. J. *Sistema Tele-ECG*. 2011. Http://www.fajbio.com.br/servico.aspx.

FREITAS, R.; CAMACHO-GUERRERO, J.; MACEDO, A. Extension of capture information in pervasive healthcare systems: A case study. In: *11th IEEE International Conference on Computational Science and Engineering Workshops (CSEWORKSHOPS '08)*. [S.l.: s.n.], 2008. p. 19–24.

FROTA, J.; OLIVEIRA, M.; ANDRADE, L.; BARRETO, I.; FILHO1, C. Integrating mobile devices in a Brazilian health governance framework. In: *Proceedings of International Conference on Advances of Information & Communication Technology in Health Care*. [S.l.: s.n.], 2011. p. 177–181.

GANAPATHY, K.; RAVINDRA, A. mhealth: A potential tool for health care delivery in India. *Making the eHealth connection*, 2008.

GEJIBO, S. H.; MANCINI, F.; MUGHAL, K. A.; VALVIK, R. A. B.; KLUNGSYR, J. I. Secure data storage for mobile data collection systems. In: *Proc. of International ACM Conference on Management of Emergent Digital EcoSystems (MEDES)*. [S.l.: s.n.], 2012. p. 1–8.

GOE. *mHealth: New horizons for health through mobile technologies*. Global Observatory for eHealth, 2011. ISBN 978 92 4 156425 0. Disponível em: <http://www.who.int/goe/publications/ehealth_series_vol3/en/>.

____. *Telemedicine Opportunities and developments in Member States*. Global Observatory for eHealth, 2011. ISBN 978 92 4 156414 4. Disponível em: <http://www.who.int/goe/publications/ehealth_series_vol2/en/>.

GUTIERREZ, M.; CESTARI, I.; HAMAMOTO, G.; BACHT, S.; REBELO, M.; SILVA, J.; LAGE, S. Development of a mobile HIS/PACS workstation to assist critical cardiac patients in an intensive care unit. In: *Medical Imaging 2008: PACS and Imaging Informatics*. [S.l.: s.n.], 2008. v. 6919, p. 691915–1–691915–8.

GUTIERREZ, M. A.; CESTARI, I. A.; HAMAMOTO, G.; BACHT, S.; REBELO, M. S.; SILVA, J. E. M. M.; LAGE, S. G. Development of a mobile his/pacs workstation to assist critical cardiac patients in an intensive care unit. p. 691915–691915–8, 2008. Disponível em: <http://dx.doi.org/10.1117/12.770565>.

HERTZMAN, C. P.; MEAGHER, N.; MCGRAIL, K. M. Privacy by design at population data bc: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. *Journal of the American Medical Informatics Association*, 2012. Disponível em: <http://jamia.bmj.com/content/early/2012/08-/29/amiajnl-2012-001011.abstract>.

HL7. *HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) - Access Control, DSTU Release 1*. [S.l.], 2013.

HODGE, J. G. Health information privacy and public health. *The Journal of Law, Medicine & Ethics*, 2003.

HOLTMANNS, S.; NIEMI, V.; GINZBOORG, P.; LAITINEN, P.; ASOKAN, N. *Cellular Authentication for Mobile and Internet Services*. [S.l.]: Wiley, 2008.

HOSPITAL, A. E. *Product: Einstein Mobile*. 2009. Http://medicalsuite.einstein.br/einstein-mobile.asp.

HOUNSELL, M.; MIRANDA, J.; KEMCZINSKI, A. Estratégias de avaliação da aprendizagem em ambientes virtuais 3D e jogos sérios. In: *International Conference on Engineering and Technology Education*. [S.l.: s.n.], 2010. p. 538–542.

HUB. *hub - Health Unbound*. 2013. Http://www.healthunbound.org/about-hub. Disponível em: <http://www.healthunbound.org/about-hub>.

HUPPERICH, T.; LöHR, H.; SADEGHI, A.-R.; WINANDY, M. Flexible patient-controlled security for electronic health records. In: *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*. New York, NY, USA: ACM, 2012. (IHI '12), p. 727–732. ISBN 978-1-4503-0781-9. Disponível em: <http://doi.acm.org/10.1145/2110363.2110448>.

INFOWAY. *A "Conceptual" Privacy Impact Assessment of the EHRS Blueprint Version 2*. [S.l.], 2008.

ISHITANI, L. H.; FRANCO, G. C.; PERPETUO, I. H. L.; FRANçA, I. Socioeconomic inequalities and premature mortality due to cardiovascular diseases in brazil. In: *Revista Saúde Pública*. [S.l.: s.n.], 2006.

ISO. *ISO/TC 215 - Health informatics*. [S.l.], 2013. Disponível em: <http://www-.iso.org/iso/home/standards_development/list_of_iso_technical_committees-/iso_technical_committee.htm?commid=54960>.

ISTEPANIAN, R.; JOVANOV, E.; ZHANG, Y. Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity. In: *IEEE Transactions on Information Technology in Biomedicine*. [S.l.: s.n.], 2004. v. 8, n. 4, p. 405–414. ISSN 1089-7771.

ITKIS, G. *Forward security, adaptive cryptography: Time evolution*. 2004. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95-.440>.

ITU. *Mobile eHealth Solutions for Developing Countries Question 14-2/2*. [S.l.], 2010. Disponível em: <http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG02.14-.2-2010-PDF-E.pdf>.

____. *The World in 2011 ICT Facts and Figures*. 2011. Http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.

IWAYA, L.; GOMES, M.; SIMPLíCIO, M.; CARVALHO, T.; DOMINICINI, C.; SAKURAGUI, R.; REBELO, M.; GUTIERREZ, M.; NASLUND, M.; HAKANSSON, P. Mobile health in emerging countries: A survey of research initiatives in brazil. *International Journal of Medical Informatics*, v. 82, n. 5, p. 283 – 298, 2013. ISSN 1386-5056. Disponível em: <http://www.sciencedirect.com/science/article/pii-/S1386505613000142>.

JONES, C. R.; NEVES, F.; PRADO, A. C.; CARDOSO, R. B.; HUTTNER, E.; RUSSOMANO, T. A telecardiology assistance project in a remote region of the Brazilian Amazon. In: *The International eHealth, Telemedicine and Health ICT Forum for Educational, Networking and Business*. [S.l.: s.n.], 2011. p. 635–639.

JORGE, E. N. L. F.; ZIVIANI, A.; SALLES, R. M. Telemonitoramento baseado no protocolo XMPP para vigilância epidemiológica. In: *Congresso Brasileiro de Telemedicina e Telessaúde*. [S.l.: s.n.], 2009. v. 4, p. p.1–5.

JOSÉ, A. B.; BARBOSA, T. M. G. A.; SENE-JR, I. G.; CARVALHO, H. S.; ROCHA, A. F.; NASCIMENTO, F. A. O.; CASTRO, L. S. S. Implementação da revisão sistemática de sintomas em sistemas móveis utilizando redes bayesianas. In: *V Workshop de Informática Médica*. [S.l.: s.n.], 2005.

J. OSSMAN, P. H. N. S. A. A. L. *Barriers and Gaps Affecting mHe-alth in Low and Middle Income Countries: Policy White Paper* . [S.l.], 2010. Disponível em: <http://www.globalproblems-globalsolutions-files.org/pdfs-/mHealth_Barriers_White_Paper.pdf>.

KALISKI, B. *PKCS#5: Password-Based Cryptography Specification Version 2.0*. [S.l.], 2000. http://www.ietf.org/rfc/rfc2898.txt.

KAPLAN, W. A. Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries? *Globalization and Health*, BioMed Central, v. 2, n. 9, 2006.

KOURROUSKI, M.; LIMA, R. Adesão ao tratamento: vivências de adolescentes com HIV/AIDS. *Revista Latino-Americana de Enfermagem*, v. 17, n. 6, p. 947–952, 2009. ISSN 0104-1169.

LACERDA, B.; TIMM, R.; KALIL, R.; PORTAL, V. L.; SPARENBERG, A. L. F. A mobile tele-ECG system for a public outpatient care unit in southern Brazil: Results from a pilot study. In: *The International eHealth, Telemedicine and Health ICT Forum for Educational, Networking and Business*. [S.l.: s.n.], 2010.

LAITINEN, P.; GINZBOORG, P.; ASOKAN, N.; HOLTMANNS, S.; NIEMI, V. Extending cellular authentication as a service. In: *Commercialising Technology and Innovation, 2005. The First IEE International Conference on (Ref. No. 2005/11044)*. [S.l.: s.n.], 2005. p. 0_90–D2/4. ISSN 0537-9989.

LIND, L.; SUNDVALL, E.; KARLSSON, D.; SHAHSAVAR, N.; AHLFELDT, H. Requirements and prototyping of a home health care application based on emerging java technology. *International Journal of Medical Informatics*, v. 68, p. 129–139, 2002. Disponível em: <http://www.ncbi.nlm.nih.gov/pubmed-/12467797>.

LU, Y.-C.; XIAO, Y.; SEARS, A.; JACKO, J. A. A review and a framework of handheld computer adoption in healthcare. *International Journal of Medical Informatics*, v. 74, n. 5, p. 409 – 422, 2005. ISSN 1386-5056. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1386505605000201>.

LUXTON, D. D.; KAYL, R. A.; MISHKIND, M. C. mhealth data security: the need for hipaa-compliant standardization. *Telemedicine and e-Health*, 2012.

MACHADO, A.; PADOIN, E. L.; SALVADORI, F.; RIGHI, L.; CAMPOS, M. de; SAUSEN, P. S.; DILL, S. L. Utilização de dispositivos móveis, web services e sotfware livre no monitoramento remoto de pacientes. In: *XIII Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2011. v. 11, p. p.1–6.

MANCINI, F.; MUGHAL, K.; GEJIBO, S.; KLUNGSOYR, J. Adding security to mobile data collection. In: *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. [S.l.: s.n.], 2011. p. 86 –89.

MARTHA, A. S.; SALOMãO, P. L.; S; ROMANI, R.; CAMPOS, C. H. R. de; SIGULEM, D. Clinic Web: PEP e interação com dispositivos móveis. In: *X Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2006. v. 1.

MATTOS, N. P. de. *Sistema de Apoio à Decisão para Planejamento em Saúde*. Dissertação (Mestrado) — PUC-PR, 2003.

MCALEARNEY, A. S.; SCHWEIKHART, S. B.; MEDOW, M. A. Doctors' experience with handheld computers in clinical practice: qualitative study. *BMJ*, v. 328, n. 7449, p. 1162, 5 2004.

MENDONCA, L.; MACADAR, M. Information systems' importance for health care action planning and policy making by the municipality of Porto Alegre - Brazil. *Revista Eletrônica de Sistemas de Informação*, v. 7, n. 2, 2008.

MENEZES-JR., J. V. de; D'CASTRO, R. J.; RODRIGUES, F. M. M.; aO, C. M. G. de G.; LYRA, N. R. S.; SARINHO, S. W. InteliMed: uma experiência de desenvolvimento de sistema móvel de suporte ao diagnóstico médico. *Revista Brasileira de Computação Aplicada*, v. 3, n. 1, p. p.30–42, 2011.

MEZAROBA, W.; MENEGON, M.; NICOLEIT, E. Registro eletrônico de paciente em uma UTI: Comunicação, interação com dispositivos móveis e previsão de expansibilidade. In: *XI Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2008.

MIRKOVIC, J.; BRYHNI, H.; RULAND, C. Secure solution for mobile access to patient's health care record. In: *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. [S.l.: s.n.], 2011. p. 296 –303.

MONTEIRO, S.; REBELLO, S.; SCHALL, V. *Zig-AIDS*. 2012. Http://www.fiocruz.br/piafi/zigzaids/.

MORAES, D. de; PISA, I.; LOPES, P. Protótipo para coleta de informações em saúde utilizando dispositivos móeis. In: *IX Congresso Brasileiro de Informática em Saúde*. [S.l.: s.n.], 2004. p. 1–4.

MORAIS, A.; MACHADO, L.; VALENCA, A. Definindo a abordagem de comunicação no planejamento de um serious games voltado para saúde bucal em bebês. In: *X Workshop de Informática Médica - WIM'10*. [S.l.: s.n.], 2010. p. 1556–1565.

MURAKAMI, A.; GUTIERREZ, M.; LARGE, S.; REBELO, M.; GUIRALDELLI, R.; RAMIRES, J. A continuous glucose monitoring system in critical cardiac patients in the intensive care unit. In: *Computers in Cardiology*. [S.l.: s.n.], 2006. p. 233–236. ISSN 0276-6547.

MURAKAMI, A.; KOBAYASHI, L. O. M.; TACHINARDI, U.; GUTIERREZ, M. A.; FURUIE, S. S.; PIRES, F. A. Acesso a informações médicas através do uso de sistemas de computação móvel. In: *IX Congresso Brasileiro de Informática em Saúde - CBIS2004*. [S.l.: s.n.], 2004.

NARDON, F. B. *The Virtual Health Pet*. [S.l.]: Sun Community Champion, 2006. Http://developers.sun.com/champions/nardon.html.

NIST. *Federal Information Processing Standard (FIPS 197) – Advanced Encryption Standard (AES)*. [S.l.], November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

NIST. *Federal Information Processing Standard (FIPS PUB 198) – The Keyed-Hash Message Authentication Code*. [S.l.], March 2002. http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

____. *Federal Information Processing Standard (FIPS 180-4) – Secure Hash Standard*. [S.l.], March 2012.

NOKIA. *Nokia Data Gathering (former MobiSUS)*. 2013. Https://projects.developer.nokia.com/ndg/wiki/projects.

NORRIS, A.; STOCKDALE, R.; SHARMA, S. A strategic approach to m-health. *Health Informatics Journal*, v. 15, n. 3, p. 244–253, 2009.

ORTIS, R. S. *Visualização Genérica de Sinais e Dados Biomédicos em Dispositivos Móveis*. Dissertação (Mestrado) — Universidade de Brasília, Brazil, 2009.

PATRICK, K.; GRISWOLD, W.; RAAB, F.; INTILLE, S. Health and the mobile phone. *American Journal of Preventive Medicine*, v. 35, p. 177–181, 2008.

PAYNE, J. D. *The State of Standards and Interoperabilty for mHealth*. [S.l.], 2013. Disponível em: <http://mhealthalliance.org/images/content-/state_of_standards_report_2013.pdf>.

PERCIVAL, C. Stronger key derivation via sequential memory-hard functions. In: *BSDCan 2009 – The Technical BSD Conference*. [s.n.], 2009. Disponível em: <http://www.bsdcan.org/2009/schedule/attachments/87_scrypt.pdf>.

PEREIRA, G. C.; SANTOS, M. A.; OLIVEIRA, B. T. de; SIMPLICIO, M. A.; BARRETO, P. S.; MARGI, C. B.; RUGGIERO, W. V. Smscrypto: A lightweight cryptographic framework for secure sms transmission. *Journal of Systems and Software*, Elsevier, v. 86, n. 3, p. 698–706, 2013.

PIMENTEL, T. R. G.; SILVA, E. M. P. da; CONCEICAO, A. F. da. Projeto Colibri: uma plataforma de coleta e processamento de dados para o Programa de Saúde da Família (PSF). In: *Workshop de Informática Médica*. [S.l.: s.n.], 2010. p. p.1471–1474.

POINTCHEVAL, D.; ZIMMER, S. Multi-factor authenticated key exchange. In: BELLOVIN, S.; GENNARO, R.; KEROMYTIS, A.; YUNG, M. (Ed.). *Applied Cryptography and Network Security*. Springer Berlin Heidelberg, 2008, (Lecture Notes in Computer Science, v. 5037). p. 277–295. ISBN 978-3-540-68913-3. Disponível em: <http://dx.doi.org/10.1007/978-3-540-68914-0_17>.

PORTOCARRERO, J. T.; SOUZA, W. L.; DEMARZO, M.; PRADO, A. F. SIAF: Um sistema de informação de atividade física. In: *X Workshop de Informática Médica - WIM'10*. [S.l.: s.n.], 2010.

PROJECT, S. *What is SRP?* 2013. The Stanford SRP Homepage. Web. 09 Jul. 2013. Disponível em: <http://srp.stanford.edu/whatisit.html>.

PRSYSTEMS. *SIAB Fácil*. 2011. Http://www.siabfacil.com.br/mobile.php.

ROEDER, T. *Something You Know, Have, or Are*. 2013. Web. 09 Jul. 2013. Disponível em: <http://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople-.html>.

ROLIM, C.; KOCH, F.; WESTPHALL, C.; WERNER, J.; FRACALOSSI, A.; SALVADOR, G. A cloud computing solution for patientś data collection in health care institutions. In: *2nd International Conference on eHealth, Telemedicine, and Social Medicine*. [S.l.: s.n.], 2010. p. 95–99. ISBN 978-1-4244-5803-5.

ROSA, M.; MARCOLIN, M.; ELKIS, H. Evaluation of the factors interfering with drug treatment compliance among Brazilian patients with schizophrenia. *Brazilian Journal of Psychiatry*, v. 27, n. 3, p. 178–184, 2005.

Sá, J.; REBELO, M.; BRETANI, A.; GRISI, S.; GUTIERREZ, M. Geohealth: A georeferenced system for health data analysis in primary care. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, v. 10, n. 1, p. 1352–1356, 2012. ISSN 1548-0992.

SANTOS, A. F.; SOUZA, C.; QUEIROZ, N. R.; PENNA, G. C.; MEDEIROS, E. M. N. P.; ALVES, H. J. Incorporation of telehealth resources in Belo Horizonteś SAMU: qualifying and improving care. In: *International Conference on eHealth, Telemedicine, and Social Medicine - TELEMED́09*. [S.l.: s.n.], 2009. p. 72–76. ISBN 978-1-4244-3360-5.

SAX, U.; KOHANE, I.; MANDL, K. D. Wireless technology infrastructures for authentication of patients: {PKI} that rings. *Journal of the American Medical Informatics Association*, v. 12, n. 3, p. 263 – 268, 2005. ISSN 1067-5027. Disponível em: <http://www.sciencedirect.com/science/article/pii-/S1067502705000150>.

SCHNEIER, B. *Applied cryptography: protocols, algorithms, and source code in C*. [S.l.]: Wiley, 1996. ISBN 9780471128458.

SETHI, M. *Security in Smart Object Networks*. Dissertação (Mestrado) — Aalto University School of Science, 2012.

SHANMUGAM, M.; THIRUVENGADAM, S.; KHURAT, A.; MAGLOGIANNIS, I. Enabling secure mobile access for electronic health care applications. In: *Pervasive Health Conference and Workshops, 2006*. [S.l.: s.n.], 2006. p. 1 –8.

SHAO, D. *A Proposal of a Mobile Health Data Collection and Reporting System for the Developing World*. Dissertação (Mestrado) — Malmö University – School of Technology, 2012.

SILVA, A. S.; LAPREGA, M. R. Critical evaluation of the primary care information system (SIAB) and its implementation in Ribeirão Preto, São Paulo, Brazil. *Cadernos de Saúde Pública*, v. 21, 2005. ISSN 0102-311X.

SILVEIRA, A.; LEãO, B.; COSTA, C.; MARQUES, E.; KIATAKE, L.; EVANGELISTI, L.; SILVA, M.; GALVãO, S.; TAKEMAE, T. *Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) Versão 3.3*. [S.l.], 2009. Disponível em: <http://portal.cfm.org.br/crmdigital/manualcertificacao.pdf>.

SNIA. *Encryption of Data At-Rest Step-by-step Checklist*. [S.l.], 2009. Disponível em: <http://www.snia.org/sites/default/files/Encryption-Checklist-2.0.090909.pdf>.

SPARENBERG, A.; KALIL, R.; PORTAL, V. Ten years of a tele-ECG system in the state of Rio Grande do Sul/Brazil: From a regional project to a multipoint network. In: *Global Telemedicine and eHealth Updates: Knowledge Resources*. [S.l.: s.n.], 2010. v. 3, p. 278–281.

SUN, H.-M.; HSIEH, B.-T.; HWANG, H.-J. Secure e-mail protocols providing perfect forward secrecy. *Communications Letters, IEEE*, v. 9, n. 1, p. 58–60, 2005. ISSN 1089-7798.

SUN, H.-M.; YEH, H.-T. Password-based authentication and key distribution protocols with perfect forward secrecy. *Journal of Computer and System Sciences*, v. 72, n. 6, p. 1002 – 1011, 2006. ISSN 0022-0000. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022000006000481>.

SUNSHINE, J.; EGELMAN, S.; ALMUHIMEDI, H.; ATRI, N.; CRANOR, L. F. Crying wolf: an empirical study of ssl warning effectiveness. In: *Proceedings of the 18th conference on USENIX security symposium*. Berkeley, CA, USA: USENIX Association, 2009. (SSYM'09), p. 399–416. Disponível em: <http://dl.acm.org/citation.cfm?id=1855768.1855793>.

SUNYAEV, A.; LEIMEISTER, J. M.; KRCMAR, H. Open security issues in german healthcare telematics. In: *HEALTHINF*. [S.l.]: INSTICC Press, 2010. p. 187–194. ISBN 978-989-674-016-0.

TACHAKRA, S.; WANG, X.; ISTEPANIAN, R.; SONG, Y. Mobile e-health: The unwired evolution of telemedicine. In: *Telemedicine and e-Health*. [S.l.: s.n.], 2003. v. 9, n. 3, p. 247–257.

TECHNOLOGIES, M. *A framework to access health management systems*. 2009. Http://www.mtmtecnologia.com.br/.

____. *An mobile application to access health management systems*. 2009. Http://www.mtmtecnologia.com.br/.

TRINDADE, C. *Identificação do comportamento das hepatites virais a partir da exploração de bases de dados de saúde pública*. Dissertação (Mestrado) — PUC-PR, 2005.

VIGOLO, M.; FADEL, F.; BASTOS, L. Coleta de dados de pacientes de hanseníase via PDA. In: *XI Congresso Brasileiro de Informática em Saúde (CBIS'2008)*. [S.l.: s.n.], 2008.

VISWANATHAN, H.; CHEN, B.; POMPILI, D. Research challenges in computation, communication, and context awareness for ubiquitous healthcare. *Communications Magazine, IEEE*, v. 50, n. 5, p. 92–99, 2012. ISSN 0163-6804.

WATER.ORG. *Millions Lack Safe Water*. 2013. Http://water.org/water-crisis/water-facts/water/.

WHO. *Declaration of Alma-Ata - International Conference on Primary Health Care, Alma-Ata, USSR, 6-12 September 1978*. 1978. Http://www.who.int/publications/almaata_declaration_en.pdf.

WHO. *The Impact of Chronic Disease in Brazil*. [S.l.], 2005. Disponível em: <http://www.who.int/chp/chronic_disease_report/media/brazil.pdf>.

____. *Country cooperation strategy at a glance: Brazil*. [S.l.], 2009. Disponível em: <http://www.who.int/countries/bra/en>.

WOZAK, F.; AMMENWERTH, E.; HöRBST, A.; SöGNER, P.; MAIR, R.; SCHABETSBERGER, T. Ihe based interoperability - benefits and challenges. In: . [s.n.], 2008. v. 136, p. 771–776. ISBN 978-1-58603-864-9. Disponível em: <http://www.ncbi.nlm.nih.gov/pubmed/18487825>.

YU, P.; COURTEN, M. de; PAN, E.; GALEA, G.; PRYOR, J. The development and evaluation of a pda-based method for public health surveillance data collection in developing countries. *International Journal of Medical Informatics*, v. 78, n. 8, p. 532–542, 2009. ISSN 1386-5056.

APPENDIX A – GENERIC AUTHENTICATION ARCHITECTURE

This section briefly describes the GAA (Generic Authentication Architecture), a mechanism that can be integrated into the GeoHealth framework as discussed in Chapter 5.

There are two main ways of using GAA (Generic Authentication Architecture). The first is based on a shared secret between the client and the server, and the second on public and private key pairs and digital certificates. The objective of this appendix is to give an overview of GBA (Generic Bootstrapping Architecture), the first way mentioned, establishing the GAA/GBA protocol to authenticate user mobile equipment.

A.1 GAA/GBA

GAA is a generic architecture for mutual authentication and key agreement (AKA). One of its fundamental building blocks is the Generic Bootstrapping Architecture (GBA) (HOLTMANNS et al., 2008), which is specified by 3GPP (3rd Generation Partnership Project) in TS 33.220 (3GPP, 2006). GBA provides mechanisms that mobile applications can rely upon for authentication between servers and clients. The user authentication is possible if the user has a valid identity in the Mobile Network Operator (MNO) (e.g., a SIM card). Figure 21 shows the main components of GBA.

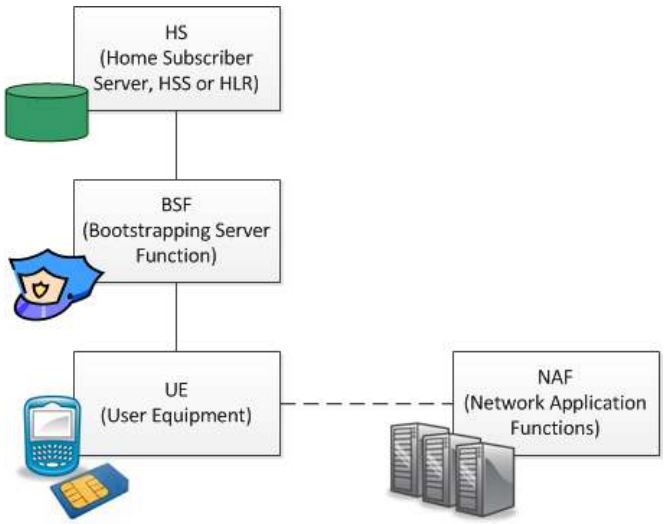


Figure 21: Simple Network model for GBA.

In (HOLTMANNS et al., 2008), each of the main components of the GBA architecture is described according to 3GPP TS 33.220, as follows:

- HS (Home Server): is the subscriber database and contains the long-term key for each subscriber. In UMTS networks, this component is known as the HSS (Home Subscriber Server), while in GSM networks, the HS is known as the Home Location Register (HLR).

- BSF (Bootstrapping Server Function): is a trusted entity which is involved in authentication and key exchange between the UE and the NAF. It is a new network function introduced in GAA, which facilitates the use of AKA to bootstrap a new GAA master session key.

- NAF (Network Application Functions): is the server functionality of each GAA server application.

Figure 22 shows a simple network model with the entities involved in the bootstrapping approach when an HSS with Zh reference point is deployed, and the reference points used between them. The reference points are specified in 3GPP TS 29.109 (Zn and Zh) and TS 24.109 (Ua and Ub) (3GPP, 2008; 3GPP, 2010). Note

that this figure includes a new entity: the SLF (Subscriber Locator Function). In the case of a larger network with several HSS servers, then a SLF might be used in order to determine the correct HSS for a given subscriber (HOLTMANNS et al., 2008).

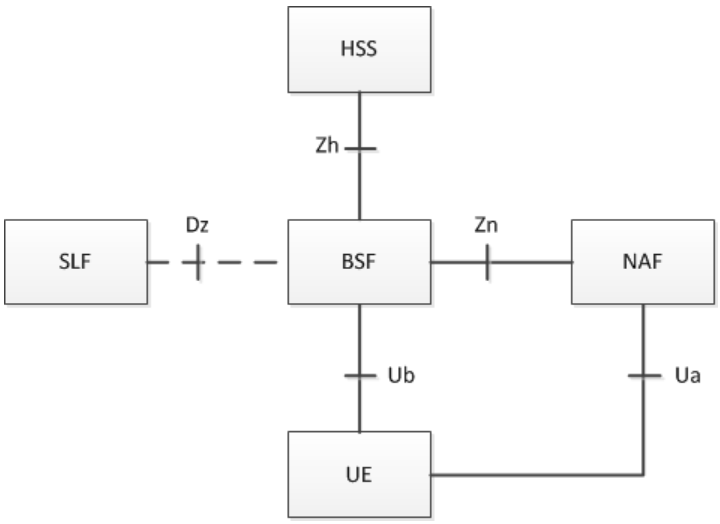


Figure 22: Network model for bootstrapping in the home network (Source (3GPP, 2006)).

In the case in which the UE has contacted a NAF that is operated in a network different from the home network, this visited NAF shall use a Zn-Proxy of the NAFs network to communicate with the subscriber's BSF (i.e., the home BSF) (3GPP, 2006). Figure 23 shows a simple network model with the entities involved when the network application function is located in the visited network.

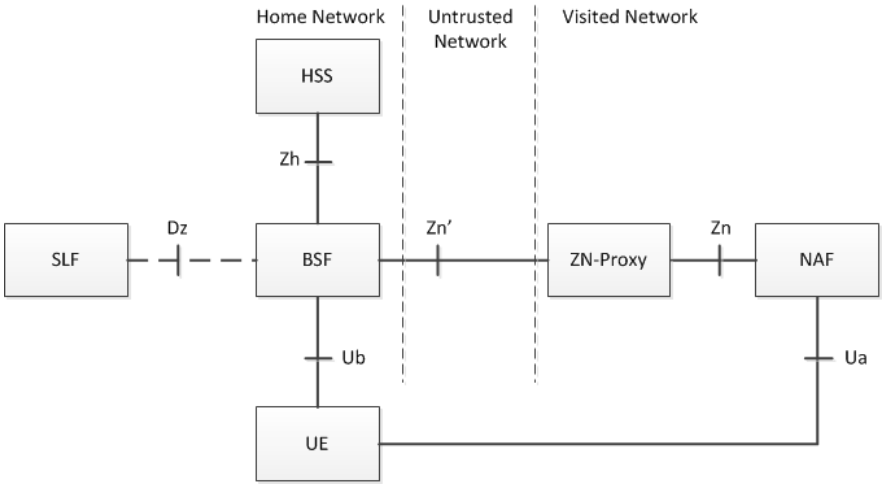


Figure 23: Network model for bootstrapping in the visited network (Source (3GPP, 2006)).

The basics of the GBA bootstrapping authentication procedure are illustrated in Figure 24 and described below.

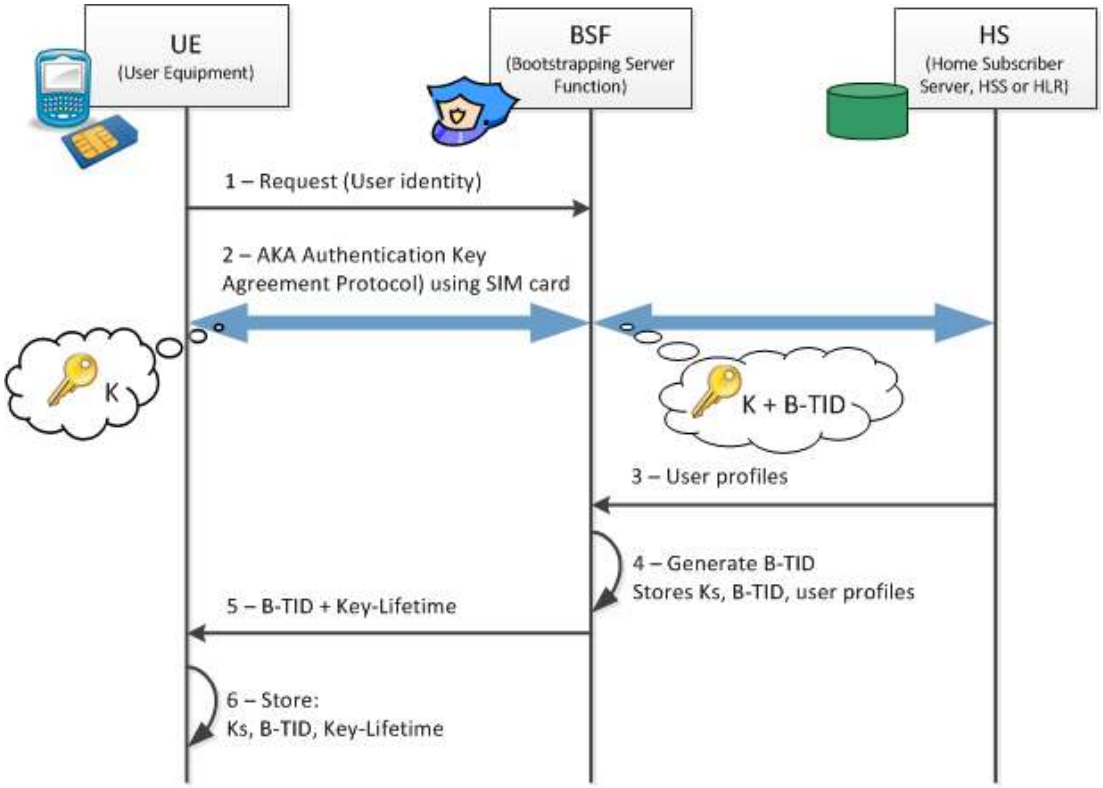


Figure 24: Operation flow for the GBA bootstrapping authentication procedure.

1. The UE sends an HTTP request towards the BSF with an $identity$ parameter.

2. This triggers a run of authentication protocol between UE and HSS, with the BSF acting as an intermediary as follows:

   - The BSF retrieves the complete set of GBA user security settings and one Authentication Vector $(AV, AV = RAND||AUTN||XRES||CK||IK)$ from the HSS. In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to this step.
   - Then the BSF forwards the $RAND$ and $AUTN$ to the UE in a 401 HTTP message (without the CK, IK and $XRES$). This is to demand the UE to authenticate itself.

- The UE checks $AUTN$ to verify that the challenge is from an authorized network; the UE also calculates CK, IK and RES.
- The UE sends another HTTP request, containing the Digest AKA response (calculated using RES), to the BSF.
- The BSF authenticates the UE by verifying the Digest AKA response.
- The BSF generates key material Ks by concatenating CK and IK.

3. The BSF receives a set of user profiles from the HSS.

4. The BSF generates $B-TID$ transaction identifier and stores Ks, $B-TID$, and the user profiles.

5. The BSF sends a 200 HTTP OK message, including a $B-TID$ and lifetime of the key Ks, to the UE to indicate the success of the authentication.

6. The key material Ks is generated in the UE by concatenating CK and IK. The UE stores Ks, $B-TID$, and $key-lifetime$.

The basics of the GBA bootstrapping usage procedure is illustrated in Figure 25 and described below.

1. The UE derives the key Ks_NAF from Ks and supplies the $B-TID$ to the NAF in order to allow the NAF to retrieve the corresponding keys from the BSF.

2. The NAF requests key material corresponding to the $B-TID$ supplied by the UE to the BSF. With the key material request, the NAF supplies a $NAF-Id$ to the BSF. (This is to allow for consistent key derivation in the BSF and UE).

3. The BSF derives the keys from the key Ks and the key derivation parameters and supplies NAF with the requested key Ks_NAF, as well as the bootstrapping time and the lifetime of that key, and the requested application-specific and potential

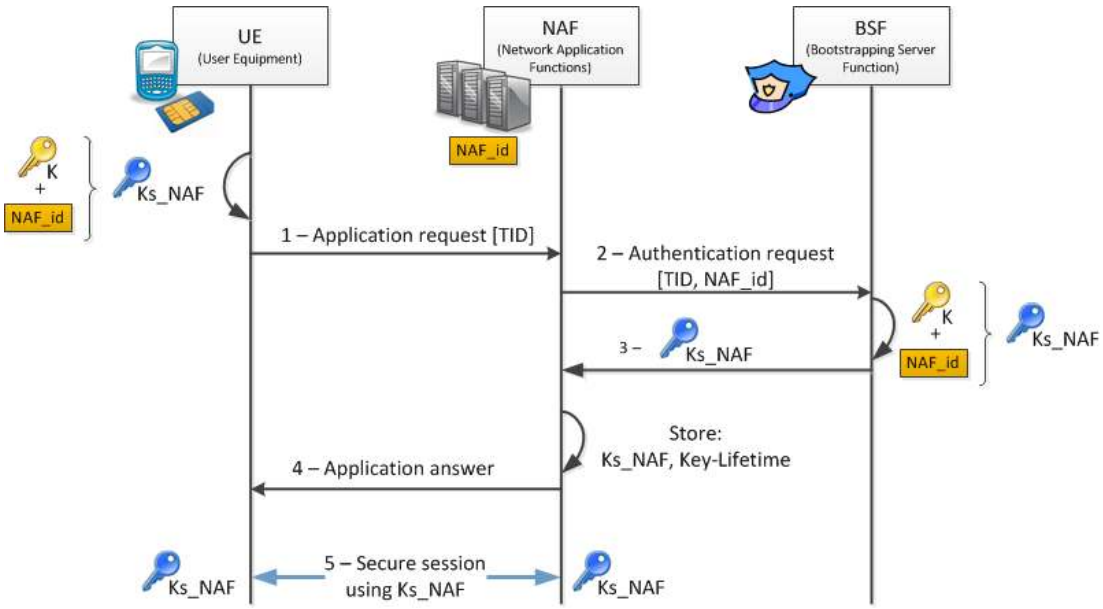


Figure 25: Operation flow of GBA bootstrapping usage procedure.

NAF group specific USSs (User Security Settings). If the key identified by the $B - TID$ supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a bootstrapping renegotiation request to the UE.

4.NAF continues with the protocol used with the UE.

5.UE and NAF can communicate in a secure way.