Abstract—Medical applications have already been integrated into mobile devices (e.g., Tablet PCs, PDAs and smart phones) and are being used by medical personnel in treatment centers, for retrieving and examining patient’s Electronic Health Records (EHR). In such mobile healthcare applications, specific attention is drawn towards the security requirements since the transmission of sensitive medical data through a public network renders the problem of communication privacy. In this paper we present an approach to transfer the medical records of an individual by using the existing infrastructure of mobile operators. To achieve that, we propose the application of existing technologies in 3G networks such as the Generic Bootstrapping Architecture (GBA) to enable the secure transfer of EHR data. The paper presents the corresponding applicability scenarios, initial results from a prototype test bed and discusses the feasibility of the proposed solution along with its limitations.

I. INTRODUCTION

Nowadays we live in the era of digital communication, digital information and digital data, where users are interested to be “always connected”, be more nomadic and have rapid access to all sorts of information. One of the most important enabling technologies that provide the platform, which allows achieving this goal, is the Universal Mobile Telecommunication Systems (UMTS) from Third Generation Partnership Project (3GPP). By using mobile devices, one can use many different kinds of services such as voice, multimedia and data services.

During the recent past, initiatives have been taken both from academia and by the industries towards improving the health care and safety of the public by using information and communication technologies. Research activities have been focused on achieving portability of medical records, monitoring real-time health status of the patients, enhancing the concept of online diagnosis, developing telemedicine solutions, which deals with remote delivery of health services by means of telecommunications, etc. In a broader sense, such health care applications can be termed as “e-health”.

One of the prominent steps, in this direction, is to adopt the “digitized” health record [1] approach, whereby “hand written” medical data has been translated into a well-defined electronic health record (EHR) and retained at a central repository. This vision will provide the capability to move the medical records, electronically, between disparate health information systems without changing the “meaning” of the exchanged information. It is foreseen that with the help of the medical informatics, better health care and services can be provided to users and hospitals can also benefit by enjoying better information management and administration. Also, it will provide the users the ability to access their medical records anywhere, anytime. Moreover, with wireless technology, physicians can use their hand-held devices such as Personal Digital Assistant (PDA), to access the clinical data repository and can view both the historical and real-time patient data such as laboratory result quickly and conveniently.

The concept of ubiquitous computing and the increasing usage of mobile devices motivate us to use mobile infrastructure to access health care applications. It is foreseen that Mobile Network Operators (MNO) play an important role in the life of a common citizen as they can track (user) location and provide appropriate location-based or even context-based services to their subscribers in a timely fashion.

The aim of this paper is to present an initial, yet a novel, approach to transfer the medical records of an individual by using the existing infrastructure to mobile operators. Although, in this paper, we restrict the applicability of the proposed approach in mobile network operators, it is possible to extend the infrastructure to other network operators e.g., WLAN provider with appropriate modifications. When distributing electronic clinical record to disparate locations, security is a major concern. It is mandatory to employ appropriate security measures to safeguard the privacy of medical information. These mechanisms include authentication, authorization, integrity, access control and privacy safeguards.

This paper is organized as follows: Section II gives a brief overview of related work, Section III presents the system architecture for exchanging medical records (EHR) and discusses the security issues involved, Section IV presents the initial prototype implementation of the proposed model and finally, Section V gives a summary of this research work and discusses possible future work items.

II. RELATED WORK

Medical services could largely benefit from the use of mobile devices and potential applications are numerous in this
domain. For instance, in the United States, PDA manufacturer Palm and a number of doctors are testing a project called ePhysician [16], in which doctors directly send prescriptions to pharmacists’ PDAs. Several groups are working at research level on mobile systems providing access to medical data. The Brigham Young University project “Poket Doktor” [21] allows a user to store EHR data on a personal electronic device and to communicate this data e.g. in a wireless manner with medical professionals when treatment is required.

Another research group has used DICOM [20] to develop a mobile client-server application for managing the information of the medical staffs. They have experimented WITH the usage of hand-held computers integrated through a wireless local computer network using the IEEE 802.11b standard [17].

The European Union has also been supporting mobile e-health projects such as HealthService24 [2] and MOBILALARM [3]. The HealthService24 project provides experimental results for the transmission of medical-monitoring results over wireless communication. This is useful in cases where patients, who need constant monitoring and are not in the hospital.

The MOBILALARM project introduces a mobile device that provides voice communication and location data. Once the user calls the service center, the device calculates the location using Global Positioning System (GPS) and transmits it to the service center. The service center can send, for instance, an ambulance to the user if necessary.

In the EU-funded project MTM [22] on mobile teleradiology systems [18], researchers have developed a mobile system based on the CHILI (joint project with the German Cancer Research Center in Heidelberg) software architecture, which provides a PACS (Picture Archiving and Communication Systems) for teleradiology. The European Union has also encouraged the electronic health card [12], [13], with which one can retrieve his medical records from a central repository by entering a PIN number through an eTEN project called Netc@rds [14]. Several European Union member countries such as Germany [10], [11], Italy [15] and Greece have already participated in this project.

In this context, much work has been done on securing the transfer of EHR information. Kambourakis et al. discussed in [4] the use of Public Key Infrastructure (PKI) and Attribute Certificates (AC) for accessing the health records in the back-end infrastructure (e.g., EHR transfer within the hospital network) using mobile networks, based on assumed trust model. It also analyzes the applicability of creating a secure channel using the Transport layer security protocol (TLS) [19] and evaluates them through experimentation results.

Although the above proposal seems attractive and effective in the context of security, it does not consider end user interactions and hence user EHR cannot be securely retrieved with this approach. However, this method could be extended to end-user interactions as well but it will need extensive certificate installations in end-user equipments. Moreover, usage of PKI in the mobile device is time and resource consuming and not effective.

A. The Generic Bootstrapping Architecture

The Generic Bootstrapping Architecture (GBA)[5] is a Third Generation Partnership Project (3GPP) [27] framework for mutual authentication of users and network applications. It describes the usage of a single authentication infrastructure for all the services, assuming the existence of service level agreement (SLA) between service providers and the network operator. It authenticates the user based on the long term credentials present in the Subscriber Identity Module (SIM) and the security of the GBA lies in the assumption that access to that long term shared secret is difficult.

![Fig. 1. The GBA reference model.](image)

Fig. 1 shows the GBA reference model with the Application Function (AF), Bootstrapping Function (BSF) and Home Subscriber Systems (HSS) communicating through appropriate reference points. To perform the service bootstrapping with the GBA, basically, the following sequence of actions will take place:

- Whenever the user agent (UE) requests the Application Function (AF), the AF informs the user to perform authentication with the bootstrapping function (BSF)
- The user contacts the BSF and in order to authenticate the BSF retrieves the credentials from the HSS
- The user and the BSF mutually authenticate each other using the specified authentication and key agreement protocol (AKA) and derive an application specific shared key
- The AF contacts the BSF, obtains the shared key from the BSF and authenticates the user, when requested

Note that for the protection of successive transactions, the AF and the user agent may derive the session keys from the shared keying material.

In the remainder of this paper, we analyze the usage and propose the applicability of generic bootstrapping architecture approach, in the context of secure EHR transfer.
III. MOBILE DELIVERY OF ELECTRONIC HEALTH CARE SERVICES

In this section, we present the architecture for secure mobile access of the electronic health care records. There are four logical components or sub-domains which are presented here, namely:

1) **User**, who requests his medical records to be sent to a particular hospital
2) **Network Operator**, who provides the platform for accessing the service and provides an identity for the user
3) **Service Provider**, who provides the service of storing, managing the user’s medical records
4) **Hospital**, which requires the medical records of the user in order to diagnose

Fig. 2 shows a Unified Modelling Language (UML) [28] use-case diagram depicting the functionality and the relationship of an integrated health information system from a top-down perspective. Integrated mobile health care services are based upon services offered by Mobile Network Operators (MNO), Service Providers (SP) and Health care providers (HP). Electronic health care services (EHS) are complex value-added services provided to the end user by many players. The MNO offers optionally Location Based Services (LBS) to the user which cooperates with the SP to find the nearest (or even context based) location of health care entities along with navigating instructions. It could also convey to the service provider the fact that the user will be hospitalized and his records will be needed. The MNO is assumed to know the user’s service provider and this could be achieved by means of subscription/configuration.

The SP is a central entity which maintains the patients’ record established by government organization such as National Health Service (NHS). It should distribute medical records on demand and it is also in charge of authorization (it makes sure that only the intended parties get the records).

In a typical scenario, HP is a hospital, which is interested in getting patients past track record. Before retrieving the records, it must also be able to authenticate to the SP in order to prove that it is the intended recipient. The hospital also distributes its own credential to health care practitioners such as doctors and nurses, which helps in maintaining the authorization level of each involved person. In special cases such as roaming scenario, the visited MNO will simply contact the home MNO for authentication and assists the user for further processing. However, to achieve that, the home MNO and the visited MNO must have trusted relationship with each other.

A. Overview of EHS Architecture

Fig. 3 shows the overview of the proposed EHS architecture and explains the relationship between the participating entities. A Service Level Agreement (SLA) is assumed to exist between the service provider and the mobile network operator, whereby service parameters are agreed upon in order to provide the EHS service e.g., allocating a special dial string for accessing the service, operating expenses, user identification, type, service duration and nature of the service etc. The user has an appropriate subscription with both the network operator and the service provider. However, the subscription between the user and the MNO allows the MNO to uniquely identify the user and the trusted relationship between the MNO and the SP allows the MNO to assert the identity of the user to the SP. When the service is accessed, the SP will provide a token to the user, which gives a reference to the user’s medical records. This token will be submitted to the hospital by the user and the hospital uses this token as a pointer to refer the user’s records.

The service provider and the hospital must mutually authenticate each other and communication between them must be protected by using a secure channel for exchanging the...
medical records of the user. One possible example could be to use Public Key Infrastructure (PKI) based systems, with Transport Layer security client certificate extensions. Note that Fig. 3 only gives a brief description of the functional architecture of the proposed system. The proposed system is presented, in more detail, in the following subsections B and C.

B. Applicability Scenario

In this section, we present the message flow model for the proposed system. The user is assumed to be in home domain i.e. he resides in the administrative domain of his MNO, where he has an account. When a user requests for electronic health care services via his mobile device, using the Generic Bootstrapping Architecture (GBA) [5], the MNO authenticates the user. This will result in creation of a shared key which will be shared between the SP and the user. The user initiates the record request to the SP and proves his possession of shared key, possibly, via a secure channel. The SP verifies the authentication of the request and if successful it responds with an authorization token to the user. The token used here could have any generic format e.g. it might contain identity information of user and service provider signed by the provider. One possible option to represent the token could be:

\[
\text{Token} = \{ \text{User Identifier, SP Identifier, Time, Validity, Other Info} \} \text{ Sig}_\text{SP}
\]

whereby the user and the service provider can be identified through the field User Identifier and SP Identifier respectively. The field Time represents the time at which the token has been issued, the time should have common reference like GMT to avoid synchronization problems. Validity shows how long the given token is valid and Other Info might contain additional information which may be user and/or service specific. The whole information should be signed by the service provider such that the token receiver can verify the information contained in the token.

This token is submitted to the hospital, where the hospital uses it as a reference to pull the records from the SP to diagnose the user. During this procedure, the hospital and the SP must mutually authenticate each other and the records will be sent as encrypted or sent through a secure channel.

As an optional step, the MNO can also supply the current location information of the requester to the SP so that the SP might also use this information and may help the user to find the nearest hospital, pharmacy etc. The user treats the obtained location information as a recommendation and has the freedom to choose the hospital.

Fig. 4 indicates the message flow model in the home scenario. The user activates the electronic health care service by sending a request to the SP. The user can request the service either by knowing the SP’s service URL beforehand or can be redirected by the network operator when a MNO URL was used (e.g. using web based access). In the redirection case, the user profile has to be configured at the MNO so that the network operator can identify the user, check his profile and redirect the query to an appropriate SP, when the user uses a certain address.

Since this service involve users’ medical record, which is sensitive and private information, it is necessary to employ appropriate security measures between the SP and the user. So whenever the user requests the service, the SP instructs the user to authenticate with his MNO by using the standard generic bootstrapping mechanism, which will authenticate the user based on his SIM credentials and will provide a shared secret between the user and the SP. Then the SP will request the MNO to retrieve the the shared secret, when required. By using this shared key, the SP can authenticate the user and can provide a token via a secure channel established between them or can encrypt the token using the key Ks derived from the shared secret.

If the location-based service is used, then the MNO will also actively involve in the communication and will provide the current location of the user so that the SP can find a list of the nearest hospital according to that user location which will be sent back with the response. The user submits the presented token at the chosen hospital. As an additional security mechanism, instead of derived key Ks, a new personal identification number (PIN) could be employed. This PIN will be user dependent, which is distributed during the initial subscription phase. The SP will apply cryptographic protection to the token using the PIN, so that the deemed user can obtain it whenever needed. The purpose of employing this PIN is to ensure the (authorized) possession of the token and cannot be forged even when the user’s mobile device is stolen.

After getting the token from the user, the hospital identifies the SP by examining the encoded pointer information in the token and contacts the appropriate SP. It is assumed that
the hospital will have appropriate PKI infrastructure, such that it proves its identity and authenticates to the SP before requesting the records (by submitting the token) from the SP. The information about the SP could also be associated with the given token. The SP validates the hospitals’ authenticity and the submitted token; if the Token is valid then the SP sends the requested EHR back to the hospital. As a final step, it might be necessary to update the EHR of the user to reflect his current status. So the EHR will be sent back to the SP later, the authorization to rewrite/append the information of the EHR is out of scope for this paper.

This architecture allows the possibility for the users to request multiple copies of medical records or even part of medical records, which can be sent to multiple hospitals for specialized treatments. It is highly possible that each hospital may need to update the record to reflect the current status of the user. For such cases, consistency check is required before updating the current medical record to ensure the integrity of the information. This is possible when medical based ontologies are put into practice, which will help to ensure standardization of data entry. However, the applicability to achieve this consistency technique is a separate research topic and left for further study.

Digital certificates can be used for mutual authentication and for securing the communication channel between the MNO and the SP and between the SP and the hospital where the Transport Layer Security (TLS) or Secure Socket Layer (SSL) can be used. Also, it is applicable to use Web Services based communication to transfer EHR by which it is possible to employ more sophisticated security mechanisms. For instance, only sensitive parts of the user record can be encrypted, using XML Encryption [23] and/or can be digitally signed using XML Signature [24].

In some cases, the user might not be in the home domain, e.g. when he is attached to a different network. The procedure for obtaining EHR is the same as in the home scenario case except that the visited MNO has to contact the home MNO for authentication. After successful authentication, the user contacts the SP in the home network with an authenticated service request. However, there are some deployment difficulties in such roaming scenarios. The token format has to be standardized across all the countries where such EHR-delivery is deployed. Moreover, it is assumed that appropriate PKI relationship exists between the requesting hospital and the SP.

C. Security Considerations

In this section, we describe the overall security features for the proposed secure access of EHR model. In this context, security can be visualized in three different layers namely access layer security, core network security and service level security, as depicted in Fig. 5.

The interfaces between the network and the service providers are assumed to be trusted. If the trust is not sufficient, they may employ security standards such as [29] to bootstrap necessary security associations. This leaves us only with the user interfaces interfaces such as the interface between UE-MNO, UE-SP and UE-Hospital.

- **UE-MNO Interface:** During the network attachment procedure, the security context between the mobile device and the access network is established [9]. This encompasses security services for lower layer like confidentiality, Integrity etc., which provides a secure communication platform for the mobile devices.

- **UE-SP Interface:** In the core network layer, we use GBA mechanism with which the users can bootstrap security association with any services. In the service layer (SP), application specific security measures can be employed e.g., HTTP with Digest and TLS by using the credentials supplied by the aforementioned core network layer.

- **UE-Hospital Interface:** This interface typically uses near field communication (NFC) such as bluetooth, Infrared and it is assumed that appropriate security mechanisms are employed to provide secure transmission of token information.

Furthermore, this proposal has the following security features,

- **Authentication:** The proposed scheme recommends to use strong authentication schemes (e.g., 3GPP AKA), which is based on SIM card credentials, in order to achieve mutual authentication between the user and the MNO. This hinders the adversaries to launch spoofing attacks. This mechanism further recommends to employ a PIN to unlock the token, which provides additional protection for the cases where the mobile is stolen.

- **Preventing Token Masquerading:** It is of interest for the attackers to manipulate the token and try to retrieve the sensitive medical records, which in tum violates the privacy of the subject user. To combat with the threat, the proposed token employs standard digital signature schemes (sighting the content with the private key of the SP) together with the validity period. The digital signature proves the integrity of the token and the validity period helps to protect the token from replaying the records at a later time.

- **Resistance to Man-in-the-Middle attacks:** There are several threat scenarios where the attacker may act as a man-in-the-middle (i.e., acting as a server to the client and vice versa) in order to retrieve the token(s) and later use them to retrieve the user records. So it is necessary for the client to authenticate the SP in order to avoid such attacks. When the UE communicates with the Application Server (AS) of the SP, it shall establish a TLS connection with it e.g. if it is web based access, the protocol HTTP could be used to trigger the TLS establishment. The AS is authenticated to the client by means of a public key certificate and the associated signature. The UE should verify that the server certificate corresponds to the Fully Qualified Domain Name (FQDN) of the AS, in-order to avoid man-in-the-middle attacks. No client authentication is performed as part of TLS (no client certificate neces-
sary) connection establishment. In the web based scenario mentioned above, the client will send HTTP messages within the TLS session and to authenticate the client, the service provider fetches the shared secret from the network provider and notifies the client with “unauthorized” error message with corresponding challenge to the UE. The UE calculates digest as described in [30] and sends it as a response to the service provider. This serves as client authentication.

- **Confidentiality:** In order to avoid unauthorized persons to have access on the EHR, it is necessary to provide confidentiality protection for the communicating hosts. To facilitate that, the communication channel between the involved entities must be established via a secure connection (e.g TLS).

From a security perspective, authorization for users to access the particular resource with fine granularity is a prime concern. So it is necessary that the network infrastructure or the service platform should support the authorization policies in a flexible manner. In our approach, we classify the authorization policies into:

1. **Application Policies:** service specific policies, supposed to be configured by the service provider.
2. **User Policies:** users may configure their own policies, scoped to a particular service. Users might create rules to satisfy their own privacy constraints.

Authorization polices are typically composed of sophisticated and complex rules, in such a way that the rules expressed in the policy might apply specifically to an access network, users or to a device.

Here the Hospital is a special entity, which communicates with the service layer to obtain certain information about the user. The communication between them is secured by using PKI based mechanism. Although, the communication between the SP and hospital is secured by strong cryptographic mechanisms, there is a need to control access of resources within the hospital. Since the hospital is involved in critical document management system, it must ensure that only the privileged users should be able to access the medical records. This can be guaranteed by employing existing authorization mechanisms such as Role Based Access Control (RBAC) [6], [7], [8] into the hospital’s access control infrastructure.

For authorization, access control model can be enforced within the hospital according to the designated policies, especially, the RBAC since it eases in scalable authorization management. This is because users receive permissions only through the roles and roles are quite stable while users and permissions are tremendous and may change frequently. For instance, the doctor is allowed to access the user’s record while the nurses cannot. RBAC guarantees that only authorized or legitimate users, even if they are not previously engaged with a particular system, are given access to protected data or resources. On the other hand, attribute certification offers a straightforward and consistent method to extend identity-based public-key certification infrastructures to support role-based authorization policies. Towards this direction, it permits decentralized authorities to manage identities, role affiliations and permissions, as well as other authorization-related objects.

Since the communication involves sensitive data, privacy of the user must be considered. In our model, we ensure the user privacy at different levels. By encrypting the information during the communication, the confidentiality protection of the medical records is provided. Moreover the user can also configure his privacy policies, we term it as “user policies” at the service provider in order to authorize certain entities to access his sensitive data.

### IV. IMPLEMENTATION

In this Section, we describe the prototyping efforts for the aforementioned approach, as proof-of-concept. Since we don’t have appropriate real-world infrastructure (like base stations) to study the feasibility, we evaluated the proposed mechanism in our test bed by using four workstations fulfilling the functionalities of user, MNO, SP and hospital respectively.

The nodes were equipped with IEEE 802.3 network card and supports IPv4. The Ethernet connection is established through the local network using a cable link. The entities user and the MNO are pre-configured with appropriate parameters, and the entities SP and the Hospital are sufficiently configured to run SSH tunneling between them.

Fig. 6 shows the test bed setup for the proposed system. The user entity performs authentication and key agreement with the MNO entity, using a publicly available Internet Key Exchange (IKE) [25] implementation [26]. IKE is run using the pre-shared-key. Although GBA uses AKA, we use IKE in this proof-of-concept since IKE is already available in SuSE Linux 9.0. Moreover AKA and IKE conceptually perform similar functionality and hence IKE was used as an alternative. The key resulting out of this process (\(K_{\text{aka}}\)) is sent to the SP from the MNO.
The user and the SP use K_AKA for authentication of EHR-request, which is signaled by using HTTP(s) protocol with digest based (only user) authentication enabled. TLS is bootstrapped beforehand, between the two entities, for enabling confidentiality protection of the token information. Once the service request is authenticated, the EHR is sent as encrypted to the hospital. The EHR information is sent over SSH tunnel between the two entities.

Note that, although we have not provided a real world implementation, the scheme proposed in this paper has been successfully verified using our in-house test bed set up. We believe that the current set up is good enough, at a higher level, to evaluate and to further refine the work.

V. SUMMARY

With the boom of mobile networks/devices, many interesting and new applications (e.g., E-Tourism, E-Health etc) have appeared in the recent past. Of that, health services are one of the most important services since it plays a vital role in driving improvements in the quality, safety and efficiency of healthcare for a common citizen. However, such a service require high reliability, secrecy and data protection due to the involved sensitive data.

In this paper, we are interested in investigating the feasibility and implementation of a secure architecture whereby end users are able to query and distribute their electronic health records to appropriate entities say, Hospital.

To achieve that, we have analyzed the applicability of the 3GPP generic bootstrapping architecture in order to perform authentication of the users and to bootstrap the security credentials between the users and the EHR service provider. However, the applicability of this approach is not limited and can be extended to public key based infrastructures as well. Also, we developed a prototype implementation of the proposed system to analyze the feasibility of the model and as a future work we planned to examine and review the current model. Furthermore, we have planned to investigate and analyze the protocol relevant details for each interface, discussed in our model as presented in Section III, to concentrate on optimization aspects and to propose minimal extensions and/or modifications, if necessary, in order to improve the proposed approach. It is important to mention that the applicability and scalability of the proposed approach, especially in roaming scenarios, has to be further studied and evaluated.

There are certain limitations for the proposed approach. For example, when the user is not the owner of the device, then wrong EHR records will be sent. Especially, in emergency cases, when a person calls for EHR service using an arbitrary mobile device then the correct EHR documents will not be retrieved. For such scenarios, manual assistance is required for delivering the appropriate EHR.

ACKNOWLEDGEMENTS

The authors would like to thank Jorge Cuellar and Tiago Gasiba for their useful, constructive and insightful comments on the manuscript. The authors would like to thank Hariharan Rajasekaran for his review.

REFERENCES


[27] The 3rd Generation Partnership Project (3GPP) http://www.3gpp.org/

