Secure Solution for Mobile Access to Patient's Health Care Record

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

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

Abstract— **Mobile devices are today widely accepted and their capability to provide access to services independent of user time and location make them well suited for provision of healthcare services to both patients and healthcare personnel. However, mobile services are still not generally allowed to operate with highly sensitive and personal data, mainly due to the lack of a defined security standard, low protection of data transferred through the mobile and wireless network and no standard and widely accepted user authentication method that ensure confidentiality. In this paper we propose a secure solution for mobile access to Electronic Health Record (EHR) systems. The proposed solution enables secure authentication and communication between a mobile device and a healthcare service provider through usage of a two-factor authentication method on a mobile phone and encryption. The proposed solution is independent of mobile network provider and type of the mobile device the application is running on, and provides multifactor authentication without the traditional requirement that the user has an additional authentication token. This simplifies use without compromising security. In the paper we present the usage scenarios, discuss the feasibility of the proposed solution together with its limitations, and present results from a prototype test bed.**

Keywords- information security; mobile communication; health information management.

I. Introduction

Recent developments in mobile and communication technologies enable implementation and deployment of various services that can be accessed over mobile devices, as voice, multimedia and data services. Utilizing mobile services in the healthcare sector can significantly improve efficiency and quality of health care delivery to a common citizen as shown in [1][2][3]. Some of the areas where mobile services are starting to be utilized today are: on-the-spot emergency, home care and situations where a care provider does not have a fixed place of work, or need to look up relevant information resources such as clinical guidelines [4]. However, the prerequisite for wide deployment of mobile healthcare services is to resolve security issues regarding protection of patient's private data. Information that is exchanged between a user and a service provider represent highly personal and sensitive data that must be protected from intruders and non-authorized parties. Limitations of the mobile terminals and mobile networks (e.g., the high cost for cellular communication links, limited data transfer rate of the mobile telephone system, limited availability of mobile Internet connectivity, many different mobile platforms [5]) are additional constraints that must be addressed when developing of a mobile security solution that is both user friendly and easy to implement in real life systems.

New security solutions in the area of mobile and wireless technologies have been emerging in recent years. The examples are development of technologies such as: Smart Cards, USB iKeys [6], SIM toolkit [7], and One-time password generators (e.g. Digipass [8]) that facilitates authentication on mobile device. Some projects report development of hardware solutions for faster performance of demanding processing functions on mobile devices, such as cryptographic operations [9]. Additionally, numerous research studies are utilizing already developed security mechanisms and adapting them for mobile devices and their limited capabilities [10][11]. Through these efforts it can be seen that mobile devices are becoming more secure and powerful, and today they possess capabilities to provide a high level of security for utilizing mobile services. However, there is still no standard and widely accepted security solution for utilization of mobile services in healthcare systems.

The aim of this paper is to present a novel approach to securely transfer medical information from Electronic Health Record (EHR) to a patient or healthcare provider at the point of need. The proposed security architecture is independent of the mobile network provider and the type of mobile device the user is using to access the healthcare service. Additionally, during development both security and usability requirements are taken into consideration.

This paper is organized as follows: Section II gives a brief overview of related work, Section III presents detailed description of security architecture for mobile access to information from EHR and its security features, Section IV describes implementation details of test environment, Section V describes results from security architecture prototype testing and Section VI gives a summary and conclusion of our research.

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

978-1-61284-696-5/11/$26.00 ©2011 IEEE

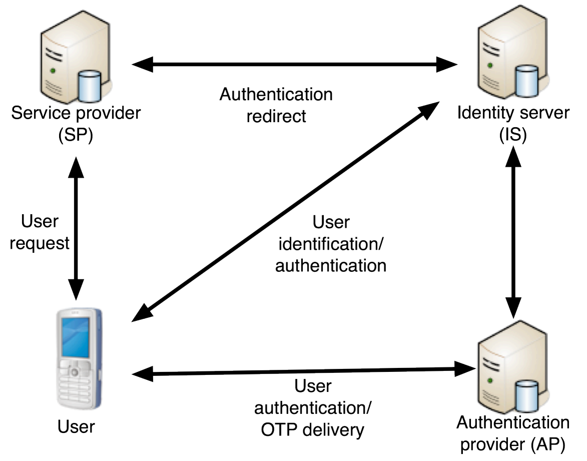


Figure 1. Reference model of security architecture for mobile access to information from patient's medical record

II. RELATED WORK

During the last few years there were numerous projects addressing utilization of mobile devices for provision of healthcare services to patients and healthcare providers. However, only a few also addressed security issues of mobile access to healthcare information.

In [12] it is described a system that performs authentication of the user through a two level operation. The first level of authentication is between the user and the device through a strong PIN number. The second level of authentication is between the user and the application and is achieved by using a digital certificate and a strong password. An appropriate Public Key Infrastructure (PKI) system is implemented and managed to provide certification service. Using PIN numbers and passwords represents a more convenient, platform-independent solution, but using just static passwords does not provide enough security for healthcare services because the system becomes vulnerable to brute force attacks. Additionally, introduction of certificates can ensure higher level of security but at the same time it can greatly influence system scalability and complexity because the certificates must be installed and maintained on every client device.

In [13] it is presented an architecture that enable secure transfer of patient's medical records using the existing infrastructure of mobile operators. The Mobile Network Operator using Generic Bootstrapping Architecture (GBA) performs authorization of the mobile device user, while authorization of the other participant in the communication (service provider, hospital, and network operator) are performed through usage of PKI. Private communication is enabled using encryption and digital signatures. Additional work of improving GBA architecture to provide higher level of security and privacy for healthcare applications is explained in [14]. Utilizing standard security mechanisms of mobile networks and providers enables benefits, such as easy implementation and utilization of a proven secure solution. However, it also introduces the issue of cooperation between service provider and mobile network provider and defining privacy and security policies regarding protection of patients' private data while transferred and managed outside the secure environment. In each country there are usually numerous mobile network providers and for health services to be available to all potential users multiple agreements and policies must be set and agreed upon between different parties. For this reason we see the need for development of a security solution that is independent of mobile operator and device manufacturer, and in this manner more accessible for majority of potential users.

III. SECURITY ARCHITECTURE FOR MOBILE ACCESS TO INFORMATION FROM EHR

In this section we present the architecture for secure mobile access to EHR.

A. Reference model

Fig. 1 shows the proposed architecture reference model with four logical components:

1) *User* with installed mobile application on his/hers mobile phone, who requests information from private medical record. The user can be both patient and health provider.

2) *Service provider* (SP), who provides the service of storing and managing the patients' medical record.

3) *Identity server* (IS), who performs authentication process for the SP.

4) *Authentication provider* (AP), who performs authentication of the user through a second communication channel and delivers One Time Password (OTP) used to authenticate user with the IS.

The SP is a central entity, which is usually Hospital Information System (HIS) that stores and maintains the patients private data regarding health status and medical records. The SP should enable access to the medical record to authorized users and ensure protection of sensitive data during communication and storage.

For performing user authentication the SP utilizes services from the IS, which stores all identity information about the users and decides what security mechanism should be used during the user authentication process. If the SP provides more than one service to the users, the same IS can be used to provide different authentication mechanisms depending on the type of service requested, type of user requesting the service and/or type of the communication channel. The IS can be part of the HIS, or it can be a third party provider. In the latter case there should be set Service Level Agreement (SLA) between two parties to ensure trust and cooperation rules. Communication between two entities must be protected utilizing a secure encrypted channel.

The user performs authentication to the IS by providing user credentials and an OTP. The OTP is sent to the mobile application through a second communication channel initiated by the AP. In our proposed security architecture the AP represents server from Encap Confirm-by-PIN security solution [15][16]. The main characteristic of the Encap Confirm-by-PIN solution is that it provides two-factor user authentication software for mobile phones and enables client authentication independent of the phone model and the mobile network provider. More details about the authentication process will be described in next sections.

The user must have an appropriate account on the IS, AP and SP. He/she is uniquely identified by accounts on the IS and AP, and when the user is successfully authenticated the IS can assert the identity of the user to the SP. When the authentication process is performed successfully, the IS sends user's unique identifier to the SP that can be used as a pointer to refer to patient's medical record information.

All communication between the AP and the IS and between mobile application and the IP, AP, and SP must be protected using a secure encrypted channel.

B. Communication flow

Here we give a more detailed description of communication flow during authentication process. The message flow model is depicted in Fig. 2. On the right side of the figure are presented authentication benchmark tasks in the context of message exchange process. We used marked tasks during prototype performance measurements to identify speed and bottlenecks of authentication process. More details about tasks are described in section four.

The communication starts with establishing a secure Hypertext Transfer Protocol Secure (HTTPS) connection between the mobile application and the SP. During the establishment of secure channel the SP is validated through the certificate and both communication parties agree on the type of encryption and length of the keys that will be used to protect data during communication [17]. When the communication channel is set, the user sends a request for private data from the medical record system. The SP checks if the user is already authenticated and if not redirects the request for authentication to the IS. The IS initiates an authentication process as defined in the cooperation agreement between the SP and IS and sends request for the user's credentials to the application to identify the specific user. The user provides the credentials: typically MSISDN and an organization identifier (orgID). MSISDN is a number uniquely identifying a subscription in a GSM or a UMTS mobile network and the orgID is used to identify the type of the user. When the IS receives user's credentials it sends a request to the AP to start a second authentication channel with this specific user. As a result it receives a challenge identifier that uniquely identifies the authentication session. The IS then sends request for an OTP to the application. When the AP receives the request from the IS, it performs a SMS push to the specified mobile client, which creates a new communication channel between the mobile application and the AP. Through established communication channel the AP sends challenge to the mobile client, together with two encryption keys that are used for decryption/encrypting of client reference stored on the device. The user is afterwards prompted to input a secret PIN number in the mobile application which is selected when the mobile application and the Encap user account (Mobile ID) is activated. Based on the inputted PIN number, the International Mobile Equipment Identity (IMEI) and the client reference from previous authentication or activation session (decrypted using received decryption key) a security code is reconstructed on the mobile application. The challenge previously received from the AP is encrypted using the generated security code and sent back to the AP where it is verified. After encrypted challenge is sent to AP all private data is deleted from the mobile device except client reference that is stored but previously encrypted using encryption key received from the AP. If the verification is performed successfully the OTP is generated on AP and sent back to the mobile application. The user is allowed to input the invalid PIN number three times, after which the Mobile ID account will be locked and it must be activated again for the mobile application to be operational. If the PIN is inputted correctly, the mobile application receives the OTP from the AP and forwards it to the IS as a response to the previously sent OTP request. The IS checks the OTP against the AP together with the challenge identifier (received in previous stage when the AP is initially called) and if both parameters are correct the user is successfully authenticated. The result of the authentication process is forwarded to the SP, together with the user's unique identifier if the authentication is performed successfully. Based on the unique identifier the SP finds the patient's private medical information and sends it back to the mobile application through the secure channel. All further communication is performed through the secure HTTPS channel, and the communication session lasts until the user sends a logout request or the mobile application is left running with no user input for more than 20 minutes.

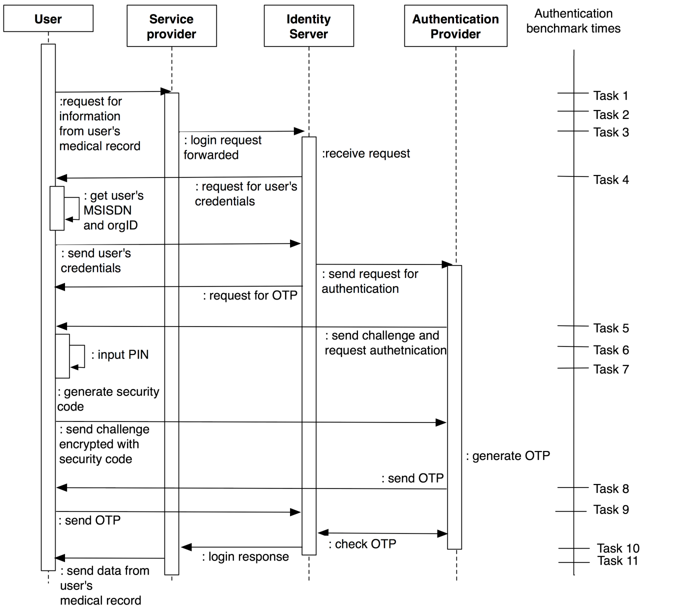

User
Service provider
Identity Server
Authentication Provider
Authentication benchmark times
:request for information from user's medical record
: login request forwarded
:receive request
: request for user's credentials
: get user's MSISDN and orgID
: send user's credentials
: send request for authentication
: request for OTP
: send challenge and request authetnication
: input PIN
: generate security code
: send challenge encrypted with security code
: generate OTP
: send OTP
: send OTP
: check OTP
: login response
: send data from user's medical record
Task 1
Task 2
Task 3
Task 4
Task 5
Task 6
Task 7
Task 8
Task 9
Task 10
Task 11

Figure 2. Message Flow Model

C. Security Considerations

In this section, we describe security features enabled in the proposed architecture.

1) Authentication

The proposed scheme provides two-factor authentication of the user over both communication channels. On the main communication channel, the user is authenticated by something he/she knows (PIN number), and something that he/she has (the mobile application that creates the second communication channel and receives a unique OTP). For user authentication on the second authentication channel a challenge string received from the AP is encrypted using a security code constructed on the mobile device based on the user's PIN code (something that user knows), IMEI (a number identifying the mobile terminal, something that user has) and a reference from a previous authentication session (insurance that the application is activated and user is registered). Activation of the second authentication channel using a SMS push mechanism adds one extra authentication factor in the authentication mechanism (user must have his/hers own SIM card to be able to receive activation SMS). In this manner the user is protected against losing his/hers mobile device, SIM card or compromising the secret PIN number. Also, the proposed authentication mechanism provides protection from copying application data to other device because just data on the device is not enough for performing successful authentication. Disabling the user account after three unsuccessful authentication requests with the wrong PIN number protects the application against a brute force attack on the stolen device. The user is also given a possibility to manually contact the SP and cancel his/her account if the mobile device is stolen.

The server is verified through the certificate that is sent during setup of a secure communication channel. In addition to the valid certificate, implementation of the mobile application should verify that the credentials on the server certificate correspond to the Fully Qualified Domain Name (FQDN) of the server. In general, web browser applications do this automatically but some mobile developer platforms do not perform this security check by default.

Performing described strong authentication process in combination with a unique ID, enables protection against man-in-the-middle attacks and provides high level of insurance that the user and the SP are communicating with a trusted party.

2) Confidentiality

The proposed security architecture enables protection of private data during client-server communication through utilization of the secure encrypted channel. Some of the vulnerabilities of the HTTPS that are known (e.g., using weak communication protocol, inappropriate cipher suite and short encryptions keys [18][19][20]) can be overcome by implementing additional verification on client and server application level. For instance, Java Platform Micro Edition (Java ME) provides support for HTTPS communication and additional verifications of encryption algorithms, cipher suits, and server credentials on the client side. Also, servers such as Tomcat and Apache can be configured not to accept weak cipher suites and short key lengths.

The additional confidentiality protection mechanisms must be implemented on the point where data are stored. In the proposed architecture no private data are stored on the mobile device so additional encryption locally on the mobile device is not required. All users' private medical records are stored on the SP side, which is usually a HIS that implements strong security mechanisms for protecting data storage and ensures protection against network and physical access by intruders.

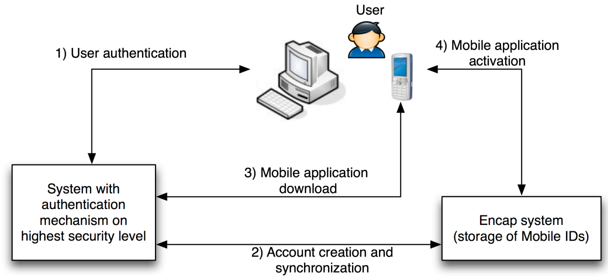

User
1) User authentication
4) Mobile application activation
3) Mobile application download
System with authentication mechanism on highest security level
Encap system (storage of Mobile IDs)
2) Account creation and synchronization

Figure 3. Proposed solution for mobile application download and activation process

During authentication process using proposed Encap Confirm-by-PIN mechanism client reference is stored locally on the device as described in the previous section. Stored data are protected with AES encryption, where encryption key is changed for each authentication session enabling on this manner easier notification of possible attacks. Also, even if an attacker succeeds in decrypting the client reference, it is still needed additional information to perform successful authentication, making possible attacks even more difficult.

3) Integrity

Besides protecting the patient's medical record against unwanted disclosure, the private data must be protected against unwanted modification and deletion during transfer and storage. Utilizing a secure HTTPS communication channel during communication between the parties enables integrity protection of the messages transferred.

The mobile application installed on the device must also be protected against unwanted modification. The Java ME platform provides option for the SP to sign the mobile application with its private key and in this manner assure the user that the application comes from the trusted provider, and that no one can make any modification on it.

4) Protection against session hijacking

When two parties are authenticated the user is provided with a session identifier (created during a HTTPS handshake protocol), which identifies the communication session. The session identifier is protected against session hijacking by encryption and a limited session duration period. The servers used in the architecture can implement additional protection against session hijacking. For example, a Tomcat server can be configured to use an additional session cookie that is protected against modifications in the message header just for HTTPS connections.

Additional protection of the authentication session established over two communication channels is performed by using challenge attributes. In both authentication processes the client is required to provide both required credentials and previously received challenge identifiers.

5) Private laws

The security architecture must meet local privacy requirements to be feasible. In the following we provide a short description of Norwegian national security requirements regarding private data security and discuss how the described architecture complies.

Norway adopted the National Strategy on IT-Security on July 2003, which aimed to reduce vulnerabilities related to information system and networks and promote a culture of IT-security and electronic commerce [21]. For protection of private medical data it is required that the security for a user authentication be on the highest (fourth) security level [22]. The highest security level requires usage of systems based on PKI that meets requirements for user authentication, identification, signature and encryption defined in [23].

Because Encap Confirm-by-PIN security solution do not support PKI and storage of user's private certificate using just the proposed architecture would not comply with requirements set for highest security level. Because of the requirement for user certificates, we propose using one of the authentication methods that is based on PKI and approved to be on the highest security level for the application download and activation process, including creation of a derived Mobile ID. When using this approach it is needed that the Mobile IDs are synchronized with the user's account used for download and activation, so if second account is compromised first account must be immediately blocked. Thus, the SP will issue and store PKI certificates linked to the authentication account – thereby satisfying the PKI-requirements. The proposed solution is illustrated on the Fig. 3.

6) Usability

Having in mind that possible users of proposed architecture are health personnel and patients, our goal was to develop a security solution that is easy to use and provide two factor authentication without requirement of any additional security token. From previous research we have seen that utilization of tokens and security cards is not well received by users [24], and implementing and managing these systems can be very expensive and demanding for a SP. Therefore we propose security solution that is independent of mobile network provider and mobile device manufacturer and can be used on any mobile and wireless network as long as user has installed and activated the application on his/her mobile device.

IV. Implementation

We developed a mobile application and a server architecture test bed to simulate the proposed solution, prove its feasibility and evaluate performance. To show how a general security solution could be adapted to a specific real life HIS we used a description of the security architecture of the University Hospital in Oslo as a platform for implementation of the proposed security mechanisms.

For development of the mobile application we used Java ME environment. The main reasons for choosing Java ME as developer platform for the mobile application are: portability of Java code and wide implementation on almost all mobile platforms, possibility to process data locally on a mobile device and reduce network traffic, and possibility to implement a flexible application level security solution in accordance to previously described security architecture. The Java ME Mobile Information Device Profile (MIDP) 2.0 specification adds support for creation and usage of HTTPS connection and enables mobile application signing. Additionally, in Java ME each application is restricted to operate in a sandbox in that manner protecting signed application and it's resources against unsigned and other signed applications. For implementing proposed user authentication method we utilized Encap Confirm-by-PIN API libraries that are integrated in the mobile application.

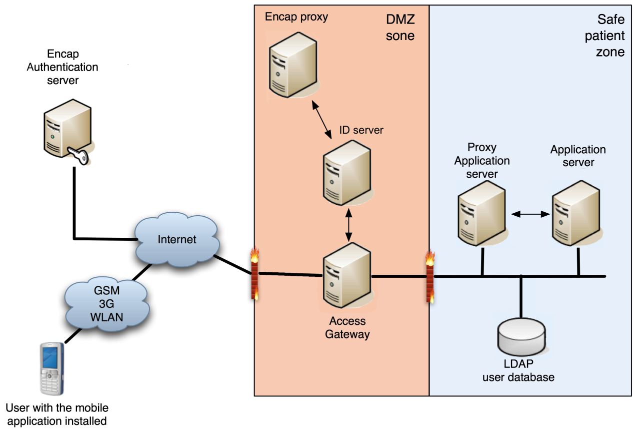


Figure 4. Security solution experimental setup

For server side implementation we used the XenServer server virtualization platform that provides us with capabilities required to create and manage a virtual infrastructure. Fig. 4 shows the implemented architecture on the XenServer platform. The server side is divided in two zones: a Demilitarized Zone (DMZ) and a safe patient zone. Access Gateway server, Identity server and Encap proxy server are located in the DMZ zone. The Access Gateway and Identity Server are implemented as components of the Novell Access Manager Server. The Access Gateway presents the only entry point to the HIS and it first checks all users requests and decides if access to other servers is permitted. The ID server performs authentication of the user for the Access Gateway, the same role as described before for the IS. The Encap proxy server is implemented on a Tomcat server and is used as a proxy in communication with Encap Authentication server that represents the AP in our test environment. Because the ID server is implemented in the HIS environment there is no need to make additional SLA agreement with a third party entity for offering functionalities of the IS. The only SLA agreement needed for real life implementation of proposed test environment is regarding cooperation and communication between the HIS and the Encap Authentication server.

Servers that manage data from patient's private medical record and a user database are located in the safe patient zone. The Proxy Application server is used to collect data requested from the mobile application and format them before sending a response. The Application server represents the HIS application platform, which store patients' private data, and can be accessed by different proxies that are used by different healthcare services. In our test bed we developed Proxy Application server in Java platform and deploy it on a Tomcat server, and used the Application server installed on Microsoft Server 2008 developed in previous phases of the project.

TABLE I
TIME NEDDED FOR AUTHENTICATION PROCESS TO BE COMPLETED USING THREE COMMUNICATION NETWORKS

Authentication step	Time [standard deviation] in seconds		
	2.5G	*3G*	*WLAN*
1) Request for information from medical record sent	0 [0]	0 [0]	0 [0]
2) Response to the Access Gateway regarding authentication method	6.1 [0.69]	4.9 [0.25]	4.1 [0.91]
3) Redirect (request sent to the ID server)	11.1 [1.22]	7.1 [0.83]	5.1 [0.94]
4) MSISDN and orgID request received from ID server	13.8 [1.34]	8.3 [1.1]	5.5 [0.93]
5) SMS Push received	26.5 [2.43]	15.6 [1.26]	14.1 [1.21]
6) Request for user to input PIN number	27.0 [2.42]	16.1 [1.25]	14.6 [1.24]
7) PIN number inputted	32.9 [2.12]	21.8 [1.15]	20.0 [1.36]
8) OTP received from the AP server	39.4 [2.61]	25.8 [1.14]	22.4 [1.34]
9) OTP sent to the ID server	42.2 [2.67]	27.6 [1.6]	23.8 [1.21]
10) Request with identity assertion sent the Access Gateway	43.2 [2.67]	28.1 [1.62]	24.1 [1.22]
11) Retrieval of originally required content (user authenticated successfully)	49.1 [2.89]	31.3 [2.04]	25.8 [1.24]

Additional protection of medical private data is implemented through two firewalls that implement strict access rules for both DMZ and private patient zone.

V. RESULTS

In this section we show test results from the implemented security architecture test bed. The tests were performed on a Nokia N95 phone with Internet access. In the HTTPS connection between mobile device and the Access Gateway it is utilized cipher with encryption algorithms: RSA algorithm for key exchange, AES with cipher block chaining with 256 bit session key for data encryption and SHA for message digest.

A. Performance measurements

Table 1 and Fig. 5 show the time needed for the authentication process to be completed (mean value of ten measured times with standard deviation value shown in brackets). For Internet access we used 2.5G, 3G and WLAN networks. The benchmark tasks are set to illustrate how much time is needed for different phases of the authentication process (described in the section three and Fig. 2) to be performed and help us to identify possible bottlenecks.

From the results we can see that the time needed for authentication is 49.1 seconds for 2.5G network, 31.3 seconds for the 3G networks and 25.8 seconds for the WLAN networks.

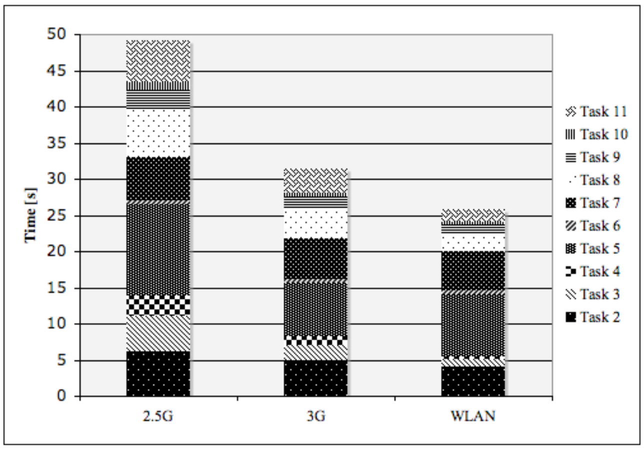
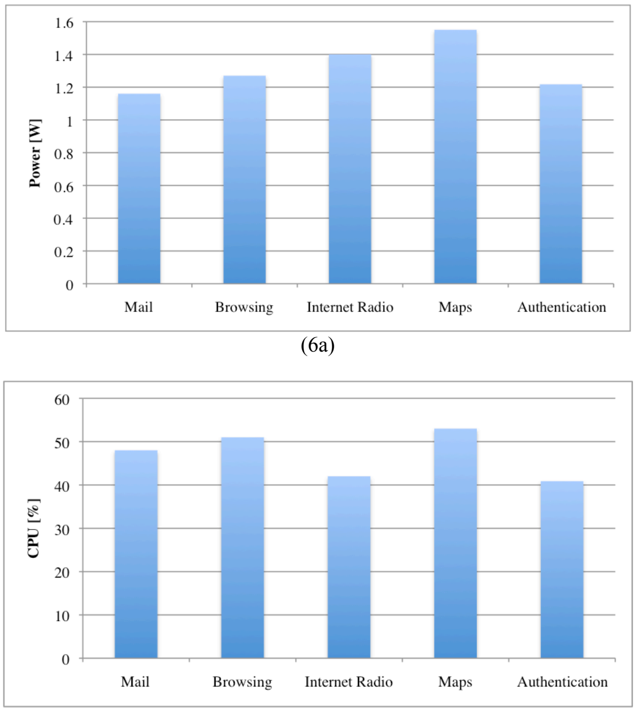


Figure 5. Graphical presentation of time needed for each step of authentication process to be completed

To evaluate measured performance in the context of current web systems that require multifactor user authentication, we measured time needed for authentication of the user to a bank web site over a browser on a PC. We recorded time needed for user to find and show the initial page, input username and password and input the OTP received over SMS on the mobile phone or read from the card. The average time was around 50 seconds for the authentication using the SMS and around 1 minute for the authentication using the code from the card. As a conclusion we can say that a similar time frame is needed for authentication of the user to our proposed security architecture using 2.5G networks as is needed for the web site that requires multifactor authentication. When utilizing more advanced communication networks such as 3G and WLAN the speed of authentication is even faster than over the web. As a future work, test with potential users could be performed to check acceptance of the proposed authentication procedure and additionally validate if time required for user authentication is acceptable for everyday use.

From the measured results we see that the largest amount of time is needed for starting second authentication channel (waiting for a pushed SMS message), and receiving the OTP from the AP. Sending and receiving a SMS message depends on the type of SMS gateway used and current mobile network traffic load. This time can vary, but in general it lasts a couple of seconds as we anticipated. The OTP password generation process is expected to last some time because it involves computationally intensive encryption calculation on both mobile client and server side.

We noticed that there is some additional communication overhead for traffic received from the Access Gateway and the ID server, which is not required for our application. The main reason for this is that the Novell Access Manager used in our test environment is more adapted for usage with a web browser and not optimized for a mobile communication. Additional improvements and optimization of the servers can be implemented to overcome this unnecessary workload and optimize the communication process. For example, there is no need for the ID server to send complete authentication form when requesting user credentials (MSISDN, organization ID and OTP) because the received form is not showed in HTML



(6a)

(6b)

Figure 6. Graphical presentation of power consumption (6a) and CPU load (6b) on the mobile device for different mobile applications

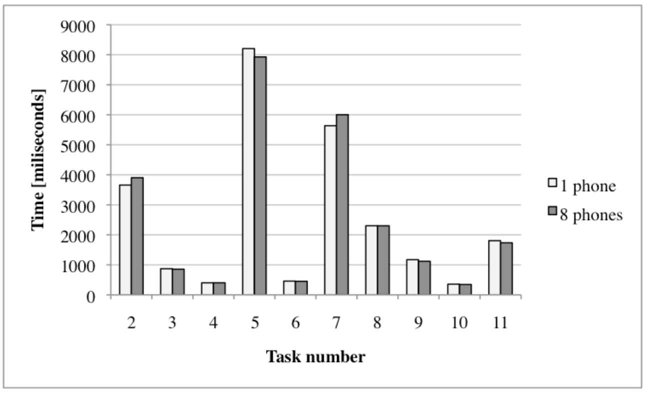


Figure 7. Graphical presentation of authentication tasks times with different loads on the proposed security architecture

format to user. Better approach would be just to send HTTPS request/response with specific parameter that would inform the mobile application to send the required information. In this manner the amount of communication content could be decreased.

Additionally, we saw that authentication of the user over second authentication channel could be optimized without decreasing security. The AP could send the notification when the user is successfully authenticated over second authentication channel directly to the ID server (or Encap proxy in our test environment) instead of sending OTP to the mobile client that must be then forwarded to ID server and additionally verified on the Encap server again. The mechanism we used in our testing environment is implemented with delivery of an OTP to the mobile client because original usage of Encap Confirm-by-PIN mechanism was to provide OTP generator that should be used for two-factor authentication of the user in a web application. In the newest version of the Encap Confirm-by-PIN mechanism authentication is besides original implementation provided also without OTP delivery. Using new capabilities of Encap Confirm-by-PIN mechanism in our security architecture can additionally fasten authentication process because some of communication could be omitted.

B. Processing in the mobile terminal

We measured the power consumption and CPU load on the mobile phone when the authentication process is performed. For capturing data it is utilized Nokia Energy Profiler Tool. From the results we saw that power is mostly consumed for communication with the server side as expected. In the mean time when the application is processing data locally the power consumption is lower. For comparison purpose we measured also power consumption and CPU usage on the phone when running mail, web browser, Internet radio and map application and the average values are presented on the Fig. 6. As a result we can see that the average power consumption and CPU load for the authentication process are similar or lower compared to other applications. We conclude that the power and memory consumed on the mobile device while performing authentication is not problematic, and the authentication process is not more demanding than running any other standard mobile applications that use Internet connection.

C. Performance with different server load

To test scalability of the proposed system we measured time and resources for authentication when servers were performing eight authentications in the same time. We compared the results to performance when just one user is authenticated and a graphical presentation is showed in Fig. 7. In the figure it is presented times needed for each step of authentication process (times are mean values for ten measures) when authentication is performed by one and by eight users. From the results we conclude that time needed for authentication in these two cases vary very little. Eight simultaneous authentications do not provide measurable difference in server load, and confirms scalability of the system.

We recognize the limitation of the presented result because in the real life systems the number of users that should be supported must be much higher. We limited our current testing on eight users because it is very demanding to create simulation environment for proposed solution with large number of clients (testing can be done only using real phones with SIM cards). So here we present the initial system scalability measure and further testing with higher number of users is planed for future work.

VI. Conclusion and Future Work

In this paper we propose system architecture for secure access to the EHR record from the mobile device. User protection is enabled through strong multi-factor authentication over two communication channels and utilization of a secure HTTPS connection. It is described how high security level can be provided to users accessing information from medical record without need of any additional tokens and mobile device and mobile network requirements.

Through the implementation of the testing environment and performed tests we showed how proposed security architecture can be adjusted to one real life system and concluded that authentication process time, load on the mobile device and scalability of the system are good. Additionally, we identified bottlenecks and places where improvements can be made in the real life system to provide better support and adaptation for future mobile services. For future work we plan to implement proposed improvement on both server and client side and see how they affect performance and security features.

Additionally, it is described how proposed security architecture could be adjusted to comply with Norwegian national security requirements. Besides proposed solution where required PKI system is utilized just for the application download and activation, one other solution that is considered for future work is securely storing user's private certificates on the mobile device. For this approach to be acceptable private certificates must be protected while stored and used on the mobile device, and additional risk and security analysis must be performed to ensure that no one else except authorized user can have access to them.

From the research reports we can see how mobile services can provide improvement in the quality, safety and efficiency of healthcare for a common citizen. However, mobile service implementation and acceptance in everyday use require high reliability, secrecy and data protection of patient private data that the proposed architecture can provide and enable access to the EHR systems for both patients and healthcare provider in a user friendly and secure manner.

Acknowledgment

We would like to thank Arne Riiber, Gjermund Johre and Knut Alnæs from Enap AS for cooperation and help during security architecture development and evaluation.

References

[1] J. Mirkovic, H. Bryhni, and C. Ruland, "Review of projects using mobile devices and mobile applications in healthcare", in Proc. Scandinavian conference on Health Informatics, Arendal, August 2009.

[2] M. E. Larsen, J. Rowntree, A. M. Young, S. Pearson, J. Smith, J., O. J. Gibson, et al., "Chemotherapy side-effect management using mobile phones", in Proc. Engineering in Medicine and Biology Society, Vancouver BC, 2008, pp. 5152-5155.

[3] J. Finkelstein and J. Wood, "Mobile eLearning Platform for Interactive Patient Education", in Proc. 2009 International Conference on Mobile, Hybrid, and On-line Learning, IEEE Computer Society, Cancun, 2009, pp. 23-27.

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

[5] R. S. H. Istepanian and J. C. Lacal, "Emerging mobile communication technologies for health: Some imperative notes on m-health", in Proc. 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Cancun, 2003, Vol.2: pp. 1414-1416.

[6] J. Fulcher, "The use of smart devices in eHealth", in Proc. of the 1st international symposium on Information and communication technologies, Dublin, 2003, pp. 27 – 32.

[7] T. Weigold, T. Kramp, and M. Baentsch. "Remote Client Authetication", IEEE Security & Privacy, vol. 6, pp. 36 – 43, July-Aug. 2008.

[8] VASCO The authentication Company, Digipass and PKI, A white paper on how Digipass enables your PKI environment. Available: http://www.ergonomics.ch/print/vasco_pki.pdf

[9] Y. Matsuoka, P. Schaumont, K. Tiri, and I. Verbauwhede. "Java Cryptography on KVM and its Performance and Security Optimization using HW/SW Co-design Techniques", in Proc. International conference on Compilers, architecture, and synthesis for embedded systems, New York, 2004, pp. 303-311.

[10] D. Weerasinghe, K. Elmufti, M. Rajarajan, and V. Rakocevic, "XML Security based Access Control for Healthcare Information in Mobile Environment", in Proc. Pervasive Health Conference and Workshops, Innsbruk, 2006, pp. 1-6.

[11] S. Rossilawati, H. Xu, and S. Dharmendra, "E-health Services with Secure Mobile Agent", in Proc. Seventh Annual Communication Networks and Services Research Conference, Moncton, 2009, pp.270-277.

[12] N. Panteli, B. Pitsillides, A. Pitsillides, and G. Samaras, "Web mobile-based applications for healthcare management", 1st edition, Idea Group Inc, 2007, pp. 100-117.

[13] M. Shanmugam, S. Thiruvengadam, A. Khurat, and I. Maglogiannis, "Enabling Secure Mobile Access for Electronic Health Care Applications", in Proc. Pervasive Health Conference and Workshops, Innsbruk, 2006, pp. 1-8.

[14] J. A. MacDonald, "Cellular authentication & key agreement for service providers", in Proc. Pervasive Computing Technologies for Healthcare, Tampere, 2008, pp. 69-72.

[15] A. M. Hagalisletto and A. Rieber, "Using the mobile phone in two-factor authentication", The First International Workshop on Security for Spontaneous Interaction, Innsbruck, 2007.

[16] H. Raddum, L. H. Nestaas, and K. J. Hole, "Security Analysis of Mobile Phones Used as OTP Generators", in Proc. WISTP2011 Security and Privacy of Mobile Devices in Wireless Communication, Passau, 2010, pp. 324-331.

[17] S. Vaudenay, A Classical Introduction to Cryptography: Applications for Communications Security. Springer, 2006, Chapter 12: From Cryptography to Communication Security.

[18] E. Rescorla, SSL and TLS Designing and Building Secure Systems, Addison-Wesley, 2001.

[19] S.Thomas, SSL and TLS essential, John Wiley & Sons, 2000.

[20] H. Xia and J. C. Brustoloni, "Hardening Web Browsers Against Man-in-the-Middle and Eavesdropping Attacks", in Proc WWW '05 Proceedings of the 14th international conference on World Wide Web, Chiba, 2005, pp. 489-498.

[21] Organization for economic cooperation and development (OECD), OECD studies in risk management, Norway Information Security, 2006. Available: http://www.oecd.org/dataoecd/36/16/36100106.pdf

[22] Ministry Of Government Administration, Reform and Church affairs, Guidelines for public entities that facilitate electronic service and interaction online. Available: http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uavviseli/4.html?id=505929.

[23] Ministry Of Government Administration, Reform and Church affairs,, Requirements specification for PKI for the public sector, January 2005. Available: http://www.regjeringen.no/en/dep/fad/Documents/Acts-and-regulations/retningslinjer/2010/requirements-specification-for-pki-in-th.html?id=611085

[24] L. A. Jones, A. I. Antón, and J. B. Earp. "Towards understanding user perceptions of authentication technologies", in ACM workshop on Privacy in electronic society, New York, 2007, pp. 91-98.