On Possible Cryptographic Optimization of Mobile Healthcare Application

Goran Đorđević[1], Milan Marković[2]

[1]AET Europe, IJsselburcht 3, NL-6825 BS Arnhem, The Netherlands, goran.djordjevic@aeteurope.com

[2]Paneuropean University Apeiron, Banja Luka, Republic Srpska, Bosnia and Herzegovina, milan.z.markovic@apeiron-edu.eu

Critical Review

DOI: **10.7251/JIT1902080DJ** UDC: **004.056.55:621.39**

Abstract: The paper deals with a possible SOA based m-healthcare online system with secure mobile communication between patients and medical professionals with medical and insurance organizations. An example of an Android-based secure mobile client application is presented which can be used in the described secure m-healthcare model and it is experimentally evaluated. In the paper, we focus on possible optimization of cryptographic algorithms implemented in the secure Android mobile client application. The presented experimental results justify that security operations related to X.509v3 digital certificate generation and XML/WSS digital signature creation/verification are feasible on some current smart phones and justify the use of the proposed optimization techniques for implemented cryptographic algorithms.

Keywords: Secure Android Mobile Application, SOA, M-Healthcare, Digital Signature, Encryption.

Introduction

This paper is related to consideration of possible secure m-healthcare model and applying secure Android Web services based mobile client application in it. Overviews of possible secure systems based on similar model, secure JAVA mobile Web service application and SOA-Based central platform are given in [4], [5], [6], and [7] where the model is conceptually and theoretically presented and evaluated in domains of m/e-government and m/e-banking.

In this paper, as an extension of the previous work, a possibility of applying the similar model in domain of m-healthcare systems is considered. Additionally, a possibility of using the secure Android based mobile client application in the proposed m-healthcare model is considered and experimentally evaluated.

First, we consider a possible model of secure SOA-based m-healthcare online systems, i.e. about secure mobile communication between patients and/or medical professionals with the medical and healthcare insurance organizations for different purposes. This model could be considered in both local and cross-border case. The latter means either crossing borders of municipalities/regions in the same country or crossing borders between countries (e.g. some medical organizations in different countries).

As a main goal of this paper, we consider a possible usage of the Android-based secure mobile Web service client application in the proposed secure m-healthcare model. A feasibility of using such Android based secure mobile client application is experimentally evaluated in the paper. An emphasis is given on possible optimization techniques of cryptographic algorithms implemented on the Android platform. In this sense, we give two approaches of possible optimization of RSA private key operations. The proposed optimization techniques are experimentally verified in the paper.

The paper is organized as follows. Security requirements in m-healthcare systems are elaborated in Section 2. The architecture of the proposed m-healthcare model is proposed in Section 3. Information about some related work in literature is given in Section 4, while some features of the secure mobile client applictions are presented in Section 5. Proposed optimization cryptographic techniques are described in the Section 6. Experimental results obtained by the secure Android-based mobile client application is given in Section 7 while conclusions are given in Section 8.

Security Requirements in M-Healthcare systems

This Section deals with the basics of security mechanisms/requirements in m-healthcare systems. Key players in Healthcare systems are: medical organizations (hospitals, clinics, pharmaceutical organizations), insurance organizations, healthcare professionals (doctors, physicians, nurses, pharmacists, etc.), and patients – end users.

Most modern Healthcare systems are information systems based on TCP/IP computer networks and they work fast move toward the electronic business in Healthcare industry – electronic Healthcare (e-Healthcare). In this environment, security mechanisms for e-business must be implemented with necessary adaptation to the Healthcare environments. There are a lot of technical and security issues for these systems that include, between the others: electronic patient record or electronic health record (EHR) must be fully private, central database of patient electronic records must be enabled for use from all players (medical organizations, professionals, insurance, patients), privacy protection of the patient records, secure communications between all players in the system, electronic order entry, enabling mobile Healthcare, HIPAA compliance, etc.

Thus, security mechanisms that are necessary to be implemented in these e-healthcare systems are: strong user authentication procedure, digital signature technology, confidentiality protection of data in the system on the application, transport and network layers, privacy protection of the patient personal data, strong protection of the central healthcare database based on multiple firewall architecture, and PKI systems, which issues X.509 digital certificates for all users of the system (Healthcare professionals and patients) - digital identities (IDs) for the users.

However, with nowadays extreme penetration of mobile communications and usage of smart mobile phones/devices, earlier e-business models and systems move fast towards m-business models and systems. The same holds for e-healthcare systems and thus in this paper we considered, elaborated and experimentally evaluated a possible m-healthcare systems based on Secure Android based Web service mobile client application and SOA based Web service front end m-healthcare system. Some initial considerations of security requirements that need to be applied in the m-Healthcare systems are given in [8].

Possible Secure M-Healthcare model

The proposed secure m-Healthcare model, depicted in Figure 1, consists of:

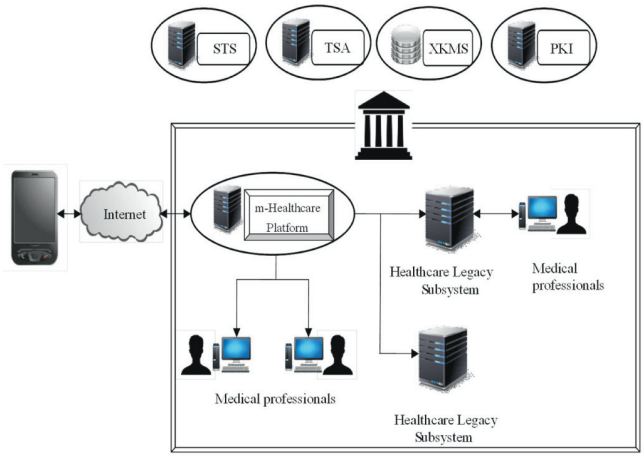

Figure 1: *A proposed secure m-healthcare model*

- **Mobile users** (patients, medical professionals) who send some Web services requests to m-healthcare platform for different purposes (sending some patient data to the central system, asking for some medical advices, checking some information about patients, checking insurance data, etc.). These users use secure Android mobile Web service client application on their mobile devices (mobile phones, smart phones, tablets, etc.) for such purpose.

- **SOA based Web service endpoint implementation** on the Platform's side that implements a complete set of server based security and business features. Well processed requests with all security features positively verified, the Web service platform's application proceeds to other application parts (i.e. legacy subsystems) of the proposed SOA-Based platform of the medical or insurance organizations.
- **External entities** such as: PKI server with XKMS server as a front end, the Authentication server, and TSA (Time Stamping Authority).

Functions of the proposed external entities are following:

- **PKI server** is responsible for issuing PKI X.509v3 electronic certificates for all users/entities in the proposed m-healthcare model (patients, medical professionals, administrators, servers, platforms, etc.). Since some certificate processing functions could be too heavy for mobile users, the PKI services (certificate location/validation) could be exposed by the XKMS server which could register users, as well as locate or validate certificates on behalf of the mobile user. This is of particular interests in all processes that request signature verification on mobile user side.
- **Authentication server (e.g. STS (Security Token Service))** is responsible for strong user authentication based on PKI X.509v3 electronic certificate issued to users and other entities in the proposed model. Possible communication between the authentication server and the user's mobile Web service application could be SOAP-based and secured by using WS-Security features. Possible scenario is that, after the successful user authentication, the STS server issues a SAML token to the user which will be subsequently used for the user authentication/authorization to the Web service of the proposed m-healthcare platform. The SAML token is digitally signed by the STS server and could consist of the user role for the Platform's user authorization. The alternative is that it could be a general-purpose Authentication server which will authenticate users by using any kind of authentication credentials, such as: username/password, OTP, PKI digital certificates, etc. In the latter case, there could be possible Web service based communication between the SOA-based central platform and the authentication server in order to authenticate users.
- **TSA server** is responsible for issuing time stamps for user's requests as well as for platform's responses (signed electronic documents). Time stamping of requests/documents could be requested from users, from the platform or from both entities.

Security operations in electronic business (e-government, e-healthcare, e-banking, e-commerce, e-payment, etc.) and mobile business (m-government, m-healthcare, m-banking, m-commerce, m-payment, etc.) systems are mostly based on two secure actions:

- Strong user authentication
- Transaction authorization

In the proposed model, the strong user authentication is based on the X.509v3 digital certificate as unique identifiers of users. Regarding the transaction authorization, it is based on digital signature of the electronic documents with additional usage of the timestamping. Since both choices represent techniques of the highest cryptographic level which are required in the Healthcare based systems, we believe that this model is the best suited for m-healthcare systems. Besides, in the proposed model, we use the encryption technique (WS-Encryption) in order to preserve confidentiality of information transmitted which represents an additional reason why this model is the best suited for m-healthcare systems.

Related Work

There are no many similar works in the literature. One work worth mentioning is the session based Web application system presented in [3]. Compared to a session based Web/application platform, presented in [3], in this paper we proposed a usage of the SOAP-based request-response technologies which is much better fitted to mobile environment. The model proposed in this paper could have the following advantages compared to the model given in [3]:

- Web service based request-response system is much more efficient system in the mobile environment than the session based Web application system. Especially when some back office processing (Healthcare legacy systems) are needed to respond on the user requests.
- Web service based model provides much more flexibilities and an easier way to implement all security features (e.g. XML security, WS-Security, Time Stamping, XKMS, PKI) compared to the Web based solution.
- Web service based system provides much more flexibilities compared to the session based Web application system in cross-border scenarios when business process includes also some processing of the user request outside of the contacted government organization.

Also, there are some conceptual discussions about security issues in the m-government systems, given in [2]. In this paper, we go further in experimental approving the usage of the secure Android mobile client application in the context of complex m-healthcare model presented in this paper.

Compared to the m-government system based on mobile qualified electronic signature in Austria (http://www.buergerkarte.at/langswitch.php?lang=en), where the mobile phone is used as a strong user authentication tool and where a server based signature is employed (user's private key is on the HSM on server side – generated and used), our proposed model is based on the „fat" client on the mobile user side where all cryptographic mechanisms are implemented in the Android based secure mobile client application. Thus, the system implemented in (http://www.buergerkarte.at/langswitch.php?lang=en) has emphasized on the authentication part of the security operations and for the transaction authorization it is implemented on the server side. In our model, both activities, strong user authentication and transaction authorization is done by using security mechanisms implemented in the mobile application.

Also, compared to some LSP (Large Scale Pilot) projects, e.g. STORK (https://www.eid-stork.eu/) and STORK 2.0 (https://www.eid-stork2.eu/), where some very complex interoperability authentication model is proposed, our proposed model could be more comprehensive and complete since the STORK models are mostly based only on user authentication mechanisms and their interoperabilities in cross-border usage. Unfortunately, there are no much discussions about possibilities of transaction authorization in the cross-border case.

Besides the above mentioned references, the authors of this paper could not find similar works in the literature related to m-healthcare systems based on Web services and Android clients. Thus, unfortunately, the presented experimental analysis does not contain a comparative experimental analysis to other achievements from the literature.

Secure Mobile Web Service Client Application

The proposed secure mobile Web service client application could comprise of following functionalities:

- **Graphical User Interface (GUI)** for presenting business functionalities to the end user. The GUI object of the proposed mobile Web service application is responsible to show user interface that enable calling of function for authentication of the end user and presenting the core functionalities to the end user. According to this, the GUI object communicates with following modules:
- User Authentication module for mobile client application of the Security module
- User PKI Registration module (XKMS module) of the Security module
- User Authentication and Authorization module for the m-government platform (SAML module) of the Security module
- Business functionalities
- **Business (core) functionalities** of the application – m-healthcare functionalities. Business functionalities have links to Security and Communication modules of the secure mobile Web service application.
- **Security functionalities.** The Security module of the considered secure mobile Web service application is responsible for overall application-level security functionalities.
- **Communication.** The communication module is responsible for establishment of secure communication between patients and medical/insurance organizations.

The security functionalities of the proposed Secure Android Mobile Client application consist of the following modules:

- **Authentication module** of the secure mobile application. User authentication for the secure mobile application should be two-step process:
- The first step would be a combination of username/password for accessing the application (password should be changeable by the user). This should be done immediately after the application starts. These credentials will be generated during the user registration process. During the initial phase of the registration application, the user will obtain the username and default password. The application has to force the user to change the initial password on the first application start.
- The second step will be in presenting a corresponding PIN code for accessing the asymmetric private key just before digital signing different m-healthcare requests.

The generation of user asymmetric public/private key pair and corresponding digital certificate should be done through user registration function of the XKMS protocol. The User Authentication module is called from the GUI object.

- **XKMS module.** XML Key Management Specification enables to simplify the use of PKI by mobile client systems.
- **STS module.** The STS module is responsible for the communication with the STS server in order to receive a SAML assertion (token) that will be used afterwards to enable access to the business functionalities by the client. The user first sends a RequestSecurityToken message to the STS (Security Token Service) server by using a SAML protocol. A protection is done by using WS Security mechanisms. After successful authentication of the user based on the client's X.509v3 digital certificate, the STS server issues a SAML token to the user which is digitally signed by the STS server. This token is securely communicated to the end user by using the WS security mechanisms.
- **XML security module.** XML security module is responsible for implementation of standard XML signature and XML encryption components. XML security module consists of:
- Implementation of the RSA private key operation for creating digital signature, as well as a function for signature verification.
- Implementation of hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512).
- Implementation of different symmetrical cryptographic algorithms (3DES, AES).
- Implementation of the RSA private key operation for decryption of encrypted symmetric message key in digital envelope.
- Implementation of the RSA public key operation for encryption of symmetric message key in digital envelope.
- **WS-Security module.** Web Service (WS) Security module is implemented as standard security mechanisms for protection of SOAP messages. WS-Security module is very important module of the Security module since it is used for protection:
- Communication with STS server.
- Communication with the proposed SOA-Based m-healthcare platform.

This way, the WS-Security module communicates with SAML module of the Security object as well as with Business functionalities object. The SAML module communicates with WS security module of the Security object as well as with the Communication object.

- **Time-Stamping module.** This module is responsible for communication with the TSA. A time-stamping service supports assertions of proof that a datum existed before a particular time. The user's application requests a timestamp token by sending a request to the TSA. As the second message, the TSA responds by sending a response, i.e. actual timestamp, to the requesting entity.

The secure mobile Web service application could secure communicate with all mentioned external entities in Section 4, i.e. it has all security functions mentioned implemented:

- Secure mobile Web service application sends Request for Security Tokens to the STS server by using WS-Secured (WS-Signature and WS-Encryption) SOAP communication.
- Secure mobile Web service applications sends digitally signed (XML signature) m-healthcare request to the Web service of the proposed m-

healthcare platform by using WS-Encrypted SOAP communication. The sent request includes the SAML token issued and signed by the STS server.
- The request is timestamped by sending a timestamp request and obtaining the corresponding timestamp response (digitally signed by the TSA).
- The secure mobile Web service application also receives the signed and timestamped response from the m-healthcare platform through WS-Encrypted communication and performs all necessary signature verifications and certificate validations (by help of the XKMS server) actions.

Optimization of Cryptographic Algorithms in Secure mobile Web Service Client Application

The Android platform ships with a cut-down version of Bouncy Castle - as well as being crippled. It also makes installing an updated version of the libraries difficult due to class loader conflicts. Different versions of Android operating system have implemented different versions of Bouncy Castle library releases. In order to avoid lack of interoperability between different devices that have implemented different operating systems and get more flexible code we used Spongy Castle functions (http://rtyley.github.com/spongycastle/). A simplified package structure of the Spongy Castle package is illustrated in Figure 2.

The Spongy Castle package contains low-level lightweight API implementing all the underlying cryptographic algorithms and a provider for the Java Cryptography Extension (JCE) and the Java Cryptography Architecture. The basic package that supports the cryptographic algorithms and padding schemes is the org.spongycastle.crypto package. The org.spongycastle.asn1 package supports the parsing and writing ASN.1 objects, which is useful in processing X.509 certificates. The utility classes in org.spongycastle.util can be used for producting and reading Base64 and Hexadecimal strings. The utility is useful if the ciphertext is required to be displayed as a Base64 string.

In order to achieve smaller and faster implementation we have partly modified Spongy Castle functions. The modification of Spongy Castle funtions is achieved in org.spongycastle.jce package. We don't want to use JCE functionalities of genuine Spongy Castle implementation because that adds a significant memory overhead. In order to avoid using the heavyweight provider for the JCE that contains implementation of many unnecessary functions we cut off a lot of functions and implement only the necessary ones. We directly call necessary Spongy Castle functions without using java.security.Provider functionalities at all. Using this approach we got smaller and faster code.

Because mobile devices have limited resources, an application designed for mobile devices should be as compact as possible. An obfuscator is a useful tool for minimizing the size of an application. We used

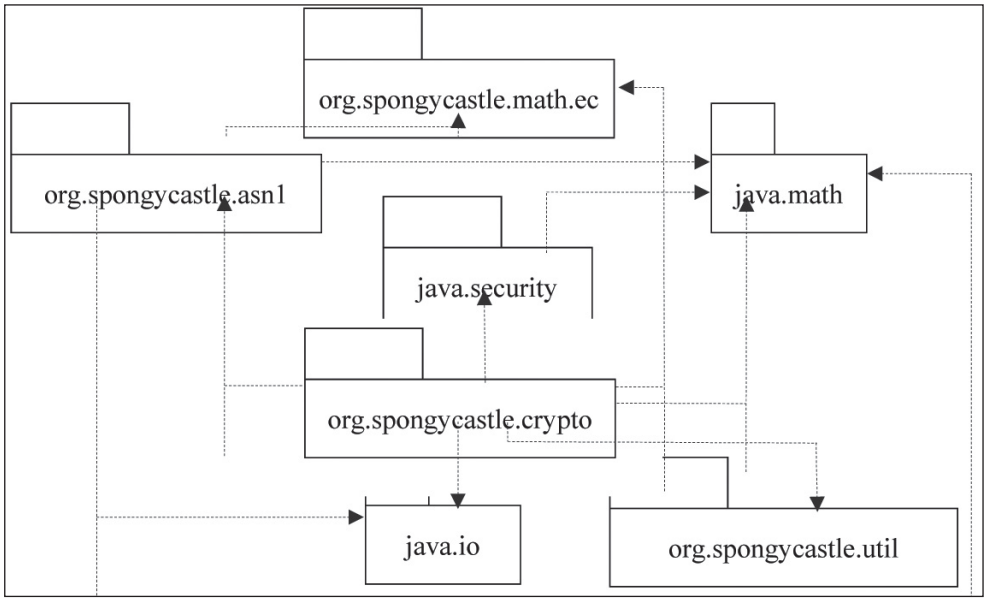

Figure 2: *Lightweight Spongy Castle API Package structure*

ProGuard obfuscator that shrinks, optimizes, and obfuscates code by removing unused code and renaming classes, fields, and methods with semantically obscure names. The result is a smaller sized .apk file that is more difficult for being reversely engineered.

In order to addionally improve performanse we have considered possibility of implementation of private key RSA operations (creation of digital signature, open digital envelope) using native code in Android Native Development Kit (NDK). A basic reason for this decision was a fact that the native code is compiled to binary code and run directly on mobile phone OS. We implemented native code on a basis of usage of OpenSSL package. In this case, a lot of cryptographic functions are implemented using C programming language. In order to additionally speedup operations with RSA private key we implemented some functions directly in assembler code. One of implemented functions in assemler code is procedure of Montgomery modular multiplication. Montgomery multiplication is a method for computing $a*b$ mod m for positive integers a, b and m. It reduces execution time on a CPU when there are a large number of multiplications to be done with same modulus m, and with a small number of multipliers. In particular, it is useful for computing a^n mod m for a large value of n. The number of multiplications modulo m in such computation can be reduced to a number substantially less than n by successively squaring and multiplying according to the pattern of the bits in the binary expression for n ("binary decomposition").

Experimental Analysis

This Section is dedicated to the experimental analysis of the cryptographic operations implemented on Android mobile phone, i.e. smart phones with Android operating system [9], as a possible example of the proposed secure mobile client application that could be used in the proposed m-healthcare model. Also, the proposed model and presented experimental results on Android mobile operating systems represent m-healthcare extension compared to the discussion presented in [1]. The presented experimental results are generated using devices (mobile phone, tablet, PC laptop and PC desktop) described in [7].

Experimental results that are presented in this section are based on the modified version of Spongy Castle functions as well as partly modified version of OpenSSL native code. In Tables 1, 2, 3, 4, a row with title 'Native code' is shown with results where operations with RSA private key are done by using native code (C code + assembler). During testing phase we have measured average time by using some number of iterations. The actual number of iterations used are shown in each table. The same code and packages are used during testing procedure in all devices. Throughout this Section, all presented experimental results are given in miliseconds – ms. In order to evaluate the possibility of using the mobile phone for secure mobile Android-based client application in m-healthcare systems based on Web service we measured times needed for creation X509 v3 self-signed certificate comprising a creation of PKCS#10 certificate request (Table 1). As a signature algorithm we used SHA-1 hash algorithm and RSA asymmetric cryptographic algorithm. Then we measured time for creation of XML-Signature and Web Service (WS) Signature (Table 2, Table 3), respectively. In all these experiments, we used a file of 1KB, RSA asymmetric algorithm and SHA-1 hash function. We also analyzed possibility of WS Decryption mechanisms (Table 4).

Some observations of the presented experimental analysis are:

Table 1: *Create X509 v3 self-signed certificate*

Device 512		RSA private key length (bits), n=50000 iterations				
		1024	2048	3072	4096	
Mobile Phone	SpongyCastle	18.11	27.41	84.41	216.89	467.95
	Native code	13.48	21.26	73.48	206.53	426.34
Tablet		34.49	46.27	116.05	283.22	548.40
PC Laptop		1.78	9.01	58.07	180.97	414.14
PC Desktop		1.33	6.78	43.92	137.36	312.90

Table 2: *XML-Signature creation*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	29.64	38.15	95.87	228.20	479.10
	Native code	25.01	32.01	84.94	217.84	437.49
Tablet		59.73	73.78	144.08	319.65	586.54
PC Laptop		2.12	9.38	58.50	181.54	414.74
PC Desktop		1.57	7.05	43.85	137.87	312.79

Table 3: *WS-Signature creation*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	63.76	74.51	131.00	266.29	507.47
	Native code	59.13	68.36	120.07	255.93	465.86
Tablet		126.99	147.68	216.81	384.48	663.93
PC Laptop		2.79	10.07	59.18	182.1	415.19
PC Desktop		2.02	7.50	44.57	138.03	311.66

Table 4: *WS-Decryption mechanism*

Device		RSA private key length (bits), n=50000 iterations				
		512	1024	2048	3072	4096
Mobile Phone	SpongyCastle	34.96	44.20	102.48	232.75	486.20
	Native code	30.33	38.05	91.55	222.39	444.59
Tablet		80.91	119.74	169.87	339.54	609.42
PC Laptop		2.41	9.67	58.88	181.79	415.98
PC Desktop		1.77	7.28	44.36	138.01	313.88

- The creation of the self-signed X.509v3 digital certificate with 2048 bits key by using the mobile phone takes 84.61 ms and even 73.48 by using optimized native code which is similar to the results obtained by PC computers.
- The operation of digital signature of XML message (XML-Signature and WS-Signature mechanisms), using 2048-bit private RSA key, takes on mobile phone 95.87 and 131 ms, respectively, and in optimized native code version 84.94 and 120.07 ms, respectively, which are comparable to the results obtained by other devices..
- The operation of decryption of WS-Encrypted message using 2048-bit private RSA key, takes 102.48 ms and in the optimized native code version 91.55 ms. It means that in one second can be implemented about 10 operations of decryption WS-Encrypted message using 2048-bit RSA private key.

These observations could lead to the conclusion that mobile phone could be used in real time for implementation of RSA private key operations in times comparable to the ones obtained on PC computers, especially when the optimized native code is used.

Conclusions

In this Paper, we presented an overview of possible secure model of m-healthcare systems as well as an analysis of possibility and feasibility of using secure Android-based web service mobile client application in it.

First, this paper is related to the consideration of some possible SOA-based m-healthcare online systems, i.e. about secure mobile communication between patients and medical professionals with medical and insurance organizations.

Second, the paper presented a possible example of an Android-based secure mobile client application that could be used in the described m-healthcare model and which is experimentally evaluated. An emphasis is given on possible optimization techniques of cryptographic algorithms implemented on the Android platform. In this sense, we give two approaches of possible optimization of RSA private key operations. The proposed optimization techniques are experimentally verified in the paper

Presented experimental results justify that security operations related to RSA private key operations (creation of X.509v3 digital certificate, XML/WS digital signature, WS-Encryption) are feasible for usage on some current smart phones. Thus, we could conclude that this application could serve as a basis for implementing secure m-healthcare system based on the model described in this paper. Also, presented experimental analysis justifies the usage of the proposed optimization of cryptographic techniques implemented on a basis of C and assembler code.

REFERENCES

[1] Braga, A. M., Nascimento, E. N.: Portability Evaluation of Cryptographic Libraries on Android Smartphones, Cyberspace Safety and Security, Lecture Notes in Computer Science, Volume LNCS-7672, 2012, pp 459-469.

[2] Kumar, M., Hanumanthappa, M., Reddy, B. L.: Security Issues in mGovernment, H. Jahankhani, K. Revett, and D. Palmer-Brown (Eds.), ICGeS 2008, CCIS 12, pp. 265-273, 2008, Springer-Verlag, Berlin Heidelberg, 2008.

[3] Lee, Y., Lee, J., Song, J.: Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce. Computer Communication. 2007. 30 (4): 893-903.

[4] Marković, M., Đorđević, G.: On Possible Model of Secure e/m-Government System. Information Systems Management. Taylor & Francis Group, LLC. 2010. 27:320-333.

[5] Marković, M., Đorđević, G.: On Secure SOA-Based e/m-Government Online Services, in Handbook "Service Delivery Platforms: Developing and Deploying Converged Multimedia Services", (pp. 251 – 278, Chapter 11), Taylor & Francis, 2011.

[6] Marković, M., Đorđević, G.: On Secure m-government and m-banking model, in *Proc of 6th International Conference on Methodologies, Technologies and Tools Enabling e-Government*, July 3 – 5, 2012, Belgrade, Serbia, pp. 100-111.

[7] M.Marković, G.Đorđević: Secure Android Application in SOA Based Mobile Government Systems, in Proc of 7th Int. Conference on Methodologies, Technologies and Tools Enabling e-Government, Luis Alvarez Sabucedo and Luis Anido Rifon (Eds.), Oct. 17 – 18, 2013, Vigo, Spain, pp. 117-126.

[8] Marković, M., Savić, Z, M., Kovačević, B.: Secure Mobile Health Systems: Principles and Solutions, chapter in the book *M-Health, Emerging Mobile Health Systems*, Series: International Topics in Biomedical Engineering Istepanian, Robert; Laxminarayan, Swamy; Pattichis, Constantinos S. (Eds.) 2006, XXX, 624 p. 182 illus., Hardcover, ISBN: 0-387-26558-9, pp. 81-106.

[9] Reto Meier, P.: Professional Android 4 Application Development, John Wiley & Sons, Inc., Indianapolis, Indiana, 2012.

Submitted: October 18, 2019
Accepted: December 3, 2019

ABOUT THE AUTHORS

Goran V. Đorđević was born 1972 in Novi Sad, Serbia. He received a BSc in Computer Science at the Technical Military Academy in 1996. Afterwards he did his post-graduate studies, at the Faculty of Electrical Engineering of University of Belgrade where he received a MSc. Currently employed as a senior software developer in AET Europe. His main areas of interest are smart card security and smart card applications, security protocol design, mobile devices, tokens, Internet of Things and information security.

Milan Marković received B.S.E.E., M.S.E.E., and Ph.D. degrees in electrical engineering from Faculty of Electrical Engineering, University of Belgrade, Serbia, in 1989, 1992, and 2001, respectively. He is an Associate Professor on College of Information Technology, Pan-European University of Apeiron in domain of information security courses. His research interests are mainly in public key infrastructure, information security, cryptographic algorithms, mobile security, identity management, secure e/m-banking and e/m-government, trust services, ISMS, Blockchain, etc. He has published more than 320 scientific papers.

FOR CITATION

Đorđević G., Marković M., On Possible Cryptographic Optimization of Mobile Healthcare Application, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:80-88, (UDC: 004.056.55:621.39), (DOI: 10.7251/JIT1902080DJ), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004