Presentation of An Efficient and Secure Architecture for Guilan Health Information Network with Smart Cards

Mohamad Nejadeh [1,], Shahriar Mohamadi [2]
[1] Information of Technology Department of International Pardis Branch of Guilan University,Rasht, Iran
[2] Faculty Member Of Khajeh Nasir Toosi University,Assistant Prof,Tehran, Iran
{m_nejadeh,smohamadi40}@yahoo.com

ABSTRACT

Nowadays a great number of activities are performed via internet. With increment in such activities, two groups of services are required for providing a secure platform: 1- Access control services, 2- communication security services. In this article we propose a secure and efficient system for establishment of secure communication in e-health. This architecture focuses on five security indicators of authorization, authentication, integrity, non-repudiation and confidentiality. In this paper, we propose an authentication architecture that uses a strong, two factor authentication mechanism for the identification of Healthcare Users in the access to GHIN Portals. This architecture uses an efficient encryption scheme, which is a combination of the public key and the symmetric key encryption systems, all of which are combined with a log strategy. In this paper we have used a new role-based control model to provide the security requirement of authorization for user's access to data. Data sensitivity is measured based on the labels given to the roles; and then these data are encrypted with proper cryptography algorithms. In a comparison of these architectures, you will see that this architecture enjoys an efficient mechanism, which is very suitable and practical for communication and interchange of data.

KEYWORDS

GHIN; access control; cryptography; digital signature; Log strategy.

1 INTRODUCTION

The sudden growth in use of internet in the recent years has had a significant effect on communication of people with each other, partnership in references and information and commercial models. Medical sector was not an exception and internet had a significant effect on that. E-health includes different types of health services presented via internet. In this relation the services are provided in different domains of training, information and various health and treatment services. E-health increases access of health services promotes presented services quality and efficiency. Therefore appearance of a secure ground in this domain is necessary, which is considered as one of the most challengeable problems in e-health domain.

Security in information systems means protection of systems against unauthorized changes and access of information. The most important aims of security systems include protection of confidentiality, integrity, availability and data guarantee. Confidentiality must be maintained to protect the patient's privacy: the patient's data, such as medical records, would affect the doctor's diagnosis and treatment decisions of a patient. Integrity must be conserved to ensure that the patient's data have not been altered and is up to date. The availability of the e-Health system is also of great importance; a person's life could be dependent upon the e-Health system [2].

On the other hand with exertion of access control on the basis of the rules, the rights for access of factors to objects are determined. Access control on systems mentions which people are authorized to access to which resources under which conditions and which actions they are authorized to perform on the resources. One of the access control models is role-based access control (RBAC) that has attracted much attention due to publicity. This model in the first presentations proved that it has a simpler security management as compared with the other models due to application of the concept of role and decreased management costs.

This paper presents an efficient and secure architecture for security of e-health services. In section 2 we discuss a proposed solution for creation of a secure communication. In the next sections, we propose the results of the former section in construction of a secure architecture for e-health services and present our proposed model that is presented as follows: section 3 presents the architecture of Guilan Health Information Network. Section 4 considers access control model. Section 5 presents an efficient and secure cryptography scheme. In section 6 we mentioned digital signature. You can study Log strategy in section 7 and our proposed architecture has been presented in section 8 and finally in section 9 our paper is ended with a conclusion.

2 THE PROPOSED SOLUTION

E-Health security studies are still in an early stage. As far as the authors are aware, there have been only several approaches on e-Health Service Authentication and e-Health Data Transmission for example in [8], an authentication protocol is developed. The protocol uses "Timestamp" to describe and verify the security properties related to the expiration of keys and the freshness of the message. The protocol heavily relies on clock synchronization of both parties, thus, the issue of trusting each other's clock becomes a problem.

In [9], a Workflow Access Control Framework is proposed to provide more flexibility in handling e-Health dynamic behavior. The idea is to model each work task in the system as state-machines. At each state, the data access permission is granted based on the resources required to move on to the next state. For any entities involved, the information of all states statuses are stored in a lookup table to improve processing speed. However, this approach consumes a large amount of memory space since an entity must store a copy of the status of all states in the system.

To design a secured applied system and establish a secure communication and message interchange, five security needs should be satisfied:

- Integrity: prevents data change. Of course any change on information, creates some changes on the text.
- Authentication: Authentication ensures the parties with right accessing to a system.
- Authorization: Determines access control on the basis of the authorized rules, which determine that factor's rights of access to objects.
- Non-repudiation: The user must not deny the performed transaction and

must provide proof in case that this situation occurs.

- Confidentiality: The confidential information must be secured from an unauthorized party.

We proposed a new style of secure architecture for e-health communications. Table 1 summarizes the requirements resulting from the security concerns, and technologies recommended. The third column of Table 1 shows the existing solutions for exertion of any of the technologies mentioned in the table.

Table 1. Security requirements along with the technologies recommended for these requirements and solutions to address them.

Security	Technology	Solution
Authorization	Access control	Role model- interaction-organization
Authentication	Using a pair of keys	Biometric and Smart card
	Digital Signature	ECDSA
Integrity	Digital Signature	
Non-repudiation	Digital Signature	
	Log	Transaction Log
Confidentiality	Encryto/ Decrypto	ECC & AES

3 GUILAN HEALTH INFORMATION NETWORK (GHIN)

GHIN is a Guilan Health Information Network which we suppose it to aiming at improving the cooperation between a local set of Healthcare Units (HCU), providing an integrated vision of the health care data in the region and the electronic communication between the Healthcare providers.

The basic element in this platform is the patient electronic healthcare record, which aggregates all the patient clinical information spread within the affiliated HCUs. It provides to care giving Professionals a more complete profile of the patient clinical situation with clear benefits to the patient, and promotes economy by, for instance, avoiding the repetition of clinical exams such as blood tests, CT scan or MRI.

The GHIN architecture, presented in Figure 1, includes Hospitals, Clinics and the GHIN Data Center, all interconnected by the Guilan Health Information Network.

The GHIN Data Center is the core of the system. It implements a set of services which includes two GHIN Portals: The Professional Portal and the Citizen Portal. It is through these Portals that both Health Professionals and Citizens access GHIN information and services.

Because of the sensitivity of clinical information, GHIN requires that all communications are made through secure channels and that all the parties are previously authenticated bilaterally. This is important to avoid unauthorized access to clinical information. Also, due to well-known problems on the use of passwords for HCU man authentication, a stronger authentication mechanism is required.

GHIN does not produce clinical data; it is a communication platform providing an aggregated and shared view of clinical data within a region. Therefore, the authentication of Health Professionals is to be used only for access control.

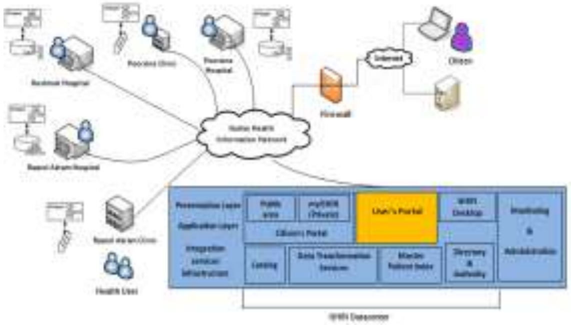

Figure 1. GHIN network architecture.

3.1 Proposed GHIN Authentication Architecture

The architecture proposed for authenticating Professionals when accessing the GHIN is based in a Public Key Infrastructure (PKI). A PKI is generally considered an appropriated technology for supporting e-Health security services [10]. Figure 2 display a diagram of our proposed architecture. The interaction between the Professional and the two servers, GHIN Portal and HCU CA, is supported by a common browser on a client machine and SSL sessions with bilateral, certificate-based authentication.

One fundamental and important aspect of this PKI is its hybrid model, built on top of private PKIs owned by the RTS and by each HCU. The rationale for each HCU to have its own private PKI, most likely a hierarchical PKI, is that they are in fact independent organizations, each managing their own computer and HCU man resources. Therefore it makes sense that each HCU manages the registration of its Users and the issuing of their public key certificates, without depending on any other organization. This can be crucial in cases where urgent need exists to issue certificates; for example, when a doctor cannot access a patient health record because he lost his credentials. Also, each User working for an HCU only needs to trust his HCU trust anchor, typically the HCU root CA certificate, for building useful trust relationships within HCU.

Our hybrid PKI uses trust relationships established between GHIN and each affiliated HCU. These trust relationships, implemented using cross-certification, allow the validation by the GHIN of certificates issued by each affiliated HCU, and vice-versa. However, from the GHIN point of view, no trust relationship is necessary between HCUs. Therefore, the GHIN is not meant to act as a bridge CA, neither GHIN requires HCUs to cross-certificate among themselves.

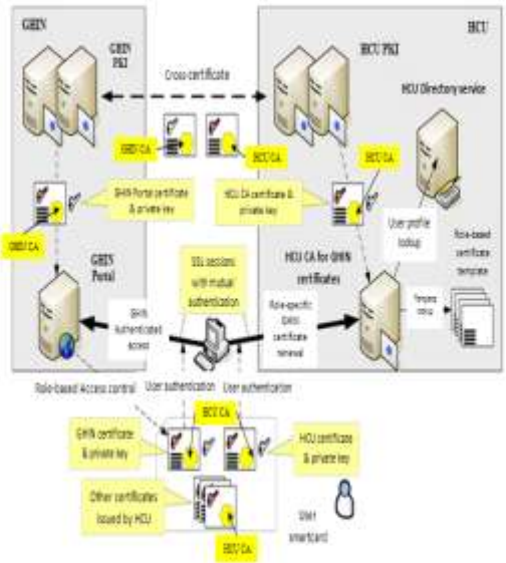
GHIN
GHIN PKI
Cross-certificate
HCU
HCU PKI
HCU Directory service
GHIN CA
HCU CA
HCU CA
GHIN Portal certificate & private key
HCU CA certificate & private key
GHIN CA
GHIN Portal
SSL sessions with mutual authentication
User profile lookup
HCU CA for GHIN certificates
Role-based certificate template
GHIN Authenticated access
Role-specific GHIN certificate renewal
Role-based Access control
User authentication
User authentication
HCU CA
GHIN certificate & private key
HCU certificate & private key
Other certificates issued by HCU
User smartcard
HCU CA

Figure 2. GHIN Proposed authentication architecture

3.2 Users' Smart Cards

In order to accomplish the requirement of strong authentication of Users, smart cards are used to store Users' credentials. A smart card enables a two factor authentication: (i) the smart card possession and (ii) the knowledge of its PIN. Smart cards are not easily tampered, which reduces the risk of compromise of secrets stored inside. The smart card carries the User's credentials and a set of certificates for certificate chain validation. The User's credentials are composed by two certificates and the corresponding private keys, including GHIN Certificate to access GHIN portal and another one is HCU certificate, which used to obtain/renew the GHIN certificate from the HCU where the User works.

The smart card of a User is initialized by his HCU and delivered personally to him. Initialization consists in inserting on it the HCU certificate, and related private key, and the certificates for certificate chain validation. A User is not allowed to renew its HCU certificate; when it expires the smart card gets useless and its reinitialization by the HCU is needed.

Smart cards are also important because of their portability. A User can always carry his smart card and therefore carry his GHIN credentials, which increases his mobility across computers connected the GHIN. The memory size of smart card is an important issue, this memory size must be enough for storing (i) HCU certificate and correspondent private key, (ii) HCU Root CA certificate, (iii) HCU Issuer CA certificate, and (iv) cross-certificate issued by the HCU Issuer CA to the public key of the GHIN Issuer CA. Smart cards must be personally delivered to Users after being properly initialized by enrolment agents of their HCU.

Users are not allowed to request or renew HCU certificates; they are included in smart cards during their initialization by enrolment agents. When they expire only an enrolment agent can request its renewal. This way, enrolment of GHIN certificates is only possible for smart cards provided and properly initialized by HCU agents.

Concerning the strong, two-factor authentication mechanism for Users, it was achieved by using personal smart cards. A User can only authenticate himself, against his HCU or against the GHIN, with his smart card and knowing the correct unblocking PIN. The lost of a smart card represents a reduced risk, as it is useful only when unblocked with the correct PIN. Nevertheless, we still cannot prevent Users from letting other people other than themselves to use their authentication credentials. A solution for this problem probably needs to integrate a third factor, biometric authentication (for example, a biometric recognition for unblocking the smart card together with the PIN).

4 ACCESS CONTROL MODEL

With using model [1] we propose a new security scheme for e-health system that is examined with different algorithms for communication in e-health and the original results are presented. With using model [1], we execute our authorization control on our system. Of course it is necessary to mention that this access control model is studied for static system and does not include a dynamic and distributed system. In this frame three main elements of interaction, role and organization have been created. This model presents them in the forms of role models, interaction models and organization models:

4.1 Role Model

The role in this system assumes a peer-to-peer model. It is both a server and a client, capable of both receiving request from other roles as well as initiating requests to other roles in the system. In this scheme, an abstract role model to classify roles is presented. The detailed responsibilities of each role are not specified at this abstract level. A role can only become functional when it is instantiated with assigned position, specific set of duties, and interactions within a specific organization. The abstract model of a role is described in Figure 3.

In this model the roles are supposed to act as initiator and reactor at the same time. If a role is able to initiate a request to other roles, then it's an initiator. If a role receives requests from other roles, then it's a reactor.

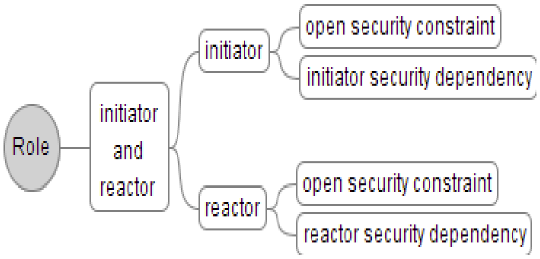

Figure 3. The Abstract Role Model [1].

Each role in this system is associated with a set of security properties called security dependency. The security dependency describes the security constraint(s), which creates impediments and limitations for some special interactions. Therefore such limitations may be exerted to roles as a set of conditions and impediments and the roles should act in such a way not to violate from the conditions and impediments. In this system four types of security dependencies have presented: 1- Open security dependency, 2- initiator security dependency, 3- reactor security dependency, 4- initiator and reactor security dependency (Figure 4).

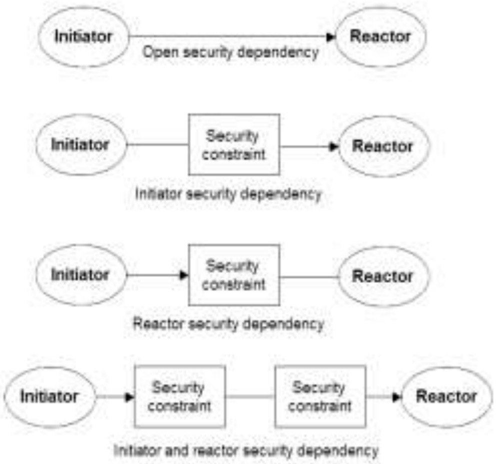

Figure 4. Different Types of Security Dependencies [1].

4.2 Interaction Model

In this system, the interaction model is divided into two categories.

- Closed interaction: The number of participants of a particular interaction is fixed and cannot be changed for that type of interaction.
- Open interaction: The number of participants can be changed over the progress of the interaction.

Regardless whether an interaction is open or closed, four types of communication methods exist, namely, one to one, one to many, many to one and many too many.

4.3 Organization Model

Most of organizations have different structures that determine different roles for classified situations. In this model each organization model contains three important properties: 1- organization structure, 2- organization positions, and 3- organization rules.

Organizational rules dictate policies and limitation on the method of information current in and out of the organization. These rules are independent to any especial definition of drawings by organizational structures. Therefore these rules are practical for different organizations: 3 basic rules are considered for each organization: 1- The requirement to play positions, 2- the interaction direction and 3- the interaction range. For the requirement to play positions defines the restriction of what a position can do, such as: a given organization position must be played by only one role during the organization’s lifetime or two positions can never be played by the same role. Interaction direction defines the information flow direction within the system. The direction can be divided into three categories, up, peers and down. The interaction range defines how far an interaction can be reached. The value can be adopted from 1 to n.

Depending on the topology of the organization, we can further divide the organizations into centralized structure, multilevel hierarchy, peers to peers and complex composite structure. When the organizational structure was selected the organization model is produced. [1]

4.4 Exertion of Role- Interaction- Organization Models on an Experimental Sample

In this section we show an original sample of e-health system, on which role- interaction- organization model has been exerted on it, in this case we have five roles, namely, a patient, a receptionist, a nurse, a general practitioner (GP) and a specialist named as role 1, role 2, role 3, role 4 and role 5. We supposed that role 1 is an initiator, role 2, 3 and 4 are initiators and reactor and role 5 is a reactor. In this model we only considered the closed and one-to-one Interaction. The transactions of each role according to the presented model in [1] are presented in the form of a label. For example I_C_S_23 means as follows: I means interaction, C means that the interaction is closed, S means that the interaction is one-to –one and 23 shows that the interaction starts from role 2 and ends with role 3 depends on the roles involved in the interaction, the numbers changed proportionally. In this stage, the roles in the current system have no clear responsibilities. For example, at this stage, there is an interaction checked in the system, I_O_S_53, which O means open interaction. As we described above, this interaction is not legitimate. We can examine the interaction from two ways. From the role model way, role 5 is a reactor role; it only receives the requests from other roles. From the interaction model way, we defined only closed interactions are allowed to be performed among roles, however, this interaction is belonged to open interaction category. Therefore, this interaction can be examined as an illegal interaction to arise.

As it was shown in Figure 5 and with a view to the real system in the real world, our original sample performs five vital activities of patients, treatment procedure, help and general medical care and high level medical care. In our original sample, we have five positions in the organization including patient, receptionist, nurse, general practitioner (GP) and specialist. That the patient is able to explain and interchange the information. The receptionist performs the activities of explanation, interchange of information, reception and helping. The nurse is able to perform the activities of explanation, interchange of information and helping. The general practitioner performs the activities of explanation, interchange of information and helping and finally the specialist performs the activities of explanation, interchange of information and helping.

As you can see in Figure 5, the interaction between the patient and the receptionist has open security dependency and no security constraint has been presented. The patient sets an appointment time with the doctor through the receptionist. The patient also has a domain of communication with the nurse, the general practitioner and the specialist. But whereas he cannot meet the requirements of the related security constraint, this interaction is not created directly. Therefore the receptionist follows the information related to the patient to meet the requirements of the security constraints related to the nurse and the general practitioner and hereby the interaction between the patient and the nurse or the doctor is established. For Example, the patient may not set an appointment time with the physician directly therefore the receptionist follows up the patient's information to provide a helping interaction and an interaction with the general practitioner. After performance and completion of such an interaction, places the data in a security constraint for establishment of an interaction between the patient and the physician to be able to understand what time the constraint is considered. Then the receptionist can establish an interaction with the patient and inform the patient of the appointment with the general practitioner. Therefore the appointment between the patient and the doctor is performed at the determined date and after completion of such an interaction, the determined security relations for such an interaction, which have been added to the security constraints, are deleted and the work is completed successfully.

Sometimes it is possible the nurse encounters problems while establishment of the interaction of helping to the patient and an interaction of helping with the general practitioner is required. Therefore the nurse for establishment of such an interaction first should meet the requirements of the security constraints related to the doctor, on the other hand with a view to setting of the communication domain and the organization structure the nurse needs to present a security constraint, which indicates the role, which will communicate, therefore the interaction between the nurse and the general practitioner is established and the nurse will be able to receive the procedure of the instructions required for patient's treatment.

If the general practitioner is unable to solve the patient's problem he should start a helping interaction for communication with the specialist and provide an appointment time with the specialist for the patient. In this type of interaction with a view to communication scope and organizational structure the general practitioner needs a security constraint, which indicates the role, which will communicate and on the other hand should meet the requirements of security constraints of the specialist and similar to appointment with the general practitioner, the patient needs to perform the interaction security constraint in appointment with the specialist.

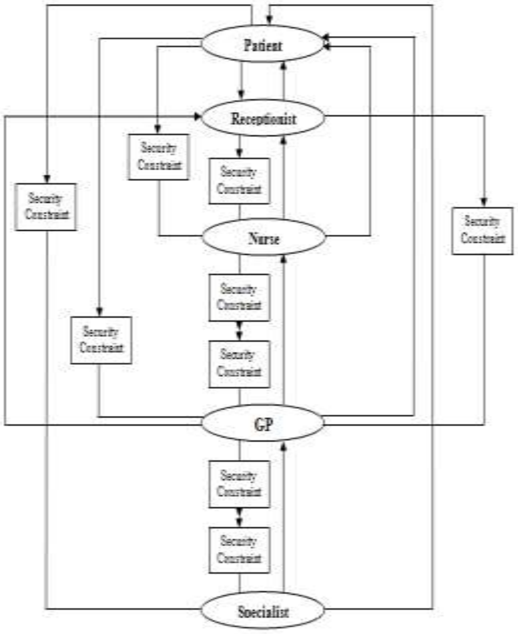

Figure 5. The Simple Case of E-health System.

5 EFFICIENT AND SECURE CRYPTOGRAPHY SCHEME

With cryptography, data can be protected from others and only the authorized users will be able to read the data with decryption. Applications of cryptography include hash function, exchange of key, digital signature and certificate. Hash function emphasizes on function integrity and investigates if the document has been altered. Some examples of hash function include MD4, MD5 and Secure Hash Algorithm/ Standard (SHA/SHS). Key exchange is used in symmetrical cryptography. Symmetrical cryptographies use identical key for encryption and decryption of a message. In this section with consideration of different cryptography algorithms, the lightest and securest algorithm is selected for the architecture.

In this section, we explain the grounds required for the proposed solution on cryptography algorithms. An algorithm is considered to be a secure algorithm if and only if a) brute force is the only effective attack against it and b) the number of possible keys is large enough to make brute force attack infeasible. There are two main types of encryption algorithms: asymmetric and symmetric key algorithms. For symmetrical encryption, there are different encryption algorithms that may be used in commerce. Symmetrical algorithms such as DES, 3DES, AES and Blowfish are often compared and used in [4] and [5]. These algorithms have different specifications that have been studied by specialists and proved. But we have used different specifications of algorithms for security of different types of information. According to comparisons in [3] that has compared algorithms with a view to key size, block size, algorithm structure, rounds number and feasibility of being cracked, AES has obtained the most scores and DES the least scores with a view to security (Table 2).

Table 2. Encryption algorithms ranking

Algorithm	DES	3DES	AES	Blowfish	DEA	RC4
Key Size	7	13	17	20	10	17
Block Size	17	17	20	17	17	13
Algorithm structure	13	13	17	13	17	20
Rounds	17	20	17	17	13	10
feasibility of being cracked	4	7	7	7	7	4
TOTAL SCORE	58	70	78	74	64	64
Ranking	#6	#3	#1	#2	#4	#4

As we know, asymmetric algorithm creates more security as compared with symmetric algorithms but symmetric algorithms have higher speed, therefore we paid attention to empowering AES, which is a symmetrical algorithm, with ECC asymmetric algorithm to combine the advantages of higher speed in the symmetric algorithm with security of asymmetric algorithms. In this state for Secrete Key transfer, which was the most important problem in key transfer in symmetric algorithms, we used ECC asymmetric algorithm, which has more speed than the other asymmetric algorithms so that besides increase of speed we can guarantee more security. In this state we have only used ECC cryptography for AES key transfer.

A relative point has been given to the criteria listed in Table 2 supposing that the algorithms are secure. The domain of this relative point is between 1 and 20 that the 20 is the higher point. After presentation of the comparisons, now it's turn to select proper cryptography algorithms for data encryption.

There are different types of information in e-health with different sensitiveness. Some of them are sensitive date such as patient's medical history, medical diagnosis and results of examinations, which should not be released to the others except the patient, doctors and the related nurses. Also some data are less sensitive or not sensitive including patient's personal data, appointment times, etc. In this research the users presented in health system include: patient, receptionist, nurse, general practitioner and specialist that their working relation was presented in section 3. As it was mentioned before the interactions between the roles are presented as a label. Certainly during such interactions and communications, different types of data are sent and received. In these transactions some data may be very sensitive and therefore needing more protection or some data less sensitive and needing less protection. We separated sensitiveness of the data on the basis of the presentable labels in communications and on that basis select the related cryptography algorithm. Table 3 presents different types of communications and also the type of the selected cryptography label and algorithm.

Table 3. Relations in e-health, presented label and the selected cryptography algorithm

Relations	Label	Cryptography algorithm type
Patient, Nurse, General Practitioner, Specialist	I_C_S_13 I_C_S_15 I_C_S_45	AES (256-Bit), ECC
Patient, Nurse, General Practitioner	I_C_S_14 I_C_S_34 I_C_S_43	AES (192-Bit), ECC
Patient, Receptionist, Nurse, General Practitioner	I_C_S_12 I_C_S_23 I_C_S_24 I_C_S_32 I_C_S_42	AES (128-Bit), ECC

6 DIGITAL SIGNATURE

A digital signature is used for one message and in brief a digital signature is an electronic signature, which may not be forged. A digital signature includes a unique mathematical fingerprint from the current message, which is also called One-Way-hash. The receiving computer receives the message and executes the same algorithm on the message, decrypts the signature and compares the results. If the fingerprints are similar, the receiver can be sure of the sender's identity and correctness of the message. This method guarantees that the message has not been altered during transfer process. In this architecture we have used a Hash algorithm for creation of a message summary and use ECDSA (Elliptical Curve Digital Signature Algorithm) [6] to guarantee Authentication. Key size in this algorithm is 192 bits including a security level equivalent to DSA (Digital Signature Algorithm) with key size of 1024. [7] The summarization algorithm used in our proposed architecture is SHA-1, which has the three following specifications:

- Message length is fixed, i.e. with each length of message its summary is the same. This length for SHA-1 is 160 bits.
- Each entrance bit is effective on exit. It means that two messages, which are only different in a bit, have different summaries.
- They are unilateral: it means that with having the message summary we cannot build the original message.

It is of special importance that with use of the mentioned method in our architecture, the security requirements of authentication, non-repudiation, integrity and confidentiality are met.

When the sender creates the message summary with use of SHA-1 function and adds it to the end of his message as digital signature and sends it to the receiver on the other part, the receiver, separated the message summary from the original message and decrypts the message summary with the sender's public key. Then he compares the summary with the original massage produced by himself and their conformity means that the sender is the person claiming so, because only he has the private key corresponding to his public key (Authentication).

Also the message data integrity has been protected, it means that the message has not been altered, because otherwise the results would not be conforming (Integrity). On the other hand, the sender cannot deny sending of message, because no other one has his private key (non-repudiation).

7 LOG STRATEGY (EVENTS REGISTRATION)

Along with the digital signature a log strategy is used to ensure non-repudiation. The log server is a security mechanism to protect a physician from a false repudiation. If a physician refuses to accept false diagnosis and treatment for a patient, the log server can provide the transaction records as proof. In fact Log strategy acts as a third party like a witness for performance of the service rendering and the service receiving performance method.

8 THE PROPOSED ARCHITECTURE

Figure 6 has presented the proposed model for security of communications in e-health. In this model there are three main areas including operator's position, security communication layer and server's position. The secure communication layer provides a proper amount of security for communication.

For entrance to the system an authentication process (biometric and smart card) is required for all roles to recognize the authorized users. After authentication process was performed successfully and authentication was guaranteed, a user can execute applied processes. Whereas the main aim is to make the communications between the two sections secure, therefore before start of interchange of any type of massage, a proper security protocol should be executed so that communication is performed according to the layer. When a user enters the system through smart card and biometric for the first time, the system creates the public key for the user. The private key is protected by the user and the public key is used as the parameters, which are issued by a certificate and signed by the server. A copy of the certificate is kept in the server.

After user's authentication and his recognition as authorized, interactions between the users are performed. As it was mentioned before, the interactions of each role are presented with a label.

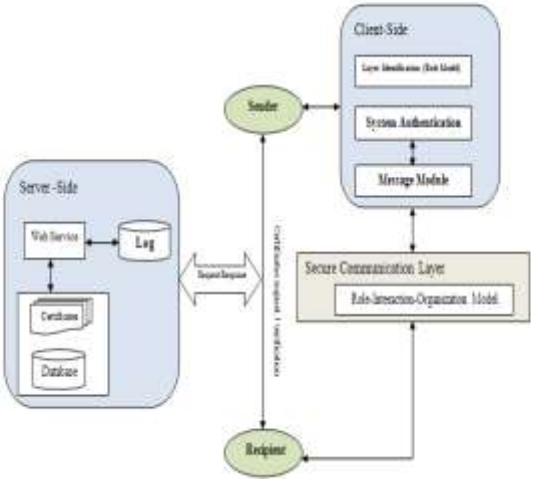

Figure 6. The proposed model for secure interchange

In Figure 6 the sender can connect to the receiver and they can distinguish each other's validity with use of the certificates. They may request the server to investigate their certificates to make sure that the certificates are valid. If a user (sender) wishes to send a message to the receiver, the sender sends a message (message opening, saving, edition and deletion) in Message Module to the receiver.

9 CONCLUSION AND FUTURE WORK

In this paper we described a modern architecture for e-health services that the authentication mechanism for Users working within the GHIN e-Health environment. Since Users access GHIN services using a browser and an GHIN Portal, the authentication of Users was mapped on top of SSL client-side authentication. The credentials used in this authentication are provided by their HCUs. These credentials are formed by a private key and a public key certificate, both stored inside a smart card.

This architecture was examined with different algorithms for communications in e-health and the original results were presented. In our proposed architecture with composition to two cryptography algorithms of ECC and AES we could present data cryptography in a more secure method. As compared with the existing architectures, which used RSA or AES algorithms (singly), our system has been appeared more efficient. Whereas in this article we have used AES for more efficient and AES besides ECC for more security and at the same time with digital signature with use of ECDSA we could increase confidentiality, integrity, security, confidentiality and non-repudiation (of both parties) and make the non-repudiation ability more definite, also with use of a new model of role- based access control we could label the interactions between the roles and determine the level of the data sensitiveness on the basis of labels and use a cryptography algorithm proportionate to data sensitiveness, so that we can execute the proposed security frame and the related mechanisms on an e-health system and examine our architecture in future. In the future project we are trying to use a more suitable access control model so that we can apply our architecture in a dynamic and distributed environment.

REFERENCES

1. Li, W., Honag,D.: A New Security Scheme for E-health System.: iNEXT – UTS Research Centre for Innovative in IT Services and Applications University of Technology, Sydney, Broadway NSW , Australia (2007).
2. Smith, E., Eloff, J.: Security in Health-care Information Systems-current Trends.: International Journal of Medical Informatics, Vol. 54(1), pp.39-54 (1999).
3. Boonyarattaphan, A., Bai, Y., Chung, S.: A Security Framework for e-Health Service Authentication and e-Health Data Transmission.: Computing and Software Systems Institute of Technology University of Washington, Tacoma (2009).
4. Dhawan, P.: Performance Comparison: Security Design Choices.: Microsoft Development Network, http://msdn2.microsoft.com/en-us/library/ms978415.aspx (2007).
5. Tamimi, A., A.-K. : Performance Analysis of Data Encryption Algorithms., http://www.cse.wustl.edu/~jain/cse56706/ftp/encryption_perf/index.html (2007).
6. Vanstone, S.: Responses to NISTs Proposal.: Communications of the ACM, 35:50–52 (1992).
7. Lenstra, A. K., Verheul, E. R..: Selecting cryptographic key sizes.: Lecture Notes in Computer Science, 1751:446–465 (1999).
8. Elmufti, K., Weerasinghe, D., Rajarajan, M., Rakocevic, V., Khan, S. : Timestamp Authentication Protocol for Remote

Monitoring in eHealth.: The 2nd International Conference on Pervasive Computing Technologies for Healthcare, Tampere, Finland, pp. 73-76 (2008).

9. Russello, G., Dong, C., Dulay, N.: A Workflow-based Access Control Framework for e-Health Applications.: Proc. of the 22nd International Conference on Advanced Information Networking and Applications - Workshops, pp. 111-120 (2008).

10. Bourka, A., Polemi, N., Koutsouris, D.: An Overview in Healthcare Information Systems Security, In: MEDINFO, 2001.