RFID TECHNOLOGY FOR SECURING E-HEALTH SYSTEM: SERVICE OF CONSULTING A DOCTOR

Mike Yuliana, ST, MT
Isbat Uzzin Nadhori, S.Kom, MT
Amang Sudarsono, ST, PhD
Electronic Engineering Polytechnic Institute of Surabaya, Indonesia

Abstract

In this research, we propose an anonymous authentication e-health system and the use of RFID smart card that contained hidden patient's personal identity, so the privacy of doctors and patients could improved optimally (for example, by hiding their identity). We employ Camenisch-Lysyanskaya Signature Scheme to achieve anonymity and Java programming for constructing our anonymous authentication e-health system. The results showed that the system that made have been able to protect the personal data of patient and doctor. For anonymous process, prover needs more time than the verifier, this happens because in the CL scheme, proof of knowledge is a combination of CL signatures with evidentiary value of the commit inside the CL signature value. Computational time that required for the authentication process with the smart card until accepted by the e-health system takes 0.6 s.

Keywords: E-health, authentication, CL signature, smart card

Introduction

Nowaday e-ID technology has developed rapidly, and widely applied in daily life - days. One of the real technology of e-ID is a Radio-Frequency Identification (RFID), that often used in the e-health services for a variety of cases, among others, patient safety and medication management (kou-hui *et al*., 2013), ubiquitous healthcare systems (Kreps and Neuhauser, 2010), inpatient-care systems [Krummenacher *et.al*, 2007], autotracking clinical interventions, and electronic-health records. All of these applications promise patient, nurse, doctor, and administrator to efficiently access relevant health information, enhance the quality of patient care, reduce healthcare errors, increase collaboration, and encourage the adoption of

healthy behaviors. E-ID basically contains information about the attributes of client, such as name, address, gender, occupation, place and date of birth, and so on. This information in a commercial case is very important and can be used in an authentication system based on client's attribute (Guo *et al*, 2012).

One of the serious issues in the systems of e-ID is related to the privacy of user information. Most of the e-ID system is leaking the privacy of information that is held by the user. Service providers can freely obtain, collect and store all information relating to each user when user access the services. One solution that can be used to overcome the leakage of the user information is anonymous credential systems(kou-hui *et al*., 2013).

In this paper, we focus on RFID technology integrated with the process consulting to doctor. In particular, the issues of performance efficiency, system security, and patient privacy will be thoroughly investigated. This system will be integrated with the database on the web server. Electronic patient identity using RFID, that contains the patient's signature to consult a doctor. The use of signature / credential is intended to hide the identities of doctors and patients (anonymous), because of the players involved in e-health system only allowed to know certain information that used when access to the system and not a players's privacy information. Thus, researchers hope will open up the eyes, giving insight, and make a commitment to the security of e-health system in Indonesia so it will increased the trust of the public.

Methods

Anonymous Credential System

The Players in anonymous credential system are issuer, user, prover and verifier. The players have a role in running the issuing protocol, where a credential created by the issuer and given to the user. On the proving protocol, user creates a proof to convince the verifier that he is a valid user. A company can act as a verifier and run proof protocol with the user. A user chooses a master secret key (m_1) based on parameters group from the system, m_1 also used to get a pseudonym that will be used as a session identifier in the communication process. To fulfill the anonymity, the user creates a new pseudonym whenever there is communication, so each communication session can not be linked (unlinkability) (Kellermann and Scholz, 2010).

Credential issuance protocol is a protocol that is run by the issuer and the recipient (Bangerter *et al.*,2004) . The credential contains a set of attributes that are used to create a proof of possession as proof of ownership attributes. Fig. 1 provides an illustration of the anonymous credential system. This system basically consists of a user and organization. Organizations can

act as verifier or credential issuers (Sudarsono *et al*, 2010). Organization have the possibility to act as issuer and verifier in one transaction, for example when issuing a credential and verify the credential upon another. The user has a role using the pseudonym and obtain a credential from the issuer, and then show the credential to another organization for verification (Sudarsono *et al.*, 2011). Even all the organizations work together, they are not able to link a pseudonym that was verified by any organization and issued by any organization. And there is the possibility to show the credential as many times to the same organization, without knowing the user (Yang *et al.*, 2009).

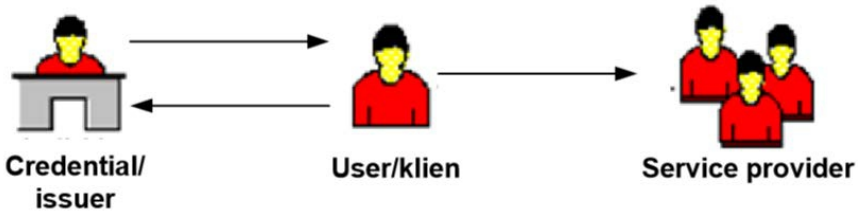

Figure 1. Credential issuance protocol

CL (Camenisch-Lysyanskaya) Signature-Scheme

We recall this signature scheme (the CL signature scheme) and the related protocols here (Kellermann and Scholz, 2010).

Key generation. On input l_n, choose an l_n bit RSA modulus n such that $n \leftarrow pq, p \leftarrow 2p' + 1, q \leftarrow 2q' + 1$ where p, q, p' and q' are primes. Choose, uniformly at random, $R_0, \dots, R_{L-1}, S, Z \in QR_n$. Output the public key $(n, R_0, \dots, R_{L-1}, S, Z)$ and the secret key .

Message space. Let l_m be a parameter. The message space is the set

$$\{(m_0, \dots, m_{L-1}) : m_i \in \pm\{0,1\}^{l_m}\} \quad (2)$$

Signing Algorithm. On input $m_0, \dots, m_{L-1}$, choose a random prime number e of length $l_e > l_m + 2$, and a random number v of length $l_v \leftarrow l_n + l_m + l_r$, where l_r is a security parameter. Compute the value A such that

$$A \leftarrow \left(\frac{Z}{R_0^{m_0} \dots . R_{L-1}^{m_{L-1}} S^v}\right)^{1/e} mod\ n \quad (3)$$

The signature on the message $(m_0, \dots, m_{L-1})$ consists of (A, e, v).

Verification Algorithm. To verify that the tuple (A, e, v) is a signature on message $(m_0, \dots, m_{L-1})$, check that

$$Z \equiv A^e R_0^{m_0} \dots R_{L-1}^{m_{L-1}} S^v (mod\ n) \quad (4)$$

where $m_i \in \pm\{0,1\}^{l_m}$, and $2^{l_e} > e > 2^{l_e - 1}$ all holds.

Secure E-health System Design

In this research, we designed a scenario for the case of e-health, that is focused on the creation of e-id, and interaction between patient and doctor.

Privacy Requirements

Doctors in many cases knowing the identity of his patients, however in certain cases the patient will choose which pieces of information that should not be known by doctors. Doctors should always get permission to access patient's health record.

Security Requirements

Some security requirements of secure e-health system are listed as follows.

Authentication. all players involved in e-health systems in each transaction must be able to pass the authentication process. It's mean that they must be able to convince the other players that they are valid players .

Data Integrity. recipes, health data center server, invoices, and other data must be valid in order to prevent interference. All players involved in the system must be able to be checked for integrity.

Confidentiality. all data / items involved in each transaction should be guaranteed confidentiality.

Players

- User act as patient
- Doctor
- Hospital

The role of each player

- Patient: requiring care / treatment or medical consultation.
- Doctor: requires access to all the patient's health history data.
- Hospital: issue credential / signature

issuing of e-id

At the Registration process in the hospital, patient will enter privacy data such as name, address, place / date of birth etc. The hospital will process that data and send it to the e-health system to obtain the signature / credentials as seen in Fig. 2. The Signature that has been obtained, then inserted on RFID card and called as e-id.

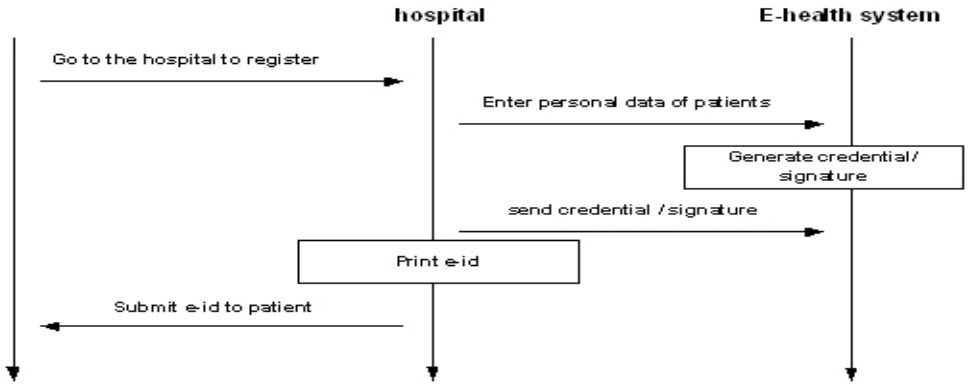

Figure 2. Issuing of e-id

Consulting a Doctor

Patient visit a doctor to get medical help. The patient identifies himself to the doctor by using e-ID. Doctor also prove his qualification by using e-ID. Patient have the authority with e-ID to allow doctor accessing his medical record. The doctor checks the patient's health, adding new information to the patient's health history data, and then providing medical recipes to patients and provide a bill of payment that can be reimbursed by the patient's health insurance company. The detail Flow Interaction between patient and doctor is shown in Fig. 3

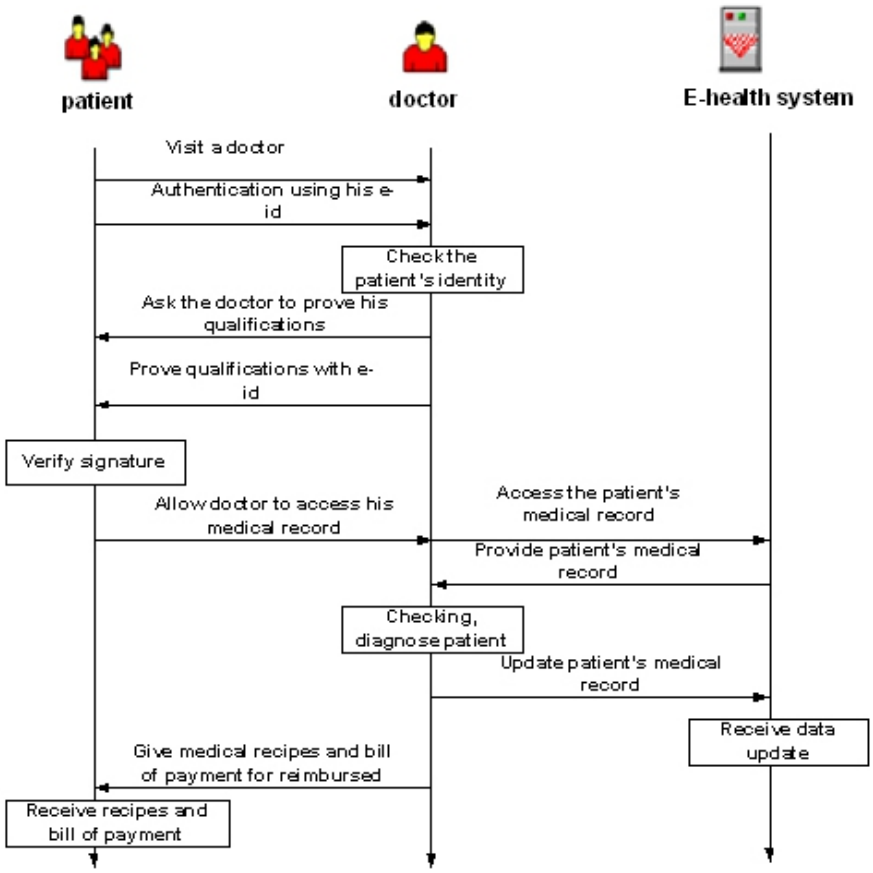

Figure 3. Flow interaction between patient and doctor

Experimental Result

In this research, the anonymous system and e-id will be tested by using PC with as shown in Table 1, and RFID reader with specifications as shown in Table 2.

Table 1. Specifications of PC used in experiment

Specification of	Remarks
Software	java
O/S	Windows 8 (64 bit)
CPU	Intel Core™ i5-3317U Processor (1.70 GHz)
RAM	4 GB

Table 2. Specifications of RFID reader used in experiment

Specification of	Remarks
Type	EM9918
Frequency	125 KHz
Card format	EM4100, GK4001/4011,T5557(EM format)
Baud Rate	9600
Interface	Serial UART RS232
Supply	9-12 V DC

E-id system created as an patient's and doctor's identity card , so they can access e-health system without reveal their personal identity. Several test that performed on the e-id system are anonymous credential system performance, security of personal data and integration of e-health systems with e-id.

a. Anonymous Credential System Performance

In this section, we discuss about the performance of an anonymous credential system, where the testing include execution time of key generation, issuing credentials and credential proving.

Table 3. Execution time of public key generation

No	Execution Time (s)	
	$l_{n=}$1024, l_{pt}=72	$l_{n=}$2048, l_{pt}=104
1	2	5
2	2	10
3	3	12
4	2	7
5	2	16
6	2	12
7	3	15
8	2	16
9	2	16
10	2	5
average	2.2	11.4

Experimental results in Table 3 and 4 showed that the public key generation requires a longer time, because the number of public key's components / elements are more than private key's components. The increase in bit RSA modulus (ln) and the generation of primes (lpt) effect on

execution time required, where the processing time of public-key increased more than private key that is equal to 9.2 s.

Table 4. Execution time of secret key generation

No	Execution Time (s)	
	$l_{n=}$1024, l_{pt}=72	$l_{n=}$2048, l_{pt}=104
1	2	4
2	2	10
3	2	11
4	1	9
5	2	10
6	2	11
7	3	12
8	2	8
9	2	9
10	2	10
average	2	9.4

Table 5. Anonymous credential process performance

No	Process	Time(s)
1	Generating key Secret Key Public Key	4.2 2 2.2
2	Issuing credential/signature	0.2
3	Proving credential/signature	0.5

Table 5 show the results of measurements for all processes on the anonymous credential system. Key generation process need the longest time 4.2 seconds,it happen because there is generation of RSA modulus. Issuing credential that consists of multiple processes which include the generation and verification of CL signatures need the fastest time. Signature generation is done by the signer and verification by the verifier. For authentication, prover requires more time than verifier. Because in the CL scheme, the proof of knowledge is a combination of a CL signature with the proof that a committed value included in the CL signature.

b. Security of Personal Data

At the time of the registration process, the patient asked to enter personal data such as name, address, place / date of birth and several other private data. The registration process will generate cryptographic personal data that known as credential/signature. Fig. 5 shows an example of credential / signature that will be inserted into smart card (e-ID). E-id which has been accepted by the patient, will be used in the authentication process for a variety of cases including the opening of patient's medical record and and payment of consultation fee .

Figure 5. Example of credential/signature

Fig. 6 show the authentication process between patient and doctor at the time of the examination and opening the patient's medical record. There must be approval from the patient by using e-id to open a patient's medical record at the time of consultation, and the doctor must shows their qualifications. If the signature of patient and doctor accepted, then the doctor can read and update patient's medical record. It shows that, the system that made has been protect the personal data of the patient because there is no display personal information such as name, address on the patient's medical record. In addition, doctor also can not open the patient's medical record if the patient does not give permission.

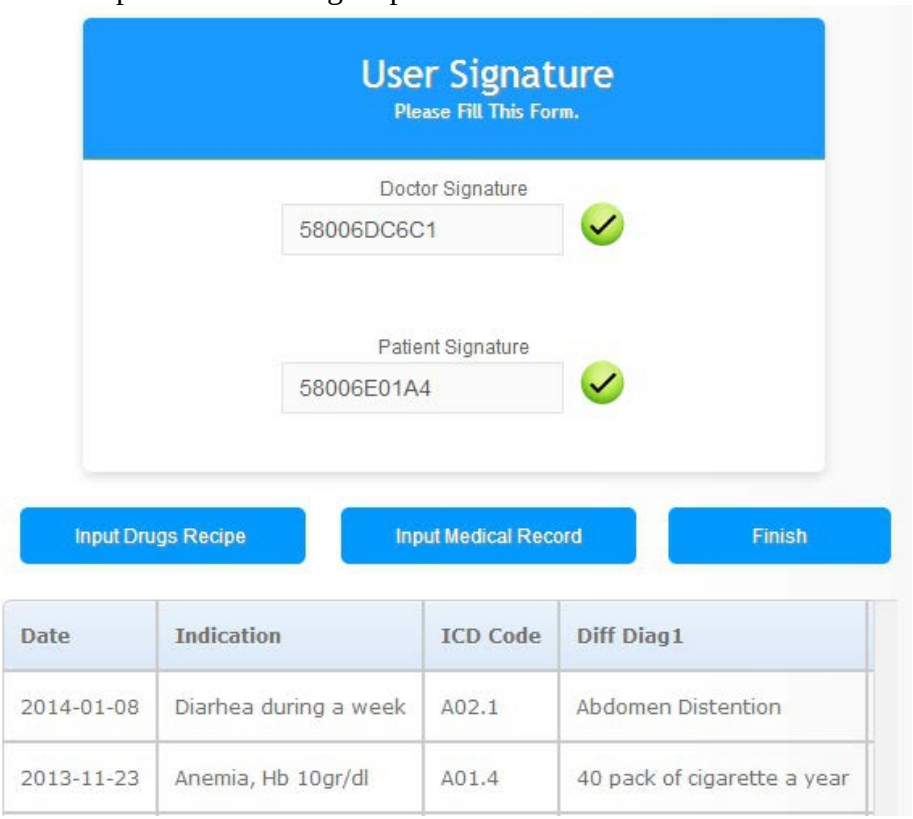

Figure 6. Authentication process between patient and doctor

At the time of payment process, patients do not need to carry a consultation card, payment processing is done by performing authentication using e-id so the cashier does not need to know the data of patients and doctors.

c. Integration of E-Health System with E-id

In this experimental test, authentication process was calculated from the e-id until accepted by the e-health system. Table 6 showed that the execution time of authentication process by using e-id is 0.63 s, and table 7 showed that various distance of the tag at the time of the authentication process does not significantly affect execution time , where the average time of the process is 0.6 s.

Table 6. Execution time of authentication process using e-id

No	Execution time (s)
1	0.7
2	0.6
3	0.6
4	0.7
5	0.6
6	0.6
7	0.6
8	0.7
9	0.6
10	0.6
average	0.63

Table 7. Execution time of authentication process from various distances tags

No	Distance of Tag(cm)	Execution time (s)
1	0	0.65
2	2	0.64
3	4	0.64
4	6	0.65
5	8	0.66

Conclusion

In this research, we present privacy protection systems of client on consulting services to doctor based e-id using an anonymous credential system, where experimental results showed that the system that made has been protecting the personal data of patients. The experimental results also showed that authentication process by using e-id need execution time around 0.6 s, whereas testing with different tags position do not influenced significantly to the time that required for authentication process.

References:

B.Kellermann and I.Scholz. Anonymous Credentials in Web Applications : A child's Play with a Prrime Core. Proceedings of IFIP AICT, pp 237-245, 2010.

Y.yang, R. H. Deng, F. Bao. Privacy-Preserving Rental services using One Show Anonymous Credential System. Security and Communication Networks, Vol 2, Issue 6. Pages 531-545, 2009.

Kou-Hui Y., Nai-Wei L., Tzong-Chen W., and Chieh W. Secure E-Health System on Passive RFID : Outpatient Clinic and Emergency Care. International Journal of Distributed Sensor Networks, Article ID 752412, 2013.

R. Krummenacher, E. P. B. Simperl, L. J. B. Nixon, D. Cerizza, and E. Della Valle. Enabling the european patient summary through triplespaces. In CBMS, pages 319–324, 2007.

G. L. Kreps and L. Neuhauser. New directions in eHealth communication: opportunities and challenges. Patient Education and Counseling, vol. 78, no. 3, pp. 329–336, 2010.

L.Guo, C. Zhang, J.Sun, Y.Fang, A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks. Proceeding of ICDCS, pp 224-233, 2012.

A. Sudarsono, T. Nakanishi, and N. Funabiki. Efficient proofs of attributes in anonymous credential systems using a pairing-based accumulator. *Computer Security Symposium 2010 (CSS2010)*, pp. 801–806, 2010.

A. Sudarsono, T. Nakanishi, and N. Funabiki. An Implementation of a Pairing-Based Anonymous Credential System with Constant Complexity. Proceeding of The International Multi Conference of Engineers and Computer Scientists 2011 (IMECS2011), pp. 630–635, March 16-18, Hong Kong, 2011.

E. Bangerter, J. Camenisch, and A. Lysyanskaya. A cryptographic framework for the controlled release of certified data. Security Protocols Workshop, volume 3957 of Lecture Notes in Computer Science, pp. 20–42. Springer, 2004.