

# Implementation of Authorization System for Tele-medical Service in Ubiquitous Environment

Youri Lee<sup>1</sup>, Donggwe Park<sup>2</sup>, Yudong Hwang<sup>2</sup>, Seungyeop Yoo<sup>2</sup>, Jongsoo Jang<sup>1</sup>

<sup>1</sup> Managed Security Research Team, Knowledge-based Information Security & Safety Research Division, [ETRI](#), Daejeon, Korea.

<sup>2</sup> Dept. of Information and Communication Engineering, SoonChunHyang University, Chungnam, Korea.

{thisglass, jsjang}@etri.re.kr, {dgpark, coppermilk,yoosy35}@sch.ac.kr

**Abstract.** Security threat connected with unlawful access of medical treatment information is involved with patient's life. We need authorization system that is strong what first of all and can do it that authoritativeness guarantee of certification service is essential. Therefore, in this paper, we implement bio device certificate for medical equipments for trust of data and user principal who user certificate, medical equipments as well as attribute certificate of users collects and prototype of authentication system that living body information certificate for confirmation is available. By verifying effectiveness of proposed system and implementation of authorization system that consider access control model which is suitable for medical treatment environment, we show that minute access control for Tele-medical service offer in Ubiquitous environment is available.

**Keywords:** Authorization System, Tele-medical service, Bio Device Authentication

## 1 Introduction

Security technology connected with privacy and authorization and authentication to protect private life information of individual is essential, because Tele-medical service handles important medical treatment information of individual. But, Ipath[1], OpenEmd[2], TeleCardio-FBC[3], Medintagra Web[4] these are representative Tele-medical system present provide authentication service that use ID and Password as user authentication. These user authentications based on ID, Password could be used by someone who knows ID and Password even if they are not principal who use service. They can use the service instead of. Therefore, need the process that use living body information of user so that only oneself may can approach to medical treatment information for privacy protection through medical treatment information.

Tele-medical service such as WBASN[5], CodeBlue[6] is using living body authentication. When information of patient was exposed to user who power does not exist by doing not authentication about user's authority even if used a living body authentication technology, patient's privacy and integrity of various data do not get

This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD, Basic Research Promotion Fund)(KRF-2008-313-20080730).

guarantee. It can be fatal to security. Therefore, it needs authentication process about authority of user.

Therefore, in this paper, we consider suitable access control model[9] in user authentication, user attribute authentication[7], bio device authentication[8], living body information authentication and medical treatment environment for Tele-medical security service offer in Ubiquitous environment and verify effectiveness of the system proposed by composing and implementation of authentication and authorization system.

Also, through a scenario, we confirm accessibility that is reliable to medical treatment information in various circumstances and environments.

## **2 Background**

Now, as user authentication and attribute authentication, in wire environment PKI and authority administration base structure are used and in wireless environment wireless PKI and wireless authority administration base structure are used. These are amiss in Ubiquitous environment because that considers wire and wireless environment separately. Therefore, we compose user authentication and user attribute authentication system in Ubiquitous environment that integrate wire and wireless environment[WPMI integration treatise].

Wire and wireless integrated system for user authentication and user attribute authentication can bring privacy infringement when medical treatment information of user who do not want to exhibit is exposed by confirming information of the user as right user even if an user who know user's personal key based on certificate is not the actual user. Therefore, we reinforce user's authentication with bio authentication technology using living body information such as fingerprint and iris so that in wire and wireless integration authentication and authorization system only the person oneself use the system.

User authentication and authentication of device that recognize patient's information are also important for Tele-medical service in Ubiquitous environment. Tele-medical service is impossible without all authoritativeness of medical devices that sense living body information of patient such as ECG, blood pressure, pulse or environment information such as position of patient in a remote place. Therefore, we applied technology that authenticates devices through certificate issuance of device at trust institution for device certification to medical device.

A device certification technology that design so that can do sensor and device authentication through bio device certification that bio device certification institution issues were studied.

The user authorization method based on ID, Password of existing Tele-medical system is not fit to Tele-medical System that handle person's life. Hence, RBAC for U-healthcare model[9] which is suitable for medical treatment service of ubiquitous environment was proposed with considering Tele-medical System special quality of Ubiquitous environment like access control and medical affairs by circumstance information such as position or time of user, condition, user privacy.

For all that reasons, in this paper, we verify effectiveness of system that is proposed by composing authentication and authorization system that consider access control model suitable for user authentication, user attribute authentication, bio device authentication, living body information authentication, medical treatment environment and implementation of prototype for Tele-medical service in ubiquitous environment.

### 3 Authentication system implementation for Tele-medical service

#### 3.1 System configuration

Authentication for Tele-medical service in Ubiquitous environment is separated into device authentication, user authentication and user attribute authentication. Figure 1 illustrates that security framework is consisted of sensor device, client and server.

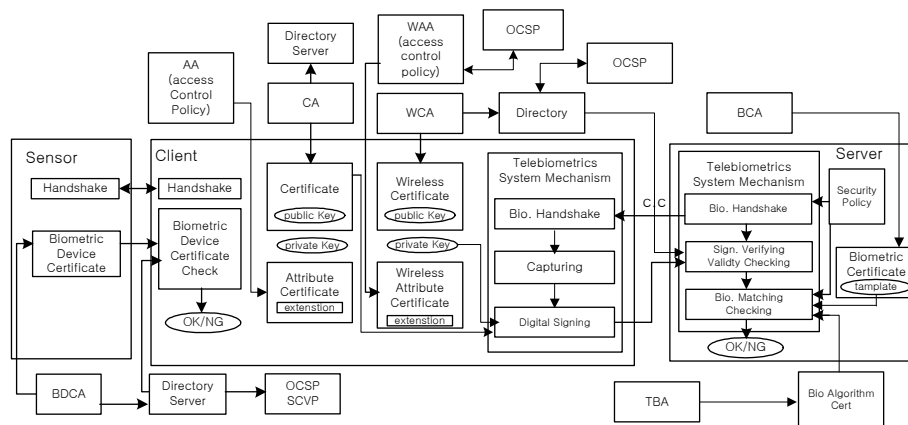
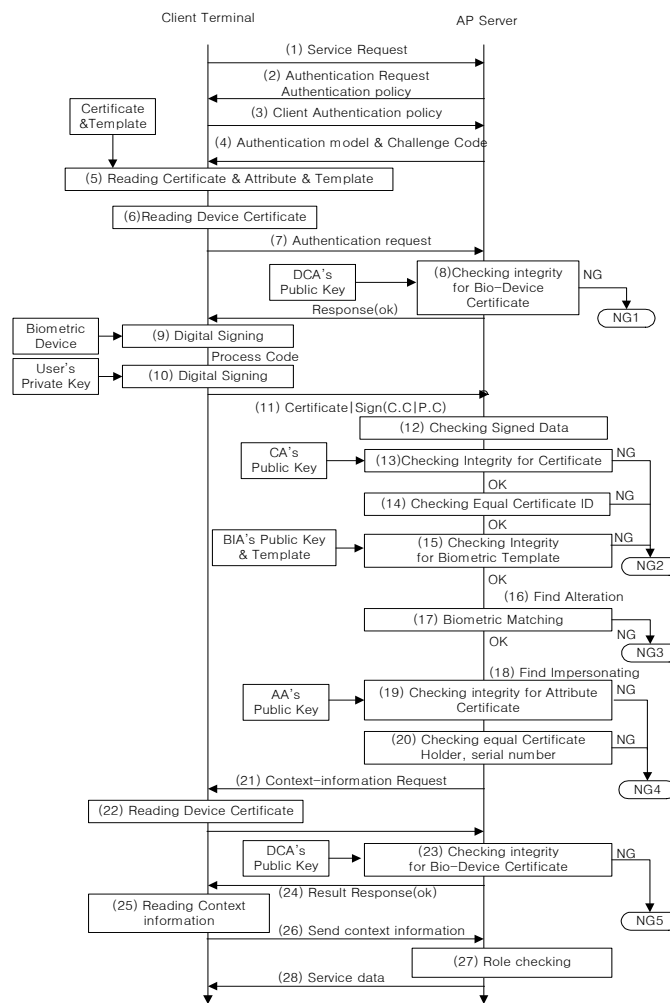


Figure 1. Security framework for Tele-medical service in Ubiquitous environment

Client use X.509 certificate issued by authentication institution for user authentication of Tele-medical system and use bio certificate based on X.509 for strong certification system. Also, for providing service which is proper for user's attribute and authority in wire environment which wish to use Tele-medical service, user's attributes are authenticated by attribute certification. For user certificate, user in wireless environment same as wire environment uses wireless public key certificate that follow X.509 certificate or wireless transmission class security protocol (WTLS : Wireless Transport Layer Security) certificate which is relatively lighter than X.509. And user's attributes are authenticated by using wireless attribute certificate proper for wireless environment. It offers user authentication that use bio information for reliable Tele-medical service offer in wireless environment. Because of worry about personal

information leakage by popularization of wireless Internet use, technical development that applies biometrics to portable telephone security has been attained. Hence, bio information abstraction such as peculiar voice of user, fingerprint, face and iris are possible using portable telephone. We verify bio certificate by comparing with template information that is registered in bio authentication institution extracting bio information.

If user authentication process ends, user acquire authority of user through RBAC for U-healthcare access control model and is provided correct reliable service in own authority through verification for attribute certificate issued for authentication.



**Figure 2.** Security process of authentication and authorization system for Tele-medical service of Ubiquitous environment

Differences between our proposed mechanism and existing mechanism are given in Table 1.

**Table 1.** Comparison proposed mechanism with existing mechanism.

	User Authentication		User Authorization		Device Authentication	Bio Authentication	Wire, Wireless Integrated Services
	wire	wire less	wire	wire less			
PKI	yes	no	no	no	no	no	no
WPKI	no	yes	no	no	no	no	no
PMI	no	no	yes	no	no	no	no
WPMI	no	no	no	yes	no	no	no
PKI+PMI	Yes	no	yes	no	no	no	no
WPKI+W PMI	no	yes	no	yes	no	no	no
Device	no	no	no	no	yes	no	no
Bio	no	no	no	no	no	yes	no
Proposed System	yes	yes	yes	yes	yes	yes	yes

### 3.2 Implementation environment

In Ubiquitous environment, apply access control model for the Tele-medical service to the wire and wireless integration Tele-medical service combined with user authentication, user attribute authentication, living body information authentication and device authentication to provide safe service that is correct in user authority of the authentication system for the Tele-medical service and implement a prototype. It's implementation environment : Windows XP for system implementation environment, Visual Basic.net and J2ME for user simulation and user GUI, TinyOS 1.0 and NesC to use Zigbee's biosensor for circumstance information and medical treatment information data collection and MySQL Server 6.0 for database.

Figure 2 illustrates security process for the prototype implementation of the system. Prototype that is implemented on the basis of process of above figure 2 consist of bio device module, personal server module, bio device authentication module, bio authentication module, user authentication module, user attribute authentication module, wireless user authentication module, wireless attribute authentication module and Tele-medical service server modulo. Each module has policy modules of authentication institution, password module for encryption such as key pair creation and authentication administration module that issues and manages certification. Also, it consists of directory server for certification and real-time certificate verification protocol for certification verification in wireless environment.

### 3.3 Authentication system for Tele-medical service in wire environment

We established a following scenario for effectiveness verification of security process in wire environment proposed in this paper. In wire environment, patient measures own present heart rate and temperature and patient wishes to request treatment to a doctor with the results. Patient connects in Tele-medical service as next figure 3.

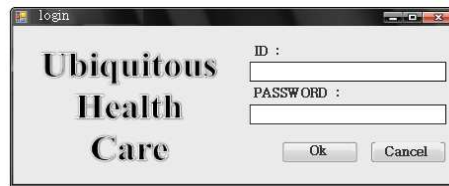


Figure 3. Tele-medical service connection

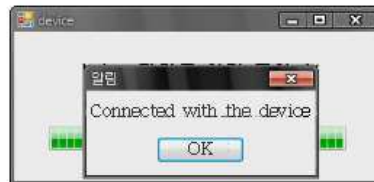
Existent Tele-medical service can use the service as a user by access control policy if input ID and password to connect in the medical treatment service as figure 3. But, the system proposed in this paper needs user authentication process that use authentication with below figure 4 so that only user who is authenticated from a reliable authentication institution can use the system.



Figure 4. User authentication with public key certificate

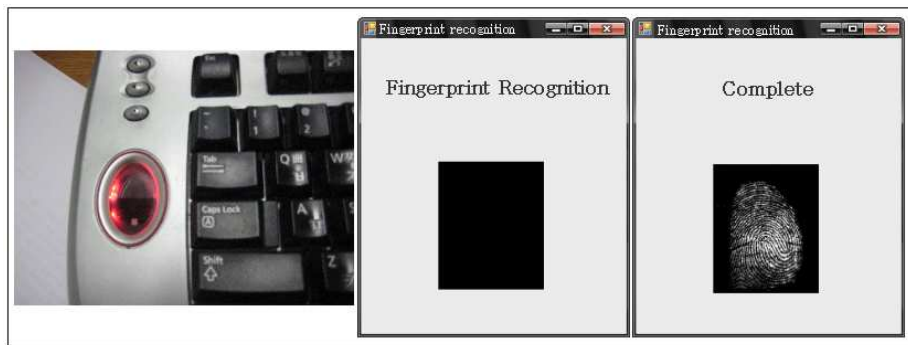
Patient takes public key certificate, attribute certificate and bio certificate that is issued from authentication institution. Patient wishes to use fingerprint recognition among own medical information to make sure certain identity. Read bio device

certificate of fingerprint recognition device and check effectiveness of certificate before connection is completed connecting bio device to use fingerprint recognition device. When bio device certificate is valid, send a message that device is connected completely as following figure 5.



**Figure. 5.** Connection to bio device

Fingerprint recognition device confirmed as reliable devices through bio device certificate operate fingerprint recognition as figure 6. Now, a lot of products are supplying programs that support fingerprint realization. Figure 6 depicts a fingerprint recognition device and a fingerprint recognition application program.

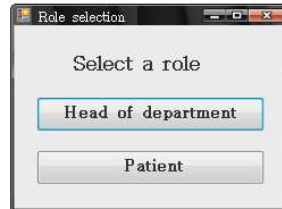


**Figure. 6.** Fingerprint recognition device and application program

Recognized fingerprint data is identified by digital signature with user's personal key and sent to a server. In the server, it checks signature data and user's certificate with public key of authentication institution. Also, it checks ID item whether template is same as user of public key certificate and checks effectiveness of bio certificate. If one is not verified among those, user can't use this system because the user is untrustworthy. If compare with template stored in bio authentication institution and fingerprint data which user sends and they are matched, the user must be reliable.

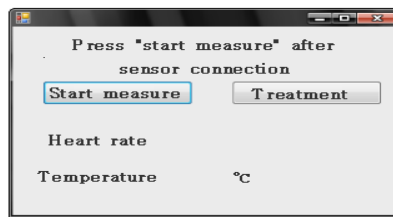
Check effectiveness by using public key of attribute authentication institution for verification of attribute certificate after user certification and ask patient circumstance information after bring attribute of user through a comparison whether owner of public key certificate, serial number and attribute certificate are matched. The server offers user service that can check role after examine circumstance information and

confirm constraints of user. This user has two roles a head of a department and patient with below figure 7 because he is working as a head of a department in hospital.



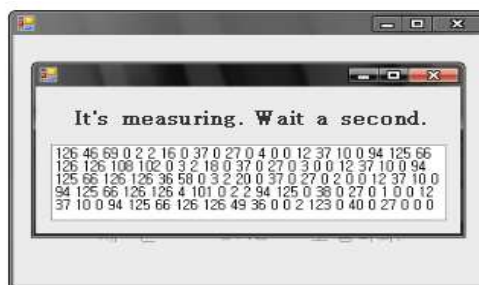
**Figure. 7.** User's role selection window

When user chose the role of the patient, the service that can measure medical treatment information of patient as next figure 8 is provided. Next figure 8 shows service window before measuring heart rate and taking temperature.



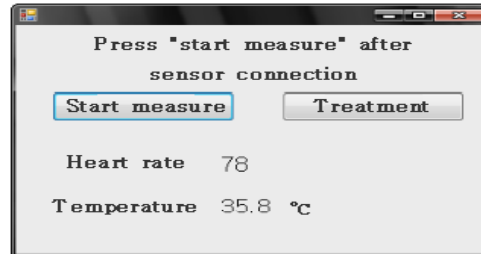
**Figure. 8.** Heart rate and temperature measurement window

When click "starts measurement", it shows a measuring window. Heart rate and temperature measurement are started through Zigbee sensor that we use for implementation of the system in this paper.



**Figure. 9.** Heart rate and temperature measurement

If measurement is finished, a result window as fig 10 is shown and user can request medical examination and treatment.



**Figure. 10.** After heart rate and temperature measurement

If a doctor of a user is assigned from 9 to 12 o'clock to give medical treatment for Tele-medical service, when patient get authenticated with patient's attribute, medical examination and treatment request time may be set from 9 till 12 o'clock. Therefore, the service may not be offered if patient tries to do medical examination and treatment request at 7 o'clock in the evening.

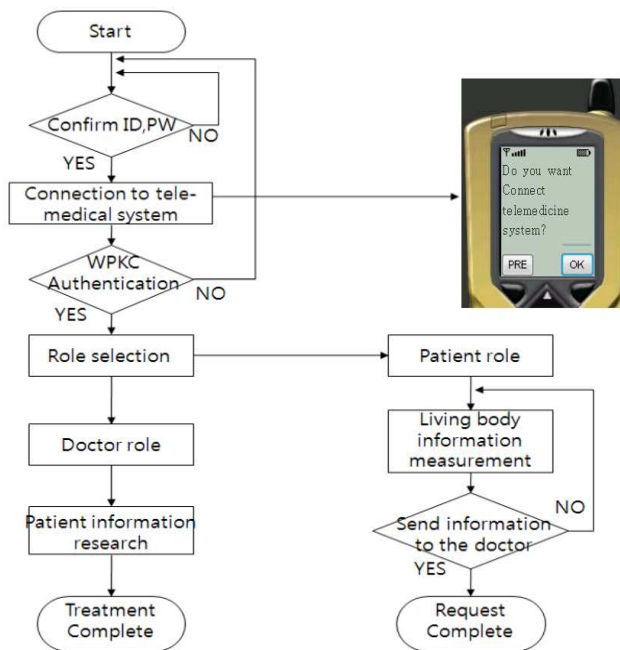
User who use this service can trust in data collected from bio device when fingerprint realization with getting bio device authentication. Hence the user can approach to own data and the user's data and privacy are protected even if someone knows the user's ID and Password.

User can get provided fluidic and reliable medical treatment service with that the user is granted by access control model suitable for Tele-medical treatment service.

### **3.4 Authentication system for Tele-medical service in wireless environment**

In this paper, it composes following scenario for effectiveness verification of security process in wireless environment of authentication and authorization system. Emergency circumstance happened in the interior that Internet is not established. A doctor of public health center in interior arrived in the place that emergency circumstance happens but the doctor could not get state information of patient. Because it is circumstance that life is threatened, it is most important for the circumstance to know medical examination treatment record about patient and all drugs prescribed in existing. Therefore, the public health center doctor connects to the Tele-medical service and examines medical treatment information of patient. The doctor must receives hospital report of charge doctor and take right steps. Using the Internet was not possible in the place happened emergency circumstance. The doctor wishes to connect to patient information by own cellular phone. URL of bio certificate, wireless public key certificate, wireless attribute certificate and device certificate exist in the public health center doctor's cellular phone. After the doctor connects to medical examination and treatment system and identifies himself through own public key certificate and fingerprint confirmation, the doctor access to doctor

patient information retrieval service through his own wireless attribute certification. According to the given information of the patient, the patient is suffering from high blood pressure. Therefore, the doctor urgently measured blood pressure. Blood pressure measurement device is the trust medical device that is issued device certificate and it sends measured data to medical treatment information system. Patient's charge doctor sees sent data and makes hospital report. Because a public health center doctor receives hospital report of a charge doctor, disposal about patient is available. Next figure 11 is an example that implements potable telephone user's authentication and house system scenario through J2ME programming.



**Figure. 11.** Remote medical examination scenario implementation in proposed system

Figure 11 is a flow chart screen that implements the scenario. A public health center doctor inputs password and connects to Tele-medical service. The doctor is authenticated with verification of wireless public key certificate. The authenticated doctor needs user authentication through living body information to identify user who try to approaches to the system actually. In 2006, Pantech PG-6200 device that is fingerprint realization phone getting approval of FCC has sold and patent application of portable telephone that use biometrics such as voice fingerprint face iris has been increasing. Biometrics process through potable telephone did not implement in this paper, but it is considered that strong user certification through biometrics would be possible while popularization of biometrics potable telephone attains.

If suppose that a public health center doctor is authenticated by user certification that use living body information such as own voice and fingerprint attribute, the

doctor can use doctor service which is a role of the public health center doctor and patient service with wireless attribute certificate verification through URL of radio attribute certificate stored to cellular phone to authenticate attribute of the public health center doctor. But, now because the doctor try to search information of patient by role of a public health center doctor, he choose a doctor and confirm information of patient connect to patient information retrieval service.

Present patient needs blood pressure measurement. Therefore, patient is measured blood pressure and prescribed with sending hospital report to a charge doctor using blood pressure measuring instrument that receive bio device authentication.

If there was no radio public key certificate, it may be impossible for the doctor who does not treat in security level degree regarding life of patient to approach the data. That circumstance is that life is threatened but if a doctor can approach patient information without public key certificate, it can't connect identity of a doctor approaching in believability approaching to patient information. Continuing if access is possible to patient information without attribute certificate, privacy infringement possibility of user is occurred with that user who doesn't have authority see patient information. Also, data that is submitted through fingerprint realization device became untrustworthy, when measurement device for the public health center doctor's fingerprint measurement was not issued device certificate.

#### **4 Effectiveness verification**

Authorization model proposed in this paper includes constraints of conditions, purposes, constituents and obligations. It simulated user authentication and authorization system that terms of user, objectives and obligations include through following scenario. The scenario is as following. A doctor diagnoses child and get permission as a purpose that submit diagnostic processing information. The doctor needs an approval of parents by condition restriction to process diagnostic information of the child and before diagnosis as to obligations, restrictions, has duty to inform child's parents of diagnostic information by a call. Also, it must attain at office hours in the doctor own room to make diagnostic information of child on other condition. Effectiveness verification of this scenario is as following.

First, set permission, condition, duty, and purpose constraint about a doctor. Following figure 12 depicts permission assignment and purpose restriction assignment. Figure 13 depicts condition restriction assignment and figure 14 allocates constraint regarding to obligations.

no.	NorP	Operation	context	object	Service	Purpose	Condition	Obligation
P1	N	RW	P	Medical office	S	Medical ma	Promotion	Condition
P2	P	RWM	P	ER	P	Treat_info	Promotion	Condition
P3	P	W	T	09:30 ~ 11:30	S	Treat_pro_in	Offer	Condition
P4	P	WM	T	13:30 ~ 15:30	P	Basic_pat_in	Offer	Condition
P5	N	RWM	P	Cancer ward	P	Emer_treatLi	Promotion	Condition
P6	P	M	T	10:00 ~ 12:00	S	Insurance in	Rebate	Condition
P7	N	RW	P	Medical office	P	Pat_healthLi	Promotion	Condition
P8	P	W	P	In Hospital	S	Treat_pro_in	Offer	Condition

**Figure. 12.** Example of permission assignment and purpose restriction assignment

In P8 of figure 12, permission is defined to be allocated to a doctor. P represents place as circumstance information and is allocated to hospital by value. Also, regarding purpose restriction assignment, constraint for submission is allocated.

PolicyID	Context Variable	Domain Element
P8	ParentConsent	Yes
P8	Room	Doctor room
P8	Time	Working Time

**Figure. 13.** Example of condition assignment

Above figure 13 illustrates allocating conditions of concession of a doctor. Must have parents agreement and it is allocated to use given permission within office hours in the own room.

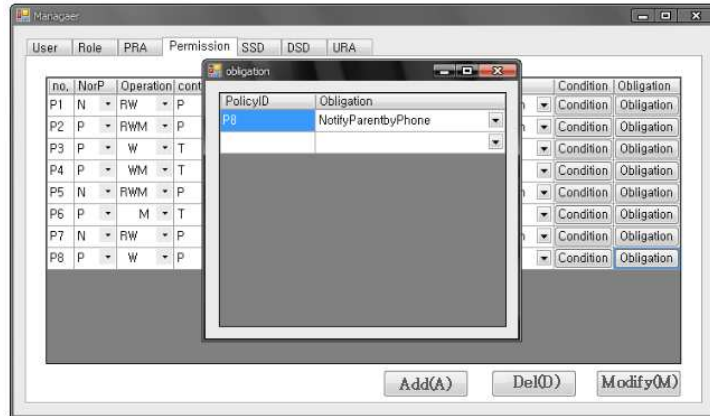


Figure 14. Example of obligations assignment

Above figure 14 illustrates allocating obligations that forewarn before execute permission with calling parents that is obligations to permission P8.

Second, following permission is allocated to a doctor after permission establishment and a doctor can use Tele-medical service with following figure 15. Below figure 15 represents simulation flow chart of a doctor who is allocated P8.

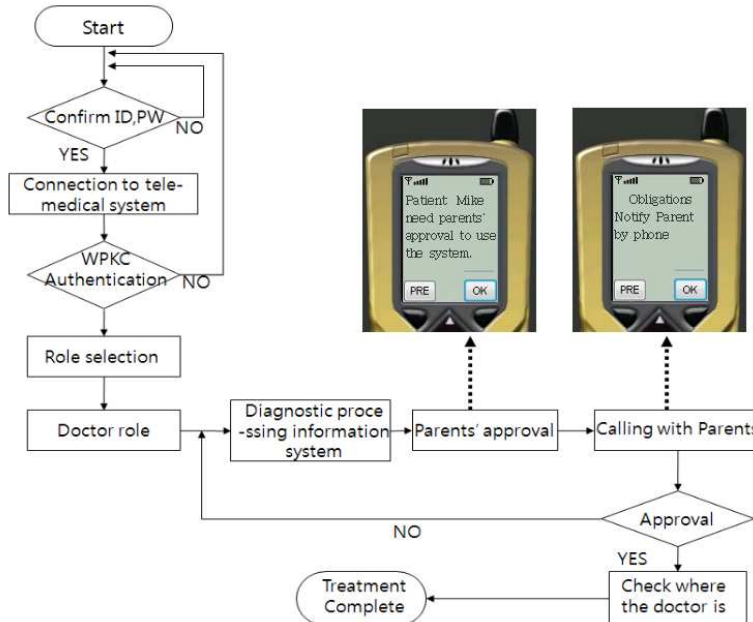


Figure 15. Simulation including conditions, objectives and obligations

Figure 15 represents user authentication and attribute authentication process with second scenario. A doctor connects to diagnostic processing information system and chooses for submission. When process diagnostic information about patient if input information about patient, constraint that parents approval is necessary is shown. If choose confirmation button, obligations as figure 8 depicts is shown and confirm whether circumstance information condition and value are matched with reading circumstance information. When the doctor own room is 208 and a room number from circumstance information is 207, it displays warning message that move to 208 without offering a doctor service. When a doctor moved to 208, check time information for office hours and when the time is within office hours, the doctor makes diagnostic processing information about patient. If the doctor leave from 208 during creating a diagnosis, display warning message that return into the again own room. We verified effectiveness of Tele-medical service that includes conditions, objectives and obligations proposed through the simulation in this paper.

## 5. Conclusion

In this paper, we implemented prototype using Visual Basic.net, J2ME, TinyOS 1.0, NesC and MySQL 6.0 in Windows XP with the model designed for authentication and authorization systems for Tele-medical treatment service in Ubiquitous environment.

Verified effectiveness to authentication and authorization system for Tele-medical service in Ubiquitous environment through simulation that use system implemented by various scenarios.

The system offered reliable Tele-medical treatment system, data security of patient, device security of medical equipment, and user privacy guarantee by equipping stronger authentication system and authorization system than existent Tele-medical service in Ubiquitous environment and implemented in this paper could do fluidic and minute user access control by using proposed access control model.

Later, it is considered that need standardization research about authentication technology and bio device authentication technology for wire and wireless integration environments.

## References

1. <http://www.ipath.info/site/en/verein>
2. <http://www.openemed.org>
3. H. Bludau and A. Koop, Mobile Computing in Medicine, Second Conference on Mobile Computing in Medicine, Workshop of the Project Group MoCoMed, GMDS Fach-bereich Medizinische Infor- matik & GI-Fachaus- schuss 4.7, 11.4.2002, Heidelberg, volume 15 of LNI. GI, April 2002
4. Apollohospitals. <http://www.apollohospitals.com> , March 2006.
5. Ahmed Faheem, "Wireless Body Area Sensor Network", [http://users.tkk.fi/virranko/sensor\\_networks/faheem1.pdf](http://users.tkk.fi/virranko/sensor_networks/faheem1.pdf) , 2006.12.12

6. <http://fiji.eecs.harvard.edu/CodeBlue>
7. Yuri Lee, Donggue Park, "tele-medical service that use bio authentication based on WPMI" Korea Information and Communications Society journal , volume 279~284, 2008.8
8. Yuri Lee, Donggue Park, "Device authentication for tele-medical service", The Korea Institute of Signal Processing and System fall conference, volume 490~493, 2008.11
9. Yuri Lee, Donggue Park, "Access control model that considers user privacy in Ubiquitous tele-medical system", Korea Institute of Information Security & Cryptology winter conference, volume 171~175, 2008