

Original Article

Toward Secure Distribution of Electronic Health Records: Quantitative feasibility study on secure E-mail systems for sharing patient records

Yuichiro Gomi¹, Hiroki Nogawa² and Hiroshi Tanaka²

1) Department of Bioinformatics, Graduate School of Medicine and Dentistry, Tokyo Medical and Dental University

2) Information Center for Medical Sciences, Tokyo Medical and Dental University

If the quality and efficiency of medical services are to be ensured, electronic health records (EHR) and EHR-supporting infrastructure must be prevalent. Many hospitals, however, have EHR systems for their internal use only, and the standardization process for the exchange of medical information is still in process. This standardization process addresses information security and is considering public key infrastructure (PKI) as one security measure, but PKI is rarely used by medical practitioners because of its poor user-friendliness.

Here we propose an effective use of the identity-based encryption (IBE) system as a security measure. This system enables us to send encrypted and signed messages without requiring the receiver to get a public key, and it enables us to deliver secured messages to ambiguous receivers like those to whom letters of reference are sent. We evaluated the feasibility of this technology by using the analytic hierarchy process, which is an effective analysis tool when selection and judgment depend on nonquantitative psychological factors, to analyze the results of an experiment in which medical workers used E-mail agents with and without PKI and IBE. We found that medical practitioners and researchers avoid using PKI

because of its poor user-friendliness and instead use IBE even though it is harder to install. We therefore think IBE would encourage medical institutions to share patient records.

Key words: security, E-mail, sharing patient record, EHR, PKI

Introduction

The Japanese Ministry of Health, Labour and Welfare's "Grand design toward information of the field of health medical care"¹ notes that the quality, efficiency, and fairness of medical services cannot be ensured in the absence of unbiased and objective information about medical practice. Such information can be collected only through electronic health records (EHR), and many advanced hospitals have developed and implemented EHR systems designed for internal use. Patient records are not widely shared between hospitals and clinics, however, because standards for the exchange of medical information are still being designed². One of the measures recommended to ensure the security of electronically recorded medical information is public key infrastructure (PKI)^{3,4}, but we have been unable to find hospitals using the PKI system successfully or to find reports of research evaluating the PKI system in medical practice. We think this is due to the user-unfriendly interfaces of present PKI technology, which requires verification software to be installed in message-receiving personal computers. This is probably why most hospitals still exchange med-

Corresponding Author: Yuichiro Gomi
Information Center for Medical Sciences
1-5-45, Yushima, Bunkyo-ku, Tokyo 113-8510, Japan.
Tel: +81-3-5803-5840 Fax: +81-3-5803-0247
E-mail: yg@hen.jp
Received July 29; Accepted September 9, 2005

ical information in the form of conventional healthcare records on paper.

Here we focus on feasibility of instead using an identity-based encryption (IBE) system⁵ that enables us to send encrypted and signed messages without first getting the public key certificate of the receiver⁶ and to deliver secured messages to ambiguous receivers like those to whom letters of reference are shown. We evaluated the feasibility of this IBE technology and examined the security consciousness of medical workers by having them fill out questionnaires after participating in an experiment using both PKI and IBE. We analyzed the questionnaire results by using the analytic hierarchy process (AHP), which is an effective tool when selection and judgment depend on nonquantitative psychological factors^{7,8}.

Health Level Seven (HL7) is a standards-developing organization producing global standards for sharing patient records⁹, but we evaluated security measures for E-mail systems because HL7 does not yet define security measures. E-mail systems are already much more widely used for sharing patient records, and there are many proposals for securing E-mails because E-mail systems have no default security measures.

In this paper we describe our experiments and results, suggest reasons that security measures for E-mails have not become popular, and discuss the feasibility of IBE for use in the exchange of medical information.

Materials and Methods

Subjects

The twelve persons voluntarily participating in our experiment were three physicians, one dentist, one nurse, one clinical laboratory technologist, three medical researchers, and three medical school students.

Basic concept

As shown in Fig. 1, PKI technology forces us to obtain a public key of the receiver from the key server before sending encrypted and signed messages to that receiver. IBE technology, however, enables us to send encrypted and signed messages without first obtaining a public key of the receiver (Fig. 2).

The key distribution of IBE systems can be summarized as follows. A key server distributes the public parameters for all users and then issues a private parameter to each user. A sender encrypts a message with

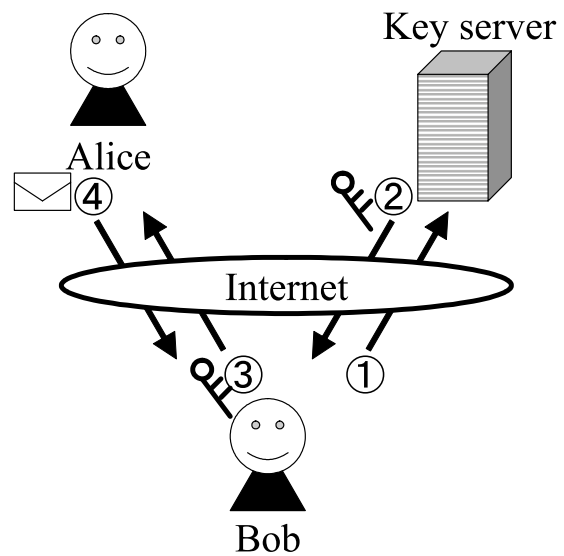


Fig. 1. Alice uses PKI service to send Bob a secure E-mail. Step 1: Bob contacts the key server, which contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements. Step 2: After authenticating Bob, the key server returns his private key and public key via a secure tunnel (like SSL). This private key can be used to decrypt all future messages received by Bob. Step 3: Bob sends Alice his public key. Step 4: Alice encrypts the E-mail using Bob's public key.

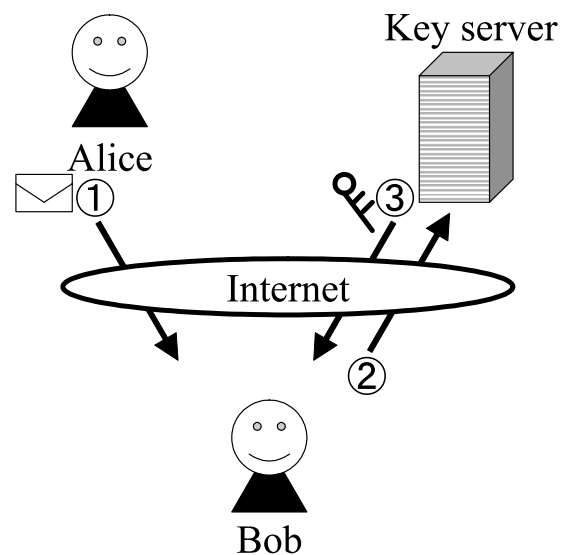


Fig. 2. Alice uses IBE service to send Bob a secure E-mail. Step 1: Alice encrypts the E-mail using Bob's E-mail address as the public key. Step 2: When Bob receives the message, he contacts the key server. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements. Step 3: After authenticating Bob, the key server then returns his private key, via a secure tunnel (like SSL), with which Bob can decrypt the message. This private key can be used to decrypt all future messages received by Bob.

Table 1. Specifications of servers used in the experiment.

Category	Name
PKI service	VeriSign Class 1 Digital ID
IBE service	Voltage SecureMail Version 2.1
Web server	RedHatLinux R9 + Apache 2.0.40
Mail server	RedHatLinux R9 + Postfix 1.1.12
Client PC	Windows (version was trier's choice)
Mailer	Outlook Express (version was trier's choice)

a public key (i.e., with both a public parameter and the receiver's E-mail address), and the receiver decrypts the message with a private key (i.e., with both a private parameter and the receiver's E-mail address).

The PKI and IBE system have different flows of public key exchange, but their security strengths are supposed to be the same. IBE uses bilinear mapping on elliptic curves to calculate a public/private key pair from a simple, well-recognized identity or role⁶.

The target E-mail agent in our experiment was Microsoft's Outlook Express (OE) because both PKI and IBE are available with this agent, and we excluded possible effects of different user-interfaces by comparing security procedures between plain OE, OE with PKI, and OE with IBE.

Method

Detailed specifications of the experiment are listed in Table 1. PKI service and IBE service were installed in separate servers, and a WWW server was configured for collection of questionnaire data. Each of these servers was connected to the Internet.

Each of the twelve participants experienced operations ranging from configuration to sending/receiving E-mails with the three different types of OE: plain OE, OE with PKI, and OE with IBE (Fig. 3)^{10,11}. Before and after the operations they filled out questionnaires through the prepared Web pages.

We prepared sample of letter of reference (32 KB, in Japanese) that was used in sending/receiving E-mails, and we used the AHP in analyzing the results because it is effective when quantitative judgment measures are not available. The AHP gives structures for evaluation elements based on a psychological model, quantizes the difference of importance for each element by pair comparison, and evaluates a plan with its substitutes.

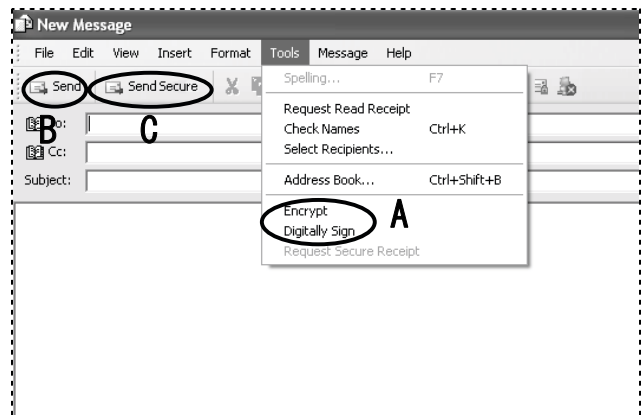


Fig. 3. Screenshots of Outlook Express equipped with PKI or IBE. PKI: The items labeled A are commands for PKI encryption and signature, and the item labeled B is an icon for sending E-mail. IBE: The item labeled C is an icon for IBE encryption and sending E-mail.

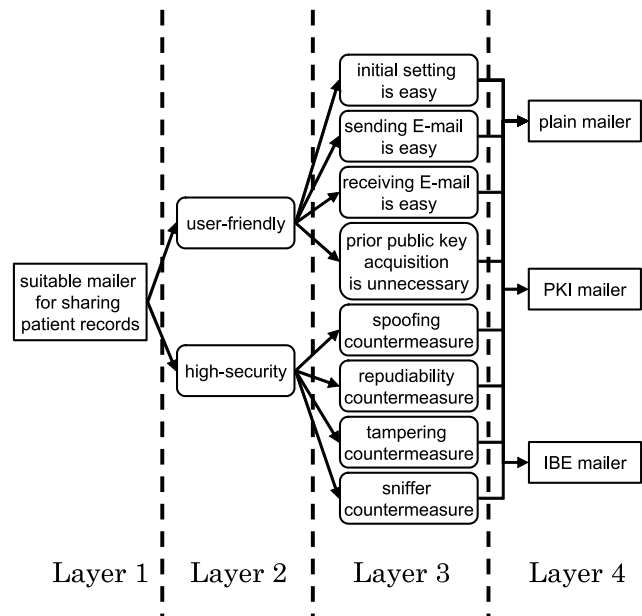


Fig. 4. Psychological structure model (AHP model) we propose for the E-mailing of letters of reference in medical institutions.

Items investigated

For AHP analysis we assumed the psychological structure model of E-mail messaging for letters of reference in medical institutions that is shown in Fig. 4.

Layer 1 shows the most abstractive notion of decision making, layers 2 and 3 are evaluation items, and layer 4 is the mailer software to be selected. We accordingly made questionnaires consisting of the set of one-pair comparisons shown in Fig. 5.

Layer 2	
Which is more important for a mailer suitable for sharing patient records?	
user friendly	+++++++ security is high
Layer 3	
Which is more important for user-friendliness?	
initial setting is easy	+++++++ sending E-mail is easy
initial setting is easy	+++++++ receiving E-mail is easy
initial setting is easy	+++++++ prior public key acquisition is unnecessary
sending E-mail is easy	+++++++ receiving E-mail is easy
sending E-mail is easy	+++++++ prior public key acquisition is unnecessary
receiving E-mail is easy	+++++++ prior public key acquisition is unnecessary
Which is more important for high security?	
spoofing countermeasure	+++++++ repudiability countermeasure
spoofing countermeasure	+++++++ tampering countermeasure
spoofing countermeasure	+++++++ sniffer countermeasure
repudiability countermeasure	+++++++ tampering countermeasure
repudiability countermeasure	+++++++ sniffer countermeasure
tampering countermeasure	+++++++ sniffer countermeasure
Layer 4	
For which is it more important that initial setting is easy ?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that sending E-mail is easy?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that receiving E-mail is easy?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that public key acquisition is unnecessary ?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that there is a spoofing countermeasure?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that there is a repudiability countermeasure?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that there is a tampering countermeasure?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer
For which is it more important that there is a sniffer countermeasure?	
plain mailer	+++++++ PKI mailer
plain mailer	+++++++ IBE mailer
PKI mailer	+++++++ IBE mailer

Fig. 5. Questionnaires made from AHP model shown in Fig. 4. The symbol “+++++++” represents a one-pair comparison scale, and our experimental participants selected one point in each scale for each item in the questionnaire.

Analysis method

One-pair comparison between items investigated in each layer was done by showing visual scales as in Fig. 6 to each volunteer. Here we denote items to be com-

pared as O_i and O_j .

When a person judges O_i to be “more important” than O_j , the score would be 2, which means that the $O_i:O_j$ importance ratio is 2:1. In contrast, when a person

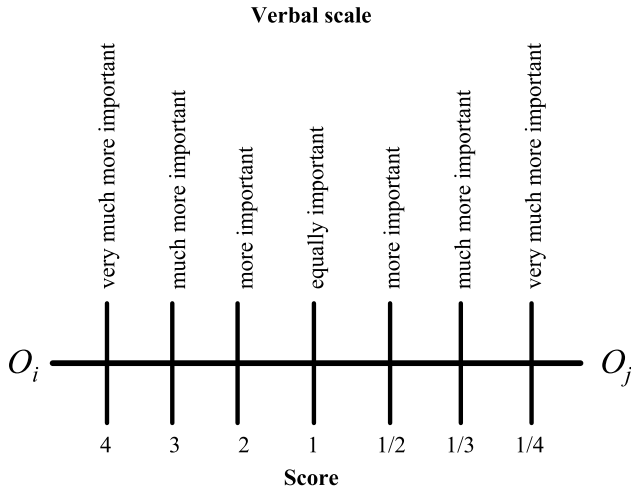


Fig. 6. Scale for comparing the importance of objects O_i and O_j .

judges O_j to be “more important” than O_i , the score would be 1/2, which means the $O_i:O_j$ importance ratio is 1:2.

The results were quantized into ratios as mentioned above, and arranged into a one-pair comparison matrix:

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (1)$$

where a_{ij} is an importance ratio of O_i to O_j , n is the number of items investigated in each layer, and

$$a_{ji} = 1/a_{ij} \quad (2)$$

An importance index of O_i was calculated as a geometric mean (GM_i) of each row of matrix A :

$$GM_i = \left[\prod_{j=1}^n a_{ij} \right]^{1/n} \quad (3)$$

Weight of importance (w_i) is a standardized importance index such that the total sum of GM_i equals 1:

$$w_i = GM_i / \sum_{i=1}^n GM_i \quad (4)$$

To evaluate results from multiple persons, we defined a_{ijk} as the importance ratio of O_i to O_j for the k_{th} person and calculated a_{ij} as follows:

$$a_{ij} = \left[\prod_{k=1}^m a_{ijk} \right]^{1/m} \quad (5)$$

where m is the number of the volunteers involved in this experiment. This calculation was repeated from the top layer to the lowest layer.

The weight of importance of each item in layer 4 was calculated by multiplication of the weights of importance of items from the top layer to the lowest along the path in the psychological model. This weight of importance represents the total evaluation value of each selection factor or substitute plan^{7,8}.

To exclude inconsistent data from the results, we calculated a consistency index (C.I.) of each person as explained below and used the results when C.I. was within a predefined standard (0.1). We first calculated

$$x = (A \cdot w) \quad (6)$$

where

$$w = \{w_1, \dots, w_n\} \quad (7)$$

and then calculated

$$\lambda_{\max} = \left(\sum_{i=1}^n x_i / w_i \right) / n, \quad (8)$$

From which we obtained the consistency index as

$$C.I. = \frac{\lambda_{\max} - n}{n - 1} \quad (9)$$

By multiplication of weights of importance calculated as explained above, we obtained a total evaluation value used to quantify the effectiveness of secure communication.

To find statistically significant differences between the total evaluation values of each mailer, we performed Friedman tests between total evaluation values for each person.

Results

Table 2 shows a result of the experiment. We used all the scores, because the adjustment degrees of scores of all the persons were within the standard value.

The total evaluation score was highest for the mailer with IBE ($w = 0.369$), lowest for the mailer with PKI ($w = 0.304$), and intermediate for the plain (non-

Table 2. Results of AHP analysis.

	weight (selection fact.)	weight (substitute plan)		
		plain mailer	PKI mailer	IBE mailer
initial setting is easy	0.131	0.071	0.021	0.040
sending E-mail is easy	0.107	0.051	0.022	0.034
receiving E-mail is easy	0.127	0.055	0.033	0.039
prior public key acquisition is unnecessary	0.172	0.082	0.030	0.060
spoofing countermeasure	0.111	0.016	0.046	0.049
repudiability countermeasure	0.085	0.013	0.036	0.036
tampering countermeasure	0.148	0.022	0.064	0.062
sniffer countermeasure	0.119	0.019	0.051	0.050
total evaluation score		0.328	0.304	0.369

The columns with “substitute plan” at the top row show weights of layer-3 items for each mailer. These weights were calculated as follows: (1) Weights of each mailer on each item in layer 3 were calculated, (2) weights of items in layer 3 were calculated, and (3) the weights calculated in steps (1) and (2) were multiplied. The total evaluation values in the lowest row are the sums of the weights in the corresponding columns.

Table 3. Statistical analysis of AHP results.

	mean	standard deviation	Friedman test			
			Group A	Group B	Group C	Group D
initial setting is easy	0.164	0.145		○	○	
sending E-mail is easy	0.092	0.036		○	○	
receiving E-mail is easy	0.106	0.029		○	○	
prior public key acquisition is unnecessary	0.170	0.109		○	○	
spoofing countermeasure	0.113	0.069		○		○
repudiability countermeasure	0.081	0.044		○		○
tampering countermeasure	0.141	0.075		○		○
sniffer countermeasure	0.134	0.085		○		○
plain mailer	0.333	0.098	○			
PKI mailer	0.289	0.087	○			
IBE mailer	0.378	0.077	○			
Significant difference			0.013	0.358	0.537	0.031

We performed Friedman tests onto answers of each person of the 12 volunteers.

Before performing Friedman tests, we categorized selection factors into four groups according to natures of selections factors. Group A categorizes mailers to be selected (layer 4), and Group B includes all selection factors excluding mailers (layer 3). Group C is a collection of selection factors in view of user-friendliness, and Group D is a selection factor group for security consciousness.

secure) mailer ($w = 0.328$). The most important factor for the 12 participants was that “prior public key acquisition is unnecessary” ($w = 0.172$), and the least important was “repudiability” ($w = 0.085$). The plain mailer tended to get high scores with regard to the importance of “user friendliness”, whereas the mailers with PKI and IBE tended to get high scores with regard to the importance of “security strength”.

The results we obtained using Friedman tests on the weights of selection factors in the AHP model are listed in Table 3. Analysis of users’ preference with arithmetic means (listed in Table 3) showed the same tendency

obtained in analysis with geometric means: $IBE > plain > PKI$. The geometric mean of each factor was within ± 1 SD of the arithmetic mean. Both “initial setting is easy” (S.D. = 0.145) and “prior public key acquisition is unnecessary” (S.D. = 0.109) showed relatively high standard deviations, and both “sending E-mail is easy” (S.D. = 0.036) and “receiving E-mail is easy” (S.D. = 0.029) showed relatively low standard deviation values.

Before performing Friedman tests, we categorized selection factors into four groups according to the natures of selections factors. Group A categorizes

mailers to be selected (layer 4 in Fig. 4), and Group B includes all selection factors excluding mailers (layer 3 in Fig. 4). Group C is a collection of selection factors in view of user-friendliness, and Group D is a selection factor group for security consciousness. After categorization, we performed Friedman tests on the answers of each of the 12 volunteers.

Friedman tests revealed significant differences in factors in Group A ($p = 0.013$) and Group D ($p = 0.031$) but it failed to show any significant difference in Group B ($p = 0.358$) and Group C ($p = 0.537$).

Discussion

Comparison between the mailers with PKI and IBE showed little difference in security-related items, and the values listed in Table 2 indicate that we can conclude that the users evaluated PKI and IBE mailers to be equally secure. The comparison showed differences in the ease of initial setting and of sending E-mail, however. We think these differences were due to some confusing instructions in the operations and could be removed by improving the GUI implementation. The above results can be summarized as follows: the mailers with PKI and IBE were evaluated to be more secure than the plain mailer, but the mailer with PKI was evaluated to be less user-friendly than the plain mailer and the mailer with IBE.

The "prior public key acquisition is unnecessary" item obtained the highest score, which means that the users find convenience more important than security. Among the security-related items, "tampering countermeasure" received the highest importance, which means that the users might fear tampering most in electronic letters of reference. The "repudiation countermeasure", in contrast, was the least important item. We think this result is because users recognize that repudiation is improbable in practical medical activities.

Statistical analysis of the AHP results (Table 3) revealed that those results are reasonable. We think that the reason for the high standard deviation values for "initial setting is easy" (S.D. = 0.145) and "prior public key acquisition is unnecessary" (S.D. = 0.109) were variations of the volunteers' knowledge about security. And we think that the reason for the low standard deviation values for "sending E-mail is easy" (S.D. = 0.036) and "receiving E-mail is easy" (S.D. = 0.029) is that sending and receiving E-mails is part of the daily work for the volunteers, so they had already formed common decision criteria for the user-friendliness of

mailers.

Friedman tests proved that both the mailer selection order (IBE > plain > PKI) determined by AHP analysis and the calculated weight of each of the selection factors in Group D are reasonable and fair.

Quantitative analysis of the results of the security surveillance study reported in this paper has shown that a sample of medical practitioners and researchers in medical institutions regard "tampering" as the most severe security threat and consider electronic signatures and encryption to be effective against it. The study also showed that PKI technology is so much complicated and less user-friendly that users do not select this technology. We think this complexity has prevented PKI service from being widely used by medical service providers. Our study however also revealed that medical practitioners use encryption technology if it is user-friendly enough; that is, if its installation and configuration do not require too much effort. The size of our surveillance sample (12) might be too small to support concrete conclusions, but we think this pilot study suggests some tendencies or inclinations of people providing medical services. It implies that IBE technology would be of much help in facilitating widespread use of electronic patient record sharing. IBE technology is also applicable across a broad spectrum of medical information fields, such as the transfer of patient records contained in electronic recording devices like DVDs and USB memories.

Acknowledgements

We thank Mitsui Bussan Secure Directions, Inc. for providing us IBE technology related software, and we thank the twelve participants who provided the data in our experiment.

References

1. Ministry of Health, Labour and Welfare. About development of grand design toward information of the field of health medical care (in Japanese). December 26, 2001. Available at <http://www.mhlw.go.jp/shingi/0112/s1226-1.html>. Accessed July 29, 2005.
2. Ministry of Health, Labour and Welfare. Final report: Standard Electronic Chart Promotion Committee (in Japanese). May 17, 2005. Available at <http://www.mhlw.go.jp/shingi/2005/05/s0517-4.html>. Accessed July 29, 2005.
3. Ministry of Health, Labour and Welfare. Final report: Medical information network base study meeting (in Japanese). September 30, 2004. Available at <http://www.mhlw.go.jp/shingi/2004/09/s0930-10.html>. Accessed July 29, 2005.
4. The Internet Society. RFC 2510. Available at <http://www>.

- apps.ietf.org/rfc/rfc2510.html. Accessed July 29, 2005.
5. Gomi Y, Ohashi K, Tanaka H. Evaluation of a secure mail system using identity-based encryption for medical use (in Japanese, English abstract). The 24th Joint Conference on Medical Informatics 2004:3-G-2-4.
 6. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. *SIAM J. of Computing* 2003;32:586-615.
 7. Saaty TL. *Decision Making for Leaders*. Pittsburgh: RWS Publications;1995.
 8. Shibata T, Tanaka H. Mathematical and statistical applications for evaluation of medical support systems (in Japanese, English abstract). *Japan Journal of Medical Informatics* 2002;22:147-153.
 9. Health Level Seven. Health Level Seven, Inc. Available at <http://www.hl7.org/>. Accessed July 29, 2005.
 10. VeriSign, Inc. Digital ID Support. Available at http://www.verisign.com/support/digital-id-support/page_dev029379.html. Accessed July 29, 2005.
 11. Voltage Security, Inc. Voltage Datasheets Voltage Security. Available at <http://www.voltage.com/datasheets.shtml>. Accessed July 29, 2005.