A Security Scheme for Exchanging Electronic Patient Records among Non-Medical Personnel Based on Smart Cards

孫立文、曹偉駿

E-mail: 9707321@mail.dyu.edu.tw

ABSTRACT

With the development of information technology and the prevalence of the Internet, conventional paper medical records can be recorded into computers and be read by others via the Internet. General people have also gradually paid more attention to the protection of personal data and privacy. However, most medical information include patient records involving personal rights. So, to assure the portability and confidentiality of electronic patient records during the transmitting process is surely an important topic. Currently under the regulations by Taiwan National Health Administration, there is a clear rule over the exchange of electronic patient records among medical organizations. Nevertheless, it calls for a definite guideline over the exchange among medical, non-medical organizations and patients. To compensate for the situation, this study integrates TMT electronic patient records into self-certified public key cryptosystems of elliptic curve cryptosystems and smart cards. The purpose is to set up a security scheme for exchanging electronic patient records among non-medical parties based on smart cards. This study aimes to solve the portability and confidentiality problems while electronic patient records are exchanged among medical, non-medical organizations and patients. With the scheme in practice, it will also eliminate the inconvenience of getting patient records proof caused by the current mechanism.

Keywords : electronic patient records ; smart cards ; elliptic curve cryptosystems ; self-certified public key cryptosystems ; information security

Table of Contents

REFERENCES

一、中文部份 中央健康保險局(2008)，健保IC卡，[線上資料]，來源: http://www.nhi.gov.tw/index.asp?menu=3 [2008, March 10]。 台灣健康資訊交換第七層協定協會(2008)，HL7簡介，[線上資料]，來源: http://www.hl7.org.tw[2007, December 21]。 行政院衛生署(2008)，法令規章，[線上資料]，來源: http://www.doh.gov.tw[2007, October 11]。 行政院衛生署委託台灣醫學資訊學(2008)，電子病歷內容基本格式，[線上資料]，來源: http://emr.doh.gov.tw[2007, December 11]。 行政院衛生署醫療憑證管理中心(2008)，醫事憑證IC卡，[線上資料]，來源: http://hca.doh.gov.tw/HCA/default.jsp[2008, May 5]。 曾紹崟(2002)，攻擊智慧卡技術簡介，資訊安全通訊，8(3)，18-34。 賴溪松，韓亮，張真誠(2004)，近代密碼學及其應用，台北:旗標出版股份有限公司。 簡文山，徐建業，楊哲銘，?信財，李友專(2007)。電子病歷跨院資訊交換環境對醫療服務之影響，醫療品質雜誌，1(6)，39-44。 顏大緯(2004)，智慧卡在數位環境應用之瓶頸與突破，台灣大學資訊管理學研究所未出版之碩士論文，台北，5-6。 二、英文部份 Caelli, W., Dawson, E., & Rea, S. (1999). PKI, elliptic curve cryptography and digital signatures. Computer & Security, 18(1), 47-66. Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics, 27, 185-196. Chang, Y. S., Wu, T. C., & Huang, S. C. (2000). ElGamal-like digital signature and multisignature schemes using self-certified public keys. The Journal of System and Software, 99-105. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469-472. Girault, M. (1991). Self-certified public keys, advances in cryptology: EuroCrypt ’ 91. Lecture Notes in Computer Science, 547, Springer-Verlag, 491-497. Gunther, C. (1991). An identity-based key-exchange protocol. Proceedings of Advances in Cryptology EuroCrypt ’ 91, LNCS, 547, Springer-Verlag, 29-37. Jurisic, A., & Menezes, A. J. (1997). Elliptic curves and cryptography. Dr. Dobb ’ s Journal, (22), 26-35. Kardas, G., & Tunali, E. T. (2006). Design and implementation of a smart card based healthcare information system. Computer methods and programs in biomedicine, 81, 66-78. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(17), 203-209. Liu, C., Yang, P., Yeh, Y., & Wang, B. (2006). The impacts of smart cards on hospital information systems-an investigation of the first phase of the national health insurance smart card project in Taiwan. International Journal of Medical Informatics, 75, 173-181. Miller, V. S. (1986). Use of elliptic curves in cryptography. Advances in Cryptology: Crypto ’ 85, Springer-Verlag, 417-426. Petersen, H., & Horster, P. (1997). Self-certified keys concepts and applications. Proceedings of Communications and Multimedia Security ’ 97, 3, 102-116. Riverst, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. Saeednia, S. (1997). Identity-based and self-certified key-exchange protocols. Information Security and Privacy: ACISP ’ 97, 303-313. Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. IEEE Computer, 29(2), 38-47. Schadow, G., (1999). HL7 V3.0 data types specification[Online]. Available: http://aurora.rg.iupui.edu/~schadow/v3dt/report.html [1999, March 22]. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. Proceedings of CRYPTO 84 on Advances in cryptology, 47-53. Stallings, W. (2003). Cryptography and network security (3rd ed.). Saddle River, New Jersey: Prentice Hall. Tsaur, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Mathematics and Computation, 168(1), 447-464. Wu, T. C. (2001). Digital signature/multisignature schemes giving public key verification and message recovery imultaneously. Computer Systems Science and Engineering, 16(6), 329-337. Wu, T. C., Chang, Y. S., & Lin, T. Y. (1998). Improvement of Saeednia ’ s self-certified key exchange protocols. IEEE Electronic Letters, 34(11), 1094-1095.