International Journal of Innovative Computing, Information and Control
Volume **4**, Number **11**, November **2008**

 ISSN 1349-4198
pp. 3047–3058

ELECTRONIC SIGNATURES FOR LONG-TERM STORAGE PURPOSE IN ELECTRONIC ANAMNESIS

Yuan Lung Yu[1], Yu Fang Chung[2] and Tzer Shyong Chen[3]

[1]Computer Science of Information Management Department
HungKuang University
Taichung, Taiwan
ylyu@sunrise.hk.edu.tw

[2]Electrical Engineering Department
[3]Information Management Department
Tunghai University
Taichung, Taiwan
{ yfchung; arden }@thu.edu.tw

Received September 2007; revised December 2007

Abstract. *Nowadays, business transactions and personal activities are increasingly accomplished through the Internet or by stored electronic data. Therefore, there is a need to establish data protection measures to uphold privacy especially in communication and cooperation in public health care and public welfare; it is also needed to ensure data integrity during specific time. Although the standard of secure technology is quite high and still continuously improving, new attacks still continue to appear. To ensure their security, electronic files need to be re-signed before the termination of their security life circle. In addition, on the basis of technology and legitimacy, we take measures to keep the files intact, and then re-encrypt and re-store both new and old keys of the files. This scheme can retain confidentiality; what is more, the same signer can still decode the encrypted data years later. For electronic anamneses to assist doctors in understanding the physical condition of their patients, they must have an access to profound diagnoses based on case history. The case history records information of patients, and therefore should have restricted access in order to ensure privacy and integrity. Hence, it is crucial that a secure and long termed storage method be used for electronic anamneses. Presently, a Trusted Third Party (TTP) is employed to facilitate interactions between two parties who trust TTP, and it is responsible for checking whether the keys and property statuses of the two parties correspond to transmission procedures.*

Keywords: Electronic signature, Electronic anamnesis, Trusted third party, Hospital information system

1. **Introduction.** The object of this study is to propose a concrete framework and a whole solution for assisting hospitals and medical centers in integrating electronic signatures onto their existing hospital information system (HIS) and to construct a complete electronic anamnesis (documents) system that meets the stipulations of electronic signatures, so as to enable it to have the same legal effect as case history on paper. Computerizing the case history effectively solves case history storage and management problems. When needed, a case history can be printed for use as medical evidence in court cases in a court of law. Consequently, the goal of non-paper can be gradually achieved, promoting environmental protection.

Conversely, there is an increasing need for exchange of medical information. Thus, the goal of this paper includes enabling sharing of medical information, authentication of