Digital authentication of medical records: have we found a solution?

Autenticação digital de documentos médicos: encontramos a solução?

Luiz Felipe Nobre[1], *Aldo von Wangenheim*[2], *Ricardo Felipe Custódio*[3]

There is no doubt regarding the expected benefits that digital certification will provide to electronic documents, moreover when the final result is a printed document such as medical report. Authentication and integrity are important elements that should be guaranteed by means of digital certification of such documents, providing them with the presumption of legal effectiveness. In an editorial and article previously published in this journal, the relevance of such a theme was discussed(1,2). Digital certification is the only technology capable of safely replacing paper documents signed by physicians by their equivalent electronic counterparts. It is known that electronic documents are easily circulated from a location to another, and are easily copied and stored, being capable of containing detailed data, such as highly accurate images and even dynamic data such as movies. However, the substitution of physical documents by their electronic counterparts has not been a simple task. There are technological, legal and political challenges as well as interfacing and acceptance issues.

With respect to technology there are practical issues to be addressed to enable physicians to utilize digital certification and thus confidently sign their electronic documents. One of the key requirements is established by the sole paragraph of Interim Ordinance MP 2200 of August 2, 2001, which provides that the holder of the digital certification is solely responsible for the generation of the cryptographic keys pair, with total control of the use of the signature key throughout the entire life cycle of the digital certificate. Complying with this provision is not exactly a simple matter for people.

ICP-Brasil has established, among others, two main types of digital certificates: the so called A1 and A3 certificates. The A1 digital certificate, which is valid for up to one year, may have its private key stored in the computer memory. On the other hand, the A-3 type certificate, which is valid for three years, must have its private key generated and stored on cryptographic hardware. The most widely known hardwares utilized for such purpose are the smartcards and the USB cryptographic tokens.

The management of the private key is easier when such cryptographic hardwares are utilized in lieu of the computer memory. In fact, the A1 certificate was specifically created for those situations in which the use of A3 certificates is not feasible such as in web servers and networking equipment.

The utilization of the A1 certificates poses a problem, as there is no way to guarantee to the physician the responsibility of the use of his signature key. On the other hand, the utilization of the A3 certificates requires the use of smartcards, which is the solution pursued by the Conselho Federal de Medicina (Federal Council of Medicine) in its digital certification project for physicians.

Is this a satisfactory solution? The answer is yes and no… Smartcards, as utilized in safe environments such as hospital intranets, without internet access, represent a safe and robust solution that can be fearlessly

[1] Professor Doctor, Laboratório de Telemedicina e Serviço de Radiologia – Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil. E-mail: luizfelipenobre@telemedicina.ufsc.br

[2] Professor Doctor rer.nat., Instituto Nacional para Convergência Digital (INCoD), Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil. E-mail: awangenh@inf.ufsc.br

[3] Professor Doctor, Laboratório de Segurança em Computação (LabSEC), Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brazil. E-mail: custodio@inf.ufsc.br

0100-3984 © Colégio Brasileiro de Radiologia e Diagnóstico por Imagem

utilized for authentication of medical prescriptions or reports. On a computer with internet access, the situation is quite different. That is the case, for example, of the utilization of teleradiology systems in which the radiologist checks the reports over an internet connection, either from his own office or from a public computer in urgent cases. If you ever find yourself at such circumstances, beware: there is risk for the physician.

Why does that happen? While the smartcard remains inserted into the reader connected to a computer, its signature module may be utilized by any software installed on such computer. This places the smartcard under the threat of malicious softwares which record the password typed by the user (PIN), and are thus free to use the smartcard. With the password, in a matter of a few seconds such type of spy softwares can sign any type of thing over the internet on your behalf! It is important to highlight that, according to the Brazilian regulations, in such a situation the risk for the patient is practically nonexistent, and the consequences will fall upon the physician holder of such certificate.

There are ways to overcome such a problem. Upon the identification of such a situation, the Computational Security Laboratory of UFSC (Laboratório de Segurança em Computação – LabSEC <http://www.labsec.ufsc.br/>), in a partnership with the National Institute for Digital Convergence (Instituto Nacional para Covergência Digital – INCoD <http://www.incod.ufsc.br>), the Santa Catarina State Health Secretary and the company Bry are working together on the FINEP CIM-Saúde project for the Santa Catarina State Telemedicine Network.

Such a project is aimed at developing a strategy which will allow physicians to safely sign medical electronic documents from any place and on any computer. This solution comprises the storage and utilization of private keys on remote signature servers with total protection against malicious softwares, the so called Hardware Security Modules (HSMs), currently not allowed in Brazil for the A3 certificates, to be jointly used with a single counter-password, which will be sent to the physician's cell phone by means of an authentication system coupled with the HSM. With this solution, the physician does not need to bear his or her smartcard, leaving it coupled to a HSM in a safe room at the certifying institution, or even utilizing a slot of such a device as if it were the actual smartcard. The risk of password capture is eliminated by means of the counter-password sent to the physician's cell phone valid for a single utilization, which can comprise a set of imaging studies tele-reported by a radiologist during a single work session. Upon willing to confirm the electronic signature for a new set of reports, the physician will receive a new counter-password on his/her cell phone, which will be valid for only a few minutes, in order to further minimize the risk.

Does such strategy solve all the problems? As far as risks can be identified, the answer is yes. However, as it usually happens with any security strategy, there will always be people committed to finding ways to circumvent it, and eventually a way will be found. We have to use common sense and ask ourselves: How difficult is it to falsify a signature on paper? Certainly, at the daily routines, digital signatures provide a better security and greater practicity than paper documents. The key attitude is to constantly question ourselves in the search of solutions to further refine support technologies for telemedicine activities, always with a view on security assurance for the professionals.

REFERENCES

1. Nobre LF, von Wangenheim A, Maia RS, et al. Certificação digital de exames em telerradiologia: um alerta necessário. Radiol Bras. 2007;40;415–21.
2. Nobre LF, von Wangenheim A. Telerradiologia: desafios a enfrentar para a quebra de um paradigma na especialidade [editorial]. Radiol Bras. 2006;39(6):vii–viii.