Revista da
ASSOCIAÇÃO MÉDICA BRASILEIRA

www.ramb.org.br

Ponto de vista

Assinatura digital de laudos médicos: um assunto ainda não resolvido☆

Digital signature of medical reports: an issue still not resolved

Aldo von Wangenheim[a], *Ricardo Felipe Custódio*[b], *Jean Everson Martina*[b], *Isabela de Back Giuliano*[c] *e Rafael Andrade*[d,*]

[a] *Instituto Nacional para Convergência Digital (INCoD) da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brasil*
[b] *Laboratório de Segurança em Computação (LabSec), da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brasil*
[c] *Programa de Pós-graduação em Saúde Coletiva, UFSC, Florianópolis, SC, Brasil*
[d] *Instituto Federal de Santa Catarina (IFSC), Florianópolis, SC, Brasil*

INFORMAÇÕES SOBRE O ARTIGO

Histórico do artigo:
Recebido em 3 de dezembro de 2012
Aceito em 20 de dezembro de 2012
On-line em 13 de maio de 2013

Nenhuma área da prática médica está sendo tão afetada pela introdução do telediagnóstico em massa como a cardiologia.[1] Em 2011, no estado de Santa Catarina (SC), o Sistema Integrado de Telemedicina e Telessaúde de Santa Catarina (STT/SC),[2] iniciativa responsável junto ao Governo do Estado pela realização de atividades de telediagnóstico para o Sistema Único de Saúde (SUS) de SC, foi responsável pela realização de 105.025 exames de tele-eletrocardiografia, o que, de acordo com o SIA/SUS, representou 29% do total de exames eletrocardiográficos realizados pelo SUS no estado de SC neste período. Em muitos municípios do interior de SC a prática de ações de telediagnóstico cardiológico permitiu elevar a oferta de exames de eletrocardiografia em mais de 300%, o que com certeza provocará alterações no perfil de morbidade dessa população, que serão perceptíveis em cinco ou 10 anos.[3] A prática da telecardiologia veio para ficar; estudos de satisfação realizados em SC demonstram que a aceitação e a utilização desse método sugere que o seu uso só tenderá a aumentar.[4]

No entanto, ainda há questões em aberto quanto à emissão eletrônica de laudos à distância, principalmente no que diz respeito às promessas dos benefícios da certificação digital em documentos eletrônicos, que devem ser impressos com o rigor da autenticação e integridade, conferindo-os à sensação da eficácia jurídica.[5] A certificação digital é a única tecnologia capaz de substituir com segurança documentos em papel assinados pelos médicos por documentos eletrônicos equivalentes. Documentos eletrônicos são mais fáceis de circular, copiar e armazenar; podem, além disso, conter informações mais detalhadas, tais como imagens de alta precisão e dados em formatos que preservam suas características dinâmicas, como uma filmagem ou angiografia.[6] No entanto, não tem sido simples substituir os documentos em meio físico

☆ Trabalho realizado na Universidade Federal de Santa Catarina (UFSC) em parceria com a Secretaria de Saúde de Santa Catarina e Bry Tecnologia, Florianópolis, SC, Brasil.

* *Autor para correspondência:* Instituto Nacional para Convergência Digital, Depto. de Informática, Universidade Federal de Santa Catarina, Florianópolis, SC, 88040-900, Brasil.
E-mail: andrade@telemedicina.ufsc.br (R. Andrade).

0104-4230/$ – see front matter
http://dx.doi.org/10.1016/j.ramb.2012.12.009

por documentos eletrônicos.[7] Há desafios tecnológicos, legais, políticos, de interface e aceitação por parte da comunidade.[5]

Para assinar um documento eletrônico, o médico precisa de um computador e de uma identidade digital emitida por uma das Autoridades Certificadores credenciadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória MP 2.200-2 de agosto de 2001.[8] A identidade digital é conhecida no mundo da tecnologia da informação como certificado digital. Atrelado ao certificado há um par de códigos criptográficos exclusivos conhecidos como chave pública e chave privada; esta última (conhecida também por chave de assinatura) é utilizada para assinar o documento eletrônico e a chave pública, para verificar a assinatura.[9]

Entretanto, em termos tecnológicos há questões de praticidade a serem tratadas para que os médicos tenham acesso à certificação digital e possam assim assinar com confiança seus documentos eletrônicos. Uma dessas questões é referente ao estabelecido pelo parágrafo único do artigo 6º da MP 2.200-2, que impõe ao titular do certificado digital a responsabilidade única pela geração do par de chaves criptográficas, com o total controle de uso da chave de assinatura durante todo o ciclo de vida do certificado. Isso não é simples de ser respeitado pelas pessoas, pois a tecnologia atual baseada em *smart cards* não dá tais garantias.[10]

A ICP-Brasil estabeleceu, dentre outros, dois tipos principais de certificados digitais — os chamados A1 e A3. O certificado A1, de duração máxima de um ano, pode ter sua chave privada armazenada na memória do computador; já o A3 é válido por até cinco anos e deve ter a chave privada gerada e mantida em *hardware* criptográfico.[11] Os mais conhecidos desses *hardwares* são o *smart card* e o *token* criptográfico USB: o primeiro é um dispositivo de *hardware* para armazenamento de chaves criptográficas em forma de cartão, e, o segundo, um *smart card* com interface USB, tal como um *pendrive*.

O controle da chave privada é muito mais seguro utilizando esses *hardwares* criptográficos do que usando a memória do computador para armazenamento. No entanto, a conexão de novos periféricos nos computadores cria um problema muito grande de interoperabilidade. Se o *smart card* ou o *token* criptográfico não estiverem devidamente instalados no computador, os usuários poderão ter problemas para executar assinaturas com a chave em *hardware* criptográfico,[9] pois com a chave restrita ao dispositivo, e o dispositivo não acessível, a assinatura não pode ser realizada.

De fato, o certificado A1 foi criado para situações onde não é possível o uso de certificados A3, tal como em servidores *web* e equipamentos de rede. O uso de certificados A1 é um problema, pois não há como atribuir ao médico a responsabilidade de uso da sua chave de assinatura. O uso de certificados A3, por outro lado, impõe o uso de *smart cards*, que é justamente o caminho de solução atualmente buscado pelo Conselho Federal de Medicina em seu projeto de certificação digital para o médico.[11]

Então, a solução atual é satisfatória?

A resposta é sim e não. *Smart cards*, enquanto forem utilizados em ambientes seguros, como intranets de hospitais, isoladas do acesso à internet, são soluções extremamente seguras. Podem ser usados sem medo, por exemplo, para autenticação de prescrições médicas ou laudos em ambientes controlados. Em um computador com acesso à internet, como acontece em um consultório médico, ou em um sistema de telemedicina, onde o profissional médico pode acessar e assinar um documento de qualquer lugar, inclusive a partir de um cibercafé, se houver necessidade de emitir um laudo de urgência, o *smart card* representa um risco para o médico; este não pode confiar no restante dos *softwares* que executam em tais computadores. Assim sendo, um *software* malicioso poderia inclusive solicitar uma assinatura ao cartão do médico sem que ele perceba.[10]

Por que isso acontece? Enquanto o *smart card* se encontra inserido no leitor acoplado a um computador, seu módulo de assinatura pode ser utilizado por qualquer programa naquele computador. Isso o coloca à mercê de programas maliciosos, como os *malware*, que registram a senha digitada pelo usuário (PIN), capturam a comunicação do teclado com o computador (os *keyloggers)* e, a seguir, estão livres para usar o *smart card*. Em questão de poucos segundos pessoas sem acesso físico ao *smart card* podem assinar todo tipo de documento na internet. É importante notar que, para o paciente, o risco é muito pequeno, salvo em casos de foco em um paciente específico. Mas quem pode sofrer consequências, inclusive em função do que coloca a legislação brasileira, é o médico, proprietário deste certificado.[8]

Um problema pouco tratado também neste quesito do uso massivo de assinaturas digitais nos ambientes médicos deve ser o tema da interoperabilidade. O uso de *smart cards* e de *tokens* criptográficos, pelo fato de ser necessário instalá-los no computador, pode se interpor entre a tarefa médica e a criação do documento eletrônico com a assinatura digital. Pode-se, por exemplo, ter problemas no momento da efetivação do laudo eletrônico, em consequência de dificuldades com a instalação dos dispositivos. Neste caso, o médico deve poder concluir o laudo em outro computador onde a interoperabilidade existe. Isso sem dúvidas causa transtornos à atividade do médico e consome um tempo que poderia estar sendo mais bem utilizado.[4]

Há caminhos para se contornarem estes problemas. Tendo identificado esta situação, o Laboratório de Segurança em Computação da UFSC (LabSEC), em parceria com o Instituto Nacional para Convergência Digital (INCoD), a empresa Bry de SC e a Secretaria de Estado da Saúde de SC, está desenvolvendo para o STT/SC, uma pesquisa para criar uma nova forma de assinatura digital de duplo fator por meio do projeto FINEP CIM-Saúde.[12,13]

Este projeto está desenvolvendo uma tecnologia que permitirá assinar eletronicamente e com segurança documentos médicos em qualquer lugar e em qualquer computador. Esta solução passa pelo armazenamento e uso das chaves privadas em servidores de assinatura, os módulos de segurança em *hardware* (HSMs). HSMs são *hardwares* para a guarda de chaves criptográficas que, além de resistirem a ataques de uma forma mais rígida que os *smart cards*, possuem um processo de auditoria integrado para garantir o correto uso das chaves. Os certificados A3, a serem utilizados pelos médicos para assinar documentos eletrônicos, serão usados em conjunto com contrassenhas únicas de confirmação geradas pelo celular do médico por um sistema de autenticação acoplado ao HSM.[14]

Com esta solução, o médico não necessita levar seu *smart card* consigo, deixando-o acoplado a um HSM instalado em uma "sala segura". Uma sala segura é um ambiente construído para controle de acesso físico extremamente rígido onde os sistemas de alta segurança usualmente residem. O risco de captura da senha é eliminado pela contrassenha gerada e enviada pelo celular, que vale apenas para uma utilização, por exemplo, para validar um lote de documentos que um cardiologista laudou em uma sessão do STT/SC finalizada com esta contrassenha. Ao desejar confirmar a assinatura eletrônica em um novo lote de laudos, o médico poderá gerar em seu celular uma nova contrassenha, que será válida por apenas alguns minutos, de forma a reduzir ainda mais o risco de invasão.[14]

Desta forma, a execução de assinaturas por parte do médico se torna muito simples: basta solicitar ao sistema para fazer uma assinatura e ele produz um código de barras multidimensional (*QRCode*) com todas as informações do documento a ser assinado. O médico então usa a câmera do seu aparelho para importar estes dados. Na tela do aparelho ele vê um termo de assinatura dos documentos que lhe explica do que se trata tal assinatura. Ele confirma e digita seu PIN de proteção no aparelho. É então gerado um código de seis dígitos que valida aquela assinatura para o serviço de telelaudos e solicita ao HSM a assinatura do documento.[14]

Este código gerado amarra todos os dados da transação de assinatura de forma que, se algum agente mal-intencionado tentar trocar quaisquer informações da autorização e assinatura, o HSM que fará a assinatura efetivamente rejeita a solicitação. É importante frisar que o médico sempre valida as informações que ele está assinando no seu dispositivo móvel e que, se algo é alterado posteriormente, isso não surte efeito no laudo armazenado no servidor do STT/SC.[14]

Além das vantagens de segurança citadas, o uso de um sistema como esse permite que o médico possa efetivamente emitir o laudo de qualquer computador em qualquer lugar, sem necessariamente confiar no computador. Isso acontece porque toda a confirmação da assinatura é feita no dispositivo móvel dele e só o código de autorização amarrado com aquela assinatura é digitado no computador não confiável. Além de ganhar tempo não tendo que instalar um *token* ou um cartão no computador, o médico tem a certeza que o processo de assinatura sempre ocorreu no dispositivo do qual ele tem total controle, que é o seu celular.[14]

Outro ponto importante da solução é o caso de *software* malicioso instalado na máquina onde o médico emite o laudo. Diferente dos *smart cards* e *tokens*, a solução com dispositivos móveis não permite a inserção de uma assinatura sem que o médico perceba, pois, uma outra grande vantagem do sistema proposto é a manutenção de um histórico de assinaturas executadas por um médico em seu celular. Caso apareçam laudos que o médico não assinou, ele pode comprovar, pelo seu histórico de assinaturas, que não as fez.[14]

Esta estratégia resolve os problemas?

Pode-se dizer que sim, mas o mundo está sempre em evolução e uma solução que parece segura hoje pode não ser no futuro. Como acontece com toda estratégia de segurança, haverá sempre pessoas empenhadas em buscar formas de burlá-la e, eventualmente, uma forma será encontrada. Aqui temos de aplicar o bom senso e nos perguntar: o quão difícil é falsificar uma assinatura em papel? Quem olha duas vezes para um papel assinado de forma ilegível e com um carimbo contendo um registro do Conselho Regional de Medicina? No dia a dia, a assinatura digital com toda certeza representa uma solução muito mais segura e muito mais prática do que o documento em papel, proporcionando segurança e agilidade ao médico. O importante é estarmos constantemente nos questionando e refinando a tecnologia, e que a segurança jurídica de todos, inclusive do médico, esteja garantida.

Suporte financeiro

Esse projeto recebeu apoio financeiro da SES/SC e do FINEP, Florianópolis, SC, Brasil.

REFERÊNCIAS

1. Andrade R, Wagner HM, Von Wangenheim A. Telemedicina em Santa Catarina, um projeto sustentável. In: XIII Congresso Brasileiro de Informática em Saúde – CBIS; 2012.
2. Andrade R, Macedo DDJ, Wallauer J, Von Wangenheim A. Building a National Telemedicine Network. IT Professional. 2008;10:12–7.
3. Savaris A, Andrade R, Macedo DDJ, Von Wangenheim A. O uso da telemedicina assistencial assíncrona em larga escala no setor público de saúde. In: CBIS'2008 - XI Congresso Brasileiro de Informática em Saúde. Campos do Jordão; 2008.
4. Von Wangenheim A, Nobre LFS, Tognoli H, Nassar SM, Ho K. User satisfaction with asynchronous telemedicine a study of users of Santa Catarina's System of Telemedicine and Tele Health. Telemed J E-Health. 2012;18:339–46.
5. Nobre LFS, Von Wangenheim A, Maia RS, Ferreira L, Marchiori E. Certificação digital de exames em telerradiologia: um alerta necessário. Radiol Bras. 40:415-21.
6. Graham RN, Perriss RW, Scarsbrook AF. DICOM demystified: a review of digital file formats and their use in radiological practice. Clin Radiol. 2005;60:1133–40.
7. Andrade R, Wallauer J, Von Wangenheim A, Macedo DDJ. A telemedicine network using secure techniques and intelligent user access control. In: The 21th IEEE International Symposium on Computer-Based Medical Systems, 2008, Jyväskylä. Proceeding of the The 21th IEEE International Symposium on Computer-Based Medical Systems; 2008.
8. Brasil. Medida provisória n(2.200-2, 24 agosto 2001. Institui a infraestrutura de chaves públicas brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília (DF); 2006 [citado 2 out 2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm
9. Stallings W. Cryptography and network security: principles and practice. 5th ed. New Jersey: Prentice Hall Press; 2010.
10. Delaune S, Kremer S, Steel G. Formal analysis of PKCS#11. In: Proceedings of the 2008 21st IEEE Computer Security Foundations Symposium (CSF '08). Washington (DC): IEEE Computer Society; 2008. p. 331–44.
11. Instituto Nacional de Tecnologia da Informação. DOC-ICP-04: requisitos mínimos para as políticas de certificado na ICP-Brasil. V. 5.0 [citado 20 nov 2012]. Disponível em:

http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/docs13082012/DOC-ICP-04_-_Versao_5.0.pdf
12. Projeto FINEP. Certificado de identificação mobile para acesso seguro a ambientes de telessaúde e telemedicina-CIMSaude [citado 20 nov 2012]. Disponível em: http://www.finep.gov.br//fundos_setoriais/ct_saude/resultados/Resultados%20no%20Portal%20-%20Chamada%20Telessa%C3%BAde%20e%20Telemedicina.pdf
13. Universidade Federal de Santa Catarina. Notícias [citado 20 nov 2012]. Disponível em: http://www.inf.ufsc.br/2012/10/30/incod-and-labsec-recebem-visita-do-presidente-do-conselho-federal-de-medicina/
14. Idalino TB, Spagnuelo D. Senhas descartáveis em dispositivos móveis para ambientes de Telemedicina. Curitiba: SBSeg; 2012.