Autenticação digital de documentos médicos: encontramos a solução?

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

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

Não há dúvidas quanto às promessas dos benefícios que a certificação digital confere aos documentos eletrônicos, sobretudo quando o resultado final é um documento impresso, como os laudos médicos. Autenticação e integridade são características importantes que devem ser garantidas através da certificação digital destes documentos, conferindo-os a presunção da eficácia jurídica. Em artigo e editorial publicados anteriormente nesta revista discutimos sobre a importância do tema em questão[1,2]. A certificação digital é a única tecnologia capaz de substituir com segurança documentos em papel assinados pelos médicos por equivalentes eletrônicos. Sabe-se que documentos eletrônicos são mais fáceis de circular, copiar e armazenar, podendo também conter informações mais detalhadas, tais como imagens de alta precisão, e até mesmo dados com características dinâmicas, como uma filmagem. No entanto, não tem sido simples substituir os documentos em meio físico por documentos eletrônicos. Há desafios tecnológicos, legais, políticos e de interface e aceitação.

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. Um dos requisitos importantes é o apresentado no parágrafo único do artigo sexto da Medida Provisória MP 2.200–2 de agosto de 2001, 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 digital. Isso não é simples de ser respeitado pelas pessoas.

A ICP-Brasil estabeleceu, dentre outros, dois tipos principais de certificados digitais. Os chamados A1 e A3. O certificado digital A1, de duração máxima de um ano, pode ter sua chave privada armazenada na memória do computador. Já o A3, válido por três anos, deve ter a chave privada gerada e mantida em *hardware* criptográfico. Os mais conhecidos desses *hardwares* são o *smartcard* e o *token* criptográfico USB.

O controle da chave privada é muito mais fácil se utilizados esses *hardwares* criptográficos para armazenamento, em vez da memória do computador. De fato, o certificado A1 foi criado para situações em que 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 garantir ao médico a responsabilidade de uso da sua chave de assinatura. O uso de certificados A3, por outro lado, impõe o uso de *smartcards*, que é justamente o caminho de solução sendo buscado pelo Conselho Federal de Medicina em seu projeto de certificação digital para o médico.

Esta solução é satisfatória? A resposta é sim e não... *Smartcards*, enquanto forem utilizados em ambientes seguros, como ambientes de rede interna de hospitais, sem acesso à internet, são soluções robustas e seguras, podendo ser usados sem medo, por exemplo, para autenticação de prescrições médicas ou laudos. Em um computador com acesso à internet a situação é bastante

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

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

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

diferente. É o caso, por exemplo, da utilização de sistemas de telerradiologia em que o radiologista confere seus laudos conectado à internet, seja de seu próprio consultório ou de um computador público, em casos urgentes. Se você se identificou com o cenário acima descrito, cuidado: aí existe risco para o médico.

Por que isso acontece? Enquanto o *smartcard* se encontra inserido no leitor acoplado a um computador, seu módulo de assinatura pode ser utilizado por qualquer programa naquela máquina. Isso coloca o *smartcard* à mercê de programas maliciosos, que registram a senha digitada pelo usuário (PIN) e, a seguir, estão livres para usar o *smartcard.* De posse dessa senha, em questão de poucos segundos este tipo de programa "espião" pode assinar todo tipo de coisa na internet por você! É importante ressaltar que, segundo o que dita a legislação brasileira, nesta situação o risco para o paciente é praticamente nulo, e quem pode sofrer consequências é o médico proprietário deste certificado.

Há caminhos para se contornar este problema. Tendo identificado esta situação, o Laboratório de Segurança em Computação da UFSC (LabSEC – http://www.labsec.ufsc.br/), em parceria com o Instituto Nacional para Convergência Digital (INCoD – http://www.incod.ufsc.br), a Secretaria de Estado da Saúde de Santa Catarina e a empresa Bry estão desenvolvendo para a Rede Catarinense de Telemedicina o projeto FINEP CIM-Saúde.

Este projeto tem por objetivo desenvolver uma estratégia que permita ao médico assinar eletronicamente e com segurança documentos médicos de qualquer lugar e em qualquer computador. Esta solução passa pelo armazenamento e uso das chaves privadas em servidores de assinatura remotos com total proteção contra o uso indevido, os chamados Módulos de Segurança Criptográfica (HSMs), hoje ainda não permitidos no Brasil para certificados A3, a serem utilizados em conjunto com contrassenhas únicas de confirmação enviadas ao celular do médico por um sistema de autenticação acoplado ao HSM. Com esta solução, o médico não necessita levar seu *smartcard* consigo, deixando-o acoplado a um HSM instalado em uma sala segura na instituição certificadora ou mesmo usando um *slot* de tal dispositivo como se fosse seu *smartcard* real. O risco de captura da senha é eliminado pela contrassenha gerada e enviada ao celular, que vale para apenas uma utilização, mas que pode ser utilizada, por exemplo, para validar um lote de exames que um radiologista telelaudou em uma mesma sessão de trabalho. Ao desejar confirmar a assinatura eletrônica em um novo lote de laudos, o médico receberá em seu celular uma nova contrassenha, que será válida por apenas alguns minutos, de maneira a reduzir ainda mais o risco.

Esta estratégia resolve todos os problemas? Até onde podemos identificar riscos, sim. Como acontece com toda estratégia de segurança, haverá sempre pessoas empenhadas em encontrar 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? 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. O mais importante é estarmos constantemente nos questionando e buscando soluções para o refinamento das tecnologias de suporte às atividades de telemedicina, sempre com a preocupação de garantir segurança aos profissionais.

REFERÊNCIAS

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.