CERTIFICAÇÃO DIGITAL DE EXAMES EM TELERRADIOLOGIA: UM ALERTA NECESSÁRIO*

Luiz Felipe Nobre[1], Aldo von Wangenheim[2], Rafael Simon Maia[3], Levi Ferreira[3], Edson Marchiori[4]

Resumo **A crescente popularização das atividades de telemedicina em todo o mundo tem exigido de médicos e demais profissionais da saúde novas abordagens em sua prática profissional. No que se refere à telerradiologia, observamos forte tendência à transformação de documentos clínicos — como resultados de exames, que até hoje existiam na forma de filmes impressos e laudos em papel — em documentos eletrônicos, disponibilizados em redes internas de clínicas e hospitais, ou pela internet. Esta tendência torna necessária a divulgação e o esclarecimento de conceitos como a certificação digital, a criptografia de dados na internet, a confiabilidade de *sites*, o documento eletrônico confiável e a assinatura digital. Os princípios básicos desses conceitos, embora por vezes complexos para os profissionais da saúde, podem ser compreendidos de forma efetiva sem que o leitor tenha de mergulhar de cabeça em labirintos como a matemática da criptografia de chaves assimétricas ou os protocolos de comunicação digital de dados. Neste artigo abordaremos de forma direta e com exemplos práticos os aspectos de segurança e confiabilidade de documentos clínicos eletrônicos baseados na internet, com o objetivo de que os usuários médicos possam interagir de forma informada, segura e bem fundamentada com serviços de telerradiologia.**
Unitermos: Telerradiologia; Segurança em computação.

Abstract *Digital certification in teleradiology: a necessary warning.*
The increasing worldwide popularization of telemedicine activities has demanded a new approach to the professional practice by physicians and other health professionals. As far as teleradiology is concerned, a remarkable trend has been observed toward the transformation of clinical documents — like radiological studies results, that so far existed as printed films and paper-based reports — into electronic documents available in internal networks of medical clinics and hospitals or through the internet. As a result of this trend, it is necessary to divulge and explain concepts such as digital certification, internet data encryption, sites' reliability, reliability of electronic documents, and digital signature. Even though the baseline principles of these concepts may seem complex for health professionals, they can be effectively understood with no need to wander through labyrinths like the mathematics of asymmetric keys cryptography, or digital data communication protocols. Security and reliability aspects related to internet-based electronic clinical documents are described in the present study, in a straight and practical way, aiming at an informed, safe and soundly grounded interaction between medical users and telemedicine services.
Keywords: Teleradiology; Safety in information technology.

INTRODUÇÃO

O intercâmbio eficiente de informação entre profissionais de saúde pode economizar tempo e dinheiro, proporcionar maior efetividade clínica, melhorar a continuidade e a qualidade da assistência, assim como facilitar as atividades de gestão em sistemas de saúde públicos e privados. Novas tecnologias proporcionam acesso facilitado a essa informação, que é transformada em uma das matérias-primas sobre as quais a sociedade contemporânea baseia seu desenvolvimento. A telemedicina tem sido utilizada como importante ferramenta neste contexto.

A radiologia é uma das especialidades médicas com maior potencial em beneficiar-se das aplicações de telemedicina. Atividades como o diagnóstico e a segunda opinião médica a distância (telediagnóstico e teleconsultoria, respectivamente), ou ainda a disponibilização de imagens e resultados de exames por intermédio da internet têm se tornado práticas cada vez mais comuns nessa nova realidade. As plataformas tecnológicas que permitem essas atividades estão hoje sendo progressivamente implantadas na rotina das clínicas radiológicas como parte de suas infra-estruturas computacionais.

No Brasil, assim como no resto do mundo, um número cada vez maior de serviços e clínicas radiológicas vem implantando sistemas de arquivamento e transmissão de imagens médicas, mais conhecidos como "sistema de comunicação e arquivamento de imagens" (*picture archiving and*

* Trabalho realizado no Projeto Cyclops/Laboratório de Telemedicina do Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brasil.

1. Doutor em Medicina, Professor Adjunto de Radiologia, Chefe do Serviço de Radiologia do Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Coordenador da Rede Catarinense de Telemedicina SES/UFSC, Florianópolis, SC, Brasil.

2. Professor Adjunto do Departamento de Informática e Estatística, Coordenador do Projeto Cyclops da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brasil.

3. Mestrandos em Ciências da Computação, Pesquisadores do Projeto Cyclops e do Laboratório de Telemedicina do Hospital Universitário da Universidade Federal de Santa Catarina (UFSC), Florianópolis, SC, Brasil.

4. Professor Titular de Radiologia da Universidade Federal Fluminense (UFF), Niterói, RJ, Coordenador Adjunto do Curso de Pós-graduação em Radiologia da Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, RJ.

Endereço para correspondência: Prof. Dr. Luiz Felipe Nobre. Rua Constancio Krumel, 1083, Praia Comprida. São José, SC, Brasil, 88103-600. E-mail: luizfelipenobre@gmail.com

Recebido para publicação em 27/11/2006. Aceito, após revisão, em, 16/4/2007.

communications system – PACS) e "sistema de informação radiológica" (*radiology information system* – RIS). Além do arquivamento e da transmissão de imagens, suportados pelos PACS, nos RIS é realizada também a manutenção e disponibilização de dados de prontuários médicos associados às imagens. A utilização desses sistemas digitais oferece inúmeras vantagens para médicos radiologistas, requisitantes e pacientes. Em médio prazo, proporciona, ainda, redução de custos, favorecendo uma menor utilização de filmes e químicos, e diminuindo a repetição de exames, seja por questões técnicas, seja por permitir o acesso facilitado a exames anteriores de um determinado paciente. Esses sistemas, se conectados entre si por meio da internet, propiciam também, intrinsecamente, a possibilidade do intercâmbio facilitado de exames e resultados, o que torna imediatamente disponível a opção da troca de serviços de laudo entre clínicas e a criação de centrais de telediagnóstico. No entanto, pouco se tem discutido, no meio radiológico, acerca de uma questão fundamental relacionada a esse novo modelo: a segurança necessária para a transmissão e a disponibilização eletrônica de imagens digitais e laudos radiológicos.

Neste artigo discutiremos a importância da certificação digital de documentos eletrônicos — tanto imagens digitais como resultados textuais de exames — disponibilizados eletronicamente pela internet, e abordaremos de forma breve os mais importantes aspectos tecnológicos associados a esses temas.

DISCUSSÃO

Assim como vem ocorrendo em todo o mundo nas últimas décadas, também no Brasil temos observado progressiva transformação digital dos serviços de radiologia, ainda que dificultada pelas limitações financeiras características da realidade econômica de nosso país. Além da tradicional utilização de aparelhos originalmente digitais em clínicas e hospitais, tais como a ultra-sonografia, a tomografia computadorizada e a ressonância magnética, ocorre em nosso meio a substituição de aparelhos convencionais de radiologia por modelos que permitem a obtenção direta ou indireta de imagens digitais, conhecidos como DR e CR, respectivamente. Imagens e laudos radiológicos passam a ser, em muitos casos, disponibilizados pela internet para pacientes e médicos requisitantes[1]. Do ponto de vista de segurança e sigilo da informação, é fundamental que esses exames e resultados satisfaçam condições técnicas e legais para serem considerados documentos eletrônicos confiáveis.

Nos últimos anos, o aumento do tráfego de dados sensíveis na internet ofereceu oportunidades que fizeram crescer o número de fraudes eletrônicas, de 2004 para 2005, em 579%[2]. As técnicas utilizadas em alguns tipos de fraudes podem também ser utilizadas para ameaçar o tráfego de dados sensíveis de pacientes e a atividade médica através da internet.

Para alívio dos atuais e futuros usuários da telerradiologia, existe um conjunto de tecnologias disponíveis para conter a falsificação de imagens e resultados de exames, oferecendo segurança e garantindo validade legal a documentos eletrônicos médicos. Conforme podemos observar na Figura 1, essas ferramentas de segurança estão divididas em três grupos, com características e ações distintas, a saber: acesso seguro, assinatura eletrônica e protocolação digital, formando o que poderíamos chamar de "tripé da segurança em telerradiologia" (TST).

O que é um documento eletrônico confiável ?

Da mesma forma que para ter valor um documento tradicional tem de ser íntegro e sem rasuras, estar assinado e devidamente datado, assim também devem ser os documentos eletrônicos. Cada um dos grupos de tecnologias da Figura 1 trabalha com um conjunto de características ou atributos necessários para a geração de um documento eletronicamente confiável e com valor legal estabelecido pela lei brasileira. No mundo digital, além das características de confidencialidade e sigilo obtidas pelo acesso seguro à internet, mediante transmissão encriptada de dados, existem algumas outras certezas que devem ser garantidas para que se possa assegurar que um determinado documento eletrônico seja confiável, que tenha origem em uma fonte segura, que não tenha sido alterado, e que tenha sido produzido num determinado momento específico no tempo. Estes requisitos de segurança, aceitos juridicamente como incontestáveis, são descritos como:

– **Autenticidade:** Do Aurélio "autêntico, que é do autor a quem se atribui". Em um documento tradicional, a autenticidade é dada por assinatura reconhecida. Já um documento eletrônico é considerado autêntico se foi assinado digitalmente, por meio do uso de um certificado digital válido.

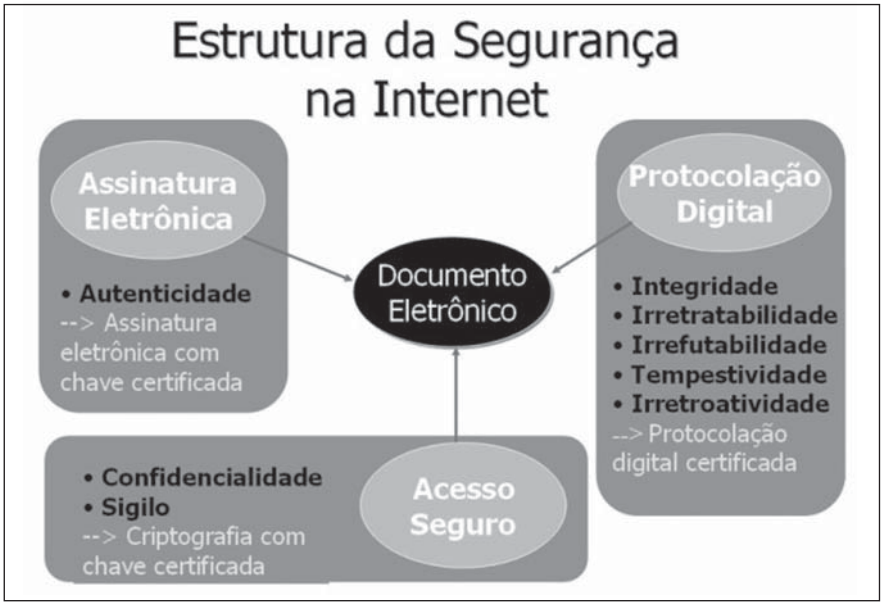

Figura 1. Tecnologias de segurança para a disponibilização e o intercâmbio de documentos eletrônicos na internet, baseadas no tripé: acesso seguro, protocolação digital e assinatura eletrônica.

– **Integridade:** "Íntegro, inteiro, completo". É a prova de que um determinado documento não foi alterado, sob nenhum aspecto. Um documento tradicional não pode estar rasurado ou adulterado.

– **Irrefutabilidade** (ou irretratabilidade): "Que não se pode refutar; evidente, irrecusável, incontestável".

– **Tempestividade** (ou irretroatividade): Possibilidade de se comprovar que um evento eletrônico ocorreu em um determinado instante específico no tempo.

Iniciaremos a discussão sobre as ferramentas atualmente disponíveis para garantir segurança ao uso de documentação eletrônica através da internet, pela questão da transmissão sigilosa dos dados médicos por meio da criptografia, o que nos permitirá desenvolver, de maneira simples, o conceito de certificado digital, essencial para que se realizem todas as técnicas do TST.

O que é criptografia?

Do grego *kryptós gráphein* – "escrita secreta", é a ciência de reescrever um texto de forma a esconder o seu significado. Também em computação refere-se ao uso de técnicas que permitem escrever em cifras ou códigos, tornando uma mensagem incompreensível. Quando substituímos palavras de uma mensagem por outras definidas em um código, o processo denomina-se *codificação*. Quando utilizamos um método matemático para alterar a mensagem, o processo é conhecido como *cifragem*. O processo de cifragem é baseado em uma regra matemática de substituição das letras da mensagem e um número que altera o comportamento desta regra, de maneira que, ao se cifrar a mensagem com números diferentes, diferentes resultados serão obtidos. Este número é chamado de *chave*, e quanto maior for, mais segura será a cifragem. Este processo visa a assegurar que apenas o destinatário consiga ler uma mensagem eletrônica, realizando o processo inverso, a *decifragem*. Quando cifragem e decifragem são realizadas com a utilização de uma senha ou chave única, denominamos o processo de criptografia simétrica (Figura 2). Esta apresenta a desvantagem de que precisamos combinar a chave a ser utilizada com quem nos vai enviar uma mensagem cifrada, e neste processo a chave pode ser interceptada. A criptografia assimétrica, ou de chaves públicas, utiliza um conceito diferente, possuindo duas chaves, denominadas chave privada e chave pública. São números muito grandes, com um relacionamento matemático entre si. Quando uma das chaves é utilizada para cifrar uma mensagem ou documento, seu conteúdo somente pode ser decifrado com a utilização da outra chave. A chave privada do emitente de uma documentação eletrônica fica guardada com ele, e somente ele tem acesso e conhecimento dela. Já a chave pública, como o próprio nome diz, é de conhecimento de todos, e normalmente fica disponibilizada na internet.

Como disponibilizar uma informação na internet garantindo sua confidencialidade?

A criptografia assimétrica permite trafegar dados confidenciais na internet de forma segura e flexível. Para a realização de acesso seguro, garantindo confidencialidade e sigilo na transferência dos dados, sejam eles de uma transação bancária ou de um paciente, a utilização de criptografia é realizada através de um protocolo denominado SSL/TLS (*secure socket layer*). Quando acessamos uma página confidencial na rede estamos estabelecendo este tipo de encapsulamento seguro entre nosso computador e o servidor da instituição bancária, ou do serviço de telemedicina em questão. Para tanto, o programa navegador (*browser*) de um determinado computador vai usar um par de chaves pública/privada que é específico daquela instalação do programa, naquele computador específico, sendo diferente das chaves utilizadas por outros navegadores, em outros computadores. Estabelecendo-se uma conexão por meio da internet, o computador em questão e o servidor acessado vão intercambiar as suas chaves públicas, de forma que cada um possa encriptar de forma "personalizada" as mensagens e dados enviados ao outro. Como forma de segurança adicional, de maneira a garantir ao usuário que quem está enviando a chave pública é realmente quem diz ser, e não um "clube de *hackers*" se fazendo passar por um serviço de telemedicina qualquer, o servidor não deve enviar apenas a sua chave pública, mas sim um certificado digital, que pode ser verificado pelo *browser*.

O que é um certificado digital?

Um certificado digital é um documento eletrônico que identifica o emissor de uma chave criptográfica. Nesse certificado, uma terceira parte confiável, denominada autoridade certificadora, atesta a autenticidade da chave pública ou privada aí contida, garantindo a identidade do seu emissor. Um certificado digital contém, além da chave

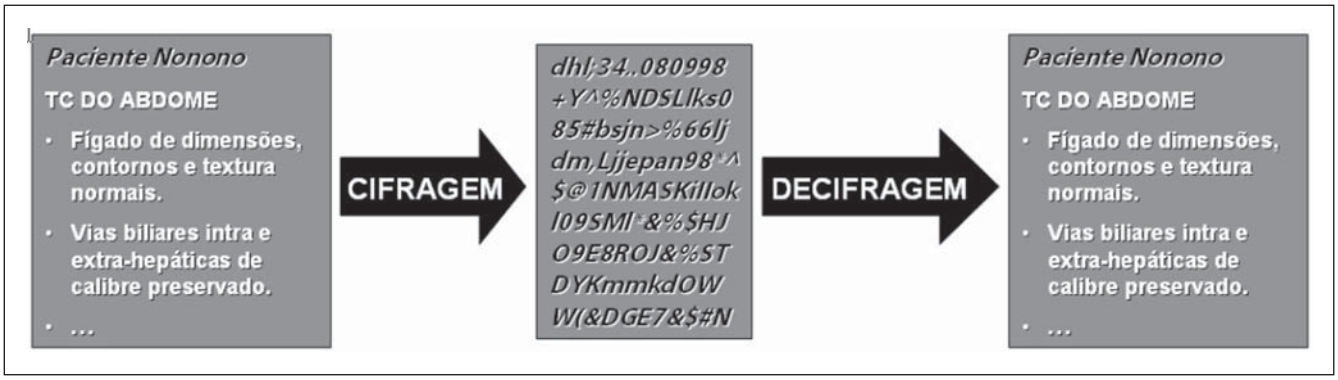

Figura 2. Criptografia de chave simétrica: texto de laudo circula na internet de forma cifrada. A senha utilizada para codificação e decodificação do texto é a mesma.

oferecida, também dados de seu titular, tais como nome, e-mail, CPF e o nome da autoridade certificadora que o emitiu, além de uma repetição dessa chave, mas assinada digitalmente pela autoridade certificadora. Na prática, funciona como uma carteira de identidade virtual, autenticada por uma entidade confiável, que garante a identificação segura da contraparte em uma transação através de uma rede de computadores (Figura 3). Existem várias empresas e órgãos governamentais que emitem certificados digitais no mercado nacional e internacional. Quem confere autenticidade aos certificados digitais emitidos em nosso país é unicamente o ICP-Brasil[3], órgão vinculado ao Instituto Nacional de Tecnologia da Informação, autarquia ligada, por sua vez, à Casa Civil. O ICP-Brasil é composto por uma cadeia de autoridades certificadoras, formada por uma autoridade certificadora raiz, autoridades certificadoras e autoridades de registro e, ainda, por uma autoridade gestora de políticas (comitê gestor). Este comitê, composto por representantes do governo e da sociedade civil, é responsável pela definição de um conjunto de regras e normas necessárias para a certificação digital, baseadas em padrões públicos internacionais.

Como saber que um *site* é confiável ?

Um *site* seguro é aquele que oferece acesso encriptado por meio de um certificado digital autenticado por uma autoridade certificadora confiável.

Para demonstrarmos como podemos discernir um certificado digital confiável de outro inválido, preparamos uma seqüência de exemplos, que veremos a seguir. Os exemplos das Figuras 4, 5 e 6 foram todos realizados com a versão em português do programa Mozilla Firefox®, um navegador de internet gratuito, que roda em Microsoft Windows®, em Linux® e em muitos outros sistemas operacionais. Outros navegadores bastante populares, como o Microsoft Internet Explorer® ou o Netscape®, também apresentam certificado digital com formato muito similar aos demonstrados em nossos exemplos.

Uma conexão segura acontece sempre que observarmos um cadeado fechado na base da página de um programa navegador (Figura 4). Todos os navegadores permitem acessar informações dessa conexão. Para ter acesso ao certificado da conexão, pode-se clicar diretamente sobre esse cadeado, ou acessar um ponto de menu do tipo "Ferramentas > Opções da Internet" no alto da janela do programa. Independentemente da opção utilizada, teremos como resultado a abertura de uma janela com dados básicos sobre a conexão encriptada, especificando, entre outras coisas, se o programa navegador foi capaz de verificar a autenticidade do certificado digital, o que, se confirmado, caracteriza o *site* como confiável. Todo programa navegador permite ainda acessar maiores detalhes desse certificado e da autoridade certificadora que o emitiu, geralmente através de um botão ou ponto de *menu* para isso.

Na Figura 5 podemos observar janelas do navegador Mozilla Firefox®, utilizado no presente trabalho, com informações sobre o certificado (a) e informações sobre a cadeia de autenticação do certificado até a autoridade certificadora raiz (b). É esta cadeia de autenticação que vai nos interessar quanto à validade do certificado digital. Todos os órgãos da mesma são entidades que são certificadas pela sua autoridade imediatamente superior, criando uma cadeia de confiança, conhecida também como *trust network*. Se em algum ponto dessa cadeia não existir uma entidade confiável, o certificado não tem validade. Como veremos adiante, considerando-se projetos de telemedicina, o Conselho Federal de Medicina (CFM) exige que a entidade que está na raiz da cadeia de confiança seja o ICP-Brasil, sendo, portanto, esta entidade que se deve procurar ao analisarmos a segurança de um *site* médico.

Para saber se uma autoridade certificadora que emitiu um certificado digital é confiável, um navegador consulta uma lista interna que ele mantém e atualiza regularmente. Esta lista, mostrada na Figura 6(a), pode ser consultada utilizando-se o *menu* de opções de internet do navegador. Se rea-

Figura 3. Correspondência entre a identificação segura de um documento nos mundos real e virtual.

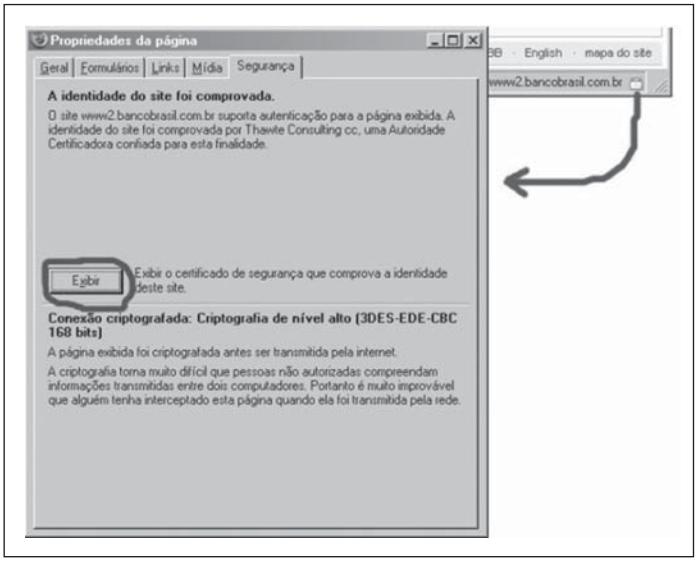

Figura 4. Propriedades de uma página segura na internet.

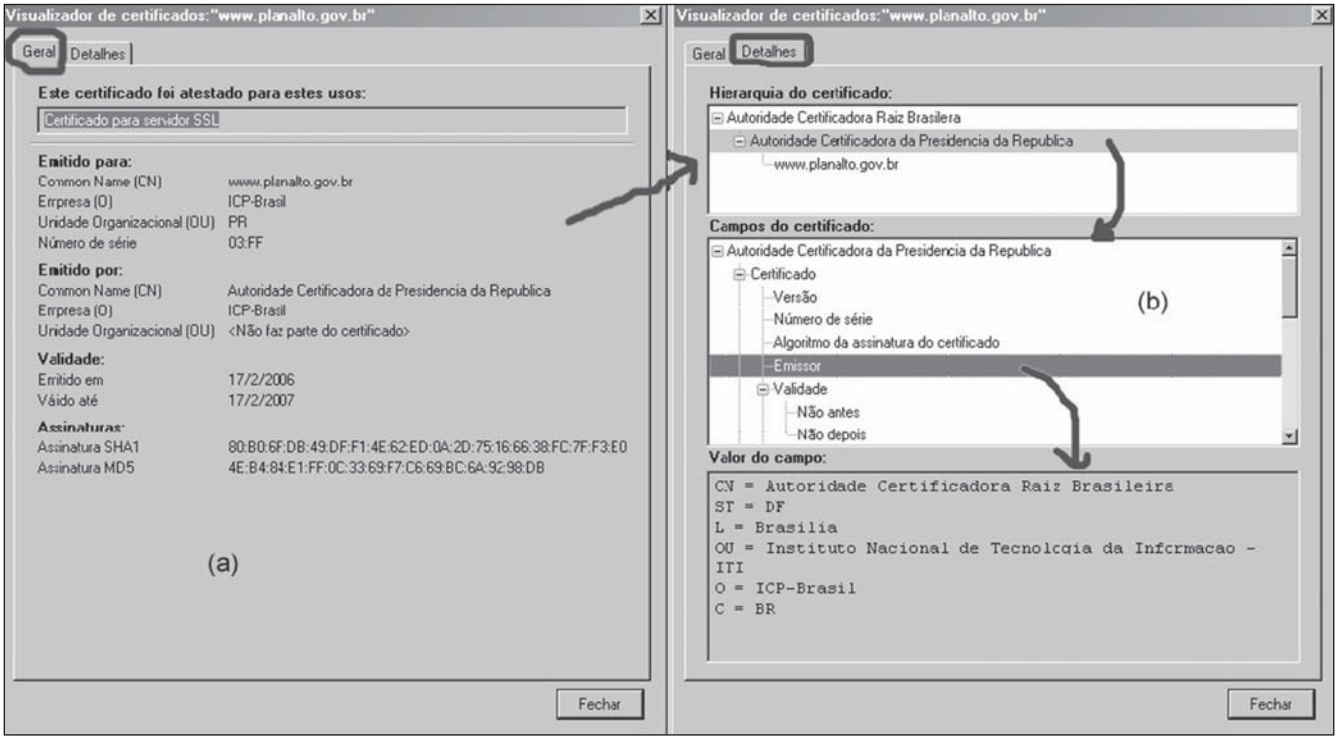

Figura 5. Detalhes de um certificado digital do Palácio do Planalto mostrando, em (**a**), dados do certificado e para que tipos de uso ele foi emitido, e ao alto em (**b**), a cadeia de certificação.

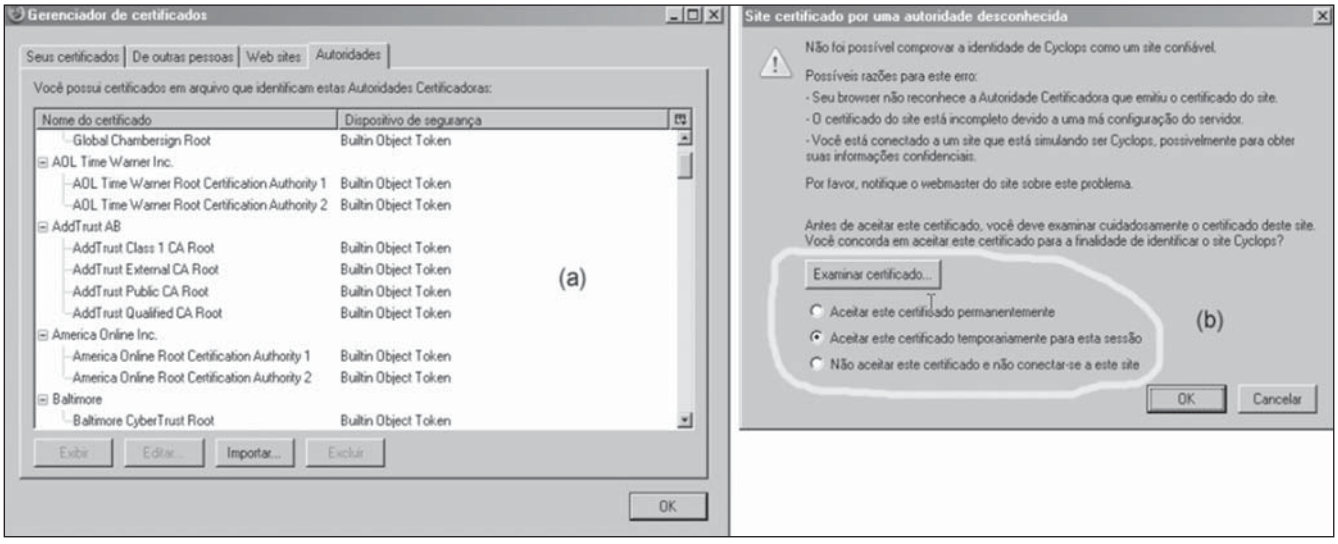

Figura 6. Em (**a**), lista de autoridades certificadoras confiáveis conhecidas do navegador, e em (**b**), janela solicitando inclusão ou rejeição de um certificado de autoridade certificadora desconhecida que não pôde ser verificado.

lizarmos uma conexão encriptada e o navegador não conseguir encontrar uma referência para alguma autoridade certificadora da cadeia de confiança do certificado, abre-se uma janela como a mostrada na Figura 6(b), solicitando que se decida manualmente se aceitamos ou não a conexão, e se confiamos ou não na autoridade certificadora que emitiu o certificado. Se aceitarmos este certificado de forma permanente, a autoridade certificadora que o emitiu vai ser incluída na lista de autoridades certificadoras confiáveis, e quando o *site* for novamente acessado, o programa aceitará o certificado digital. Às vezes, a lista de autoridades certificadoras de um navegador pode estar desatualizada, e essa inserção manual pode ser necessária, mas deve-se sempre tomar muito cuidado ao se fazer isso.

O que é assinatura eletrônica?

A assinatura eletrônica utiliza o mesmo mecanismo da criptografia com chave certificada digitalmente. Ao assinarmos um

documento eletronicamente, cria-se primeiro um resumo desse documento por meio de um método pré-definido, chamado *hash* unidirecional. Este será, ainda, imediatamente encriptado com uma chave privada pessoal, devidamente certificada. Esse código *hash* é denominado unidirecional, pois é impossível inverter a operação e, a partir dele, reobter-se a mensagem original, ou seja, podemos gerar um código *hash* a partir da mensagem, mas não podemos recuperar a mensagem novamente a partir do código *hash*.

Todas as pessoas que receberem o documento assinado digitalmente vão poder decriptá-lo com sua chave pública e ver que foi assinado com uma chave confiável certificada por uma autoridade certificadora, que nesse caso atua como "cartório digital" de autenticação de sua assinatura. Isto possui ainda mais uma vantagem: a técnica permite não só verificar a autoria do documento, como estabelece também uma "imutabilidade lógica" de seu conteúdo, pois qualquer alteração deste invalidaria a assinatura digital.

Faz-se necessário, entretanto, distinguir assinatura eletrônica, ou digital, da assinatura digitalizada. A assinatura digitalizada é a reprodução da assinatura autógrafa por um equipamento tipo *scanner*, originando um arquivo de imagem, que pode ser facilmente anexado a um documento. Ela não garante a autoria e a integridade do documento eletrônico, porquanto não existe uma associação inequívoca entre o subscritor e o texto digitalizado, uma vez que ela pode ser facilmente copiada e inserida em outro documento.

Como discutimos anteriormente, documentos eletrônicos não-certificados e assinados digitalmente têm o potencial risco de alterabilidade e fácil falsificação. Entretanto, percebamos que a assinatura digital não torna o documento eletrônico sigiloso, pois ele em si não é cifrado. O sigilo do documento eletrônico poderá ser resguardado apenas mediante a cifragem da mensagem com a chave pública do destinatário, pois somente com o emprego de sua chave privada poderá o documento eletrônico ser decifrado. A assinatura em um documento digital é feita utilizando-se o código pessoal contido na chave privada. Através dele o documento pode ser cifrado, de forma que só possa ser decifrado com a utilização de sua chave pública, identificando assim quem o assinou. Quando o portador de uma chave digital produz um documento e o assina digitalmente, este documento é encriptado e enviado junto com a sua chave pública, só podendo ser acessado por intermédio dela. Quando for necessário agregar segurança e confiança a qualquer documento eletrônico (contratos, laudos médicos, procurações, projetos, etc.), basta selecionar-se o arquivo desejado e assiná-lo com sua identidade digital. A partir desta operação, o arquivo recebe os atributos de autenticidade e integridade lógica. Entretanto, note-se que com as técnicas até aqui mencionadas ainda não garantimos a temporalidade de um documento, o que veremos como fazer a seguir.

A chave privada para assinaturas digitais pode ser armazenada em seu próprio computador, ou em *hardwares* portáteis que funcionam como mídias armazenadoras (*smart cards* ou *tokens*). O acesso às informações neles contidas é feito por meio de uma senha pessoal, determinada pelo titular, o que fornece um segundo nível de segurança. O *smart card* assemelha-se a um cartão magnético, sendo necessário um aparelho leitor para seu funcionamento. Já o *token* assemelha-se a uma pequena chave e requer a utilização de uma porta USB para conexão, localizada, geralmente, na CPU do computador (Figura 7). Infelizmente, mesmo com o uso de um sistema digital de assinatura, é sempre possível que o roubo ou extravio do dispositivo onde a chave privada esteja armazenada possa comprometer o nível de segurança de sua utilização, tal como o roubo de uma chave física pode comprometer a segurança de um local.

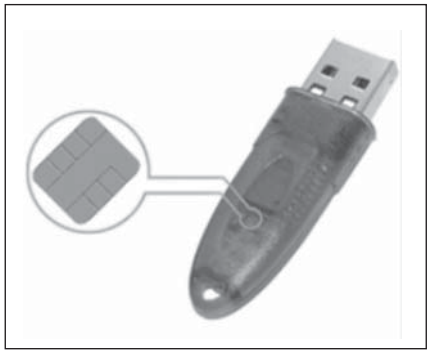

Figura 7. *Token*, ou mecanismo portátil de memória USB, utilizado para armazenamento da chave privada.

Além dessas tecnologias de cifragem ou criptografia, certificação e assinatura digitais, informações de tempo em documentos eletrônicos devem ser exigidas por diversas razões, por exemplo, para se comprovar que um documento foi assinado antes da revogação de um certificado digital, ou do comprometimento de uma chave privada, ou mesmo antes de um procedimento ao qual estava temporalmente relacionado. Imaginemos, como exemplo aplicável à telerradiologia, a importância da garantia de que um determinado laudo foi emitido **antes** da realização de uma cirurgia, cujo planejamento se baseou nas informações fornecidas pelo citado laudo.

Uma maneira de garantir-se a tempestividade em documentos eletrônicos de forma segura é pelo uso de uma "protocolizadora digital de documentos eletrônicos" (PDDE). Uma PDDE é um computador servidor que garante segurança temporal nas transações eletrônicas, fornecendo meios de verificar-se se um documento se mantém íntegro ou não, desde o momento de sua protocolação. É composta por uma plataforma computacional, uma identidade digital (chaves privada e publica, por exemplo), um *hardware safe module* (HSM) — memória inviolável para armazenamento dessas chaves — e um programa para fazer as interações necessárias. A PDDE utiliza como fonte de tempo a hora do Observatório Nacional, através do protocolo *network time protocol* (NTP). De posse desse dado, ela o assina com sua chave privada (seguramente guardada por *hardware* à prova de violação) e o envia de volta na forma de um recibo. Antes disso, porém, ela armazena uma cópia do recibo gerado em seu banco de dados. Com essas características, a PDDE garante, em respeito à informação temporal do documento:

– Privacidade: acesso ao resumo do documento, não ao documento original.

– Integridade: ao receber o recibo, pode-se verificar a assinatura digital da PDDE e confirmar se ele foi alterado.

– Irrefutabilidade: o recibo fornece evidência da existência do documento e de sua protocolização. O cliente não pode negar existência, e a autoridade de datação não pode negar ato de protocolização.

– Confiança: equipamento de datação lacrado e com padrões de segurança física e lógica auditável.

– Facilidade de comunicação e armazenamento: só o resumo do documento é utilizado.

Quais as conseqüências dessas tecnologias para a telerradiologia?

Na prática, abordando o caso específico da telerradiologia, torna-se fundamental que essas diferentes ferramentas sejam utilizadas para garantir a segurança e a confiabilidade de um resultado de exame disponibilizado eletronicamente na internet. Imagens, individualmente ou em conjunto, e o laudo médico associado a elas podem ser assinados e protocolados digitalmente, assegurando-se, dessa forma, que tenham sido enviados pelo remetente, em determinado período do tempo, e que o seu conteúdo não tenha sofrido alteração entre os momentos do envio e do recebimento. A protocolação digital por meio de uma PDDE é a única forma de assegurarmos este tipo de segurança aos documentos eletrônicos[4].

Entretanto, no que diz respeito especificamente à telemedicina, existe ainda em nosso País apenas uma resolução do CFM (nº 1643/2002) que regulamenta os requisitos necessários para o armazenamento, acesso e transmissão seguros de dados médicos[5]. Lendo-se atentamente a resolução, logo se percebe que em seu artigo 2º exige-se apenas que as transferências de informações médicas por telemedicina utilizem um canal de criptografia segura entre o servidor de internet e o programa navegador do usuário. Essa transferência segura deve ser realizada por meio de um canal criptográfico, utilizando-se o protocolo SSL e uma chave criptográfica fornecida e autenticada pela entidade certificadora estadual. Na verdade, não existe nesta resolução do CFM nenhuma exigência quanto a qualquer tipo de certificação, protocolação ou mesmo assinatura digital de documentos. Entretanto, é importante que observemos que a mesma resolução do CFM, em seu artigo 4º, diz que "a responsabilidade profissional do atendimento cabe ao médico assistente do paciente. Os demais envolvidos responderão solidariamente na proporção em que contribuírem por eventual dano ao mesmo". Resta saber se em atividades de telediagnóstico e segunda opinião, não-protocoladas digitalmente, o médico assistente terá plena confiança em responsabilizar-se integralmente por um laudo fornecido por um radiologista a distância, sabendo que nada garante que tal laudo não possa ter sido fraudado digitalmente. No Estado de São Paulo, a Resolução Cremesp nº 97/2001 também trata de assuntos relacionados à telemedicina, e em alguns trechos, mais especificamente de atividades de telerradiologia[6]. Em seu item 5, relativo ao envio de resultados de exames pela internet, dispõe: "...procedimento cada vez mais comum é o envio de resultado de exames diagnósticos (radiografias, exames de sangue, de urina e outros) pela internet. Para evitar a quebra de sigilo e de privacidade, quem envia as informações deve tomar precauções técnicas adicionais, como o uso de criptografia ou de servidores especiais que barram a entrada de quem não está autorizado". Aqui também só se fala em acesso restrito e confidencial aos resultados, por intermédio de senhas, e transmissão encriptografada por e-mail, deixando "aberta a porta" para a fraude digital em documentos não-protocolados.

CONCLUSÃO

Novas tecnologias, associadas à carência de profissionais especializados em regiões remotas do País e do mundo, tendem a tornar as atividades de telediagnóstico e segunda opinião práticas cada vez mais freqüentes em telerradiologia. Da mesma forma, a disponibilização eletrônica de resultados de exames radiológicos apresenta-se como alternativa viável e interessante na agregação de valor à assistência para médicos requisitantes e pacientes, e para redução de custos. No entanto, em função da vulnerabilidade observada na circulação de informação e dados pela internet, uma série de conceitos de segurança deve ser tratada quando da implementação de um projeto de telemedicina, sobretudo em relação à privacidade, idoneidade e temporalidade das informações disponibilizadas eletronicamente.

A informação médica deve ter garantias quanto à idoneidade de sua fonte e integridade de seu conteúdo, bem como do momento de sua geração, transmissão, manipulação e armazenamento. Nesse contexto se inserem as tecnologias de assinatura e certificação digital e as autoridades certificadoras. Todo registro de imagem ou procedimento médico deve, por intermédio desses mecanismos, ser digitalmente assinado e certificado. Com esses procedimentos, tanto a idoneidade de sua fonte como a segurança e tempestividade de seu conteúdo são garantidos para o armazenamento, a transmissão e a disponibilização eletrônica de imagens e textos de laudos em redes interna e externa de computadores. Todo e qualquer acesso a um documento médico só deve ser possível mediante identificação de sua fonte pelo mecanismo de chaves (privada e pública), e qualquer tentativa de alteração desse documento será detectada pela não-concordância com o seu certificado digital.

O que consideramos fundamental é que os conceitos relacionados neste artigo sobre segurança eletrônica sejam discutidos por um número cada vez maior de colegas radiologistas, que devem tomar consciência das dificuldades que podem resultar de uma utilização inadequada de projetos não-certificados de telerradiologia.

REFERÊNCIAS

1. Azevedo-Marques PM, Caritá EC, Benedicto AA, Sanches PR. Integração RIS/PACS no Hospital das Clínicas de Ribeirão Preto: uma solução baseada em "web". Radiol Bras 2005;38:37–43.
2. Instituto Nacional de Tecnologia da Informação. [Acessado em: 12/5/2006]. Disponível em: http://iti.br/twiki/bin/view/Main/CertFaqs
3. ICP Brasil: Infra-estrutura de chaves públicas brasileira. [Acessado em: 12/5/2006]. Disponível em: http://www.icpbrasil.gov.br
4. Certificados digitais – tire suas dúvidas. BRy tecnologia. [Acessado em: 12/5/2006]. Disponível em: http://www.bry.com.br/cursos/certificados.asp
5. Resolução CFM nº 1.643/2002. [Acessado em: 12/5/2006]. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/20021643_2002.htm
6. Resolução Cremesp nº 97, de 20 de fevereiro de 2001. [Acessado em: 12/5/2006]. Disponível em: http://www.portalmedico.org.br/resolucoes/CRMSP/resolucoes/2001/97_2001.htm