O que o cirurgião-dentista precisa saber sobre certificação digital

What does the surgeon dentist need to know about digital certification

Recebido em: out/2007
Aprovado em: mai/2008

Nayene Leocádia Manzutti Eid
Mestre em Radiologia Odontológica pela Faculdade de Odontologia de Piracicaba – Unicamp

Raphael Navarro Aquilino
Professor Responsável pelas Disciplinas de Radiologia Oral e Orientação Profissional – Curso de Odontologia – Universidade Regional de Gurupi – Unirg

Cléber Bidegain Pereira
Especialista em Ortodontia pelo Conselho Regional de Odontologia do Rio Grande do Sul

Endereço do autor:
Nayene Leocádia Manzutti Eid
Av. Beira Rio, 565 - Setor União V
77413-820 - Gurupi - TO
Telefax: (63) 3312-0175
nayene_eid@yahoo.com.br

RESUMO

A necessidade de comprovar a autenticidade de documentos e atribuí-lhes um valor legal, seja através de uma assinatura de próprio punho, de um carimbo, ou de um selo de autenticação, é uma prática diária. Com o crescente avanço tecnológico e a migração dos documentos, até então em papel, para digital, faz-se necessário utilizar subsídios que permitam aos usuários de arquivos eletrônicos, efetuarem troca de informações e armazenagem de documentos com a devida segurança física e jurídica. A tecnologia da Certificação Digital e a possibilidade de assinar arquivos eletronicamente vêm transpor as relações de confiança que já existiam no universo físico para o ambiente digital. Assim, o objetivo deste artigo é esclarecer aos profissionais da área odontológica, importantes conceitos de Certificação e Assinatura Digital.

DESCRITORES: jurisprudência; legislação.

ABSTRACT

The necessity to prove the authenticity of documents and to attribute them a legal value, either through a signature of proper fist, a stamp, or an authentication stamp, is a daily practice. With the crescent technological progress and the migration of the documents until then in paper for digital one, becomes necessary to use subsidies that allow to the users of electronic files, make exchange of information and storage of documents with the due physical and juridical safety. The technology of the Digital Certification and the possibility to sign files electronically come to transpose the trust relationships that already existed in the physical universe for the digital format. Thus, the aim of this article is to explain to the dentists important concepts of Certification and Digital Signature.

DESCRIPTORS: jurisprudence; legislation.

INTRODUÇÃO

A opção pelo uso de arquivos eletrônicos e imagens digitais na odontologia vem crescendo de forma contínua e vários profissionais de todas as especialidades já têm se beneficiado das inúmeras vantagens destes em relação aos documentos em papel1.

Segundo recomendações do Conselho Federal de Odontologia, os documentos de pacientes devem ser arquivados, por questões legais, por um período de, no mínimo, 20 anos após o último registro em consultório. Os arquivos digitais, além da melhoria nos processos de aquisição, gerenciamento e arquivamento de dados, garantem agilidade na busca por fichas clínicas ou prontuários de pacientes e maior aproveitamento de espaço físico. Porém, a facilidade com que os arquivos eletrônicos e imagens digitais podiam ser manipulados e ter, em alguns casos, o conteúdo de suas informações alteradas, era motivo de preocupação para muitos profissionais[1].

Assim, o governo brasileiro, pela Medida Provisória 2200-2, publicada em 24 de agosto de 2001, instituiu a infra-estrutura de Chaves Públicas Brasileiras - ICP-Brasil, com poderes para formar no Brasil a Cadeia da Certificação Digital, criada para garantir a autenticidade, integridade e validade jurídica dos documentos eletrônicos, bem como a realização de transações eletrônicas seguras[2, 3, 4, 5]. Dessa forma, aqueles que dispõem da assinatura digital já podem efetuar troca e armazenagem de documentos e informações com a devida segurança física e jurídica. Uma vez que a tecnologia da Certificação Digital e a possibilidade de assinar arquivos eletronicamente vêm transpor as relações de confiança que já existiam no universo físico para o ambiente digital[6, 7,] o propósito deste estudo foi esclarecer aos profissionais da área odontológica importantes conceitos de Certificação e Assinatura Digital.

O QUE SÃO CERTIFICADOS DIGITAIS?

Certificados Digitais são meios eletrônicos de autenticação e verificação da identidade digital das partes envolvidas numa transação. Essa tecnologia possibilita o reconhecimento da assinatura das pessoas que trocam informações ou realizam transações digitais, com segurança, sigilo e autenticidade[7].

A Certificação Digital garante, além do sigilo e privacidade de documentos, a segurança dos mesmos, impedindo que estes sejam adulterados6.

A possibilidade de manter os registros de pacientes somente em meio digital tem trazido repercussões na classe odontológica, que tenta abster-se da obrigação de manter os registros sob suporte em papel, meio atualmente predominante na armazenagem de informações clínicas de pacientes, e passar a usufruir as inúmeras vantagens de manter os documentos em formato digital, uma vez que estes facilitam o acesso, busca e manipulação de informações, além do fácil compartilhamento e armazenagem otimizada.

Através da tecnologia implementada pelo Instituto de Tecnologia da Informação - ITI, dispomos das garantias básicas necessárias à legalização dos documentos digitais; tornando possível a utilização de qualquer documento digital, em qualquer formato de arquivo, de forma segura e confiável[8].

De forma prática podemos exemplificar a utilização dos certificados digitais e sua aplicação nas documentações odontológicas. Após a aquisição das imagens radiográficas e fotográficas digitais, o profissional pode assinar estes arquivos protegendo-os de possíveis manipulações, dando valor jurídico aos mesmos e resguardando sua atuação frente ao caso clínico em questão. Da mesma forma, o profissional pode realizar a assinatura de um receituário, atestado ou plano de tratamento, armazenando seus registros de forma otimizada, sem necessitar de amplo espaço físico e facilitando o acesso às informações.

Na troca de informações com outros profissionais, o radiologista, ou mesmo, um cirurgião-dentista que utiliza certificados digitais, pode ter a certeza de que a informação mantém-se segura e íntegra durante o trajeto remetente – destinatário, garantindo o sigilo clínico. Em contrapartida, o profissional que recebe a informação, ao devolver seus comentários assinados digitalmente, assegura sua autoria, criando uma cadeia segura de troca de informações em meio digital5. O profissional pode ainda utilizar os serviços de um cartório de notas e digitalizar seus documentos antigos armazenados em papel, prontuários, imagens clínicas, receituários, planos de tratamento, entre outros, sem perder a integridade das informações originais. Os documentos digitais deverão ser autenticados pelo cartório de notas e assim, com os arquivos digitais assinados, os documentos em papel poderão ser eliminados[9].

TIPOS DE CERTIFICADOS DIGITAIS

São oito os tipos de certificados digitais para usuários finais da ICP-Brasil, sendo quatro relacionados com assinatura digital (A1, A2, A3, A4) e quatro com sigilo (S1, S2, S3, S4) [10].

A seqüência de números de 1 a 4, indicada acima, define escalas de requisitos de segurança, nas quais certificados dos tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos[10].

Certificados relacionados à assinatura (A1, A2, A3 e A4) são utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Certificados relacionados ao sigilo (S1, S2, S3 e S4) são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo. Certificados de quaisquer dos tipos relacionados acima podem, conforme a necessidade, ser emitidos para pessoas físicas (e-CPF) ou pessoas jurídicas (e-CNPJ) [10,11].

Em fóruns realizados pelo Conselho Regional de Odontologia dos Estados do Rio Grande do Sul, Goiás e São Paulo, em março e novembro de 2003 e março de 2004, respectivamente, foi recomendado aos cirurgiões-dentistas, que utilizam arquivos digitais, que passem a assinar seus documentos com Certificado Digital tipo A3 padrão ICP-Brasil[3].

A INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA (ICP-BRASIL)

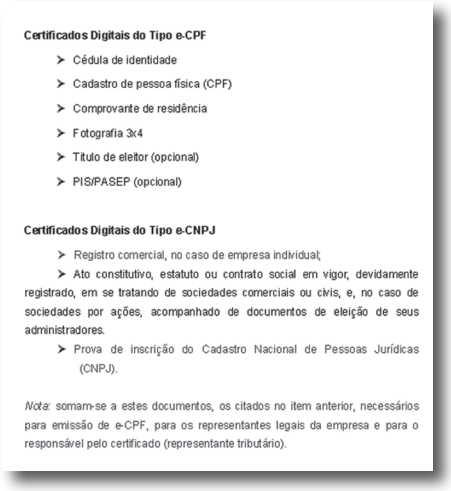
O ITI, autarquia federal vinculada à Casa Civil da Presidência da República, atua como Autoridade Certificadora Raiz (AC-Raiz). É a primeira autoridade na Cadeia de Certificação Digital e tem por função fiscalizar e auditar continuamente as demais Autoridades

Certificadoras (AC's) e prestadores de serviços habilitados na ICP-Brasil. AC-Raiz não emite certificados digitais diretamente para o usuário final. Quem faz isso são as Autoridades Certificadoras[6]. Às AC's compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários a lista de certificados revogados. As Autoridades Certificadoras podem ser instituições públicas ou organismos privados. Como exemplos de Autoridades Certificadoras de primeiro nível são exemplos a Certisign, a Secretaria da Receita Federal - SRF (que credencia outras autoridades certificadoras para emitir certificados em seu nome), a Presidência da República (que só emite certificados para uso próprio), a SERASA, o SERPRO e a Caixa Econômica Federal[7].

As entidades de nível subseqüente às AC's são chamadas Autoridades de Registro (AR's). Estas são operacionalmente vinculadas à determinada AC e a elas compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC's e manter registro de suas operações. Como exemplo de AR's poderíamos citar a AR SERPRO e AR ANOREG (Associação dos Notários e Registradores do Brasil). As duas são subordinadas à AC SERPRO e algumas instituições financeiras subordinadas à SRF.

COMO ADQUIRIR UM CERTIFICADO DIGITAL?

A emissão de certificados para pessoa física ou jurídica é obrigatoriamente presencial. Ninguém pode emitir um certificado digital em nome de outra pessoa. Assim, o interessado primeiramente deve acessar na internet a página de uma Autoridade Certificadora (AC) de sua escolha (Certisign, SERPRO, SERASA ou Caixa Econômica Federal) e escolher o tipo de certificado e mídia armazenadora de sua preferência. Neste momento, ele cadastra uma senha de identificação para compra e escolhe a forma de pagamento que lhe for conveniente. O solicitante deverá efetuar o pagamento do seu certificado e então apresentar-se se à AC. Esta confirma a sua identidade, recebendo e armazenando os documentos comprobatórios de identificação dos titulares dos certificados emitidos (Figura 1)[5]. O interessado preenche e assina um termo de adesão e responsabilidade do certificado em duas vias, sendo que uma delas ficará com o titular do certificado e a outra com a Autoridade Certificadora.



Certificados Digitais do Tipo e-CPF

- Cédula de identidade
- Cadastro de pessoa física (CPF)
- Comprovante de residência
- Fotografia 3x4
- Título de eleitor (opcional)
- PIS/PASEP (opcional)

Certificados Digitais do Tipo e-CNPJ

- Registro comercial, no caso de empresa individual;
- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.
- Prova de inscrição do Cadastro Nacional de Pessoas Jurídicas (CNPJ).

Nota: somam-se a estes documentos, os citados no item anterior, necessários para emissão de e-CPF, para os representantes legais da empresa e para o responsável pelo certificado (representante tributário).

FIGURA 1
Documentos necessários para a emissão de Certificados Digitais[5]

Após o cadastro do solicitante, será gerado um par de chaves criptográficas que será armazenado em mídias eletrônicas convencionais, ou ainda, em token ou smart card (Figura 2), dependendo do tipo de certificado solicitado, protegido com uma senha pessoal. O token é um hardware criptográfico, com dimensões semelhantes a de uma chave doméstica e com dispositivo para ser acoplado na porta USB, presente na maioria dos computadores fabricados atualmente. O smart card e um cartão criptográfico, com as mesmas dimensões de um cartão de crédito bancário, por necessitar de uma leitora de cartões, e porque nem todo computador possui essa peça, seu uso é mais restrito[12].

Uma vez geradas e armazenadas no dispositivo escolhido, as chaves criptográficas estão totalmente protegidas, não sendo possível exportá-la para outra mídia, nem retirá-las da mídia em que estão; assim, não são expostas ao risco de roubo ou violação[12].

FIGURA 2
- Dispositivos de armazenamento dos Certificados Digitais Token (A) e Smart Card (B).

VALIDADE DOS CERTIFICADOS DIGITAIS

O certificado digital é considerado válido a partir do momento de sua emissão. Com ele, o indivíduo poderá assinar todos os documentos emitidos na forma eletrônica. Através de um software para assinatura de documentos (alguns disponíveis gratuitamente na internet – X Sign, por exemplo) poderá selecionar qualquer arquivo, não importando seu formato (texto, imagem ou vídeo) e inserir sua assinatura (Figura 3). A partir do momento em que um arquivo eletrônico estiver assinado digitalmente, não poderá ser alterado, de forma que se isso ocorrer será indicado que houve violação de seu conteúdo após a assinatura. Assim, um documento eletrônico assinado tem a garantia de integridade (pois a informação não pode ser modificada), de não repúdio (a origem não pode ser negada) além da garantia da autenticação (pois identifica a pessoa de quem a informação procedeu) [13].

Diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, o certificado digital possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. É possível, no entanto, conferir as

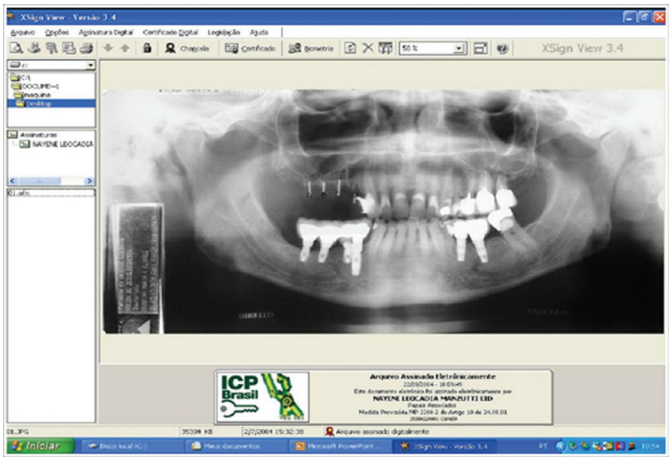


FIGURA 3
Arquivo eletrônico assinado digitalmente.

assinaturas realizadas mesmo após o certificado expirar[14].

O certificado digital pode ser revogado antes do período definido para expirar. As solicitações de revogação devem ser encaminhadas à AC que emitiu o certificado ou para quem foi designada essa tarefa. A AC, ao receber e analisar o pedido, adiciona o número de série do certificado a um documento assinado chamado Lista de Certificados Revogados (LCR) e a publica. Essas listas são públicas e podem ser consultadas a qualquer momento para verificar se um certificado permanece válido ou não. Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado. Mas, como obter essa informação? Existem meios para atribuir a indicação de tempo a um documento chamadas carimbo de tempo. Estes carimbos adicionam uma data e hora à assinatura, permitindo determinar quando o documento foi assinado[14].

O usuário pode solicitar a renovação do certificado para a AC após a perda de validade deste. Mas, por que não emitir os certificados sem data final de validade? Porque a cada renovação da validade do certificado renova-se também a relação de confiança entre seu titular e a AC. Essa renovação pode ser necessária para a substituição das chaves criptográficas por outras tecnologicamente mais avançadas ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo reforçar a segurança em relação às técnicas de certificação e às informações contidas no certificado[14].

AUTENTICAÇÃO DE DOCUMENTOS COM CERTIFICADOS DIGITAIS FORA DO PADRÃO ICP- BRASIL

A MP 2200-2 reconhece que entidades não vinculadas à ICP-Brasil podem emitir certificados, porém estes só terão validade quando reconhecidos pelas partes e, nessa condição, em caso de litígio, se não houver acordo prévio entre as partes, a validade dessa assinatura digital poderá ser contestada. Já no caso de arquivos assinados com Certificados Digitais padrão ICP-Brasil, os documentos eletrônicos gozarão de veracidade incontestável fundamentada da legislação atual (MP – 2200-2 24/08/01 Art. 10 § 1°)[10, 15].

CONSIDERAÇÕES FINAIS

Não existe uma previsão para que a cultura papel entre em desuso, porém, sabe-se que os arquivos no formato eletrônico são amplamente utilizados. Desta forma, o uso de assinaturas e certificados digitais é extremamente importante, principalmente por assegurar a autenticidade, integridade e validade jurídica dos arquivos eletrônicos. Logo, o uso de certificados digitais pode chegar a ser imprescindível. Há muito ainda a ser discutido sobre o assunto, mas entre as divergências existentes, é unânime a importância dessa tecnologia para a era da informação eletrônica na qual adentramos.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Pereira CB. Confiabilidade dos documentos digitais. Jornal do Site. 2003; 5 (68). [acesso 2006 Nov 7]. Disponível em http://www.jornaldosite.com.br/arquivo/anteriores/bidegain/artbidegain67.htm
2. Brasil. Medida Provisória n° 2.200-2. Presidência da República, Casa Civil, Subchefia para assuntos jurídicos. Brasília, 24 ago. 2001. [acesso 2006 Sep 6]. Disponível em: http://www.planato.gov.br/civil_03/MPV/2200-2.htm.
3 Pereira CB, Eid NLM. Validação Jurídica dos Documentos Digitais. Jornal da ABRO 2004; 14: 5.
4. Blum RMSO. A certificação digital e o direito. [acesso 2006 Jun 8]. Disponível em: http://www.opiceblum.com.br/artigos/09.htm.
5. Garbin CAS, Góis BC, Eid NLM, Aquilino RN, Garbin AJI, Haiter-Neto F. Aspectos legais dos arquivos digitais: Já podemos utilizar documentos digitais amparados juridicamente? Revista da Associação Brasileira de Radiologia Odontológica. 2005; 6 (2): 5-10.
6. Pereira CB, Eid NLM. Validação Jurídica dos Documentos Digitais. Jornal Ortodontia 2004; 75: 04.
7. Eid NLM. Certificação Digital na Odontologia. Jornal Ortodontia 2004; 76: 05.
8. Portugal JH. Saiba mais: Sigilo e privacidade. Transcrito da Revista Tema, Brasília, jun. 2003 – SEPRO. [acesso 2005 Sep 3]. Disponível em: http://www.cleber.com.br/certifi4.html
9. Lemos A. Entenda melhor os arquivos eletrônicos autenticados. [acesso 2005 Aug 18]. Disponível em: http://www.webodonto.com/html/artigo06.htm
10. Certisign Ltda. "O que é um certificado digital?" [acesso 2006 Mar 7]. Disponível em: http://www.certisign.com.br
11. Serpro. Chaves eletrônicas, transações seguras. Rev. Tema. Ed. 165, Janeiro 2003.
12. Certisign Ltda. "Identidade digital". [acesso 2006 Jul 7]. Disponível em: http://www.certisign.com.br/produtos/id/identidade_digital.jsp
13. Pereira CB. Confiabilidade dos documentos digitais. Jornal do Site. 2003; 5 (68). [acesso 2006 Nov 7]. Disponível em http://www.jornaldosite.com.br/arquivo/anteriores/bidegain/artbidegain67.htm
14. Alecrim E. Infowester. 2005. [acesso 2007 May 22]. Disponível em: http://www.infowester.com/assincertdigital.php
15. Pereira CB. Arquivos digitais autenticados são legais. 2003. [acesso 2006 Jan 18]. Disponível em: http://www.craneum.com.br/artigos/cleber/arquivos_digitais_legais.htm