

Arquivos digitais na Odontologia

DIGITAL ARCHIVES IN THE DENTISTRY

- Milton Gonçalves Soares
Aluno de Mestrado do Programa em Biopatologia Bucal, Área Radiologia Odontológica da FOSJC/Unesp.
- Mari Eli Leonelli de Moraes
Professor Doutor de Radiologia da FOSJC – Unesp/SP.
- Luis Cezar de Moraes
Professor Titular de Radiologia da FOSJC – Unesp/SP.
- Edmundo Medici Filho
Professor Titular de Radiologia da FOSJC – Unesp/SP.
- Julio Cezar de Melo Castilho
Professor Doutor de Radiologia da FOSJC – Unesp/SP.
- Wilton Mitsunari Takeshita
Aluno de Doutorado do Programa em Biopatologia Bucal, Área Radiologia Odontológica da FOSJC – Unesp.

RESUMO: Com o advento da informática, a Odontologia está se desenvolvendo e se modernizando. É nosso propósito, por meio de uma revisão de literatura, apresentar, de uma maneira didática, algumas orientações para se fazer à certificação digital de documentos odontológicos em forma eletrônica. Este sistema oferece segurança, praticidade e rapidez das informações, além de garantir a integridade e a validade dos documentos. Para tanto, o governo brasileiro dispõe sobre documentos produzidos e arquivados em meios eletrônicos e dá outras providências pela Medida Provisória 2200-2, de 24 de agosto de 2001, que dá amparo a ICP-Brasil, Infra-Estrutura de Chaves Públicas brasileira, com poderes para formular no Brasil a cadeia de certificação digital.

DESCRIPTORIOS: Radiografia, Certificação digital, Arquivo de imagem radiológica.

ABSTRACT: The advent of computer science, the Dentistry is developing and is modernizing. It is our intention, through a literature revision, to present, in a didactic way, some orientation to become to the digital dentistry document certification in electronic form. This system offers security, practicality and rapidity of the information, besides guaranteeing the integrity and validity of documents. For in such a way the Brazilian government it makes use on documents produced and filed in half electronic and gives other steps for Provisory Remedy 2200-2, of 24 of August of 2001, that it gives to support ICP-Brazil, Infrastructure of public keys Brazilian, with being able to formulate in Brazil the chain of digital certification.

DESCRIPTORS: Radiography, Digital certification, Radiology information systems.

INTRODUÇÃO

Assim como em outras áreas, o avanço tecnológico e científico na Odontologia tem tido um crescimento expressivo. Dentre os avanços tecnológicos, citamos o advento dos computadores, que permitiu guardar documentos em forma eletrônica: os arquivos digitais; uma tendência em todas as áreas, trazendo muitos benefícios no campo profissional¹⁰. Os arquivos digitais oferecem praticidade, rapidez das informações, permite atualização rápida de dados, além de otimizar o aproveitamento do espaço físico^{1-2,4}.

O certificado digital contém as seguintes informações: a chave pública, o nome do emissor, endereço eletrônico, validade da chave pública, a Autoridade Certificadora que emitiu o certificado digital, o número

de série do certificado e assinatura digital da Autoridade Certificadora^{3,7,14-15,18}.

Com a certificação digital de arquivos eletrônicos, os documentos em papel podem ser eliminados e guardados em CD (Compact Disk), eliminando, portanto pilhas de arquivos. Contudo, a certificação digital de arquivos eletrônicos apresenta muita resistência por parte de alguns cirurgiões-dentistas que desconhecem o novo sistema, principalmente com relação à validade jurídica em caso de processos. Porém, o governo brasileiro dispõe sobre documentos produzidos e arquivados em meios eletrônicos e dá outras providências pela Medida Provisória 2200-2, de 24 de agosto de 2001, que dá amparo a ICP-Brasil, destinada a garantir a autenticidade, a integridade e a validade jurídica de do-

cumentos em forma eletrônica e sua utilização como meio de prova processual. Em vista disso, é propósito do presente trabalho servir como um meio de orientar os cirurgiões-dentistas para obtenção de arquivos eletrônicos com certificado digital.

Obtenha os seus arquivos eletrônicos com certificação digital

Primeiramente, para se fazer uso da certificação digital é necessário que o computador esteja adaptado com programas específicos e terminais para conexão com este sistema. Os computadores utilizados para certificação devem apresentar entrada USB para uso do *token*. O *token* é um hardware criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais.

Uma vez geradas essas chaves, elas estarão totalmente protegidas, não sendo possível exportá-las para uma outra mídia nem retirá-las do *token* e não serão expostas a risco de roubo ou violação. Sua instalação e utilização é muito simples e pode ser conectado a qualquer computador através de uma entrada USB. A maioria dos computadores fabricados atualmente permite este mecanismo. Existe outro meio: o *smart card*, um cartão criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Mesmo que o computador seja atacado por um vírus ou até mesmo um

hacker, essas chaves estarão seguras e protegidas. Os múltiplos níveis de proteção que compõem a solução, incluindo recursos físicos e lógicos, asseguram a identificação do assinante, permitirão que a integridade e o sigilo das informações sejam protegidos e impossibilitarão o repúdio do documento em momento posterior⁶. Entretanto, para o *smart card* é necessário outra peça acoplada ao computador: o leitor de cartão, que torna o seu uso mais restrito, pois nem todos computadores possuem este leitor.

A emissão de certificado digital envolve as seguintes autoridades: 1. Autoridade Certificadora Raiz, (AC-Raiz) é a primeira autoridade certificadora da cadeia de certificação. Ela emite, distribui, revoga e gerencia os certificados das Autoridades Certificadoras, geren-

cia lista de certificados emitidos, revogados e vencidos, e executa atividade de fiscalização e auditoria das AC e AR; 2. Autoridade Certificadora (AC) são entidades credenciadas a emitir certificados digitais, vinculando pares de chaves criptográficas ao titular. É de sua competência, emitir, expedir, distribuir, revogar e gerenciar os certificados; 3. Autoridade de Registro (AR) são entidades operacionalmente vinculadas a uma determinada AC. Sua função é identificar e cadastrar usuários na presença deste, para depois encaminhar solicitações de certificados às Autoridades Certificadoras e manter registro de suas operações. Algumas entidades estão credenciadas, pela ICP-brasil, como Autoridades Certificadoras (AC): Serpro¹³ - Atende o mercado governamental e tem parceria com a Associação de

Notários e Registradores do Brasil; Anoreg-B e Serasa - Atuam no mercado financeiro; Certisign⁶ e Unicert¹⁶ - Atuam no mercado privado e público em geral.

Para aquisição de certificado digital é necessário, em primeiro lugar, entrar em uma página na Internet de alguma Autoridade Certificadora reconhecida pela ICP-brasil. Para isto têm-se a Certisign⁶, Serpro¹³ e Unicert¹⁶; enviar seus dados pessoais e um par de chaves criptográficas. Um par de chaves é formado por uma chave pública e uma privativa. Estas são utilizadas como as chaves de uma fechadura, sendo uma para proteger a fecha-

dura e outra para abri-la. Quando você tem um par de chaves, seu aplicativo de software utiliza uma chave para criptografar o documento¹⁸. Este, ao ser recebido, só poderá ser lido com o auxílio de uma chave correspondente, que irá decriptografar a mensagem⁶. É necessário também que se tenham senhas que farão a identificação do usuário; em seguida faz-se um contrato de prestação de serviço de certificação digital de pessoa física ou jurídica, junto a uma Autoridade de Registro (AR) - entidades operacionalmente vinculadas a uma determinada autoridade certificadora (AC), que têm como função identificar e cadastrar usuários na presença destes, para depois encaminhar solicitações de certificados às autoridades certificadoras e manter o registro de suas operações. É exigida a pre-

Os computadores utilizados para certificação devem apresentar entrada USB para uso do token.

O token é um hardware criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas essas chaves, elas estarão totalmente protegidas, não sendo possível exportá-las para uma outra mídia nem retirá-las do token e não serão expostas a risco de roubo ou violação.

sença física do interessado com os documentos de identificação e cópias dos mesmos: cédula de identidade, Cadastro de Pessoa Física (CPF), comprovante de residência, título de eleitor. Após o cadastro, será gerado um par de chaves criptográficas que serão inseridas em um *token* ou *smart card*. O interessado escolhe o tipo de certificado, preenche e assina o termo de adesão e responsabilidade do certificado em duas vias; uma fica com o titular do certificado e a outra com a Autoridade de Registro (AR). Os tipos de certificados são: A1, A2, A3 e A4, usados em aplicações como: confirmação de identidade na web, correio eletrônico, transações eletrônicas, redes privadas virtuais, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Na Odontologia, utiliza-se o tipo A3 que é normatizado e regulamentado pela ICP-brasil. Representado pelo *smart card* ou *tokens*, dispositivo portátil que atua como mídia armazenadora, que se liga a uma das portas dos computadores pessoais. O *smart card* é um cartão plástico do tamanho de um cartão de banco ou de crédito. Com microchip embutido que armazena, processa e troca informações. Em seus chips podem ser armazenadas as chaves criptografadas, sistema cifrado que consiste numa mistura de dados indecifráveis, onde é necessário o uso de chave privada para cifração e decifração de informações. Esta chave decorre de equações matemáticas aplicadas a partir do conteúdo do arquivo, podendo também derivar de sua associação a outros dados digitalizados.

De acordo com o padrão Serpro, uma das autoridades certificadoras, a emissão segue os seguintes passos: o responsável pela (AR) verifica o completo e correto preenchimento da solicitação do certificado, aprova a solicitação, disponibilizando o certificado para a instalação por seu solicitante. O software da AC emite automaticamente uma notificação ao solicitante informando que o certificado está disponível para busca.

O certificado é considerado válido a partir do momento de sua emissão. Portanto, o usuário poderá fazer a sua assinatura digital nos documentos arquivados em forma eletrônica. Bastando para isto, abrir seu arquivo e inserir o *token* ou o *smart card* no computador para que a certificação digital seja feita. Portanto, o próprio usuário poderá certificar seus documentos em forma eletrônica. Entretanto, certificar um documento manipulado é crime, colocando em jogo a ética profissional, pois a idoneidade do cirurgião-dentista será colocada à prova a partir do momento em que se questiona a autenticidade do documento digital, podendo o cirurgião-dentista passar por um processo judicial¹⁵.

Quando for necessário fazer certificação de documentos digitalizados, por exemplo, um prontuário, podemos digitalizar este prontuário e guardá-lo em arquivo digital, confiar o original ao paciente e pedir a ele que assine um documento, com todos os dados contidos no prontuário, comprovando a transferência⁵. Portanto, é necessário levar os documentos originais a uma autoridade certificadora, que os digitaliza e os transforma em documentos e certificados digitalmente com a certificação do responsável pelos documentos, pelo responsável pela digitalização e pelo tabelião de notas para dar fé pública de que o documento agora é digital correspondente ao original. Em caso de grandes quantidades de documentos, a autoridade certificadora vai até ao cliente e faz todo o procedimento no local desejado.

- Os arquivos digitais oriundos de digitalização deverão ser controlados pelo Gerenciamento Eletrônico de Documentos (é o processo de converter documentos em suporte de papel em eletrônicos e o seu gerenciamento por meio de um software específico). Este sistema deve apresentar as seguintes características: mecanismo próprio de captura de imagem em preto e branco e colorida, independente do equipamento scanner.
- Base de dados própria do armazenamento dos arquivos digitalizados.
- Método de indexação que permita criar um arquivamento organizado, possibilitando a pesquisa futura de maneira simples e eficiente.
- Mecanismo de pesquisa utilizando informações sobre os documentos, incluindo os campos de indexação e o texto contido nos documentos digitalizados, para encontrar imagens armazenadas na base de dados e mecanismo de controle de acesso que garanta o acesso a documentos digitalizados somente por pessoas autorizadas¹¹.

DISCUSSÃO

A certificação digital de documentos em forma eletrônica já é uma realidade e tem sido utilizada por vários segmentos profissionais, inclusive a Odontologia. Levando-se esse fato em consideração e lembrando-se dos inúmeros benefícios já oferecidos pela informática, temos que aproveitar estes benefícios e otimizar os métodos de trabalho na Odontologia⁷⁻⁸. Uma das áreas mais beneficiadas é a Radiologia odontológica, pois pode-se guardar arquivos inteiros de radiografias em CD (Compact Disk)⁹.

Com a certificação digital, podemos garantir a autenticidade, a integridade, a confidencialidade e o não

repúdio de um documento em forma eletrônica, principalmente as radiografias Odontológicas, pois a mesma pode ser usada por diferentes profissionais e se manipulada será detectada a violação^{10,12,17,19}. Caso ocorra manipulação do documento com a certificação digital a fraude será flagrada, pois o documento se torna imutável. Sendo assim, o sistema de certificação digital se torna plenamente seguro e confiável.

Na Odontologia, o modelo brasileiro de certificação digital de documentos eletrônicos também é amparado pela ICP-Brasil. Somente certificações vinculadas a ICP-Brasil apresentam condições adequadas de confiabilidade técnica de gestão e operação, garantindo autenticidade derivada da lei. Documentos com certificação digital feita por entidades certificadoras não vinculadas mantêm validade relativa.

O sistema de certificação digital, implantado pela ICP-Brasil, garante segurança para todos os integrantes do sistema, mas os usuários devem se precaver, pois o usuário tem responsabilidades sobre o seu Hardware, cartão inteligente (*smart card*) ou *token*. Ambos têm o mesmo valor jurídico, porém o *token* poderá ser levado para qualquer lugar, pois hoje em dia, qualquer computador pessoal tem entrada para este dispositivo. O *smart card* não apresenta esta facilidade; necessita de um leitor de cartão acoplado ao computador. Estes dispositi-

vos são protegidos por senhas. Os usuários também são responsáveis pelo gerenciamento de sua senha. Quando o usuário escolher sua senha, ela deve ser memorizada, não deve ser divulgada. Evitar usá-la quando alguém estiver por perto. Se for necessário anote em agenda pessoal de forma invertida e troque-a quando suspeitar que ficou comprometida. Estas dicas são fundamentais para que o usuário do sistema não tenha problemas futuros com violação de seus arquivos.

Acreditamos que os conselhos de classe possam nos oferecer um serviço de suporte, servindo como intermediário entre os profissionais e as Autoridades Certificadoras. Desta maneira poderíamos fazer um cadastro de certificação digital no próprio conselho e este encaminharia para uma Autoridade Certificadora, permitindo melhor uso do tempo e também participando de uma nova sociedade, a "Sociedade da Informação".

CONCLUSÃO

Com base na revisão de literatura, concluímos que: os documentos em forma eletrônica podem ser usados como prova em processos judiciais, desde que estes estejam com certificados digitais vinculados a ICP-Brasil, pois este garante a autenticidade, integridade e a validade jurídica de documentos digitais.

REFERÊNCIAS

1. Araujo AC. Os efeitos da certificação digital, como a sociedade pode se beneficiar da regulamentação eletrônica. Rev. E-commerce 2001;2(18):98.
2. Boscolo FN, Almeida SM, Haiter Neto F, Oliveira AE, Tuji FM. Fraudulent use of radiographic images. J Forensic Odontostomatol 2002;20(2):25-30.
3. Boss J. Digital signature and the electronic health records: Providing legal and security guarantees. Int J Bio-med Comp 1996;42:157-63.
4. Calvielli ITP, Modaffore PM. A validade dos arquivos digitais como meio de prova processual. Rev Assoc Paul Cir Dent 2003; 57(1):63-5.
5. Carvalho GP. Prontuários clínicos digitais em Odontologia. Disponível em: www.ibemol.com.br/forense2000/094.asp. Acesso em julho de 2005.
6. Certisign. Acesso em Outubro de 2004. Disponível em: http://www.certisign.com.br/produtos/ecpf/e_cpf_precos.jsp#
7. Ciocler J, Melani RH. Documentação odontológica informatizada: aspectos legais do uso. RPG Rev Pos Grad 1999;6(3):290.
8. Horner K, Brettle DS, Rushton VE. The potential medical-legal implications of computed radiography. Br Dent J 1996;180(7):271-3.
9. Jones GA, Behrents RG, Bailey GP. Legal considerations for digitized images. Gen Dent 1996;2:242-4.
10. Jones M, Roth T, Nair S, Lehmann J. Is going digital legal? A discussion of the legal issues concerning the implementation of PACS in place of conventional radiological film for patient diagnosis. Adm Radiol 1994;13(11):46-53.
11. Pereira CB. Entenda a validação jurídica dos arquivos eletrônicos – Arquivos digitais – legalidade. Disponível em: <http://www.cleber.com.br>. Acesso em 3 set. 2004.
12. Richardson ML, Frank MS, Stern EJ. Digital image manipulation: constitutes acceptable alteration of a radiologic image. AJR Am J Roentgenol 1995;164(2):479-83.
13. Serpro. Acessado em Outubro de 2004. Disponível em: <http://www.serpro.gov.br/>
14. Smith JP. Authentication of digital medical images with digital signature technology. Radiology 1995;194:771-4.
15. Soares MG, Takeshita WM, Moraes LC, Medici-Filho E, Castilho JCM. Verdades e Mentiras sobre a legalidade da radiografia digital na Odontologia. RBO Rev Bras Odont 2004;61(1):22-4.
16. Unicert. Acessado em Outubro de 2004. Disponível em: <http://www.unicert.com.br/>
17. Visser H, Kruger W. Can dentists recognize manipulated digital radiographs? Dentomaxillofac Radiol, 1997;26(1):67-9.
18. Wang HA, Wang YZ, Wang S. Digital signature technology for health care applications. South Med J 2001;94(3):281-6.
19. Wenzel A. Computer-aided image manipulation of intraoral radiographs to enhance diagnosis in dental practice. Int Dent J 1993;43(2):99-108.