O QUE O CIRURGIÃO-DENTISTA PRECISA SABER SOBRE CERTIFICADO DIGITAL

Resumo

A necessidade de comprovar a autenticidade de documentos e atribuir-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 arquivo 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 Certificados e Assinaturas Digital.

DESCRITORES: jurisprudência: legislação.

INTRODUÇÃO

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

Segundo recomendações do Conselho Federal de Odontologia documentos de pacientes devem ser arquivados, por questões tais, por um período de, no mínimo, 20 anos após o último retro em consultório. Os arquivos digitais, além da melhoria no sucessos de aquisição, gerenciado e arquivamentos de dados, matem agilidade na busca por fichas clinicas ou prontuários pacientes e maior aproveitamento de espaço físico. Porém, a agilidade com que os arquivo eletrônicos e imagens digitais podem ser manipulados e ter, em alguns casos, o conteúdo de suas formações alteradas,era motivo de preocupação muitos profissionais!

Assim, o governo brasileiro, pela medida provisória 2200-2 aplicada em 24 de agosto de 2001, instituiu a infra – estrutura Chaves Públicas Brasileiras – ICP –Brasil, com poderes para mar no Brasil a Cadeia de Certificação Digital, criada para garantir autenticidade, integridade e validade jurídica dos documentos eletrônicos, bem como a realização de transações eletrônicas. Dessa forma, aqueles que dispõem da assinatura digital já podem efetuar troca e armazenagem de documentos e formações 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 queexistiam no universo físico para o ambiente digital 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 modificação 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.

A certificação digital garante, além do sigilo e privacidade de documentos, a segurança dos mesmos, impedindo que sejam adulterados.

A possibilidade de manter os registros de pacientes somente por meio digital tem trazido repercussões na classe odontológica.e tenta abster-se da obrigação de manter os registros sob suporte em papel, meio atualmente predominante na armazenagem de formações clinicas de pacientes, e passar a usufruir as inúmeras vantagens de manter os documentos em formato digital, uma vez e 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 á legalização dos documentos digitais; tornando possível a realização de qualquer documento digital. Em qualquer formato de arquivo, de forma segura e confiável.

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 d resguardando sua atuação frente ao caso clinico em questão. Da mesma forma otimizada, sem necessitar de amplo espaço físico e facilitando o acesso ás informações.

Na troca de informações com outros profissionais, o radiologista, ou mesmo, um cirurgião-dentista que utiliza certificados digitais, pode ter certeza de que a informação mantém-se segura e integra durante o trajeto remetente – destinatário, garantindo o sigilo clinico.em contrapartida, o profissional, 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 digital. O profissional pode ainda utilizar os serviços de uma cartório de notas e digitalizar seus documentos antigos armazenados em papel, prontuários, imagens clinicas, receituários, planos de tratamentos, entre outros, sem perder a integridade das informações originais. Os documentos digitais de verão se autenticados pelo cartório de notas e assim, com os arquivos digitais assinados, os documentos em papel poderão ser eliminados.

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).

A sequencia de números de 1 a 4,indicada acima, define escalas de requisitos de segurança, nas quais certificados dos tipos A1e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

Certificados relacionados á 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).

Em fóruns realizados pelo Conselho Regional de Odontologia dos estados de 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 ti A3 padrão ICP- Brasil.

A INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS

(ICO- BRASIL)

O ITI, autarquia federal vinculada á Casa Civil da residência da república, atua como autoridade Certificadora Raiz (AC- Raiz).

É a primeiraautoridade 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 certificado digitais diretamente para o usuário final. quem faz isso são as autoridades certificadoras ás AC's compete emitir, expedir, distribuir, revogar e gerenciar os certificados,bem como colocar á 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 o uso próprio), a SERASA, o SERPRO e a Caixa Econômica Federal.

As entidades de nível subsequente ás AC's são chamadas Autoridades de Registro (AR'S). Estas são operacionalmente vinculadas á determinada AC e a elas compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados ás AC's e manter registro de suas operações. Como exemplo de Ar'sporíamos citar a AR SERPRO e algumas instituições financeiras subordinadas á 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 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 tiopo de certificado e mídia armazenadora de sua preferência. Nesse 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 á AC,que confirmará a sua identidade, recebendo e armazenando os documentos comprobatórios de identificação, dos titulares dos certificados emitidos (figura1) 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.

Certificado Digital do Tipo o CPF

Cédula de identidade

Cadastro de pessoa Física (CPF)

Comprovante de residência

Fotografia 3x4

Titulo de4 eleitor (opcional)

PIS/PASEP (opcional)

Certificados Digitais do tipo o CNPJ

Registro comercial, no caso de empresa individual,

Ato constitutivo

Documentos necessários para a emissão de Certificados Digitais

Após o cadastro do solicitante, será gerado um par de chaves criptográficas que será armazenado em mídias eletrônicas convencionais, ou ainda, em token ou smartcard (figura 02), dependo 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 smartcard e um cartão criptográfico, com as mesmas dimensões de um cartão de credito bancário,po necessitar de uma leitora de cartões, e porque nem todo computador possui essa peça, seu uso é mais restrito. Uma vez geradas e armazenadas no dispositivo escolhido , as chaves criptográficas estão totalmente protegidas, não sendo possível exporta-las para outra mídia, nem retirá-las da mídia em que estão; assim, não são expostas ao risco de roubo ou violação.

VALIDADES DOS CERTIFICADOS DIGITAIS

O certificado digital é considerado válido a partir do momento de sua emissão. Com ele, o individuo 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 deu formato (texto, imagem ou vídeo)e inserir sua assinatura (figura 03). A partir do momento em que uma arquivo eletrônico estiver assinado digitalmente, não poderá ser alterado, de forma que se isso ocorrer será indicado que ouve violação de seu conteúdo após a assinatura. Assim, um documento eletrônico assinado tem 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).

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 valido. É possível, no entanto, conferir as assinaturas realizadas mesmo após o certificado expirar.

O certificado digital pode ser revogado antes do período definido antes de expirar. As solicitações de revogação devem ser encaminhadas á alguém que emitiu o certificado ou para quem foi designada essa tarefa. Ao receber e analisar o pedido, adiciona o número de série a um documento assinado chamado lista de certificado 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 validas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta revogação foi realizada durante o período de validade do certificado. Como obter essa informação? Existem os meios para atribuir a revogação de tempo á um documento chamado carimbo de tempo. Os carimbos adicionam uma data e hora á assinatura, permitindo determinar quando o documento foi assinado.

O usuário pode solicitar a renovação do certificado para 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 ás técnicas de certificação e ás informações contidas no certificado.

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

A MP 2200-2 reconhece que entidades não vinculadas á ICP-Brasil podem emitir certificados, porem estes só terão validade quando reconhecidos pelas partes e, nessa condição, em caso de litigio, 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$1º)

Considerações finais

Não existe uma previsão para que a cultura do papel entre em desuso, porém, sabe-se que os arquivos no formato eletrônico são amplamente utilizados. Dessa forma, o uso de assinaturas e certificado digitais é extremamente 9importante, 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.