ISSN 0030-5944

Série Prata

Original desde 1967

Volume 38 • Nº 4 • Outubro | Dezembro 2005

OrtodontiaSPO

Informação e cultura para o especialista.

Trabalhos de pesquisa e estudos clínicos

Ortodontia Estética - Tratamento ortodôntico em pacientes adultos - Parte I: Estética Periodontal

Odontopediatria auxilia no diagnóstico precoce das más-oclusões

Responsabilidade Civil

SOCIEDADE PAULISTA DE ORTODONTIA E ORTOPEDIA FUNCIONAL DOS MAXILARES

46 anos

Certificação digital - Segurança da informação na internet

MOACYR MENÉNDEZ
Cirurgião-Dentista, mestre e doutor em Prótese Dental e ex-professor titular da Disciplina de Informática Odontológica do curso de Odontologia da Universidade de Guarulhos.

O domínio da informação é, sem dúvida, um dos maiores bens que o ser humano pode desejar nos dia de hoje. Pessoas bem-sucedidas são pessoas sempre bem informadas.

A informação transita hoje com a melhoria das formas de comunicação e o aparecimento da Internet de forma muito rápida e ágil; podemos dizer que ela transita em "Tempo Real".

As mudanças advindas da era da comunicação nos levam ao que chamamos hoje de a "Sociedade da Informação", onde todos participam, de alguma forma, com a predominância da informação eletrônica.

A segurança ou confiabilidade das mensagens ou documentos que circulam pela via eletrônica são motivos de grande preocupação. Algumas características em particular devem ser consideradas ao falarmos em documentos eletrônicos:

- **Autenticidade**: a autoria, origem e o destino do documento eletrônico devem ser sempre preservados.
- **Disponibilidade**: o documento ou informação deve estar sempre disponível para consulta ou atualização.
- **Integridade**: documento sempre fiel ao seu conteúdo original, sem sofrer qualquer tipo de alteração.
- **Confidencialidade**: a informação relacionada a um indivíduo, empresa ou entidade deve ser protegida da ação indevida de terceiros, seja para conhecer ou tratar essa informação.
- **Irretratabilidade**: nos dá a garantia de que qualquer transação efetuada não poderá ser negada pelo autor.

A Internet segura torna possível estabelecer transações e comunicações sem risco para as partes envolvidas, o que só é possível com a utilização de certificados digitais, ou seja, documentos eletrônicos que assinam, protegem e geram recibos digitais dessas transações e comunicações.

Quando se utiliza um certificado digital, as partes envolvidas tornam-se responsáveis (e sofrem conseqüências) por todas as comunicações ou transações de que participaram.

As soluções tecnológicas para implementarmos estas condições são várias; falaremos sobre algumas delas.

A Criptografia pode ser definida como um conjunto de métodos e técnicas utilizadas com a finalidade de proteger o conteúdo de qualquer documento eletrônico contra as alterações ou modificações não autorizadas.

Existem dois tipos de criptografia a Simétrica e a Assimétrica. Um conceito deve ser compreendido antes de falarmos da criptografia em si: o conjunto de regras que determina as transformações de um documento é chamado de "algoritmo" (uma seqüência de cálculos matemáticos) e o parâmetro que determina as condições da transformação é chamado de "chave".

As mensagens que recebemos diariamente, junto com fotos ou documentos, não possuem uma identificação incontestável juridicamente, ou seja, não recebemos mensagens assinadas digitalmente, nem muito menos criptografadas, isto não nos dá certeza de que este ou aquele documento possa ter sido alterado ou lido por outras pessoas na sua viagem através dos caminhos percorridos pela mensagem e, em alguns casos, com a negativa do suposto remetente não temos como provar a origem da mensagem. Nestes casos precisaremos de um expert ou perito para tentar localizar as provas que necessitamos.

A primeira tentativa de criptografia foram as Chaves Simétricas que é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta. Neste caso o emissor envia uma mensagem criptografada com senha pessoal, e o destinatário só poderá ler a mensagem de posse da senha secreta, que deve ser passada utilizando algum outro método confiável, preferencialmente num encontro pessoal ou por telefone. Essa técnica por si só já nos dá idéia da dificuldade de se manter em segurança a senha, que depende exclusivamente da capacidade do emissor e do destinatário em manter a senha em segredo; por esses motivos essa técnica não é muito utilizada.

A Criptografia de Chave Assimétrica baseia-se em algoritmos que utilizam duas chaves diferentes, relacionadas matematicamente através de um algoritmo, de forma que o texto cifrado pela chave 1 do par somente poderá ser decifrado pela chave 2 do mesmo par. Na Criptografia Assimétrica existem duas Chaves, uma chamada de "Chave Privada" com a qual o remetente pode assinar ou criptografar a sua mensagem e a "Chave Pública" que é de conhecimento geral e pode ser utilizada pelo destinatário para ler a mensagem. A certificação digital garante a autenticidade, integridade, confiabilidade e o não repúdio de uma mensagem.

Qualquer um de nós, seja pessoa física ou jurídica, pode fazer uso da Certificação Digital. É só o contratar uma Autoridade Certificadora, ou seja, órgãos responsáveis por emitir o documento. Hoje, no Brasil temos seis delas. Primeiramente o interessado comunica os dados ao site, é orientado a cadastrar seus dados pessoais e também um par de chaves criptográficas (dispositivos que farão a identificação do usuário e o reconhecimento da certificação). A partir daí, ele precisa ir pessoalmente à Autoridade Certificadora para registrar seus dados e levar as provas dos dados que forneceu on-line e o processo está pronto, ele recebe as chaves criptográficas e sua assinatura digital. (consulte o site da ICP Brasil - Infra-Estrutura de Chaves Públicas Brasileira - http://www.icpbrasil.gov.br/)

Algumas aplicações para o cirurgião-dentista (pessoa física) podem ser encontradas nos sites das Autoridades Certificadoras - AR. Como exemplo utilizaremos as opções da CertiSign http://www.certisign.com.br

Com o **e-Mail Seguro** Pessoal suas mensagens eletrônicas podem ser enviadas com sua assinatura digital, além de permitir o envio e a leitura de conteúdos sigilosos, utilizando a criptografia.

O **Assinador de Documentos** é uma ferramenta desenvolvida para permitir que os usuários possam assinar e verificar digitalmente seus documentos eletrônicos, em seu próprio computador. Principais características: Assinatura digital de arquivos salvos em formato Word, PowerPoint, Excel e arquivos de imagem, entre outros; Verificação de documentos assinados digitalmente; Proteção (criptografia) de documentos; Eliminação de papel.

Segundo o Conselho Federal de Odontologia não existem mais impedimentos legais para que sejam utilizados os meios eletrônicos desde que a ausência do documento em papel, do filme radiográfico ou do negativo fotográfico seja suprida necessariamente pela certificação digital que lhes confere a mesma fé pública.

O **Certificado Digital**, por si só, já é válido para dar autenticidade a um documento, mas deve-se ainda enviar via Internet uma cópia autenticada do documento a um dos Cartórios integrante do sistema ICP, para registro e autenticação, o que lhe confere fé pública.

Todas as digitalizações de fichas clínicas em papel e/ou imagens convencionais (radiografias ou fotografias) devem ser escaneadas, certificadas e registradas em cartório pelo sistema ICP-BRASIL. Estes procedimentos não eliminam as normas do conselho para os prontuários ou fichas clínicas tradicionais.

Atualmente temos conhecimento de que a Empresa Easy Dental estará lançando em 2006 o seu software odontológico, habilitado para trabalhar com certificação digital. Consulte o site www.easydental.com.br para mais informações.

O **e-CPF**, documento utilizado pelo contribuinte para relacionamento com a Secretaria de Receita Federal, agora, em formato eletrônico, dá acesso a todos os serviços oferecidos pelo Governo Federal na Internet. Com o e-CPF você pode enviar sua declaração do Imposto de Renda via Internet, consultar e atualizar seu cadastro como contribuinte pessoa física, recuperar informações sobre seu histórico de declarações e verificar sua situação na "malha fina". Além disso, você pode obter certidões da Receita Federal, cadastrar procurações e acompanhar processos tributários eletronicamente, com a conveniência de não precisar deslocar-se até um posto de atendimento.

Identidade Digital é a credencial eletrônica mais completa e segura emitida no país, permitindo que o cidadão brasileiro utilize os serviços digitais implementados pelo Governo através da Internet. Além do acesso privilegiado aos serviços governamentais, com maior comodidade e rapidez, você pode assinar documentos eletronicamente, preservar o sigilo de informações pessoais e garantir uma navegação mais segura pela Internet em um único produto de fácil utilização.

Dessa maneira, você poderá trocar mensagens de e-mail com pessoas em todo o mundo, tendo a garantia de sigilo e integridade na comunicação digital.

A Certificação digital pode ser armazenada de duas formas, dependendo do tipo de certificação digital. O A-1 e o A-3. O A-1 é aquele em que a assinatura digital e os dados do usuário são armazenados em uma mídia móvel, como um CD, por exemplo.

O A-3 representa os smart cards ou tokens, hardwares portáteis que atuam como mídias armazenadoras. Em seus chips podem ser armazenadas as chaves privadas dos usuários.

Para utilizar o Certificado Digital é muito fácil: quando o usuário entra em um site oficial o Browser que já possui funções de criptografia (Internet Explorer - Netscape) reconhece que está entrando em um site com certificação. No caso do usuário final ou portador ele pode fazer o mesmo através da assinatura digital. ■