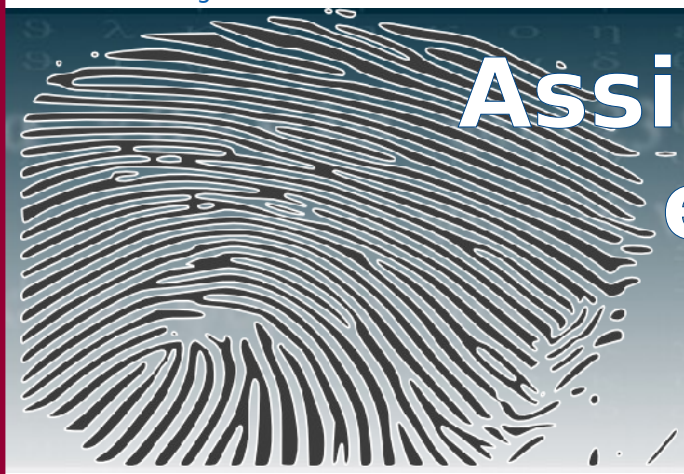
Artigo



Assinatura digital e BrOffice.org

Breve descrição e sua forma de utilização

Por: Edgard Alves Costa

Desde os primórdios dos tempos quando o homem começou a fazer negócios e guerras, a informação e sua segurança tornaram-se uma das principais preocupações. Tem-se notícias que egípcios e romanos já usavam técnicas de criptografia para manter seus documentos a salvo de seus inimigos.

Criptografia, do grego Kriptós *= escondido, oculto;* grafia *=escrita, é a técnica de se escrever em cifra ou em códigos utilizando formas para tornar um texto ilegível, de forma a permitir que apenas o destinatário consiga decodificar a mensagem e entendê-la. Basicamente foi durante a segunda guerra mundial que a criptografia chegou ao seu auge, com a invenção do computador, utilizando complexas seqüências matemáticas denominadas algoritmos, que ainda hoje, tem aplicação comercial.*

Chaves: o que são e como são usadas

Chaves constituem-se nos elementos fundamentais para cifrar e decifrar mensagens. Para o usuário comum, a chave trabalha da mesma forma que uma senha. Se a senha estiver correta, lê-se o arquivo, caso contrário o arquivo continua intacto.

Conceito de Chave Simétrica e Chaves Assimétricas

Criptografar por chaves simétricas é o conceito pelo qual tanto o emissor quanto o receptor compartilham a mesma chave, sendo guardada por ambos em completo segredo. Se por ventura aconteça algo com uma das partes, sem haver a correta divulgação, o segredo pode estar comprometido.

Chaves assimétricas, modelo usado pelo Governo Brasileiro, é constituída por pares de chaves, sendo uma chave pública e uma privada. A chave pública deverá ser amplamente divulgada.

O conceito é o seguinte: Uma vez usada a chave pública para a encriptação de um arquivo, só com a chave privada é que faz o processo contrário e vice-versa. Caso máquinas e pessoas, envolvidas no processo forem confiáveis, podemos afirmar que há um bom nível de segurança.

O conceito é o seguinte: Uma vez usada a chave pública para a encriptação de um arquivo, só com a chave privada é que faz o processo contrário e vice-versa. Caso máquinas e pessoas, envolvidas no processo forem confiáveis, podemos afirmar que há um bom nível de segurança.

Dos métodos utilizados para a obtenção de chaves assimétricas usados nos certificados digitais destaca-se o algoritmo RSA, que baseia-se na obtenção dos fatores primos de um número longo.

Há grande confusão de uso entre assinatura digital e assinatura digitalizada. Assinatura digital é uma assinatura eletrônica e a assinatura digitalizada trabalha com a captura de dados biométricos como leitura da Iris, impressão digital e assinatura manuscrita.

A assinatura digital baseia-se em:

a) chaves assimétricas;

b) o documento assinado não poderá ser alterado;

c) a assinatura não é reutilizável;

d) a assinatura não pode ser repudiada, ou seja, se a assinatura for reconhecida pelo receptor, o autor não pode negar a autenticidade da mesma.

Artigo

Certificados Digitais

Certificados digitais determinam a inclusão de dados pessoais intransferíveis a um par de chaves assimétricas, como se fosse um documento oficial, determinando validade jurídica.

A estrutura para a obtenção de um certificado digital baseia-se em uma autoridade certificadora (AC) e uma autoridade de registro (AR). Isto não nos é desconhecido. Fa-zemos uso desta estrutura todos os dias sem nos dar conta.

E quem faz o papel de AC e AR? O cartório. Só que ele faz os dois papéis ao mesmo tempo. O de autoridade de registro e de certificação.

Explicando melhor. Quando desejamos que nossa assinatura seja reconhecida em um determinado documento, vamos ao cartório com os nossos documentos pessoais e preenchemos um determinado formulário assinando-o algumas vezes, (registro). Quando fazemos uma procuração, a sua validação só acontece quando a assinatura contida no texto é reconhecida e confirmada pelo oficial do cartório (certificação). Os bancos fazem o mesmo. São autoridades de registro, quando abrimos uma conta e de certificação quando confirmam que a assinatura contida no cheque é verdadeira.

Os certificados digitais compõem-se de: Certificado Raiz, Certificado da Autoridade Certificadora e Certificado pessoal.

Especificamente, no caso brasileiro, o ICP, Infra-estrutura de Chaves Públicas, http://www.icpbrasil.gov.br/ é orgão gestor e responsável pela metodologia, práticas e fundamentos técnicos.

O ITI, Instituto Nacional de Tecnologia de Informação, http://www.iti.gov.br é a autoridade certificadora raiz.

As Autoridades Certificadoras, são empresas públicas ou privadas, que oferecem o certificado digital designados pelo ITI, sendo responsáveis pela emissão, guarda e revogação dos certificados.

Autoridades de registro, também podem ser empresas públicas ou privadas, ligadas ou não, as autoridades certificadoras e são responsáveis pelo recebimento e verificação dos documentos das pessoas que desejam seu certificado, bem como a guarda dos documentos apresentados no momento do registro.

Exemplos de autoridades certificadoras: Certisign, Serpro, Imprensa Oficial do Estado de São Paulo, Serasa, Arisp etc..

Certificados Digitais: Legislação

Por medida provisória sob o nº 2200-2 em 24 de agosto de 2001, o governo Brasileiro sob a presidência do Prof. Dr. Fernando Henrique Cardoso, institui o ICP. Nesta medida provisória, já modificada por vários decretos e resoluções, altera o ITI para que se torne uma autarquia. Desta forma, o ITI cria autonomia técnica para gerir recursos e dar formato ao Certificado Brasileiro.

Em agosto de 2002, o Ministro-Chefe da Casa Civil da Presidência da República, Ministro Pedro Parente, ingressa com o projeto de lei 7316/2002, disciplinando o uso do certificado digital.

Como este decreto ainda não foi votado nos dias atuais, há interpretações das mais diversas sobre a validade jurídica da assinatura digital, mesmo a do ICP-ITI Brasil. Porém, entre vários juristas consultados por este articulista, fica claro que, se as partes envolvidas pactuarem o uso de um determinado certificado para a assinatura de documentos trocados entre si, estes terão força de lei, desde que haja contrato firmado, assinado e registrado em cartório, confirmando o aceite da assinatura digital. Portanto, certificados emitidos pela Cacert, empresa que oferece certificados sem custos, sob a bandeira Open-Source, GPG e X-509 podem ser usados, desde que as partes envolvidas, obedeçam o que rege a lei dos contratos, como já foi citado, firmando em cartório o compromisso de uso.

Tipos de Certificados e aparelhos físico/eletrônicos usados pela ICP Brasil

Os tipos básicos de certificados oferecidos no Brasil pelas autoridades certificadoras são basicamente e_CPF e e_CNPJ do tipo: A1, A2, A3, A4, para assinatura e S1, S2, S3 e S4 para sigilo. Quanto mais alto o número mais complexo é o nível de criptografia do certificado. Existem outros tipos de certificados, como o SSL, que basicamente é para sites. Este é outro capítulo.

O certificado A1, do ICP-ITI, bem como outros certificados como o da CACert, por exemplo, tem a mesma forma de configuração e atuação depois de ter sido feito o download. É ideal para pessoas que não se movimentam muito ou usam o certificado em um notebook.

Certificados A3, normalmente são acompanhados de dispositivos físicos/eletrô-nicos como tokens e smartcards.

Quem precisa se locomover muito para várias cidades, países, deve usar o token.
O smartcard pode ser usado em vários lugares, porém é necessário leitora. O smartcard é também utilizado como meio de reconhecimento em redes, como senha. Bastante útil esta solução. Em empresas em que os funcionários podem estar em vários departamentos ou em várias sedes diferentes, o cartão serve de login automático. As imagens dos dispositivos são mostradas abaixo.

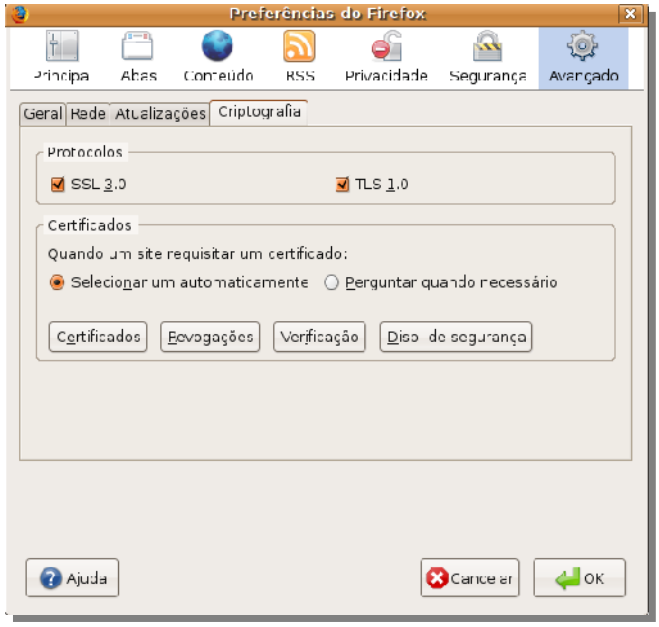
Smart Card

Token

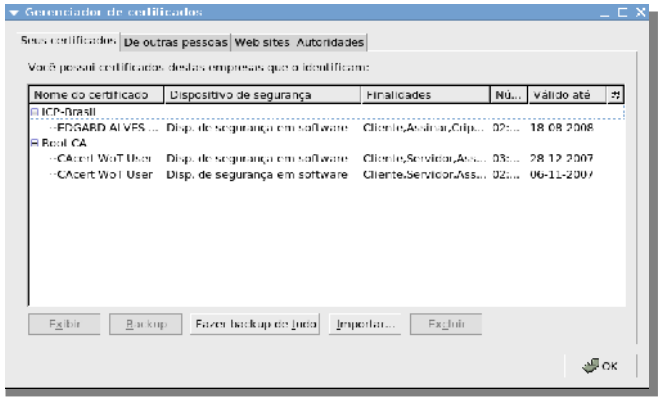
Configuração do Sistema via navega-dor para usar Certificado Digital.
Vimos anteriormente um apanhado do que são os Certificados digitais em suas várias formas. Só que não falamos nada em como instalá-los.
Como a navegação via internet é comumente feita pelos navegadores: Internet Explorer, Firefox, Mozilla, Konqueror, Epiphany entre tantos outros, a instalação e sua configuração se faz neste ambiente. Não existe mistério nenhum nisto. Não há necessidade de chamar técnico para proceder a configuração.
Vamos imaginar que você já foi à AR (Autoridade de Registro) e escolheu um certificado do tipo A1, o mais simples.
obs.-> Serve para todos os certificados

Passo 1
Baixe todos os certificados da forma que você foi orientado pela AR. Salve em disco. Normalmente é um arquivo *.pfx.

Passo 2
Abra seu navegador e procure a opção de instalação dos certificados. Mais ou menos igual a imagem a seguir.



Esta posição varia de navegador para navegador. Por questões de praticidade, vou mostrar a instalação no FireFox. Os passos não são diferentes para os outros softwares não importando o sistema operacional. Veja a imagem abaixo depois de clicado no botão certificados:



Observe que podemos ter vários certificados digitais pessoais. Podemos selecionar o que nos é apropriado no momento que desejarmos. Mas você não tem nenhum ainda.
Clique, então, em ***Importar***. Navegue até a pasta onde salvou o certificado. Pronto. Depois de senhas configuradas o seu certificado estará pronto para ser usado. Todos os certificados devem ser instalados neste ambiente. O de raiz e o pessoal. Certificados colhidos durante o trabalho, como por exemplo de emails ou de documentos, ficam armazenados neste ambiente na aba: ***de outras pessoas***.
Ao se clicar sobre um certificado para ver suas propriedades você deverá obter algo assim:

Clicando-se na aba detalhes observaremos todas as ramificações deste certificado.

Fazer Backup

Isto é importantíssimo. Você deve salvar seu certificado em pasta que não esteja em nenhum compartilhamento e também em pasta que não seja usada por nenhum outro usuário de sua máquina. Se possível deve estar salvo em pasta que permita senha para acesso e seja oculta. Para realizar esta etapa basta clicar em **Fazer Backup de tudo**. As telas de configuração são intuitivas e não precisam de nenhum comentário adicional.

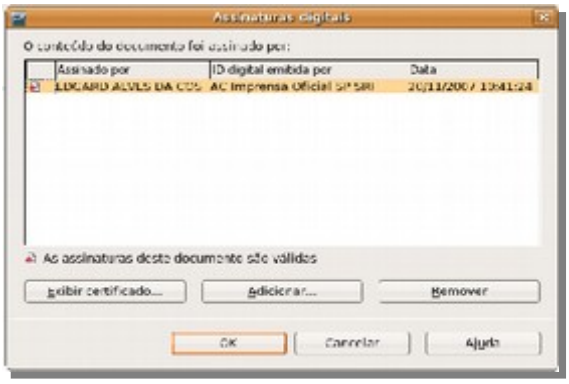
Certificados e o BrOffice.org

Suítes como BrOffice.org, OpenOffice.org permitem que os textos, planilhas e outros trabalhos, nativamente, possam ser assinados e enviados com segurança, além de ter como padrão, o Open Document Format (ODF), o que permite uma maior interoperabilidade entre várias suítes de desenvolvedores diferentes. Para exemplificar mostro abaixo como é fácil esta operação:

Texto digitado, no ***Write***, na tela de trabalho. No menu principal vá em ***Arquivo -> Assinaturas Digitais.***

Veja a figura ao lado.

Clicando-se em **Assinaturas digitais** temos na tela de trabalho os certificados salvos na máquina ou os certifi-ados físicos como smartcard ou pendrives habilitados, resultando a figura abaixo.



Selecionado o certificado o sistema mostra que o arquivo está salvo, mostrando este ícone na barra de menu inferior.

Importante frisar que se este arquivo, por acaso, tivesse co-autores, todos poderiam ter sua assinatura inserida neste documento sem prejuízo da qualidade e da validade jurídica. Qualquer modificação feita, as assinaturas imediatamente desaparecem.

Portanto, basta assinar e enviar via email.

O destinatário, como dito antes, apenas terá que ter sua assinatura salva para verificar a integridade do arquivo.

As imagens abaixo ilustram bem um documento assinado por vários autores e bem vindo ao mundo da assinatura digital.