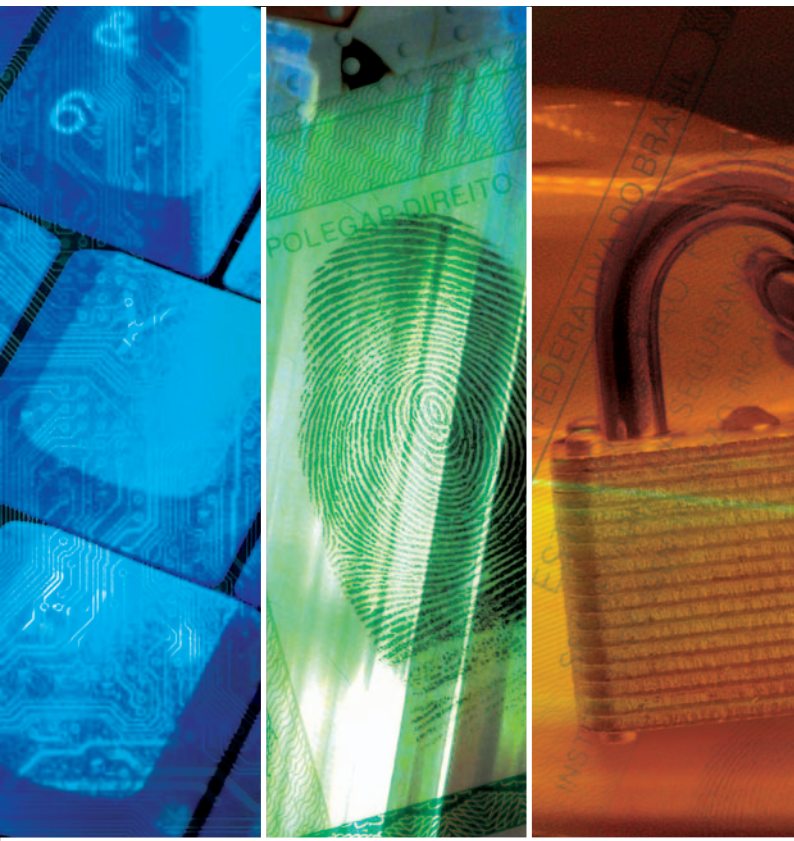
1ª Edição - Especial FENACON

CERTISIGN CERTIFICADORA
DIGITAL S A

Digitally signed by CERTISIGN CERTIFICADORA DIGITAL S A
DN: CN = CERTISIGN CERTIFICADORA DIGITAL S A, O = CertiSign Certificadora Digital S.A., OU = Autenticado por CertiSign Publico
Reason: I am the author of this document
Location: São Paulo, SP
Date: 2005.09.26 10:24:13 -03'00'

IdentidadeDigital



Torne a sua vida mais prática e segura

CERTISIGN
A Sua Identidade na Rede

FENACON

Sheila Train

1ª Edição - Especial FENACON

IdentidadeDigital

Torne a sua vida mais prática e segura

Sheila Train

Identidade Digital
Torne sua vida mais prática e segura

Dados Técnicos

Autoria:
Sheila Train (jornalista – Mtb 46.219)

Coordenação:
Eduardo Cardoso, CertiSign Certificadora Digital
Carlos Castro, FENACON - Federação Nacional dos Contadores

Revisão Técnica:
Marcos Raul de Oliveira

Diagramação e Ilustração:
Vivian Torres

1ª Edição - Especial FENACON

Setembro 2005

O objetivo deste livro é apresentar ao leitor o universo de uma nova tecnologia, que, de forma extremamente rápida, ocupa cada vez mais espaço na mídia, nas discussões do governo e, claro, no nosso dia-a-dia.

A tecnologia, no caso, é a Certificação Digital. Um sistema complexo em termos tecnológicos, porém, simples para utilização, que permite agregar muito mais segurança e praticidade na execução das tarefas cotidianas. Não só no ambiente de trabalho como na burocracia da vida pessoal.

O livro não é voltado para especialistas em tecnologia, mas para o cidadão comum. Aquele que inevitavelmente terá de conhecer e lidar com esse novo sistema de identificação em um curto espaço de tempo, pois, ele já está presente em serviços básicos do cotidiano, como nas obrigações fiscais com a Receita Federal, que lançou o Serviço Interativo de Atendimento Virtual – Receita 222. O serviço tem por objetivo prestar amplo atendimento aos contribuintes pela Internet. Para usar os serviços da Receita 222 é necessário ter um certificado digital.

Entretanto, quase como um making of, o livro também atende à curiosidade dos leitores sobre os mecanismos tecnológicos que possibilitam a criação de uma identidade digital segura.

A partir do momento que se compreende o processo de funcionamento, há confiança para a adesão à Certificação Digital. O próximo passo é fazer uso dela para tornar a vida mais prática e segura.

A vida digital não é o futuro. Ela acontece hoje

Os estudiosos classificam e denominam este período de nosso tempo como a INFOERA. A principal característica desta época pós-industrial é a velocidade gigantesca com que coisas, processos e hábitos se transformam, de forma que mudanças constantes fazem parte da nossa vida cotidiana.

As análises sobre os benefícios e as perdas que essa imensa propagação de conhecimentos e alta evolução tecnológica podem trazer, serão deixadas para os estudiosos debaterem. No entanto, um fato é consenso: esse processo é irreversível. Não há como parar o mundo de novidades instantâneas que surge à nossa frente diariamente.

A moeda forte deste período é o conhecimento. Mais do que útil, ele é necessário. Tecnologias que há pouquíssimo tempo estavam a serviço apenas de laboratórios de pesquisas, ou grandes corporações que podiam pagar seus altos custos, hoje fazem parte do nosso dia-a-dia.

O Professor Doutor João Antônio Zuffo, da Universidade de São Paulo, afirma em seu livro "A Infoera – O Imenso Desafio do Futuro", que a atual agilidade na propagação dos conhecimentos tecnológicos não tem precedentes. O que no período industrial demorava de 200 a 400 anos para ser disseminado e no período subseqüente, o pós-industrial, tardava 20 a 40 anos para se expandir, hoje leva de dois a quatro anos para tornar-se corriqueiro.

[...]"A principal característica da Infoera será a razão de máxima mudança, que ocorrerá com tal regularidade e uniformidade, que ninguém notará, tornando-se parte da vida cotidiana [...]".

A certeza de que não tardiamente vamos ter de nos adaptarmos a muitas inovações tecnológicas fica evidente

quando vemos alguns serviços públicos brasileiros, como a Receita Federal com o seu Serviço Interativo de Atendimento Virtual – Receita 222, e setores privados, como os bancos, exigirem cada vez mais a adesão ao chamado mundo digital.

Existem vários índices sobre o número de pessoas que usam Internet no Brasil, que se alteram constantemente. Em 2004, segundo diversas instituições de pesquisa, a taxa ficou em torno de 20 milhões de usuários.

Os serviços na Internet tornam-se, dia a dia, mais populares. O número de brasileiros que fazem compras pela Web cresce todo ano, pois, hoje existe muito mais confiança nesse setor. As facilidades e as vantagens apresentadas pelo varejo on-line, como as promoções e as opções de pagamento, contribuem para o aumento de compradores virtuais, calculados no ano passado em torno de quatro milhões no país. Pode não ser muito, mas não há expectativa de retração no mercado.

Mas se ainda não se pode dizer que comprar na Internet seja uma realidade para o brasileiro comum, alguns itens do mundo virtual tendem a se tornar essenciais na vida das pessoas em geral, em pouco tempo. Um dos grandes destaques é a Identidade Digital.

A Identidade Digital (os tipos mais conhecidos são o e-CNPJ e o e-CPF) é um documento eletrônico considerado seguro, que permite ao seu portador executar, de maneira muito mais rápida e sigilosa, operações corriqueiras do seu dia-a-dia, como assinatura de documentos, movimentação de conta bancária e compromissos públicos, por exemplo, declaração de imposto de renda. O seu status de "item de necessidade" deve-se exatamente a essas características: praticidade, segurança e privacidade de suas informações.

Porém, é importante já distinguir que a identificação digital não é simplesmente a transposição de uma cópia de sua assinatura em papel para o meio eletrônico, por exemplo, por meio de um scanner (aparelho que copia e transfere dados em papel para a forma digital). O processo de assinatura no meio eletrônico, nesses moldes, nada mais é do que uma "assinatura digitalizada", que não fornece nenhuma segurança quanto à sua validade e autenticidade. Por sua vez, a "assinatura digital", que faz parte do certificado digital, é concebida a partir de processos matemáticos e tecnológicos seguros. Esta sim, tem validade legal.

Quem não quer facilitar a vida e se sentir mais seguro, hoje em dia?

Paranóia moderna: segurança

Pode-se dizer que uma das principais paranóias de nosso tempo refere-se às questões de segurança. A sensação geral é que nunca se viveu de forma tão apreensiva como atualmente.

As crescentes e rápidas evoluções de conhecimento e tecnologia a que somos submetidos de forma freqüente são, naturalmente, mais alguns desencadeadores de insegurança.

Nós sofremos, cada vez mais, com a dose excessiva de informações recebidas. A quantidade imensa de notícias sobre o mundo virtual, que é preciso assimilar, acaba por gerar um estranhamento desse universo. Em vez de sentir alívio pelas benesses que esses avanços trazem, opta-se, freqüentemente, por não conhecer ou utilizar as facilidades do meio eletrônico como se poderia.

Entretanto, quando se presta atenção nesse mundo

eletrônico, percebe-se que propiciar segurança é um de seus principais focos. A preocupação em proteger a integridade e o sigilo de dados que trafegam por esse meio é o centro das atenções dos que atuam no setor tecnológico.

Se o mundo físico, ou "mundo de tijolo e concreto" como também é definido, está cheio de ameaças, o mundo eletrônico inexoravelmente também sofre com a atuação dos mesmos adversários: ladrões, falsificadores, spammers (pessoas que disparam milhares de e-mails de propaganda sem autorização), desenvolvedores de vírus e por aí afora. Os criminosos são velhos conhecidos. A forma de atuação é que mudou.

O meio eletrônico passa a ser um novo lugar para o exercício de atividades criminosas, e suas ameaças não são tão diferentes assim do mundo físico. A metodologia, essa sim, é bem diferente. E sofisticada.

Em vez de instrumentos para roubar documentos e talão de cheque, o criminoso do mundo eletrônico pode manipular conexões digitais para acessar banco de dados e informações pessoais sigilosas.

Alarmes e trancas já não garantem tanta proteção às pessoas. Contudo, se no mundo físico a diminuição da insegurança é algo muito mais complexo, no mundo eletrônico as soluções de segurança se apresentam de forma mais ágil e eficiente. Como no mundo de tijolo e concreto, o importante é estar sempre atento às novas opções de segurança.

Num lugar onde existem estatísticas para quase tudo, como os Estados Unidos, o número de pessoas que tiveram seus dados pessoais "roubados" na Web, inclusive dados bancários, somaram mais de 11% em 2004, de acordo com dados do Better Business Bureau e Javelin Strategy

& Research. Embora a proporção de fraudes seja muito maior e mais fácil no "mundo de tijolo e concreto", esse é um índice que já não passa despercebido.

Mesmo sem estatísticas precisas sobre o número de pessoas, no Brasil, que passam pelo mesmo problema, sabe-se que a segurança nas transações virtuais encabeça, hoje, a lista de prioridades de governo e empresas quando o assunto é investimento em tecnologias da informação.

Não por acaso, os bancos são os que mais estão atentos a esse tipo de problema. A identidade digital, que pode ajudar a diminuir os riscos do uso indevido de dados pessoais dos clientes, provavelmente deve ser adotada em larga escala pelas instituições financeiras brasileiras, em curtíssimo prazo.

Essa é uma evolução tecnológica que traz muitos benefícios para os correntistas de banco. Diretores de grandes instituições financeiras nacionais já declararam à imprensa que o uso da identidade digital é realmente um processo irreversível, e um grande aliado na prevenção de fraudes.

Além, claro, da tão almejada maior segurança para a troca de informações pessoais e de trabalho, o uso da identidade digital também traz algo bastante valioso nos dias atuais: praticidade.

Drama moderno: falta de tempo

Se segurança é a paranóia moderna, podemos dizer que a falta de tempo é o drama moderno. As exigências e as pressões crescentes do mercado de trabalho, em conjunto com o aumento do caos urbano, como congestionamentos e filas por toda a parte, fazem com que tenhamos cada vez menos tempo para as atividades do dia-a-dia.

Todo esse cenário leva a uma busca por soluções práticas para a administração do cotidiano. Aqui, as facilidades do mundo eletrônico também são grandes aliadas.

Você deve se perguntar: como uma identidade digital pode trazer mais segurança e praticidade para a sua vida? Ou mais provável ainda: o que é uma identidade digital?

A imagem que provavelmente vem à mente, quando esse é o assunto, deve ser a dos filmes que trazem espiões e militares fazendo uso de inventivos aparatos tecnológicos em suas missões.

No entanto, as utilidades desse novo documento são várias e você perceberá aqui a importância de contar com uma identidade digital.

Mas claro: verá também que o processo para a confecção dessa identidade digital pode, novamente, remeter-lhe às imagens de filmes clássicos de espionagem, já que envolvem termos como criptografia, chaves secretas, entre outros.

Essas informações tecnológicas, embora não sejam fundamentais para o manuseio de seu documento eletrônico, são importantes para que você possa compreender, de forma mais abrangente, como ele funciona.

Quanto mais aplicações e usos você tiver para a sua identidade digital, maior será o seu entendimento sobre seus termos e funções técnicas, que, longe de parecerem um bicho-de-sete-cabeças, se tornarão cada vez mais simples.

Então vamos ler alguns exemplos do uso da identidade digital. Mais adiante, detalharemos o processo operacional.

O uso da identidade digital

A Receita Federal é uma das instituições públicas brasileiras que se destaca no uso de sistemas avançados da

chamada tecnologia da informação. Uma das últimas inovações adotadas pelo órgão foi, justamente, o lançamento do CPF Eletrônico, ou o e-CPF.

Postos autorizados pelo Governo já emitem o e-CPF, o documento eletrônico que consiste em um cartão com chip, onde são armazenadas digitalmente suas informações. Ele pode ser utilizado pelo seu portador para executar diversos serviços públicos e de instituições privadas.

Com o e-CPF é possível consultar e realizar, de maneira bem mais prática, diversos serviços relacionados com a Receita Federal, por meio do Serviço Interativo de Atendimento Virtual – Receita 222. Com a identidade digital não é mais necessário dirigir-se até um posto de atendimento da Secretaria da Fazenda para efetuar a maioria dos serviços fiscais. A partir deste ano, 2005, já é possível realizá-los de sua própria casa ou local de trabalho, por meio da Internet, pelo Receita 222.

Um exemplo é a possibilidade de checar seu histórico de declarações de renda e, se for o caso, sua situação na "malha fina". O contribuinte também pode obter eletronicamente, com o e-CPF, certidões da Receita Federal, solicitar a emissão de comprovantes de arrecadação de pagamentos realizados e cadastrar procurações eletrônicas.

Há uma versão da identidade digital para empresas: trata-se do e-CNPJ. Da mesma maneira que o documento eletrônico para pessoas físicas, a versão para pessoa jurídica permitirá a realização de serviços no Receita 222 que, anteriormente, precisavam ser efetuados em postos de atendimento.

Com essas identidades digitais é possível assinar digitalmente documentos, por meio de uma operação tecnológica que garante a autenticidade e a integridade de

seus dados após a assinatura. Também permite a verificação e validação de sua identidade pelo recebedor dos dados. Os correntistas de banco também podem utilizar a identidade digital para realizar operações bancárias de forma mais segura.

Os documentos eletrônicos e-CPF e e-CNPJ lançados recentemente pela Receita Federal

O processo tecnológico e operacional que resulta em sua identidade digital é conhecido como Certificação Digital, e já está em aplicação em várias etapas de serviços públicos e privados, sendo uma realidade também no ambiente de trabalho.

Realizar alguma operação na Internet, de forma segura, é possível por meio da Certificação Digital, que assina, autentica, protege e gera recibos digitais das comunicações e transações eletrônicas.

O e-CPF e o e-CNPJ são exemplos de certificado digital. Porém, é importante ressaltar que existem outros modelos de certificados digitais que seguem as mesmas regras e normas estabelecidas pelo governo (como a

chamada ICP-Brasil, como você verá mais adiante). Portanto, apresenta a mesma validade jurídica.

O Tribunal Regional do Trabalho da 4ª Região, em Porto Alegre, no Rio Grande do Sul, colocou em prática, recentemente, o primeiro Sistema de Peticionamento Eletrônico do Brasil, que utiliza Certificação Digital. Esse sistema permite o envio, por meio da Internet, de petições, que ficam armazenadas em meio eletrônico, sem a necessidade da apresentação posterior dos originais.

O resultado é um ganho de tempo e dinheiro, uma vez que muitos advogados tinham que se deslocar de outras cidades, até Porto Alegre, para protocolar as petições.

A Certificação Digital, como você descobrirá logo mais, permite que as partes envolvidas no negócio ou na comunicação comprovem sua identidade e a integridade dos dados que estão sendo enviados e recebidos.

Certificação Digital

Breve história

As normas, diretrizes e o próprio uso da Certificação Digital são relativamente recentes no Brasil, bem como a sua tecnologia. No entanto, como assistimos com quase todos os avanços tecnológicos nos últimos anos, a sua disseminação e popularização têm acontecido muito rapidamente, por conta de fatores já apresentados aqui, como a necessidade, cada vez maior, de segurança, privacidade e agilidade nos processos burocráticos do dia-a-dia.

O certificado digital pode ser definido como um documento eletrônico que identifica as pessoas. Como qualquer documento, ele contém informações importantes sobre o seu portador, por exemplo, nome, data de nascimento e endereço.

Entretanto, o certificado digital contém mais um item bem peculiar - para a identificação de uma pessoa: a chave pública do titular. A função dessa "chave" é estabelecer um parâmetro técnico que possibilite atribuir segurança a uma informação, mas que permita também que esse mesmo dado seja acessado quando necessário e desejado. No capítulo adiante você entenderá como isso funciona na prática.

No momento, basta dizer que o certificado digital é usado para relacionar um nome – tanto de uma pessoa como de uma empresa – a uma "chave criptográfica" que, trocando em miúdos, é um sofisticado mecanismo de assinatura digital, que envolve tecnologia e cálculos matemáticos para *criptografia (1)*.

---

(1) Nota: Criptografia pode ser definida como um conjunto de métodos e técnicas que têm por objetivo proteger o conteúdo de uma informação, não permitindo alterações que não foram autorizadas, bem como, a integridade de sua origem.

Para definir as regras e administrar todo esse contingente de "chaves públicas", o governo federal decidiu criar uma medida provisória, a MP 2.200-2, em agosto de 2001, para organizar o que se denominou "Infra-Estrutura de Chaves Públicas do Brasil", ou para facilitar, simplesmente ICP-Brasil.

O uso das chamadas tecnologias da informação estava (e ainda está) se disseminando na sociedade e portanto se faz necessário criar parâmetros de atuação que fizessem com que as partes envolvidas falassem a mesma linguagem.

O processo de definição de regras para a ICP-Brasil levou em conta desde experiências internacionais de padronização, como as características culturais, sociais e o próprio sistema jurídico brasileiro, para definição das normas.

Resumindo: a ICP-Brasil foi criada com o objetivo de garantir a autenticidade, integridade e a validade jurídica dos documentos em forma eletrônica.

Os gerenciadores

Para evitar uma burocracia eletrônica indesejada, a ICP-Brasil foi concebida dentro de uma estrutura hierárquica que estabelece um relacionamento de confiança com outras instituições e empresas, de forma que o processo de emissão dos certificados digitais para os usuários possa ser facilitado. Assim, a ICP-Brasil é formada por uma autoridade gestora de políticas (Comitê Gestor) e pela cadeia de autoridades certificadoras. O Comitê Gestor é quem estabelece as normas da ICP-Brasil, e aprova políticas e diretrizes para a certificação. É também função deste Comitê a definição de normas técnicas e regras operacionais para a emissão dos certificados digitais.

A coordenação do Comitê Gestor da ICP-Brasil é exercida pelo representante da Casa Civil da Presidência

da República, órgão ao qual é vinculado. Para compor o Comitê são designados representantes da sociedade civil, integrantes dos setores interessados no tema, designados pelo Presidente da República e, ainda, representantes de ministérios e outras autarquias, como Ministério da Ciência e Tecnologia e Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor também se mantém atento para atualizar, ajustar e revisar as práticas e os procedimentos estabelecidos para a ICP-Brasil, a fim de promover a atualização tecnológica do sistema, em conformidade com as políticas de segurança.

A cadeia de Autoridades Certificadoras é composta pela Autoridade Certificadora Raiz (AC Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR).

E o que vem a ser essas "Autoridades"?

Vamos apresentar a primeira da cadeia de certificação – a Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil, que é o Instituto Nacional de Tecnologia da Informação (ITI).

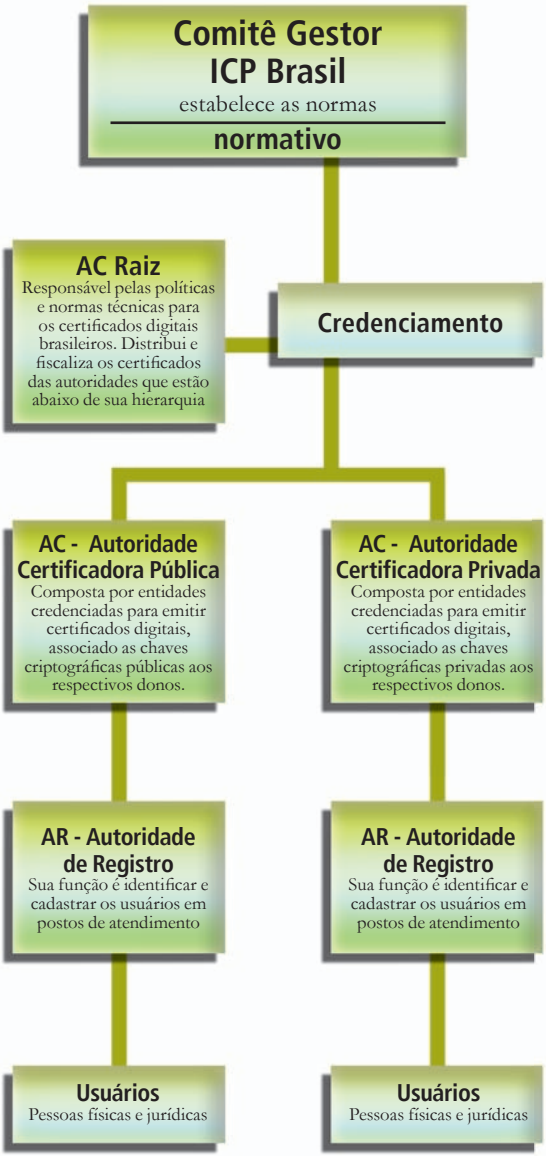
A Autoridade Certificadora Raiz (AC Raiz) é responsável por executar as políticas e as normas técnicas e operacionais para os certificados brasileiros, portanto, ela tem como principal função expedir, distribuir, gerenciar e fiscalizar os certificados das autoridades que estão logo abaixo do seu nível hierárquico – as Autoridades Certificadoras (AC) e as Autoridades de Registro (AR).

Não é diretamente daqui que seu certificado digital sairá, pois, a AC Raiz não emite certificados para o usuário final.

Quem emite, então? É a próxima da hierarquia – a Autoridade Certificadora (AC).

A Autoridade Certificadora é composta por entidades credenciadas pela AC-Raiz para emitir certificados

Estrutura ICP Brasil



digitais associando as chaves criptográficas aos seus respectivos donos.

E, por fim, a última no processo hierárquico, a Autoridade de Registro (AR). A AR é composta por entidades vinculadas operacionalmente a uma determinada Autoridade Certificadora (AC). Sua função é identificar e cadastrar os usuários, em postos de atendimento que os mesmos possam comparecer e, a partir daí, encaminhar as solicitações de certificados para uma AC.

Novo conceito de confiança

Geralmente, quando fazemos compra em um estabelecimento comercial, e usamos o talão de cheque para pagamento, somos solicitados a apresentar um documento com assinatura que ateste que realmente somos a pessoa que consta como titular da conta bancária, como o RG ou o CPF.

O mundo digital tende a estabelecer esse mesmo conceito de "confiança", a exigência de um documento de identificação em que se possa acreditar. No início das operações da Internet no Brasil circulava na Web a seguinte máxima – famosa na boca dos vendedores de produtos eletrônicos em barracas de camelô – *"la garantia soy yo"*.

Hoje, a realidade é outra. Imagine como você procederia no mundo de tijolo e concreto se precisasse validar qualquer transação, por exemplo, a compra de uma casa.

Provavelmente, iria até um cartório, onde um tabelião validaria a compra e venda da casa, mediante algum tipo de identificação sua. Para ficar mais próximo da realidade, você teria que "abrir firma" no cartório, processo de checagem em arquivos de papel que atesta que sua assinatura realmente pertence a você.

Outra maneira bem comum de gerar confiança entre as partes em negociação é o uso de uma terceira pessoa, de boa-fé. Ela presencia e confirma a validade dos termos propostos pelos envolvidos para o negócio, como a compra e venda da casa, em nosso exemplo. Em termos jurídicos, a testemunha garante que o contrato realmente aconteceu.

Na Certificação Digital da ICP-Brasil, esse terceiro de confiança é representado pela Autoridade Certificadora, que publicamente atesta a validade da identidade apresentada pelo seu portador ou o assinante de um documento.

Todo esse aparato tecnológico, como assinatura digital, criptografia e certificação, visa garantir a existência de alguns conceitos fundamentais na concepção e utilização dos documentos eletrônicos: privacidade, autorização e integridade.

Privacidade

O documento com certificado digital garante o sigilo e a proteção das informações, que ali estão armazenadas, contra o acesso de pessoas não autorizadas.

Autenticação e Autorização

A criptografia garante que somente as pessoas autorizadas por você terão acesso ao seu documento eletrônico.

Integridade

Por meio da assinatura digital, os dados do seu documento eletrônico têm sua integridade garantida contra alterações e violações não autorizadas por você, ou seja, sua informação chegará ao destino final da maneira correta.

Um exemplo prático: o correio eletrônico, ou e-mail, que normalmente usamos para nossa comunicação de trabalho ou pessoal não possui mecanismos de segurança capazes

Certificação Digital segurança na comunicação

de garantir a autenticidade e a integridade dos dados ali expostos. Em uma analogia próxima, poderia se dizer que é o equivalente a uma carta escrita a lápis e enviada sem o envelope estar colado, ou seja, qualquer um poderia ler ou alterar as informações que quisesse.

Se não enviamos cartas nesses moldes, pouco podemos fazer com relação ao sistema padrão de e-mails, pois, ao enviar uma mensagem eletrônica ela passa por servidores diferentes, de empresas diversas, onde os operadores desses serviços podem ter acesso aos seus e-mails.

Se as fraudes em uma carta ou documento em papel podem ser mais facilmente percebidas, isso dificilmente ocorre com a informação eletrônica, pois, copiar ou alterar dados nesse sistema não deixa rastros ou informações que permitam alguma identificação. Com a Certificação Digital, são mantidos, justamente, o sigilo, a integridade e a autenticidade de suas mensagens e documentos.

Validade legal

A responsabilidade que você assumirá por uma declaração, negócio ou por qualquer outro ato, não irá desaparecer porque o meio em questão é o eletrônico.

Os "e-docs" (documentos eletrônicos) têm garantia legal, igualmente como acontece com os documentos em papel. A já comentada Medida Provisória 2.200-21* assegura a validade jurídica da Certificação Digital, como pode ser observado em um de seus artigos, o Artigo 10, parágrafo 1º-:

Art. 10º- Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

"§1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916 - Código Civil".

Existe ainda uma série de decretos e resoluções relativas à ICP-Brasil que garantem o embasamento jurídico para as transações com documentos eletrônicos.

**A medida provisória pode ser lida na íntegra em: www.iti.gov.br/medidaprovisoria.htm*

Decifrando a tecnologia

Quando não entendemos bem, nem de tecnologia ou funções matemáticas, e temos que lidar com termos como assinatura digital, criptografia e chaves públicas, a tendência é achar que tudo isso é complicado demais, ou que seja apenas conversa de "futuristas".

Na verdade, você não precisa saber exatamente como funcionam todos os mecanismos de assinatura digital, criptografia e outros itens que envolvem a produção de um documento eletrônico para poder utilizá-lo com facilidade e confiança.

Ao solicitar seu certificado digital junto à Autoridade de Registro, todos esses itens já estão prontos para serem usados e instalados em seu computador, de maneira simples.

No entanto, pelo menos para conhecimento inicial, é mais fácil do que parece compreender esse universo de identidades seguras, dados secretos e decifração de códigos.

Criptografia

Como define o Dicionário Houaiss de língua portuguesa, criptografia é o *"conjunto de princípios e técnicas empregados para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas"*. Ou seja: somente é possível transformar um texto cifrado em um texto simples de se ler, se os códigos utilizados são de conhecimento do emissor e do destinatário.

O uso da criptografia é antigo. Esse conjunto de técnicas para embaralhar um texto é utilizado há milhares de anos. A palavra é de origem grega e formada pelas partes que, em português, significam *secreta* (cripto) e *escrita* (grafia).

O objetivo desde o início, claro, era impedir que um texto fosse lido por outra pessoa que não o destinatário da mensagem.

O conjunto de operações que possibilita as transformações do texto legível em texto cifrado é chamado de *algoritmo*.

A "chave", termo constantemente utilizado em criptografia, nada mais é que o parâmetro que determina as condições da transformação do texto legível em texto codificado.

Possuir a chave e ter o conhecimento prévio dos códigos utilizados entre o emissor e o destinatário. Para o usuário do sistema é fundamental ter essa chave, pois, é ela que iniciará o processo de decodificação de um texto.

Quando se tem essa chave, torna-se possível ler a mensagem cifrada recebida, porém, quando não se tem, fica praticamente impossível conseguir entender o conjunto desconexo de letras e números que estão ali.

Existem dois tipos de algoritmos criptográficos:

Criptografia simétrica

É fundamentada em operações (algoritmos) que dependem da mesma chave, conhecida como "chave secreta". Na criptografia simétrica, uma chave pode codificar e decodificar uma mensagem. Somente a pessoa que enviará a mensagem e a pessoa que a receberá devem conhecer a chave secreta. A segurança na comunicação, aqui, depende do segredo dessa informação.

Criptografia assimétrica (ou de chaves públicas)

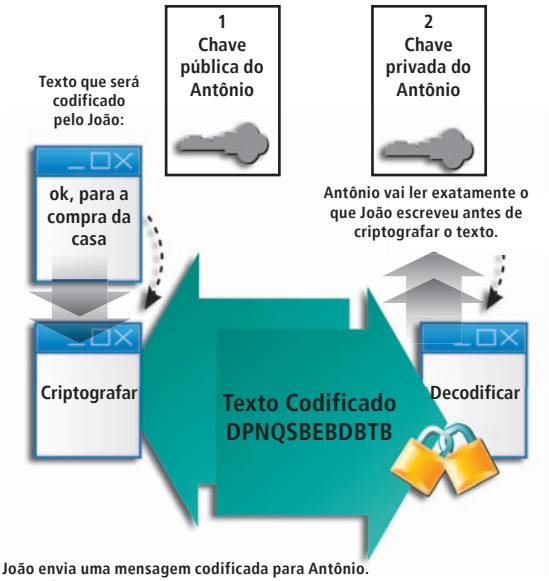
Trabalha com algoritmos que necessitam de pares de chaves, ou seja, duas chaves diferentes para cifrar e decifrar uma informação. A mensagem codificada com a chave 1 de um par somente poderá ser decodificada pela chave 2 deste mesmo par.

As duas chaves utilizadas no método de criptografia assimétrica são chamadas de chave pública e chave priva-

da (secreta). A chave pública qualquer um pode saber qual é, porém, a chave privada somente o seu dono deve conhecer. Apenas com a chave pública é impossível decodificar a mensagem ou descobrir qual seria a chave privada do destinatário.

Neste sistema, então, cada pessoa tem duas chaves, uma pública e outra privada. As mensagens são codificadas usando uma delas e decodificadas usando a outra.

Criptografia Assimétrica (ou de chave pública)



1- João envia uma mensagem codificada para Antônio. Para codificar o texto ele usa a chave pública de Antônio.
2- Para Antônio decodificar e ler a mensagem que recebeu do João ele terá que usar a chave privada, relacionada à chave pública usada no processo por João. Somente Antônio conhece a chave privada.

Por meio desse método, um emissor codifica seu documento com a chave pública da pessoa que receberá a mensagem. O texto codificado apenas poderá ser decodificado pelo destinatário, pois, somente ele tem a chave privada relacionada à chave pública que originou o texto cifrado.

Analise o exemplo: João usa a chave pública de Antônio para criptografar uma mensagem que enviará a ele. A partir daí, apenas o Antônio, com sua chave secreta *(que está relacionada com a chave pública que produziu o texto codificado),* poderá decodificar a mensagem que recebeu de João.

A associação de uma chave pública a um determinado usuário é feita através de um certificado digital.

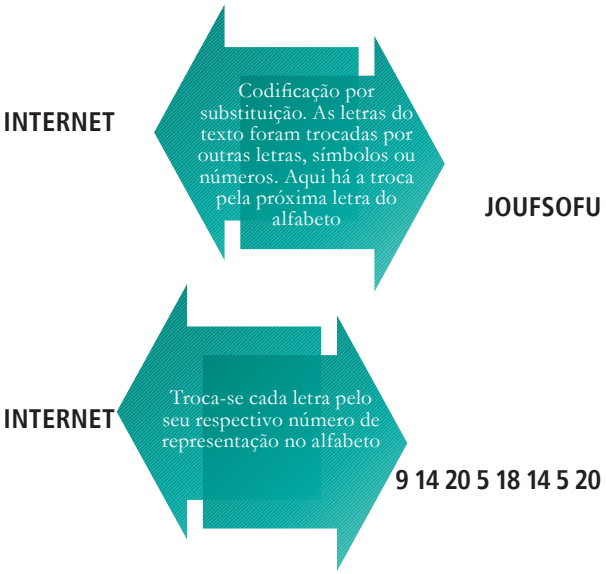
Alguns exemplos de criptografia.

Como já foi dito, criptografia nada mais é do que uma maneira de embaralhar as informações, de forma que apenas a pessoa que tenha a chave para entender o processo usado consiga decifrar o texto.

Como existe um número imenso de chaves criptográficas é muito difícil descobrí-las tentando violar o sistema de segurança, pois, seria necessário realizar uma quantidade enorme de testes. Portanto, quanto maior a chave mais seguro é o sistema. Os códigos usados atualmente precisariam de muitos anos para serem quebrados (mesmo com computadores potentes, pois, o conjunto de alternativas possíveis é muitas vezes maior do que as possibilidades de se acertar sozinho a Mega-sena).

Sem querer torná-lo mestre em criptografia, veja como o processo de codificação pode ser simples, desde que você tenha as informações necessárias sobre a técnica.

Alguns exemplos com a palavra Internet



Neste exemplo hipotético, se você soubesse que a codificação usada numa mensagem recebida foi a substituição por número, por exemplo, você pegaria a tabela correspondente (abaixo), e conseguiria decifrar a mensagem, pois, sabe o código aplicado. Esse é um modo de criptografia simples. Nos processos eletrônicos de Certificação Digital essa decodificação fica a cargo das chaves criptográficas, que processam a decodificação automaticamente no seu computador.

Substituição simples

No exemplo, usamos a substituição simples, em que troca-se cada um dos caracteres do alfabeto ocidental atual (com 26 letras) por caracteres numéricos, de acordo com a tabela pre-estabelecida abaixo, para obter-se um texto cifrado.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

.Assinatura digital.

Se a criptografia possibilita o sigilo das informações, uma vez que os dados são transmitidos codificados, a assinatura digital permite atestar a autenticidade desses dados e da pessoa que os enviou. Aliada à criptografia, a assinatura digital é mais um requisito para gerar uma comunicação segura na Internet.

Desde o final de dezembro de 2004, o atual governador de São Paulo, Geraldo Alckmin, recebe por computador alguns processos que antes se acumulavam em pastas sobre sua mesa. Os despachos nesses documentos oficiais, ou seja, sua assinatura, agora são feitos digitalmente.

A quantidade de processos que o governador de São Paulo e o seu secretario da Casa Civil assinam, por dia, varia de 10 a 100. Com a assinatura digital, a burocracia administrativa ganha muito mais agilidade. Depois de receber a assinatura digital do governador, os processos são encaminhados eletronicamente para

serem publicados no Diário Oficial. A vantagem, além da eliminação de papel, é que mesmo fora do gabinete o governador pode assinar e acompanhar o andamento dos processos de forma eletrônica.

O Governo de São Paulo é pioneiro nesse processo, mas outros Estados devem avançar, muito em breve, com o chamado Governo Eletrônico.

A conclusão aqui é que a assinatura digital já pode ser considerada corriqueira e que, em pouquíssimo tempo, também passará a ser exigida dos cidadãos comuns.

Mas o que é uma assinatura digital? Muitos podem estar imaginando que é apenas a transposição da sua assinatura em papel para o meio eletrônico.

Não é bem o caso. Uma assinatura digitalizada dessa maneira até poderia identificar corretamente o seu titular, porém, as chances dela ser forjada ou fraudada nesse processo seriam imensas. Por exemplo, uma assinatura diferente poderia ser adicionada ao texto ou à mensagem.

A alternativa para esse frágil sistema é o uso da sua chave privada para gerar sua assinatura digital segura.

Porém, como fazer isso?

A assinatura digital é o resultado da aplicação de uma função matemática chamada "função de Hash". Ela é fundamental para a assinatura digital, pois, gera uma espécie de impressão digital de uma mensagem.

O primeiro passo no processo de assinatura digital de um documento eletrônico é a aplicação dessa função de Hash, que fornece uma seqüência única para cada documento.

O resultado dessa função (a seqüência única) é conhecido como "resumo", e a partir dele não é possível recuperar o original. Caso haja alguma tentativa de alterá-

lo, a mensagem gera automaticamente um novo código Hash. A assinatura digital é, portanto, uma forma segura de se conseguir uma autenticação.

No passo seguinte, o "resumo" é codificado com a chave privada do emissor da mensagem. A conseqüência disso é a geração de um arquivo eletrônico que representa a assinatura digital dessa pessoa. A partir daí, a assinatura digital gerada é anexada ao material que será enviado eletronicamente, compondo a mensagem ou o documento.

Quando o destinatário da mensagem recebe o documento com a assinatura, ele aplica a função Hash para obter o chamado "resumo 1". A assinatura é, então, decifrada com o uso da chave pública do emissor da mensagem e, neste processo, se descobre o "resumo" da assinatura. Basta, então, comparar o "resumo" com o "resumo 1". Se os dois forem iguais a conclusão é que o documento realmente foi enviado pelo remetente da mensagem, uma vez que a sua chave pública, que foi usada pelo destinatário, fez a decodificação corretamente.

Claro que isso é feito de forma automática pelo sistema instalado em seu computador para operar com a assinatura digital. Vamos voltar ao João e ao Antônio para exemplificá-la.

O João usa sua chave privada para assinar uma mensagem que enviará para o Antônio. Apenas o João pode criar essa assinatura digital, pois, somente ele tem acesso à sua chave secreta.

Quando o Antônio recebe a mensagem, ele usa a chave pública do João para conferir a assinatura digital. Se ele conseguir decodificar a mensagem, está provado que foi realmente o João que a enviou.

Assinatura Digital

João cria um documento

Chave privada de João: usada para codificar a mensagem

Função Hash é aplicada

É gerado o arquivo eletrônico que representa a assinatura digital do João

"Resumo": Sequência única para cada arquivo

Resumo

é obtido o "Resumo"

documento eletrônico assinado

Assinatura Digital

Antônio recebe um documento assinado

Chave pública de João: usada para decodificação

Resumo

Resumo 1

Função Hash é aplicada

Compara-se o "Resumo" com o "Resumo 1"

Resumo 1

é obtido o "Resumo 1"

Se forem iguais, o documento vem o mesmo do João

Guia prático para obter uma Identidade Digital

É mais fácil do que se imagina obter sua Identidade Digital. Como já explicado aqui, quem operacionaliza o certificado digital para os usuários são as Autoridades de Registro. Aproximadamente 98% dos certificados digitais emitidos no país são emitidos pela empresa CertiSign.

A CertiSign é habilitada pela Secretaria da Receita Federal (uma Autoridade Certificadora / AC-SRF) para expedir em seu nome os Certificados Digitais e-CPF e e-CNPJ. Como explicado no capítulo 1, em "O uso da Identidade Digital", o e-CPF e o e-CNPJ são exemplos de certificado digital, contudo, existem outros formatos de certificados emitidos pela CertiSign que seguem as mesmas regras e normas estabelecidas pelo governo na ICP-Brasil. Portanto, com a mesma validade jurídica.

Além de atuar como Autoridade de Registro, a CertiSign também está credenciada pela AC-Raiz da ICP-Brasil para operar como Autoridade Certificadora, podendo validar a identidade das instituições que quiserem emitir certificados digitais.

O guia prático para conquistar sua Identidade Digital é com base, então, na metodologia aplicada por esta Autoridade de Registro (AR), a CertiSign.

Como solicitar a identidade digital?

O primeiro passo é solicitar e preencher no site desta AR, a CertiSign - www.certisign.com.br, um formulário de requisição do e-CPF, e-CNPJ ou identidade digital. Na área de aquisição desses documentos você terá que seguir as instruções para a geração do par de chaves pública e privada.

Após enviar a solicitação, você deve ler e imprimir o

Termo de Titularidade, que é gerado automaticamente pelo sistema. Este documento terá que ser levado até um posto de validação* para conferência de um agente credenciado.

É importante memorizar ou guardar em local seguro a Frase de Identificação (FI) que fornecer nesta etapa, pois, ela será necessária na hora de retirar o Certificado Digital.

Depois de fazer o pedido de seu certificado digital, você deve comparecer a um posto de validação da CertiSign para fazer a validação presencial, apresentando alguns documentos.

Quais os documentos necessários?

Para ter seu certificado digital é preciso comparecer a um posto de validação para fazer a validação presencial. Você precisa levar os documentos (originais) especificados abaixo, além do Termo de Titularidade preenchido e assinado para conferência de um agente. O Termo deve ser impresso no momento da solicitação on-line.

Documentos necessários para o e-CPF:

- Foto recente em tamanho 3x4 ou em formato digital (alguns postos de validação possuem serviço de fotografia digital, portanto, em alguns lugares não há necessidade de se levar foto. Para saber quais locais possuem esse serviço consulte-os na lista em "Anexo").

- Cédula de Identidade (pode ser RG, carteira profissional, documento funcional ou carteira de habilitação).

** Nota: consulte mais informações sobre os postos de validação em www.certisign.com.br/ars*

- CPF (Cadastro de Pessoa Física).
- Comprovante de residência;
- Título de Eleitor (opcional);
- PIS-PASEP (opcional).

Cópias dos documentos serão arquivadas no posto de validação. A habilitação da identidade digital é feita no próprio local.

Não podem solicitar o e-CPF as pessoas que estejam com o seu CPF na condição de cancelado pela Receita Federal.

Documentos necessários para a Identidade Digital

- Foto recente em tamanho 3x4 ou em formato digital (alguns postos de validação possuem serviço de fotografia digital, portanto, em alguns lugares não há necessidade de se levar foto. Para saber quais locais possuem esse serviço consulte-os na lista em "Anexo").
- Cédula de Identidade (pode ser RG, carteira profissional, documento funcional ou carteira de habilitação).
- CPF (Cadastro de Pessoa Física).
- Comprovante de residência.

Documentos necessários para o e-CNPJ

- Documentação da empresa (cópia autenticada ou original):

1 · Registro comercial, no caso de empresa individual.

2 · Contrato social, estatuto ou ato constitutivo em vigor, no caso de sociedades comerciais ou civis. No caso de sociedade por ações, deve constar ainda documento de eleição dos administradores.

3 · Última versão/alteração do contrato social, estatuto ou ato constitutivo.

- CNPJ (Cadastro Nacional de Pessoas Jurídicas).

- Foto (3x4) recente dos representantes legais da empresa cadastrados na Receita Federal (alguns postos de validação possuem serviço de fotografia digital, portanto, em alguns lugares não há necessidade de se levar foto. Para saber quais locais possuem esse serviço consulte-os na lista em "Anexo").

- Comprovante de residência dos representantes legais da empresa cadastrados na Receita Federal.

Para a validação presencial do e-CNPJ devem comparecer o representante legal e os representantes cadastrados junto à Receita Federal com os documentos relacionados. Caso o contrato social ou documento equivalente de sua empresa determine que o representante cadastrado na Receita Federal não possa assinar isoladamente, será necessário que as demais pessoas listadas no documento como representantes legais compareçam para validação presencial, com os seus documentos (documentação dos representantes legais, cédula de identidade, CPF, comprovante de residência).

As empresas solicitantes do e-CNPJ não podem estar com o seu CNPJ na condição de cancelado, suspenso ou inapto.

Observação: Consulte sempre a Autoridade de Registro para mais detalhes sobre a retirada e emissão da sua documentação.

Documentação (original) necessária do responsável pelo certificado, cadastrado na Receita Federal

- Foto 3x4 recente ou em formato digital.
- Cédula de Identidade.
- CPF (Cadastro de Pessoa Física).
- Comprovante de residência.

O representante cadastrado na Receita Federal precisa comparecer pessoalmente ao posto de validação, uma vez que a mesma não pode ser feita por meio de procuração.

Retirada do Certificado Digital

Após a conclusão do processo de validação presencial, o Certificado Digital é gerado com suas chaves pública e privada. Existem duas maneiras padrões de armazenamento físico do certificado: em um smart card ou em um token USB.

Smart Card (Cartão Inteligente)

Consiste em um cartão criptográfico que gera e armazena as chaves criptográficas que compõem o certificado digital.

Token USB

O token é um hardware criptográfico que gera e armazena as chaves criptográficas que compõem o certificado digital, da mesma maneira que o smart card. Este pode ser conectado em um computador pela entrada USB e funciona simultaneamente como um smart card e uma leitora.

Forma de armazenamento físico do Certificado Digital

O certificado digital do Tipo A3 é processado e armazenado no smart card ou no token, conforme sua escolha. Nesta forma de armazenamento o certificado permanece único, pois, é gerado em um hardware (token/ smart card) que não permite qualquer tipo de reprodução ou exportação da sua chave privada. O certificado Tipo A3 necessita de senha de acesso para utilizar a chave privada

(PIN), e permite que você se desloque com ele, podendo realizar transações eletrônicas onde desejar.

e-CNPJ Tipo A3

Da mesma maneira que o e-CPF (documento eletrônico para pessoa física), o documento eletrônico para pessoa jurídica, o e-CNPJ Tipo A3, fica guardado em um token ou smart card.

Cursos

Os certificados digitais são simples de serem adquiridos e usados, no entanto, existem cursos voltados para ajudar os usuários a entenderem, de forma mais detalhada, esse novo mundo eletrônico.

A CertSign, a Autoridade de Registro usada como exemplo neste guia, oferece diversos cursos sobre Certificação Digital para usuários e empresas, com vários níveis de informações, conforme a necessidade de cada um.

O treinamento noções básicas sobre o certificado digital e seu uso no dia-a-dia. Também existem cursos voltados para profissionais que precisam implantar certificados digitais em suas empresas.

As informações sobre esses cursos, turmas e horários podem ser encontradas no site da CertiSign: www.certisign.com.br/treinamento.

Cuidados com o seu Certificado Digital

É importante seguir as orientações da Autoridade de Registro sobre os cuidados com o certificado digital.

Algumas ações podem inutilizar seu certificado digital Tipo A3, portanto, atente-se às seguintes dicas:

· Guarde bem seu hardware. Perder o smart card ou token significa também a perda do seu certificado.

· Perda de senha do seu smart card ou token.

· Bloqueio dos identificadores PIN (senha primária) e PUK (senha mestra) do seu smart card.

· Bloqueio de senha do seu token.

· Formatação ou limpeza do seu smart card.

· Remoção das chaves do seu token.

Caso ocorra uma das situações acima, será necessário um novo comparecimento à Autoridade de Registro, como feito inicialmente.

Leia com atenção os manuais do smart card ou token que acompanham o hardware. Estes normalmente estão disponíveis no site do fabricante deste.

No caso do PIN ou a senha serem bloqueados, é necessário contactar o SAC (Serviço de Atendimento ao Cliente) da sua autoridade Certificadora para auxílio.

Dúvidas Frequentes

Quem pode ter uma identidade digital?

Qualquer pessoa que tenha um CPF válido pode solicitar sua identidade digital. Da mesma maneira, as empresas que tenham um CNPJ válido também podem solicitar um e-CNPJ.

Qual a melhor opção de certificado digital?

O certificado digital Tipo A3 oferece mais segurança e mais praticidade, pois, é gerado e armazenado em um hardware, ou seja, em um smart card ou token. Eles são invioláveis e apresentam a vantagem de poderem ser transportados para onde quer que seja, de forma que você possa realizar transações on-line em outros locais.

A identidade digital é segura?

Sim, a identidade digital é segura.

O certificado digital de sua identidade digital trabalha com as chamadas chaves criptográficas, sendo uma pública e a outra privada. A chave privada é somente de seu conhecimento, sendo necessária uma senha para acessá-la, em qualquer modelo escolhido, o que garante a privacidade.

A criptografia utilizada na autenticação dos documentos eletrônicos assegura que somente pessoas autorizadas por você terão acesso àquele documento.

A assinatura digital protege seu documento de violações e garante que ele chegará ao destino final de maneira correta.

Ao gerar meu par de chaves criptográficas para o certificado digital, além de armazenar minha chave pública, a Autoridade de Registro também fica com uma cópia da minha chave privada?

Não. A Autoridade de Registro (AR) que emitiu seu certificado digital não mantém nenhuma cópia de sua chave privada. Portanto, é importante manter sua senha de acesso a chave bem guardada e que a mesma seja apenas de seu conhecimento.

Quais os cuidados que a Identidade Digital exige?

Qualquer que seja a opção de armazenamento para seu certificado digital, smart card, token ou no seu computador, o cuidado que se deve ter é sempre com sua senha de acesso à chave privada. Sem essa senha não é possível acessá-la.

A sua senha deve ser somente de seu conhecimento.

Onde posso utilizar meu certificado digital?

Atualmente, o certificado digital está sendo solicitado para inúmeros serviços públicos, sendo o mais expressivo deles o Serviço Interativo de Atendimento Virtual – Receita 222, da Receita Federal. Ele já pode ser utilizado para efetuar a declaração de imposto de renda e para solicitar diversos documentos de forma on-line no site da Receita.

Contudo, com a adoção do certificado digital em diversas esferas do serviço público e privado, ele já pode ser considerado parte da rotina de trabalho de muitas pessoas que precisam "conversar" entre si, no ambiente

de trabalho, de forma segura e rápida.

As transações feitas com a identidade digital têm validade jurídica?

Os documentos eletrônicos têm garantia legal, igualmente como acontece com os documentos em papel. A Medida Provisória 2.200-2 assegura a validade jurídica da Certificação Digital.

Qual a validade do certificado digital? É preciso renovar, como outros documentos?

A validade do seu certificado digital pode variar de 1 a 3 anos. Após o vencimento é necessário fazer a renovação novamente com a Autoridade de Registro.

Bibliografia e Referências

Better Business Bureau
www.bbb.org

CertiSign Certificadora Digital
www.certisign.com.br

Dicionário Houaiss Língua Portuguesa -1ª Edição, Rio de Janeiro, Editora Objetiva, 2001

Fenacon
www.fenacon.org.br

Governo Eletrônico
www.governoeletronico.gov.br

ITI – Instituto Nacional de Tecnologia da Informação
www.iti.gov.br

Secretaria da Receita Federal
www.receita.fazenda.gov.b

Tribunal Regional do Trabalho da 4ª Região
www.trt4.gov.br

Zuffo, João Antonio – A Infoera, O Imenso Desafio do Futuro, São Paulo, Editora Saber Ltda., 1997.

Glossário

A

ACEITAÇÃO - Demonstração da concordância quanto à correção e adequação do conteúdo e de todo o processo de emissão de um certificado digital, feita pelo indivíduo ou entidade que o solicitou. A aceitação ocorre através do recebimento e reconhecimento de uma notificação sobre o conteúdo do certificado, conforme os termos da Declaração de Práticas de Certificação – DPC. O certificado é considerado aceito ao ser instalado no sistema do solicitante, a partir de sua primeira utilização, ou após haver decorrido o prazo pré-estipulado para sua rejeição.

ACESSO - Estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações. A partir do acesso podem ocorrer a transferência de dados e a ativação de processos computacionais.

ADMINISTRADOR DE PKI GERENCIADA (MANAGED PKI ADMINISTRATOR) - Indivíduo designado para controlar e administrar as funções de uma infra-estrutura de chaves públicas – PKI Gerenciada.

ADWARE – Software que exibe publicidade. O adware muitas vezes inclui spyware, de modo que os anúncios podem ser dirigidos segundo interesses e hábitos do usuário.

AICPA – AMERICAN INSTITUTE OF CERTIFIED PROFESSIONAL ACCOUNTANTS - Instituto de profissionais de contabilidade norte-americano que estabeleceu os padrões de auditoria conhecidos como

SAS-70 Statement of Audit Standards, utilizados como procedimento em auditorias sobre os controles físicos e de acesso das instalações de segurança de empresas e organizações.O site da AICPA funciona no endereço: http://www.aicpa.org.

AGATE (APPLICATION GATEWAY) - Componente do Internet Transaction Server (ITS) em aplicativos SAP. O Application Gateway é um processo servidor ativo que funciona independente de um servidor web em particular. Ele estabelece conexão com o servidor do aplicativo SAP, gerencia o processo de conexão e controla o contexto e o tempo de inatividade (time-out) da sessão. Além disso, gera páginas HTML e fornece conversões das páginas de códigos e suporte para o idioma local.

ALGORITMO (ALGORITHM) - Série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema. Em criptografia, um algoritmo representa o processo matemático utilizado para "embaralhar" os dados.

ALGORITMO CRIPTOGRÁFICO (CRYPTOGRAPHIC ALGORITHM) - Processo matemático especificamente definido para criptografar e decriptografar, mensagens e informações, normalmente com a utilização de chaves.

ANSI – AMERICAN NATIONAL STANDARDS INSTITUTE - Organização privada sem fins lucrativos cujo objetivo é promover o uso internacional de padrões norte-americanos, a defesa de políticas e posições técnicas dos

EUA em entidades de padronização locais e internacionais, e o estímulo à adoção nos EUA de padrões internacionais que atendam às necessidades da comunidade de usuários. O site do ANSI funciona no endereço: http://www.ansi.org.

API – APPLICATION PROGRAMMING INTERFACE - Interface de programação de aplicativos que permite a comunicação entre programas ou entre um programa e o kernel (de um sistema operacional), estabelecendo as convenções e os parâmetros a serem seguidos.

ARQUITETURA (ARCHITECTURE) -
Modo de configuração de um sistema, incluindo o relacionamento entre suas partes. Arquitetura de Hardware é a configuração dos componentes físicos do sistema (servidores e firewalls). Arquitetura de Software é a configuração dos componentes (programas, sistemas operacionais ou scripts) dentro do sistema.

ASSISTENTE DE AUTENTICAÇÃO - Componente do serviço de PKI Gerenciada CertiSign disponível através do Centro de Processamento da CertiSign, que permite ao administrador personalizar o modo como o usuário será autenticado para que se dê a aprovação ou rejeição de uma solicitação de certificado digital.

ASSINANTE - Indivíduo ou organização para quem foi emitido um certificado digital dentro de uma hierarquia criptográfica. O assinante é o titular da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra

.ASSINATURA DIGITAL (DIGITAL SIGNATURE) - Transformação de uma mensagem eletrônica através da aplicação de uma função matemática e da encriptação do seu resultado com a chave privada do remetente, de modo que o destinatário da mensagem possa verificar sua origem e integridade. A assinatura digital garante que um conjunto de dados (mensagem ou arquivo) realmente provém de determinado remetente e não foi adulterado após o envio.

AUDITORIA (AUDIT) - Procedimento realizado por agentes independentes e utilizado para verificar se todos os controles, equipamentos e dispositivos estão preparados e são adequados às suas funções. Inclui o registro e análise de todas as atividades importantes para detectar vulnerabilidades ou abusos em um sistema de informações.

AUTENTICAÇÃO (AUTHENTICATION) - Processo de confirmação da identidade de um indivíduo ou organização, ou de comprovação da posse ou integridade de certas informações. Um administrador executa a autenticação das solicitações de certificados através da validação da identidade do solicitante e da confirmação dos dados da solicitação.

AUTENTICAÇÃO AUTOMÁTICA (AUTOMATED AUTHENTICATION) - Processo pelo qual uma solicitação de certificado é aprovada por comparação automática dos dados da solicitação com informações previamente disponíveis em um banco de dados. As opções de autenticação automática oferecidas pela PKI Gerenciada CertiSign são a Automated Administration (Auto-Admin) e a Autenticação por Passcode.

ADMINISTRAÇÃO AUTOMATIZADA (AUTOMATED ADMINISTRATION - AUTO - ADMIN) - Componente dos Serviços de PKI Gerenciada (e PKI Grenciada Full) CertiSign que substitui o processo de aprovação manual de solicitações de certificados por um software personalizado, mantendo todo o processo dentro das instalações da organização. Disponível somente com os serviços de PKI Gerenciada (e PKI Grenciada Full), o Auto-Admin aprova as solicitações de certificados sem a participação do administrador, comparando os dados da solicitação com informações previamente cadastradas pela organização assinante dos serviços de PKI Gerenciada.

AUTORIDADE CERTIFICADORA – AC (CA – CERTIFICATE AUTHORITY) - Entidade autorizada a emitir, suspender, renovar ou revogar certificados digitais. Cabe também à Autoridade Certificadora emitir listas de certificados revogados (LCR) e manter registros de suas operações. A principal competência de uma AC, no entanto, é emitir certificados que vinculem uma determinada chave pública ao seu titular. Na hierarquia dos Serviços de Certificação Pública CertiSign, as ACs estão subordinadas à Autoridade Certificadora Primária (AC-Raiz) da VeriSign, enquanto as ACs abaixo da hierarquia da ICP-Brasil subordinam-se à AC-Raiz da ICP-Brasil. A AC é identificada por um nome distinto - distinguished name (dn) em todos os certificados que emite.

AUTORIDADE EMISSORA – AE (IA – ISSUING AUTHORITY) - A Autoridade Emissora (AE) pode ser uma Autoridade de Certificação Primária (AC-Raiz), uma Autoridade Certificadora (AC) ou uma AC Subordinada, que somente pode emitir certificados válidos e confiáveis,

com a aprovação prévia da AC-Raiz da hierarquia. Uma AE pode delegar as responsabilidades de avaliar, aprovar e recusar solicitações de certificados a uma ou mais ARLs (Autoridades de Registro Local), que não pertençam nem sejam operadas por aquela AE. Quando isso ocorre, o termo "AE" deve incluir as ARLs para efeito de obrigações, garantias e exclusões.

AUTORIZAÇÃO (AUTHORIZATION) - Concessão de direito ou permissão que inclui a capacidade de acessar informações e recursos específicos em um sistema computacional.

B

BANCO DE DADOS (DATABASE) - Conjunto de informações relacionadas que são criadas, armazenadas e/ou manipuladas por um sistema de informações gerenciado por computador.

BACK DOOR – Uma vulnerabilidade na segurança instalada por vírus ou trojan para facilitar o acesso de um invasor – normalmente secreto – a um computador, driblando salvaguardas.

BIOMETRIA (BIOMETRICS) - Ciência que utiliza propriedades físicas e biológicas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz.

BIT - BINARY DIGIT - Dígito binário (Binary digit), que pode ser 1 ou 0.

BLOCO (BLOCK) - Seqüência de bits de comprimento fixo.

BROWSER - Vide Navegador de Internet / Web Browser

C

CA – CERTIFICATION AUTHORITY - AUTORIDADE CERTIFICADORA – AC - Vide Autoridade Certificadora

CADEIA DE CERTIFICADOS - CERTIFICATE CHAIN - Lista ordenada de certificados contendo um certificado de assinante (entidade final) e um ou mais certificados de nível superior até a AE – Autoridade Emissora, que permite a um destinatário verificar que o remetente e todas as AEs envolvidas são confiáveis.

CANAL SEGURO - Canal de comunicação criptograficamente seguro para transmissão de informações.

CAPI - CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE - Interface de programação de aplicativos criptográficos para módulos de software que permite o acesso a funções criptográficas pertencentes a outros programas relacionados.
CENTRO DE CONTROLE - CONTROL CENTER - Conjunto de páginas web no serviço de PKI Gerenciada CertiSign/VeriSign, que permite aos Administradores visualizar, aprovar, recusar, suspender e revogar os certificados solicitados.

CERTIFICAÇÃO CRUZADA - Situação em que uma AC Primária emite um certificado cujo assunto (subject) é

uma entidade emissora de certificados que representa outro domínio de certificação, ou vice-versa. A certificação cruzada permite compartilhar a confiança entre diferentes entidades e redes de PKI.

CERTIFICAÇÃO DIGITAL - Processo de emissão de certificados digitais por uma Autoridade Emissora.

CERTIFICADO DE AFILIAÇÃO - Certificado emitido para indivíduos ou entidades afiliadas. Um certificado de afiliação fornece uma comprovação de identidade adequada, sem necessariamente afirmar que o indivíduo ou entidade em questão possui autorização para agir em nome da entidade à qual é afiliado.

CERTIFICADO DE CHAVE PÚBLICA (PUBLIC KEY CERTIFICATE) - Credencial eletrônica cujos requisitos mínimos são: declarar o nome ou identidade da respectiva Autoridade Emissora (AE); identificar o respectivo titular; conter a chave pública referente ao titular; identificar o período operacional; conter o número de série do certificado e a assinatura digital da AE. Os Certificados Digitais são utilizados para autenticar o remetente e confirmar a integridade dos dados enviados, podendo também fornecer elementos que impeçam ou dificultem o repúdio infundado a atos ou transações. Além disso, os Certificados podem ser utilizados para criptografar dados e enviá-los ao seu titular. Os Certificados Públicos CertiSign podem ser publicados através da VeriSign Trust Network (VTN) e estabelecer comunicação fora de seu domínio. Os Certificados Privados CertiSign não fazem parte da VTN e não podem estabelecer comunicação fora do seu domínio.

CERTIFICADOS DIGITAIS DE CLASSE 1/2/3 - Certificados com nível específico de segurança e confiança dentro da hierarquia VeriSign Trust Network:– Classe 1: fornece o nível mais baixo de segurança e confiança. Os certificados de classe 1 validam apenas o endereço de e-mail do indivíduo para quem o certificado foi emitido.– Classe 2: oferece nível médio de confiança. Os certificados de classe 2 validam a identidade do indivíduo com a utilização de um banco de dados de clientes on-line e verificação do e-mail, ou então através de uma partição secreta.– Classe 3: fornece o mais alto nível de confiança. Os certificados de classe 3 validam indivíduos através do comparecimento em pessoa dos mesmos perante um agente autorizado, além de outras comprovações específicas de identidade. Os certificados de classe 3 validam organizações através de bancos de dados de terceiros (como o Cadastro Nacional de Pessoas Jurídicas - CNPJ) e outros meios independentes.

CERTIFICADO DE DEMONSTRAÇÃO (DEMO)
DEMO CERTIFICATE - Certificado emitido por uma Autoridade Emissora com a finalidade exclusiva de apresentação e demonstração, não podendo ser utilizado para comunicações seguras ou confidenciais.

CGI (COMMON GATEWAY INTERFACE) - Protocolo que especifica como um servidor de Internet executa e troca dados com um programa.

CHAVE COMUM (COMMON KEY) - Partição física em um sistema de hardware criptográfico, armada através de um processo de partição secreta que exige que a partição física permaneça anexada ao hardware quando armada.

Não se presume que seja secreta, já que não permanece continuamente sob o controle de um indivíduo.

CHAVE DE SESSÃO - Chave para sistemas criptográficos de chave simétrica utilizada pela duração de uma mensagem ou sessão de comunicação. O protocolo SSL (Secure Sockets Layer) utiliza as chaves de sessão para manter a segurança das comunicações via Internet.

CHAVE DISTRIBUÍDA - Chave dividida em várias partes e compartilhada entre diferentes participantes.

CICLO DE VIDA DO CERTIFICADO - Período de tempo que se inicia com a solicitação do certificado e termina com sua expiração, renovação ou revogação.

CIFRA ASSIMÉTRICA (ASYMMETRIC CIPHER) - Algoritmo criptográfico que utiliza uma chave para criptografar e outra para decriptografar. A criptografia de chaves públicas é um exemplo de cifra assimétrica.

CIFRA DE BLOCO (BLOCK CIPHER) - Cifra simétrica que criptografa um arquivo dividindo-o em blocos e criptografando cada bloco.

CLIENTE - Programa, normalmente, utilizado pelo usuário como interface para acessos a um conjunto de serviços tornados disponíveis por um servidor, em relações cliente/servidor.

CERTIFICADO DE ASSINATURA DE CÓDIGO - (CODE SIGNING CERTIFICATE)- Certificado emitido

para empresas que desenvolvem software, permitindo que assinem digitalmente o código-objeto de programas, o que garante a origem, e a integridade absoluta para quem recebe o código pela Internet.

COMPONENTE DE RETAGUARDA (BACK-END COMPONENT) - Programa, dispositivo ou equipamento não diretamente visível para o usuário em sistemas, produtos ou serviços CertiSign. Os componentes de apoio são geralmente protegidos por "firewalls" para garantir sua segurança.

COMPONENTE DE INTERFACE (FRONT END COMPONENT) - Componente de um sistema, produto ou serviço CertiSign diretamente visível para o usuário.

COMPROMETIMENTO (COMPROMISE) - Violação concreta ou suspeita de violação de uma política de segurança, onde possa ter ocorrido divulgação não autorizada ou perda do controle sobre informações sigilosas.

CPM - CERTIFICATE PARSING MODULE - Módulo de análise de certificados, parte de produtos CertiSign que extrai informações dos certificados de cliente apresentados a um servidor de Internet e as torna disponíveis para aplicativos que utilizem certificados digitais.

COOKIE - Uma espécie de arquivo que alguns websites põem nos computadores dos usuários para permitir a personalização do conteúdo da Web. A maioria dos cookies é inofensiva, mas alguns registram hábitos de navegação na Web e informação pessoal e são considerados spyware.

CONFIDENCIALIDADE (CONFIDENTIALITY) - Condição na qual dados sigilosos são mantidos em segredo e revelados somente a pessoas autorizadas.

CONTROLE DE ACESSO -Conjunto de componentes dedicados a proteger a rede, aplicações Web e instalações físicas de uma Autoridade Certificadora – AC contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados possam utilizá-las.Vide também Lista de Controle de Acesso / Access Control List.

CONTROLE DISCRICIONÁRIO DE ACESSO (DISCRETIONARY ACCESS CONTROL - DAC) - Conjunto de meios de restrição de acesso a objetos baseado na identidade dos titulares e/ou dos grupos a que pertencem. O controle é discricionário no sentido de que um titular com determinada permissão de acesso é capaz de transferir essa permissão (talvez até indiretamente) para qualquer outro titular a seu critério.

CREDENCIAMENTO (ACCREDITATION) - Declaração formal feita por uma autoridade competente para afirmar que um sistema de informações, organização ou profissional foi considerado apto a executar determinadas tarefas ou operar em um modo de segurança específico, após cumprir um conjunto de condições preestabelecido.

CRIPTOGRAFIA - Processo de embaralhamento de dados para que não possam ser recuperados sem a utilização do processo inverso de decriptografia. A criptografia é uma ciência matemática usada para assegurar o sigilo e

a autenticidade das informações, convertendo-as em uma versão ininteligível que só pode ser decifrada com a chave e o algoritmo criptográfico corretos.

CRIPTOGRAFIA DE CHAVES PÚBLICAS - PUBLIC KEY CRIPTOGRAPHY - Tipo de criptografia que usa um par de chaves criptográficas matematicamente relacionadas. A chave pública está disponível a todos que desejem criptografar informações e enviá-las ao dono da chave privada, ou verificar uma assinatura digital criada com aquela chave privada. A chave privada é mantida em segredo por seu dono e pode decriptografar informações ou gerar assinaturas digitais.

CRON JOB - Script configurável utilizado para executar uma tarefa simples e repetitiva (como gerar um registro) dentro de um cronograma definido.

CPS (CERTIFICATION PRACTICE STATEMENT) - Vide Declaração de Práticas de Certificação – DPC

CSR (CERTIFICATE SIGNING REQUEST) - Vide Solicitação de Assinatura de Certificado.

CSV – COMMA - (SEPARATED VALUE) - VALOR SEPARADO POR VÍRGULA - Formato de arquivo também conhecido como flat file (arquivo plano), que pode ser transferido entre aplicações baseadas em tabelas, como bancos de dados e planilhas. Este tipo de arquivo contém uma série de linhas de texto ASCII onde os valores das colunas são separados por uma vírgula, dando início a cada novo registro na linha imediatamente inferior.

D

DES (DATA ENCRYPTION STANDARD) PADRÃO DE CRIPTOGRAFIA DE DADOS - DES - Sistema de cifragem em blocos desenvolvido pela IBM e pelo governo dos EUA nos anos 70 como padrão oficial. Está definido no documento de padronização FIPS 46-1.

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DPC CPS (CERTIFICATION PRACTICE STATEMENT) - Documento, periodicamente revisado e republicado, que contém as práticas e procedimentos implementados por uma Autoridade Certificadora para emitir certificados. É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento, das práticas e políticas que fundamentam a emissão de certificados e de outros serviços relacionados. É utilizado pelas Autoridades Emissoras para garantir a emissão correta dos certificados e pelos Solicitantes e Partes Confiantes para avaliar a adequação dos padrões de segurança empregados às necessidades de segurança de suas aplicações.

DECRIPTOGRAFIA - Processo que transforma dados previamente criptografados e ininteligíveis (ciphertext) de volta à sua forma legível (plaintext).

DIGITAL ID - Nome comercial e marca registrada da VeriSign para um certificado digital.

DAP(DIRECTORYACCESSPROTOCO)-PROTOCOLO DE ACESSO A DIRETÓRIOS - Protocolo que permite a um usuário de diretórios (um indivíduo ou outro aplicativo de software) acessar um diretório compatível com X.500.

DIM (DIRECTORY INTEGRATION MODULE) (DIM) - MÓDULO DE INTEGRAÇÃO DE DIRETÓRIOS - Módulo da opção Auto-Admin (Automated Administration) da PKI Gerenciada CertiSign que permite ler dados de autenticação a partir do diretório compatível com LDAP da organização e inserir informações de certificados no diretório.

DISPONIBILIDADE - Capacidade de utilizar informações e processos sob demanda, permitindo o acesso autorizado a recursos e a performance de operações críticas em tempo hábil.

DN (DISTINGUISHED NAME) - NOME DISTINTO - Conjunto de dados que identifica de modo inequívoco uma entidade ou indivíduo pertencente ao mundo físico no mundo digital (por exemplo: país=BR, estado=Rio de Janeiro, nome organizacional=Sua Empresa S.A., nome comum=José da Silva).

DNS (DOMAIN NAME SERVICE) - SERVIÇO DE NOMES DE DOMÍNIO - Processo que transforma endereços IP (1.2.3.4) em nomes hierárquicos, que podem ser lidos por seres humanos (www.companyname.com), e vice-versa.

DOCUMENTO - Registro que consiste em informações inscritas num meio tangível, como uma folha de papel, ao contrário das informações baseadas em sistemas de computação.

E

EMISSÃO DE CERTIFICADO - Ação desempenhada por uma AE (Autoridade Emissora) na criação de um

certificado e subseqüente notificação ao seu solicitante, ou seja, à pessoa ou organização listada no conteúdo do certificado, que se torna assinante a partir da aceitação.

ENTIDADE AFILIADA (AFFILIATED ENTITY) - Entidade relacionada à outra: (i) como matriz, subsidiária, sócia, joint-venture, contratada ou agente, (ii) como membro de uma comunidade de interesses registrada, ou (iii) como entidade que mantém relacionamento com uma entidade principal, que mantém negócios ou registros capazes de fornecer comprovação adequada da identidade da afiliada.

EULA - Abreviação de "end-user licence agreement", ou acordo de licença do usuário final, os contratos que acompanham a maioria dos programas e governam os termos de uso. A maioria dos usuários com computadores infectados por adware e spyware concordam em instalar os programas ao clicar em "Aceito" no pé dos eulas que acompanham software shareware e outros programas gratuitos.

EXTENSÃO .PFX - Extensão de arquivo associada a todos os Certificados Digitais exportados do navegador Microsoft Internet Explorer que incluem as chaves pública/privada em formato PKCS #12.

EXTENSÃO .CER - Extensão de arquivo associada a Certificados Digitais

F

FERRAMENTA DE ADMINISTRAÇÃO DE CHAVES DA AC - Componente do Centro de Processamento utilizado

para testar e inicializar os cartões Luna, gerar pares de chaves, certificados e solicitações de certificados.

FRASE DE IDENTIFICAÇÃO - Seqüência de números e/ou letras criada por um solicitante de certificado no momento da solicitação e utilizada mais tarde para renovar e revogar o certificado digital, conforme exigido pela DPC. A frase de identificação é também utilizada por um detentor de partição secreta para autenticar a si próprio perante o emissor das partições secretas.

G

GERENCIADOR DE CONEXÕES - Mecanismo de transações que executa operações básicas dentro do Centro de Processamento, tais como aprovação, renovação, revogação e recusa de solicitações de certificados.

H

HASHING - É um algoritmo que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resumo - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão), e que o processo reverso também não seja realizável. Dado um hash, não é possível recuperar a mensagem que o gerou.

HIERARQUIA DE CERTIFICADOS - Estrutura de validade de certificados que permite verificar se o emissor de um certificado digital é confiável. Os certificados são emitidos e assinados por outros certificados, localizados

em posição superior na hierarquia. A validade de um determinado certificado é estabelecida pela respectiva validade do certificado anterior.

ICP (INFRA-ESTRUTURA DE CHAVES PÚBLICAS) (PKI - PUBLIC KEY INFRASTRUSTURE) - São as técnicas, a arquitetura, a organização, as práticas e os procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de chave pública.

INDIVÍDUO AFILIADO (AFFILIATED INDIVIDUAL) - Indivíduo relacionado a uma entidade (i) como presidente, diretor, funcionário, sócio, contratado, estagiário ou outra função dentro da entidade, (ii) como membro de uma comunidade de interesses registrada, ou (iii) como um indivíduo que mantém relacionamento com uma entidade principal, que possui negócios ou registros capazes de fornecer comprovação adequada da identidade dos afiliados.

INTEGRIDADE DE DADOS (DATA INTEGRITY) - Situação onde é possível comprovar que um conjunto de dados não foi adulterado ou destruído sem autorização durante sua transferência entre sistemas ou computadores.

INTERFACE DE LINHA DE COMANDO (COMMAND LINE INTERFACE) - Interface de usuário em sistemas operacionais ou aplicativos na qual o usuário digita um comando em uma linha específica, recebe uma resposta do

sistema, digita uma nova linha e assim por diante. O aplicativo Prompt de Comando MS-DOS no sistema operacional Windows é um exemplo de interface de linha de comando.

K

KEY LOGGER - Uma forma de spyware que registra cada batida no teclado ou outra atividade no sistema. Esses programas podem coletar números de cartão de crédito, senha e outros dados delicados e transmiti-los a terceiros.

KRB - Bloco de Recuperação de Chaves.

L

LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL) - LDAP é um protocolo de acesso a diretórios 'leves', que permite a localização de arquivos, pessoas físicas e jurídicas em rede, tanto na Internet como em Intranets corporativas, podendo conter Certificados Digitais de usuários.

LISTA DE CERTIFICADOS REVOGADOS - LCR (CRL - CERTIFICATE REVOCATION LIST) - Lista assinada digitalmente por uma Autoridade Emissora (AE) e publicada periodicamente ou sob demanda, contendo certificados que foram suspensos ou revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programados, além dos números de série dos certificados revogados ou suspensos e das datas e motivos específicos para a suspensão ou revogação.

LISTA DE CONTROLE DE ACESSO (ACL ACCESS CONTROL LIST) - Lista de indivíduos ou entidades (e respectivas senhas) com permissão de acesso a certas áreas específicas de um servidor, rede, aplicação de Internet ou instalações físicas de uma Autoridade Certificadora.

M

MÉTODO DE AUTENTICAÇÃO - Processo de verificação da identidade de um solicitante e da veracidade dos dados da solicitação, como parte do processo de aprovação de uma solicitação de certificado digital. O Serviço de PKI Gerenciada CertiSign oferece três métodos de autenticação: Autenticação Manual, Autenticação por Passcode e Autenticação Automatizada.

MÓDULO CRIPTOGRÁFICO (CRYPTOMODULE) - Software ou hardware que fornece serviços criptográficos, como criptografia, decriptografia, geração de chaves, geração de números aleatórios ou suporte para cartões inteligentes (smart cards).

N

NAVEGADOR DE INTERNET - Aplicativo utilizado para visualizar arquivos HTML, VRML, textos, arquivos de áudio, animação, videoclipes e/ou correio eletrônico pela Internet. Entre os principais navegadores disponíveis no mercado estão: Microsoft Internet Explorer, Netscape Navigator, Opera, etc.

NOME COMUM (COMMON NAME) - Atributo

especificado dentro do Assunto - Nome Distinto (Distinguished Name) - de um certificado. Para certificados de servidor de 40 bits ou 128 bits, o nome comum é o FQDN (Fully Qualified Domain Name) ou nome do "host" DNS do site a ser certificado. Para um Certificado de Assinatura de Software, o nome comum é o nome da organização. Em certificados de assinante, o nome comum é normalmente composto pelo prenome e sobrenome do assinante.

O

OCSP - Protocolo On-line de Status de Certificados.

ONSITE FOR MULTIPLE SERVER IDS - Ver OnSite Server

ONSITE FULL PKI Gerenciada para SSL - versão Premium

ONSITE LITE - PKI Gerenciada Lite

ONSITE SERVER - PKI Gerenciada para SSL

P

PADRÃO DE SINTAXE DE SOLICITAÇÃO DE CERTIFICADO (CERTIFICATE REQUEST SYNTAX (CRS) STANDARD) - Padrão PKCS (#10) que define as informações e o formato exigidos para uma solicitação de certificado de assinante.

PÁGINAS DE ADMINISTRAÇÃO DE CERTIFICADOS (CERTIFICATE MANAGEMENT

PAGES) - Páginas HTML onde o Administrador da PKI Gerenciada desempenha as tarefas diárias de administração dos certificados, como aprovação ou recusa de solicitações.

PERÍODO OPERACIONAL - Período que começa na data e hora em que o certificado foi emitido e termina na data e hora que expira o certificado ou no momento em que ele for suspenso ou revogado.

PKCS #12 - Padrão que especifica um formato portátil para armazenar e transportar as chaves privadas e os certificados dos usuários. Vide também EXTENSÃO .PFX

PKI (PUBLIC KEY INFRASTRUSTURE) - Vide ICP (INFRA-ESTRUTUR D CHAVES PUBLICAS).

PKI GERENCIADA PRIVADA (MANAGED PKI PRIVATE) - Produto que gerencia os processos de solicitação, aprovação, manutenção, renovação e revogação de certificados digitais privados e individuais. Os certificados de PKI Gerenciada Privada de Cliente são assinados por um certificado de AC-Raiz privada e fazem parte de uma hierarquia privada. Por não serem interoperáveis com os aplicativos de uso comum na Internet, como navegadores, servidores e programas de e-mail, estes certificados permitem maior controle em um ambiente fechado.

PKI GERENCIADA PÚBLICA (MANAGED PKI PUBLIC) - Produto que gerencia os processos

de solicitação, aprovação, manutenção, renovação e revogação para certificados digitais públicos e individuais. Os certificados de PKI Gerenciada Pública são assinados pela Autoridade Certificadora Primária de Classe 2 da VeriSign e fazem parte da VeriSign Trust Network. Os Certificados de Cliente Públicos devem aderir a DPC. Os certificados de PKI Gerenciada Pública de Cliente são inter operáveis com aplicativos de uso comum na Internet, como navegadores, servidores e programas de e-mail, permitindo que o usuário deste tipo de PKI comunique-se fora do seu domínio privado.

PC - POLÍTICA DE CERTIFICADOS DA CERTISIGN - É um conjunto de regras que indica a aplicação de um certificado para uma comunidade particular e/ou classe de aplicação com requisitos de segurança. A política de certificado pode ser usada por um usuário certificado para ajudar a decidir se um certificado é confiável o suficiente para uma dada aplicação.

PROGRAMA CGI (COMMON GATEWAY INTERFACE PROGRAM) - Programa executável que obedece às especificações do protocolo CGI – Common Gateway Interface e é utilizado para estender as funcionalidades e capacidades de um servidor de Internet.

PROVEDOR DE SERVIÇOS CRIPTOGRÁFICOS (CRYPTOGRAPHIC SERVICE PROVIDER) - Software que gera o par de chaves pública/privada e executa todas as operações criptográficas, como encriptação e assinaturas digitais, para uma API específica.

PTA (PERSONAL TRUST AGENT) - Módulo da PKI Gerenciada que permite controle de acesso, assinatura digital de formulários e a administração de chaves e certificados.

R

RAIZ - É a primeira CA em uma cadeia de certificação, cujo certificado é auto-assinado, podendo ser verificado através de mecanismos e procedimentos específicos, sem vínculos com este.

RECIBO DIGITAL (DIGITAL RECEIPT) - Bloco de dados assinado digitalmente, incluindo um Selo Cronológico Digital, que forma o recibo ou resíduo enviado a uma parte solicitante para provar que certa transação ocorreu. A CertiSign age como testemunha e emite o recibo digital para confirmar que a transação ocorreu em um momento específico. O Recibo Digital inclui um resumo do documento ou transação, juntamente com a data e hora fornecidos por um serviço confiável de informação de dia e hora, e esse pacote é assinado por uma Autoridade Certificadora CertiSign. Como o recibo é um objeto de dados que persiste no tempo, pode servir como comprovação não-repudiável da ocorrência de uma transação.

REGISTRO AUTENTICADO (AUTHENTICATED RECORD) - Documento assinado contendo a comprovação relevante de autenticação da mensagem, com a assinatura digital verificada por uma parte confiante.

Para fins de notificação de suspensão e revogação, no entanto, a assinatura digital contida na referida mensagem de notificação deve ter sido criada pela chave privada que corresponde à chave pública contida no certificado.

REGISTRO DIGITAL (DIGITAL RECORD) - Serviço oferecido pela CertiSign (e componente dos Serviços de Validação), no qual é emitido um selo cronológico digital e armazena uma comprovação de determinada transação digital (um recibo digital) como parte do Serviço de Notarização Digital. Os registros digitais são armazenados por um período de tempo específico e podem ser disponibilizados no futuro às partes interessadas para fins de auditoria e resolução de disputas, se necessário.

RETIRADA - Processo pelo qual um solicitante de certificado acessa um endereço digital fornecido pela Autoridade Certificadora para retirar um certificado digital pendente, após o envio da solicitação e respectiva aprovação. Depois de retirado, o certificado digital passa a ser considerado emitido.

RSA - É o mais popular sistema criptográfico de chaves públicas criado por Rivest, Shamir e Adleman, capaz de fornecer assinaturas digitais e criptografar textos.

S

SELO CRONOLÓGICO DIGITAL (DIGITAL TIMESTAMP) - Serviço que registra, no mínimo, a data e a hora correta de um ato, além da identidade da pessoa ou equipamento que enviou ou recebeu o selo cronológico. O

Selo Cronológico Digital cria uma confirmação assinada digitalmente e à prova de fraude sobre a existência de uma transação ou documento específico.

SELO DE SITE SEGURO (SECURE SITE SEAL) - Símbolo que indica um ambiente seguro para transações digitais. A presença do selo demonstra que um site possui um Certificado de Servidor de VeriSign ou ICP-Brasil. Além disso, o selo funciona como link para uma página segura que fornece detalhes sobre o certificado digital e o programa CertiSign de Sites Seguros.

S/MIME - Especificação para segurança de e-mail que implementa uma sintaxe de mensagem criptografada num ambiente de Internet MIME. (método seguro de envio de e-mails que utiliza o sistema de criptografia Rivest-Shamir-Adleman). Este método foi sugerido pela RSA como padrão, além de ser utilizado nos softwares de navegação da Microsoft e Netscape.

SENHA - Informações confidenciais de autenticação que em geral são compostas por uma série de caracteres usados para dar acesso a um recurso computacional.

SERVIÇOS DO CICLO DE VIDA - Refere-se à extensão de atividades relacionadas com a manutenção e gerenciamento de Certificados Digitais – tais como revogar, substituir e renovar um Certificado Digital.

SERVIDOR DO BANCO DE DADOS (DATABASE SERVER) - Servidor da área interna do Centro de Processamento que armazena todas as informações

relativas a solicitações de inscrição para certificados (como os certificados emitidos ou revogados).

SERVIDOR DO CENTRO DE CONTROLE (CONTROL CENTER SERVER) - Servidor localizado na área visível ao usuário do Centro de Processamento, que funciona como interface para todas as tarefas executadas por um administrador no gerenciamento de um programa de certificados, incluindo a aprovação e recusa de solicitações de certificados e o download de arquivos.

SERVIDOR DE CERTIFICADOS (CERTIFICATE SERVER) - Programa de software que permite às organizações manter suas próprias infra-estruturas de chaves públicas, podendo criar, assinar e gerenciar certificados digitais sem depender dos serviços de uma Autoridade Certificadora externa. Além do software, as organizações precisam também adquirir o hardware para executar o programa, estabelecer instalações seguras para abrigar o servidor, aprender a configurar e utilizar o software, administrar e fazer cópias de segurança do banco de dados de certificados e garantir a manutenção do sistema ao longo do tempo, o que implica um investimento consideravelmente maior do que o empregado na aquisição de um serviço de PKI Gerenciada.

SERVIDOR DE DIRETÓRIO (DIRECTORY SERVER) - Servidor que hospeda o diretório LDAP em uma empresa ou organização.

SERVIDOR WEB DE GERENCIAMENTO DO ADMINISTRADOR (ADMIN MANAGER WEB

SERVER) - Servidor Web hospedado no Centro de Processamento da CertiSign usado pelos administradores para gerir os certificados de PKI Gerenciada relativos a Empresas, Organizações e Administradores de Sistema.

SIGNATÁRIO - É a pessoa/entidade que cria uma assinatura digital para uma mensagem com a intenção de autenticá-la.

SOLICITAÇÃODEASSINATURADECERTIFICADO CSR (CERTIFICATE SIGNING REQUEST) - Formulário Internet de requisição de um certificado digital no ambiente CertiSign. A CSR, normalmente, contém a chave pública e o Nome Distinto (Distinguished Name) do solicitante.

SOLICITANTE DE CERTIFICADO - Indivíduo ou organização que solicita a emissão de um certificado de chave pública a uma Autoridade Emissora (AE).

SPYWARE – Software que monitora hábitos no computador, como padrões de navegação na Web e transmite a informação de terceiros às vezes a explicita autorização ou consentimento do usuário.

SSL (Secure Sockets Layer) - Protocolo de segurança que provê privacidade na comunicação através da Internet. O Protocolo permite que aplicativos cliente e servidor comuniquem-se utilizando mecanismos criados para proteger o sigilo e a integridade do conteúdo que trafega pela Internet.

SUBSTITUIÇÃO DE CERTIFICADO - Um dos serviços

do Centro de Certificação Digital é o processo de obtenção de substituição de certificado uma vez que o certificado tenha sido revogado usando uma frase de identificação.

T

TÉCNICODEEQUIPAMENTOSCRIPTOGRÁFICOS (CRYPTOGRAPHIC EQUIPMENT TECHNICIAN) - Funcionário do Centro de Processamento responsável por armazenar e manter a segurança/integridade das chaves da Autoridade Certificadora, das chaves Luna e de outros componentes criptográficos. O Técnico de Equipamentos Criptográficos é também responsável pelo transporte de materiais de chaves e pela destruição das chaves obsoletas.

TERCEIRO DE CONFIANÇA - Um terceiro de confiança, em geral independente e imparcial, que contribui para a máxima segurança e confiabilidade das informações permutadas entre os computadores. A CertiSign é um exemplo.

TERMOS DE ADESÃO - É o contrato executado entre o assinante e uma Autoridade Emissora para a provisão dos serviços de certificação de acordo com sua DPC.

TEXTO CIFRADO (CIPHERTEXT) - Conjunto de dados criptografados e ininteligíveis. Vide também Texto Simples, plaintext.

TITULAR DO CERTIFICADO - Uma pessoa, física ou

jurídica, para a qual um certificado tenha sido emitido, que é capaz de usá-lo e que foi autorizada a usá-lo, possuindo a chave privada correspondente à chave pública incorporada ao certificado.

TROJAN - O cavalo de tróia é um programa que parece ter uma função útil, como um game, mais inclui recursos escondidos e potencialmente maliciosos. Às vezes driblam mecanismos de segurança ao tapear os usuários e fazê-los autorizar o acesso aos computadores.

U

UNIFORM RESOURCE LOCATOR (URL) - Um mecanismo padronizado para identificar e localizar certos cadastros e outros recursos localizados na World Wide Web. A maioria das URLs aparecem na forma familiar de endereços de sites, tal como (www.certisign.com.br).

V

VALIDAR CERTIFICADO - Processo realizado por um destinatário ou parte de confiança para confirmar que o certificado de um titular - usuário-final - é válido e era operacional na data e hora que uma assinatura digital pertinente foi criada.

VERIFICAÇÃO (de uma ASSINATURA DIGITAL) - Para determinar com precisão que (i) a assinatura digital foi criada durante o período operacional de um certificado válido por uma chave privada correspondente à chave pública contida no certificado e (ii) que a

mensagem associada não tenha sido alterada desde que a assinatura digital foi criada. (Cf., AUTENTICAÇÃO; CONFIRMAÇÃO)

VERIFICADOR DE CONFIGURAÇÃO (CONFIGURATION CHECKER) - Utilitário fornecido pela CertiSign para o Microsoft Enhanced Cryptographic Provider (1024 bits) durante a instalação do "Go Secure! para Microsoft Exchange". Caso o provedor criptográfico não exista ou esteja incorretamente configurado, o Verificador de Configuração instrui o usuário a instalar o provedor de serviços criptográficos apropriado.

VÍNCULO - Afirmação feita por uma AE - Autoridade Emissora, ou por sua ARL - Autoridade de Registro Local, confirmando o relacionamento entre determinada empresa ou organização e sua chave pública.

VTN (VeriSign Trust Network) - Rede de Confiança da VeriSign

X

X.509 - Modelo ITU-T (International Telecommunications Union-T) para certificados. O X.509 v3 refere-se ao certificado que contenha ou seja capaz de conter extensões.