# Soluções Tempest de Certificação Digital

# Proteção para documentos eletrônicos e aplicações web

**Versão 1.0**

TEMPEST technologies

Rua Jerônimo da Veiga, 164 – 5º Andar
Itaim Bibi – São Paulo – SP – CEP 04536-001
Fone: +55 (81) 3071-4727  Fax: 3168-7452

SAS Qd 01 BL N Ed. Terra Brasilis, 1205/1206
Brasília – DF – CEP 70070-010
Fone: +55 (61) 3225-6773  Fax: 3223-1321

Av. Marquês de Olinda, 126 – 5º Andar – Edf. Citibank
Bairro do Recife – Recife – Pernambuco – CEP 50030-901
Fone/Fax: +55 (81) 3424-3670

# Resumo Executivo

Certificação Digital é o nome genérico de um conjunto de tecnologias que viabilizam diversas formas de proteção para transações eletrônicas realizadas através de redes abertas tais como a Internet. Este texto foca em duas das suas principais aplicações:

- **Proteção contra alterações não autorizadas em documentos eletrônicos**, para que sejam tão amplamente aceitos como como meio de prova de atos jurídicos quanto o são documentos em papel. Exemplo: antes, contratos em geral só eram aceitos juridicamente quando impressos e assinados. Hoje, através da certificação digital, isso pode ser feito em forma totalmente eletrônica – inclusive a assinatura das partes, dispensando até mesmo imprimir o contrato. O resultado é maior agilidade e menores custos.
- **Substituição da identificação via "nome e senha"** comuns em *sites* de serviços, tais como bancos via Internet, lojas virtuais, etc. – hoje fortemente vitimados por emails fraudulentos de recadastramento que exploram uma eventual ingenuidade do usuário final.

Há outros problemas para os quais a Certificação Digital também pode oferecer soluções, tais como guarda de informações confidenciais e sigilo de emails e de comunicações em geral. Todavia, esses problemas já são relativamente bem tratados por outras soluções de mercado; por isso, serão mencionados neste documento de forma bastante superficial.

Este documento está dividido em três partes. A primeira dá uma visão geral da área de certificação digital, sob a ótica de como usá-la para as aplicações citadas acima. A segunda parte detalha a linha de produtos Tempest para usuários finais e provedores de serviços web que se baseiem em certificação digital. A terceira parte cita casos de sucesso onde esses produtos e serviços demonstraram seu valor para nossos clientes e para o público em geral.

O texto foi concebido para ser lido por gestores de TI interessados em ter um primeiro contato com os benefícios da certificação digital e com as soluções Tempest. Tentou-se prover uma abordagem abrangente e didática, mas sem sacrificar o rigor técnico nem quanto aos conceitos, termos e técnicas da área de informática nem quanto às interações com as questões jurídicas.

# Desafio I: Documentos Eletrônicos como Meios de Prova

## Documentos Eletrônicos são Frágeis

Documentos eletrônicos (também chamados de "documentos digitais") são fáceis de modificar sem deixar rastros. Esta é a razão pela qual a maior parte dos contratos, recibos e outros documentos formais ainda são mantidos primariamente em papel – ainda que sejam gerados e gerenciados eletronicamente. É quase um paradoxo: escrevemos nossos textos no computador e quase erradicamos a velha máquna de escrever, mas eles acabam indo parar na impressora – nossos trâmites formais ainda são em papel e não se beneficiam da agilidade e baixo custo das redes de computadores.

O cerne do problema é que, dados dois documentos eletrônicos (digamos, duas versões de um contrato), não há como saber se o primeiro foi feito a partir de uma alteração no segundo ou vice-versa. No mundo digital, os conceitos de "cópia" e "original" se fundem: toda cópia é perfeita e, portanto, indistinguível do original.

De fato, adulterações no mundo digital podem ser feitas de forma a não deixar nenhum rastro perceptível por um perito. Dois exemplos triviais e um mais tecnicamente sofisticado ilustram esse fato:

- Qualquer usuário do Photoshop sabe como é fácil alterar os *pixels* de um documento digitalizado, tal como feito rotineiramente para retocar fotos digitais;
- O administrador de um banco de dados tem poderes irrestritos para alterar qualquer coisa – passando ao largo do controle de acesso e das regras de negócio da aplicação que usa esse banco; e independente se foi autorizado por seu chefe ou não;
- Qualquer bom estudante de informática sabe alterar os bits de um documento do Word para trocar, digamos, "contratante" por "contratada", sem alterar nem o tamanho do arquivo nem a data/hora de alteração registrada pelo sistema operacional.

Todos esses truques técnicos podem ser usados para inverter o sentido de cláusulas de contratos, bem como retirar ou acrescentar signatários. Por isso, em caso de uma disputa contratual, pode se tornar extremamente difícil estabelecer qual versão é a correta e qual é a fraudulenta. Isso freqüentemente leva a avaliações indiretas, subjetivas, requerendo interpretação detalhada do contexto (que dá muito mais trabalho e leva bem mais tempo), com resultados nem sempre justos ou satisfatórios para as partes.

Essa é uma das razões mais fortes pelas quais os operadores do Direito relutam em adotar os meios eletrônicos e insistem em usar o "bom e velho papel": eles temem que a fragilidade dos documentos eletrônicos dificulte seu trabalho, ao invés de ajudar.

## O Par de Chaves e a Assinatura Digital

A certificação digital traz a solução para esse problema – a cada usuário são distribuídas duas peças:

- **Uma chave privada:** um número especial que representa unicamente o usuário dentro dos sistemas de certificação digital. Esse número, quando usado em conjunto com programas de computador apropriados, permite que o usuário crie as chamadas *assinaturas digitais* que podem vir a ter tanto valor quanto sua assinatura manuscrita.
- **Um certificado digital de usuário:** um outro arquivo de computador que contém a) uma *chave pública* que corresponde unicamente à chave privada mencionada acima e que permite que assinaturas digitais por ela realizadas possam ser *conferidas* – ou seja, ter sua autenticidade verificada; e b) uma *identificação* (nome civil, matrícula, RG, CPF, etc) do titular daquelas chaves.

Consideremos um exemplo: Tício quer firmar um contrato digital com Caio. Após redigir o contrato, ele gera uma assinatura digital, usando três insumos:

- o próprio documento a ser assinado;
- sua chave privada;
- um programa gerador de assinaturas digitais (ou apenas **assinador**, para abreviar).

A assinatura digital resultante é um número que serve como código de conferência que é anexado ao documento e será usada logo adiante para determinar sua autoria e autenticidade.

O cálculo da assinatura digital é um procedimento matemático já amplamente conhecido e estudado pelos cientistas, cujos detalhes omitiremos por simplicidade; nesse documento, interessam-nos mais os resultados e menos a técnica. Tudo que precisamos saber é que existem programas de computador capazes de efetuar esses cálculos e peritos que entendem como eles funcionam.

O conjunto documento+assinatura, apelidado de **documento assinado**, é então enviado a Caio, digamos, via correio eletrônico ou através de um *web site*.

Ao receber o contrato assinado, a primeira coisa que Caio deve fazer é conferir a assinatura. Para isso, usa quatro ingredientes:

- o documento a ser conferido;
- a assinatura digital que veio com o documento;
- a chave pública do signatário presumido, normalmente contida dentro do seu certificado digital;
- um programa conferidor de assinaturas (ou apenas **conferidor**, para abreviar).

Há dois possíveis resultados que o programa conferidor pode fornecer:

- Se a assinatura estiver **INVÁLIDA**, tem-se uma "rasura digital": ou o documento conferido não é idêntico ao assinado, ou foi assinado por uma chave privada que não corresponde à chave pública usada na conferência. Se isso acontecer, Caio deve simplesmente desconsiderar o documento.
- Se a assinatura estiver **VÁLIDA**, significa que o documento conferido é idêntico bit a bit ao que foi assinado; e significa, também, que ele foi assinado pela chave privada que corresponde à chave pública usada na conferência. Lembrando que o certificado traz a identificação civil do titular daquelas chaves, fica então estabelecida a identidade do signatário. Nessa situação, Caio tem tudo para aceitar o documento.

Após aceitar o documento, Caio contra-assina; ou seja, usa seu programa assinador para gerar uma nova assinatura a partir daquele documento e da sua chave privada. Essa nova assinatura é anexada ao documento, que Caio envia de volta para Tício. Este, por sua vez, confere a assinatura de Caio e, se estiver válida, o contrato virtual está firmado.

Naturalmente, esse processo não funciona só com contratos; pode funcionar de forma análoga com processos judiciais, notas fiscais, ordens de serviço, laudos, diplomas e muitos outros tipos de documentos.

## Documentos Assinados são Robustos

A seção anterior nos ensina que ao agregarmos assinaturas digitais aos documentos eletrônicos, elas agem como uma espécie de lacre: qualquer tentativa de adulterá-los "quebra os lacres", tornando a adulteração fácil de detectar.

Assim, incorporando-se a conferência da assinatura como etapa essencial para a aceitação de um documento, pode-se dizer que isso agrega aos documentos eletrônicos um "poder de atuar como prova de uma verdade" comparável, se não maior, do que gozam os documentos em papel. Por se basearem em uma técnica científica, convencem não apenas as partes, mas também terceiros – tornando-os especialmente adequados para perícias científicas e, portanto, servindo como forte evidência em caso de disputas judiciais.

Isso nos autoriza a usar o termo "documento assinado", deste ponto em diante no texto, como significando "documento eletrônico com uma ou mais assinaturas digitais anexas". Qualquer outro significado, como no caso de assinaturas manuscritas em papel, será explicitado.

Vale enfatizar esse ponto: *qualquer* intermediário que adultere um documento assinado invalida a assinatura, o que será prontamente detectado pelo receptor ao conferi-la. Esse intermediário pode ser até o administrador da rede, com todas as senhas administrativas ou de "super-usuário" dos sistemas que gere, ou mesmo uma agência de inteligência internacional, não importa – a técnica na qual as assinaturas digitais se baseiam oferece garantias científicas de que ninguém tem como nem adulterar um documento digital assinado, nem forjar assinaturas digitais, sem poder ser detectado. É justamente a extrema força dessa garantia que tem tornado essa tecnologia tão desejável.

Outro apelo forte desta tecnologia é que a conferência das assinaturas é inteiramente automatizada, viabilizando criar sistemas que simplesmente rejeitem documentos que não estejam com as assinaturas válidas e dos signatários esperados – conciliando, assim, segurança jurídica com a agilidade e baixo custo da automação.

Para que as assinaturas digitais possam então realizar seu potencial de proteger transações eletrônicas, é essencial ter ferramentas de geração e conferência de assinaturas digitais que sejam fáceis, práticos de usar e que se integrem bem com o que já existe. Estes são alguns dos objetivos do Tempest ViaCert: atuar como assinador/conferidor para o usuário leigo de forma fácil, conveniente, totalmente integrada ao navegador e ao sistema operacional.

## O Certificado Digital e as Autoridades Certificadoras

Se não existissem os certificados digitais, os programas de conferência nos mostrariam a chave pública dos signatários quando as assinaturas fossem classificadas como válidas. Uma vez que as chaves públicas são números de mais de duzentos dígitos, não seria muito fácil saber a quem ela se refere. Com o certificado digital, os programas de conferência nos mostram qual o nome do titular daquela chave pública. É muito mais intuitivo ler o nome do signatário do que um número gigante.

Ou seja, o certificado digital é um tipo de “cartão de visita” para o mundo eletrônico: ele associa seu nome (ou CPF, ou número de identificação funcional, ou alguma coisa que faça sentido no âmbito em que for usado) a uma chave pública. A despeito da mística em torno do certificado digital, sua função é apenas essa: traduzir um número que o computador entende – a chave pública – em algo que, nós, humanos, entendemos – o nome do titular.

Tal como um cartão de visita, é do nosso interesse distribuir várias cópias do certificado – isso faz com que nossas assinaturas possam ser reconhecidas. É comum enviá-lo anexado às assinaturas digitais, precisamente para facilitar a vida de quem for conferi-la.

Se o certificado digital fosse apenas a junção do nome do titular com sua chave pública, ele seria apenas um documento digital comum – e como tal, tão fácil de forjar quanto qualquer outro. Isso não ocorre porque ele foi assinado previamente por uma entidade chamada Autoridade Certificadora (ou AC, para abreviar).

A função de uma Autoridade Certificadora é oferecer algum tipo de garantia de que um dado certificado seja mesmo daquele titular. Em geral, elas só assinam os certificados se os titulares puderem provar quem são; os critérios exatos e o rigor variam de AC para AC – algumas requerem sua presença física e cópias de seus documentos, conferem sua foto com a da sua cédula de identidade, entre outros requisitos. Outras simplesmente verificam se o candidato consegue receber correio eletrônico no endereço que ele especificou.

O significado legal exato dessa garantia depende do contrato de prestação de serviços de cada AC. Elas publicam documentos chamados Declarações de Práticas de Certificação (DPCs, para abreviar) explicitando esses procedimentos e garantias.

Todo programa que usa certificados digitais confere as assinaturas digitais neles contidos antes aceitá-los. Se forem válidas, os programas exibem os nomes dos titulares baseando-se nas garantias oferecidas pelas ACs. Caso contrário, alertam o usuário de que a identidade dos signatários não é garantida.

## Documento Digital vs em Papel, Assinatura Digital vs Manuscrita

Um outro ângulo interessante de encarar essa tecnologia é contrastar o mundo digital com mundo do papel. Abaixo apresentamos um quadro comparando esses dois mundos sob vários aspectos.

| QUADRO COMPARATIVO: CARACTERÍSTICAS DOS DOCUMENTOS E ASSINATURAS DIGITAIS VERSUS EM PAPEL | | |
|---|---|---|
| Característica | Assinatura Digital em Documento Eletrônico | Assinatura Manuscrita em Documento em Papel |
| *Natureza* | É um número grande; | É um traço de tinta desenhado em um papel; |
| *Como é criada* | Por um programa de computador, através de um processo matemático, sob as ordens do signatário; | Pelo próprio punho do signatário; com uma caneta, diretamente no papel; |
| *Insumos que o signatário precisa ter* | Computador com programa assinador, identidade digital (chave privada+certificado) já emitida, documento a ser assinado em um arquivo; | Caneta e documento em papel a ser assinado; |
| *Velocidade da geração* | Dezenas a milhares por segundo, quando automaticamente por um computador; quando requer interação do usuário, leva alguns segundos, a maior parte deles na digitação da frase-senha; | Alguns segundos, por humanos. Quase nunca feito por computador; |
| *Relação com o teor do documento* | Calculada em função do teor documento, de sorte que a validade da assinatura implica em que os bits do documento conferido são idênticos aos do assinado; | Nenhuma, de sorte que assinatura e teor do documento são avaliados independentemente; |
| *Como é conferida* | Por um programa de computador, através de outro processo matemático, sob o comando de quem recebe o documento assinado; | Visualmente, por semelhança com um padrão; Computadores também são capazes de detectar as semelhanças, mas são menos precisos |
| *Insumos que o conferidor precisa ter* | Computador com programa conferidor, documento assinado (documento + sua respectiva assinatura digital), certificado contendo a chave pública do signatário (normalmente contido dentro da própria assinatura) | Para uma verificação não-rigorosa, basta a capacidade de visão inata do ser humano; Verificação altamente rigorosa pode requerer lupas, microscópios e luzes especiais, além de conhecimentos em caligrafia, tipo de papel, redação e estilística, etc. |
| *Velocidade da conferência* | Centenas a dezenas de milhares por segundo, automaticamente, por computador; trabalhosa demais para ser feita por um humano; | Uma a cada alguns segundos, por humanos; dezenas por segundo, por computador; |
| *Exclusividade presumida do signatário* | A chave privada; | A habilidade de grafar consistentemente um traço específico; |
| *Unicidade* | Sempre diferente para cada documento; | Aproximadamente a mesma para diferentes documentos; |
| *Precisão típica da conferência* | 100%, por se basear em um processo matemático exato; | Menor que 98%[1], no caso de verificação por computador. |
| *O que informa* | Tanto a identidade do signatário quanto a integridade do documento; posse da chave privada no momento da assinatura. | Apenas a identidade do signatário; nada informa sobre o conteúdo em si. |

[1] Baseado no melhor resultado apresentado no relatório da I Competição Internacional de Verificação de Assinaturas (http://www.cs.ust.hk/svc2004). Vale observar que a abordagem das soluções automáticas de reconhecimento de assinaturas usada nesse concurso é a chamada *verificação dinâmica*, em que o usuário rascunha sua assinatura em uma prancheta digitalizadora, de sorte que o computador tem acesso a informações de movimento e pressão da caneta. Na literatura técnica do ramo, há um consenso de que técnicas de *verificação estática*, como no caso de uma assinatura previamente feita em papel e digitalizada com um *scanner*, são substancialmente menos precisas. Note-se, porém, que apesar da taxa de erro relativamente alta, tecnologias desse tipo são amplamente empregadas no setor bancário.

| QUADRO COMPARATIVO: CARACTERÍSTICAS DOS DOCUMENTOS E ASSINATURAS DIGITAIS VERSUS EM PAPEL | | |
|---|---|---|
| Característica | Assinatura Digital em Documento Eletrônico | Assinatura Manuscrita em Documento em Papel |
| *Alvo preferido do fraudador: documento ou assinatura?* | Irrelevante – qualquer alteração tanto no documento quanto na assinatura é prontamente detectado pela conferência; | Costuma ser mais fácil adulterar o documento do que alterar a assinatura ou inventar uma assinatura do nada, mas todas essas possibilidades acontecem na prática; |
| *Viabilidade técnica de forjar* | Impraticável, mesmo com acesso aos maiores supercomputadores do mundo; tão difícil que na prática raramente é tentado, posto que ludibriar o usuário por outros meios parece mais viável; | Em meio físico, viável, variando com a habilidade do falsário em imitar o traço e os materiais (papel, tinta) à sua disposição;<br>Em meio eletrônico, extremamente fácil, com uso de programas de edição de imagens e retoque digital; |
| *Viabilidade técnica de conferir* | Acessível a qualquer um que tenha acesso a um computador pessoal comum e a um programa conferidor; | Intuitiva, inata ao ser humano, por semelhança visual, ainda que o rigor varie bastante;<br>Viável por computadores, ainda que com menos precisão; |
| *Facilidade de enganar um conferidor casual* | Muito difícil – como a conferência é feita por computador, nenhuma conferência é casual; todas são rigorosas. | Fácil; |
| *Facilidade de enganar um perito* | Extremamente difícil – a natureza matemática do processo dá resultados extremamente precisos; há muito pouca margem para interpretação subjetiva, sendo fácil obter consenso entre vários peritos; | Difícil, mas acontece: há diversos casos na história em que diferentes peritos discordam; |
| *Ocorrência de falsificações na prática que causaram prejuízo* | Não se tem notícia de nenhum caso que tenha envolvido falha na tecnologia em si; alguns casos isolados em que hove falha humana no processo de identificação dos usuários; | Rotineira, com milhares de casos registrados na História; há filmes de Hollywood inspirados em histórias verídicas de falsários bem sucedidos; |
| *Tempo desde a invenção* | Três décadas – o primeiro sistema viável foi introduzido em 1976; | Milhares de anos – não há consenso entre os historiadores sobre quando começou a ser usada; |

## Validade Jurídica dos Documentos Eletrônicos

Um tema recorrente nas discussões sobre o uso de assinaturas digitais em documentos eletrônicos é se elas têm ou não validade jurídica quando feitas com os certificados dessa ou aquela Autoridade Certificadora ou Infra-Estrutura de Chaves Públicas. A resposta curta é: sim, independente de qual Autoridade Certificadora o emitiu.

A resposta longa requer primeiro entender que próprio termo "validade jurídica" é inapropriado, pois, segundo vários juristas, ele não tem significado algum. Explica-se: o código civil brasileiro afirma que a forma de acordo entre as partes é livre e admite até contratos verbais. Nesse contexto, pode-se afirmar que *qualquer coisa* pode ter validade jurídica – a questão é como provar.

Dois exemplos tornam essas distinções claras: se Tício e Caio firmam um contrato verbal e depois o disputam em juízo, a decisão será difícil porque será a palavra de um contra a do outro; os testemunhos das partes tendem a se equilibrar. Contudo, se Caio fez a promessa televisionada ao vivo e gravada, a gravação e o fato de ter sido vista por muitas pessoas é uma evidência forte o bastante para favorecer uma das partes bem mais que a outra.

No jargão jurídico, diz-se que a gravação do evento televisionado tem maior **eficácia probante** – ou seja, capacidade de servir como evidência de um fato – do que um testemunho, por ser feita por um processo que nada tem a ver com os interesses das partes.

A lição é: no Direito, diferentes tipos de evidência podem ter diferentes eficácias probantes. Textos em papel são amplamente aceitos como sendo mais adequados como evidência do que meros testemunhos, especialmente quando seguindo regras de forma e conteúdo padronizados. Isso se fundamenta no fato que

um texto, uma vez colocado no papel, não muda sozinho; e qualquer mudança deixa evidências físicas que, em princípio, podem ser rastreadas por um perito em caso de dúvida.

Essa mesma lógica explica por que as assinaturas digitais agregam alta eficácia probante aos documentos eletrônicos: por se basearem em processos matemáticos, qualquer dúvida sobre a autoria ou autenticidade de um documento pode ser resolvida com uma perícia técnica de forma objetiva, contundente e auditável.

Na prática, raramente há a necessidade de se recorrer ao perito: através de programas de computador tais como o Tempest ViaCert, é possível mesmo para leigos conferir assinaturas com a mesma precisão de uma perícia técnica.

Diferentes Autoridades Certificadoras usam diferentes dispositivos legais para conferir maior ou menor força em juízo às assinaturas geradas por identidades digitais por elas emitidas. Para dar alguns exemplos:

- À época em que esse documento foi escrito, as autoridades certificadoras da ICP-BR (www.icpbrasil.gov.br) se calcavam na Medida Provisória 2200-2;
- A ICP-OAB (http://cert.oab.org.br) se vale do seu Provimento 97/2002 e do Estatuto Advocacia e da Ordem dos Advogados do Brasil (Lei Nº 8.906 de 4 de julho de 1994, publicada no Diário Oficial da União de 5/07/94);
- Autoridades Certificadoras internas de empresas particulares – por exemplo, uma empresa que queira fazer com que seus funcionários assinem digitalmente seus trâmites – se sustentam em seus próprios contratos de trabalho;
- Empresas privadas que queiram tramitar em âmbito digital podem firmar um instrumento particular em que reconhecem mutuamente os certificados umas das outras, ou elegem uma Autoridade Certificadora em que confiem;
- Certas instituições públicas têm autonomia para identificar seu público dentro da sua área de atuação: por exemplo, secretarias da fazenda têm alguma autonomia para identificar seus contribuintes, podendo optar por hospedar sua própria Autoridade Certificadora ou contratar os serviços de alguma AC de mercado.

## Desafio II: O *Site* Precisa Saber Quem Sou

Quando um *site* na *web* quer oferecer serviços personalizados aos usuários, a maneira padrão de identificá-lo é associando-lhe um **nome e senha**. Esse nome pode ser um número identificador, o endereço de correio eletrônico do usuário, seu nome civil, número do CPF, etc; pode ser também o número da sua conta e agência, no caso dos bancos. Todas essas soluções têm um ponto comum: a guarda conjunta – tanto por parte do *site* quanto do usuário – de uma senha secreta.

É difícil negar que o uso de senhas está atingindo o limite da exaustão – o usuário *online* hoje tem tipicamente tantas senhas em tantos serviços que acaba colocando a mesma senha na maioria, senão em todos; furto de bancos de dados de senhas vez por outra viram manchetes. Contudo, os falsos emails de "promoções" e "recadastramento" – os chamados *phishing scams* – são sem dúvida os ataques que mais causam prejuízos a bancos, lojas virtuais e outras instituições.

As assinaturas digitais provêem um meio para se proteger dessas ameaças: com elas, os *sites* podem reconhecer seus usuários sem jamais precisarem tomar conhecimento de suas respectivas senhas. A idéia é reconhecê-los pelos seus certificados digitais e por sua capacidade de gerar assinaturas digitais válidas.

Conceitualmente, funciona através de um esquema chamado **protocolo desafio-resposta**: o *site* gera um documento eletrônico consistindo de um número aleatório (grande, da ordem de uns quarenta dígitos) chamado **desafio** e manda para o navegador do usuário. Este, por sua vez, assina digitalmente esse documento usando sua chave privada e manda a chamada **resposta**. O *site* então usa o certificado digital para conferir a assinatura contida na resposta. Se estiver válida, ela consiste em uma **prova de posse**: demonstra cientificamente que o usuário do outro lado da linha detém *naquele momento* a chave privada correspondente àquele certificado digital (ou, mais precisamente, à chave pública contida naquele certificado digital).

### O Protocolo HTTPS

O protocolo HTTPS é um aprimoramento do HTTP que incorpora autenticação através de desafio-resposta e proteção contra interceptação. Praticamente todos os servidores web modernos, tais como o Apache e o IIS (Microsoft Internet Information Services), já o suportam nativamente – bem como a maioria dos navegadores, tais como o Internet Explorer, o Mozilla ou o Firefox. O famoso "cadeado amarelo" aparece na barra de status do navegador para indicar quando ele está conectado ao servidor através de uma conexão HTTPS.

Nesse momento, é oportuno distinguir as duas modalidades de autenticação oferecida pelo protocolo HTTPS:

- **Autenticação do Servidor:** o servidor *web* tem sua própria chave privada e a usa para assinar desafios enviados pelo navegador. Se a assinatura digital da resposta estiver válida; o certificado estiver dentro da validade e tiver sido classificado como legítimo; e o nome do site que consta no certificado for o mesmo do site que estamos tentando acessar, significa que podemos contar com a garantia da Autoridade Certificadora de que estamos acessando o site correto.

  Essa é a modalidade usada atualmente por praticamente todo banco via Internet e pelos grandes *sites* de comércio eletrônico, tais como a `amazon.com`, `americanas.com`, etc. Ela é superior ao HTTP puro porque pelo menos dificulta a captura de senhas à medida em que trafegam pela Internet. Entretanto, esses sites ainda precisam manter bancos de dados das senhas de seus usuários e pedi-las toda vez que precisarem saber quem é o usuário. Isso os torna sucetíveis a ataques técnicos, vazamento acidental ou intencional dessas senhas, ou, mais frequentemente, a sites-clone e falsos emails de recadastramento que tentam induzir o usuário a fornecerem seu nome+senha.

- **Autenticação Mútua:** tanto o servidor se autentica perante o cliente quanto o cliente se autentica perante o servidor. Nessa situação o *site* não pede a senha do usuário; ao invés, manda um desafio para ser assinado. Relembrando que a cada chave privada está associada uma única chave pública; e que o certificado carrega consigo o nome do titular da chave pública, o *site* sabe quem é o titular com quem está falando – cuja identidade goza das garantias oferecidas pela Declaração de Práticas de Certificação da Autoridade Certificadora que emitiu o certificado.

  Tudo isso traz vantagens únicas: a senha do usuário jamais trafega pela Internet nem o *site* sequer precisa ter conhecimento dela. Do lado do servidor, desaparece a figura do banco de dados de senhas, sendo substituído por um banco de dados de certificados – cuja guarda, por serem públicos, dispensa cuidados especiais.

  Até bem pouco tempo atrás esse método era pouco popular, pois requeria mudanças profundas nas aplicações *web* e devido ao fato de o uso de certificados digitais de usuário ser rebuscado nos navegadores populares. Usando-se a suite ViaCert e ViaProxy, tudo isso mudou: o ViaProxy permite migrar a autenticação de um site de nome+senha para certificado digital virtualmente da noite para o dia, quase sempre sem a necessidade de alteração no código; e o ViaCert complementa o navegador, tornando o uso do certificado digital fácil e simples no lado do usuário.

## Outras Aplicações da Tecnologia de Certificação Digital

A certificação digital é, na realidade, uma sub-disciplina de uma área da ciência chamada "Criptografia de Chaves Públicas". Essa área do conhecimento oferece também proteções contra outras ameaças; por exemplo, pode-se usar as mesmas chaves privadas e certificados digitais usados na assinatura digital para um propósito totalmente diferente: transmitir mensagens "embaralhadas" (**criptografadas**, no jargão da área) para que um interceptador que porventura esteja "grampeando a linha" não as compreenda. Em outras palavras, esse recurso oferece **sigilo de comunicações**.

De fato, o ViaCert oferece esse recurso na parte de identificação segura em sites web: além da assinatura digital servir como prova de posse da chave, o canal de comunicação usa as técnicas de criptografia mencionadas anteriormente para evitar que qualquer intermediário compreenda os dados transmitidos.

# As Soluções Tempest

## Tempest ViaCert

O ViaCert é um programa utilitário que agrega ao seu sistema operacional, seja ele Windows ou Linux, várias funcionalidades para geração e conferência de assinaturas digitais, criação de novas identidades digitais (pares chave privada + certificado digital) e gerência do seu ciclo de vida. Ele acrescenta ao seu sistema operacional suporte ao formato padrão de assinaturas digitais, chamado PKCS#7 e vários outros tipos de arquivos correlatos, como certificados digitais, chaves privadas, listas de certificados revogados, etc – de modo análogo a como o WinZIP agrega suporte a arquivos compactados pelo formato ZIP.


**Figura 1:** O **ViaCert** acrescenta suporte a geração e conferência de assinaturas digitais facilmente, através de um clique no botão direito do mouse por sobre o ícone do arquivo, ou simplesmente dando um duplo-clique nos arquivos tipo .P7S, que são o formato padrão para assinaturas digitais.

Além disso, o ViaCert também oferece esses mesmos recursos no ambiente Web. Através deles, o usuário pode assinar compras ou contratos eletrônicos de forma natural e intuitiva.

Através do ViaCert, o usuário tem a disposição os seguintes recursos:

- **Geração de Assinaturas:** pode-se criar assinaturas digitais em arquivos ou em formulários web que atuam como "lacre de proteção" contra alterações; vários signatários podem assinar um mesmo documento – essencial para contratos ou abaixo-assinados digitais que envolvem múltiplas partes;
- **Conferência de Assinaturas:** ferramentas para conferir a validade das assinaturas de forma rápida e simples; assinaturas válidas garantem que não houve rasura digital, ao mesmo tempo em que identificam os signatários;

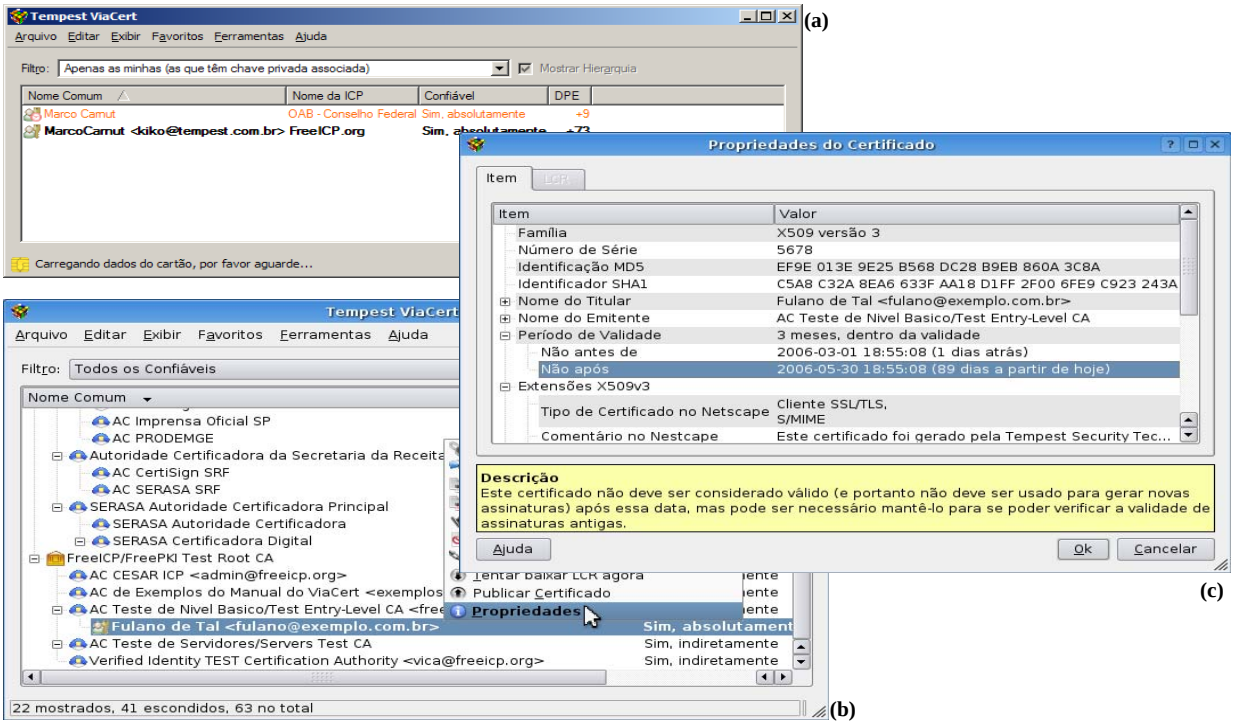


**Figura 2:** Uma demonstração do **ViaCert** em várias plataformas e como ele pode satisfazer tanto leigos quanto usuários avançados. Em **(a)**, tem-se um instantâneo do uso da versão Windows. Inicialmente, o **ViaCert** só mostra as identidades digitais que pertencem ao próprio usuário; neste exemplo, ele tem duas, emitidas por ICPs diferentes. Uma delas está mostrada em vermelho e com um ícone de um relógio, simbolizando que está para expirar em poucos dias (nove, de acordo como campo "Dias Para Expirar"). A foto foi tirada no momento em que o usuário acabara de inserir um *smart card*, como evidencia a mensagem na barra de status. Em **(b)**, vemos o **ViaCert** para Linux, rodando sob o KDE 3.4 com o esquema visual "Plastik". Nesse exemplo, o usuário ativou a exibição de todos os certificados classificados como confiáveis, fazendo aparecer a árvore hierárquica das várias ICPs e suas Autoridades Certificadoras. O usuário pediu as propriedades desse certificado, mostradas em detalhe em (c), ilustrando como o **ViaCert** pode prover todos os detalhes técnicos para satisfazer até mesmo peritos técnicos.

- **Login seguro:** Permite usar assinaturas digitais para acesso em sites web ao invés de nome e senha: proteção natural contra *phishing scams* e outras fraudes comuns;
- **Emissão Simplificada da Identidade Digital:** Simplifica a emissão de certificados digitais tanto em Autoridades Certificadoras gratuitas quanto comerciais;
- **Gerência do Ciclo de Vida dos Certificados:** Avisa quando os seus certificados estão próximos de expirar e facilita o processo de renovação;
- **Simplificação dos Backups e exportação/importação:** Gerencia os vários certificados digitais do próprio usuário e dos indivíduos/instituições com quem interage, inclusive realizando cópias de segurança (*backups*) das chaves privadas e sua respectiva recuperação, além de auxiliar na transferência segura da chave privada de um computador para o outro;
- **Suporte a Revogação de Certificados:** Gerencia Listas de Certificados Revogados, avisando quando seus certificados ou de terceiros tiverem sido revogados;
- **Compatibilidade Ampla:** Compatível com qualquer certificado aderente ao padrão X.509/RFC3280, o que inclui todas as Autoridades Certificadoras brasileiras (incluindo as da ICP-BR, ICP-OAB, FreeICP) e do exterior (VeriSign, Thawte, etc.), inclusive com os certificados tipo A1 e A3 da ICP-BR; e com qualquer programa que utilize o formato PKCS#7 para assinaturas digitais;
- **Assinaturas Digitais na Web:** Integra-se naturalmente aos navegadores que suportam proxies, entre eles o Internet Explorer e o Mozilla, entre outros, permitindo usar os recursos de assinatura digital em sites Web que tenham suporte a esses recursos.

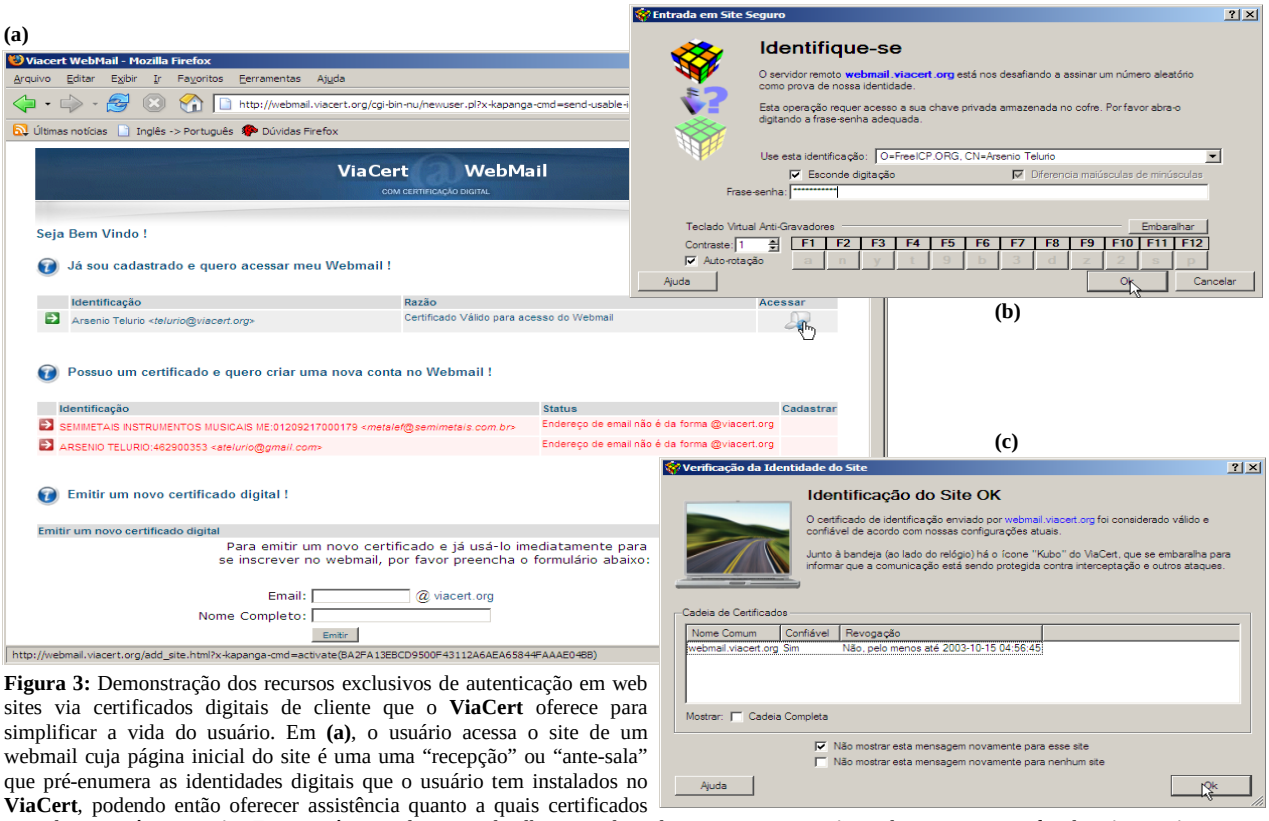


**Figura 3:** Demonstração dos recursos exclusivos de autenticação em web sites via certificados digitais de cliente que o **ViaCert** oferece para simplificar a vida do usuário. Em **(a)**, o usuário acessa o site de um webmail cuja página inicial do site é uma uma "recepção" ou "ante-sala" que pré-enumera as identidades digitais que o usuário tem instalados no **ViaCert**, podendo então oferecer assistência quanto a quais certificados considera aceitáveis ou não. Este site é particularmente detalhista, explicando exatamente as razões pelas quais os certificados são ou não aceitos. No final da página, vemos que o usuário pode até iniciar o processo de emissão de um novo certificado digital diretamente desta página. No exemplo, contudo, o usuário já tem um uma conta no webmail associada a um dado certificado; por isso, ele prossegue diretamente para dar entrada no sistema. Ao clicar no ícone "acessar", o **ViaCert** mostra a janela de autenticação **(b)**, onde o usuário é convidado a digitar a frase-senha que autoriza o uso da sua chave privada para gerar a asssinatura do desafio enviado pelo site. Note que essa senha jamais sai do computador do usuário nem em momento algum transita pela rede. Em **(c)** o site retribui, autenticando-se também, quando então aparece uma janela indicando que o **ViaCert** considerou a identificação do site válida de acordo com suas configurações atuais e que o certificado do site não foi revogado pelo menos até a última edição da Lista de Certificados Revogados emitida por sua Autoridade Certificadora. Essa mensagem normalmente só aparece na primeira vez que se entra em um site, para não aborrecer o usuário com o óbvio toda vez. O usuário tem a chance de examinar o certificado do site, caso deseje. Assim, tem-se a perfeita combinação de rapidez e simplicidade com a possibilidade de entrar em detalhes sempre que o usuário quiser.

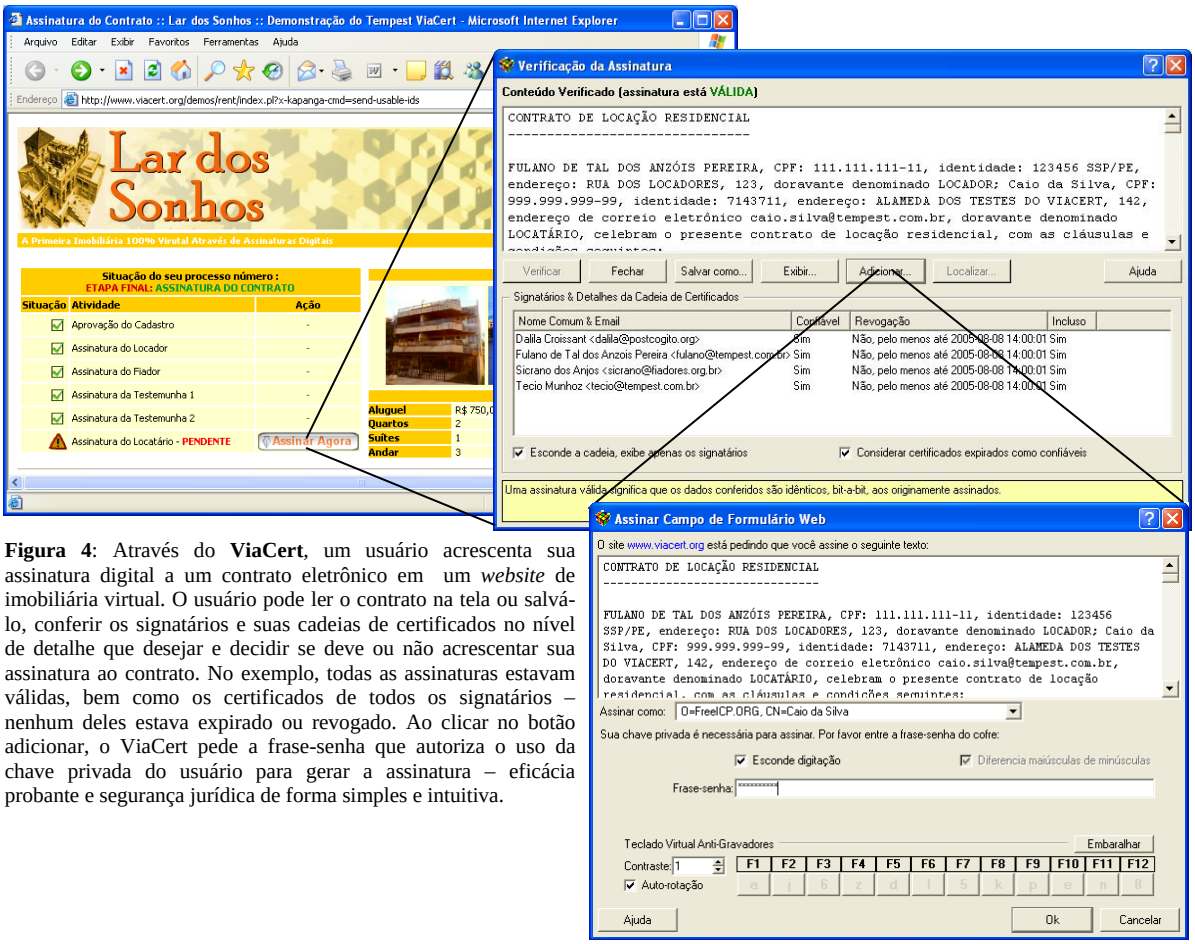


**Figura 4**: Através do **ViaCert**, um usuário acrescenta sua assinatura digital a um contrato eletrônico em um *website* de imobiliária virtual. O usuário pode ler o contrato na tela ou salvá-lo, conferir os signatários e suas cadeias de certificados no nível de detalhe que desejar e decidir se deve ou não acrescentar sua assinatura ao contrato. No exemplo, todas as assinaturas estavam válidas, bem como os certificados de todos os signatários – nenhum deles estava expirado ou revogado. Ao clicar no botão adicionar, o ViaCert pede a frase-senha que autoriza o uso da chave privada do usuário para gerar a assinatura – eficácia probante e segurança jurídica de forma simples e intuitiva.

- **Gerência dos Documentos Assinados na Web:** Armazena formulários Web assinados digitalmente pelo usuário ("recibos digitais"), para consulta ou referência futura;
- **Suporte a dispositivos criptográficos:** as chaves privadas e certificados podem ser armazenados em *smart cards* ou *tokens* criptográficos aderentes ao padrão PC/SC;
- **Suporte a guarda das identidades digitais em mídia removível:** suas chaves privadas e certificados podem ficar armazenados em *pendrives* ou CD-ROMs.
- **Multiplataforma:** O ViaCert está disponível tanto para Windows quanto Linux; e se integra automaticamente com o Internet Explorer, o Mozilla e o Firefox.

## Tempest ViaProxy: Migração Rápida de seus Aplicativos Web

Apesar dos servidores Web modernos (tais como o Apache e o IIS - Internet Information Services da Microsoft) já oferecerem suporte a proteção baseada em certificados digitais, um desenvolvedor que deseje agregar aos seus serviços web a proteção oferecida pela tecnologia de certificação digital invariavelmente se depara com a necessidade fazer alterações profundas nos seus servidores e sistemas aplicativos: identificar os usuários por certificado digital nativamente requer instalação de bibliotecas adicionais para suportá-los e mudanças significativas nas regras de negócio das aplicações.

Aliado ao fato que a maioria dos desenvolvedores de soluções Web têm pouca familiaridade com o uso dessa tecnologia, historicamente os resultados ficavam bastante aquém do esperado, com os prazos e custos envolvidos muito além da expectativa inicial.

Quando instalado em uma rede, o Tempest ViaProxy permite transformar um site que identifique seus usuários por nome e senha em um que os identifique por certificado digital literalmente da noite para o dia, quase sempre sem a necessidade de alterar praticamente nada no site original e sem a necessidade de se tornar um especialista em certificação digital.

Ele consiste em um software que é executado em um computador separado que se interpõe entre os servidores de aplicação e a Internet. É uma espécie de "*firewall* de certificação digital": ele recebe as

transações web protegidas via o protocolo HTTPS, valida os certificados digitais e/ou assinaturas digitais que vierem e os repassa já validados para os servidores de aplicação originais. Esse processo oferece os seguintes benefícios:

- **Proteção:** Agrega ao site todos os benefícios da proteção por certificação digital, tais como identificação segura do usuário e validação instantânea de assinaturas digitais.
- **Compatibilidade Retroativa:** Não é necessária reescrita de código, reengenharia nem nenhum tipo de mudança ou intervenção nos servidores de aplicação: a migração é suave, rápida e indolor;
- **Coexistência e migração gradual com nome+senha:** É possível ter-se autenticação por nome e senha e por certificado digital simultaneamente; pode-se configurar para que nome+senha seja um meio de autenticação alternativo caso o usuário não tenha ainda certificado, a autenticação tenha falhado por alguma razão (certificado revogado, encadeamento incompleto, etc) ou por qualquer outro critério desejado;
- **Performance:** O impacto de performance causado pela criptografia é tratado no próprio ViaProxy – os servidores web originais não sentem esse impacto, mantendo as características conhecidas de performance e estabilidade do sistema, reduzindo o risco associado a migrações complexas;
- **Escalabilidade e Confiabilidade:** dois ou mais ViaProxies podem ser configurados em agrupamento tipo "cluster", permitindo um aumento gradual da capacidade de atendimento do site de acordo com a necessidade e em configurações de alta disponibilidade, onde um monitora o funcionamento do outro e assume suas funções automática e instantaneamente caso o outro fique fora do ar.
- **Simplicidade e compartimentalização das funções:** toda a complexidade da certificação digital, tais com a manutenção da base de certificados digitais dos usuários, verificação de validade das assinaturas digitais, checagens de expiração e revogação, são tratadas pelo próprio ViaProxy – a

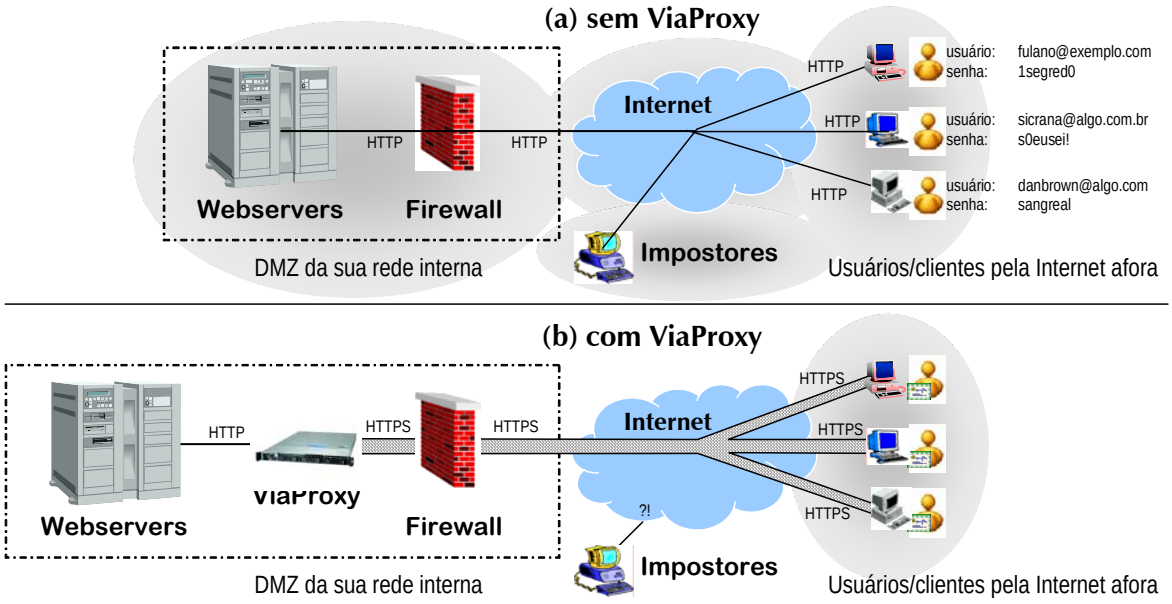


**Figura 5:** Em **(a)**, vemos a arquitetura de rede macro de um site de serviços na Internet (digamos, um portal, banco via internet ou site de vendas) sem o **ViaProxy**. Nesse caso, o site se comunica via HTTP comum e seus usuários se autenticam por nome e senha. Há quatro principais áreas de risco, indicadas pelas ovais sombreadas: a própria aplicação web pode vazar a senha dos usuários, alem de que o administrador do banco de dados tem poderes absolutos para alterar qualquer coisa sem deixar rastros; a própria Internet é um risco, pois as senhas podem ser interceptadas em trânsito; há o perigo de sites impostores visualmente idênticos ao seu, ludibirando o usuário a entregar seus dados e senhas; e o próprio usuário é um risco, pois podem emprestar ou partilhar suas senhas com outros usuários, bem como usar a mesma senha em outros sites menos seguros que o seu. O cenário **(b)** mostra a arquitetura após a introdução do **ViaProxy,** ao mesmo tempo em que realça as diferenças em relação ao cenário anterior. O ViaProxy foi inserido entre o *firewall* e o servidor de aplicação, criando perante os usuários a ilusão de que o site fala HTTPS; na realidade, é o ViaProxy que traduz as requisições HTTPS vindas dos usuários em HTTP comum e os repassa para a aplicação web. Além disso, os usuários provam suas identidades através de assinaturas digitais, de sorte que nenhuma jamais trafega pela rede nem fica armazenada no seu banco de dados. O ViaCert traduz as assinaturas digitais em pares nome+senha que a aplicação entende. Desse modo, a aplicação tem a ilusão de que nada mudou em relação ao cenário anterior, quando na realidade é o ViaCert que está provendo essa "ilusão". Há, portanto, uma dramática redução na quantidade de áreas vulneráveis: resta apenas uma – os próprios usuários. As outras três deixam de ser críticas: como processo de autenticação não transmite senhas ou segredos, a Internet deixa de ser uma preocupação, bem como os impostores que nela habitam. A própria aplicação também deixa de ser uma vulnerabilidade, na medida em que as senhas deixam de ser seu mecanismo de autenticação.

aplicação Web original nem sequer toma conhecimento de nada disso.

- **Usabilidade:** o ViaProxy trata e diagnostica problemas relacionados ao certificado digital, guiando o usuário a fazer a coisa certa com mensagens claras, simples e diretas: o certificado do usuário está revogado? O ViaProxy informa e opcionalmente redireciona o usuário para a Autoridade Certificadora onde poderá renová-lo; o usuário ainda não tem um certificado digital? O ViaProxy repassa o usuário para o site da Autoridade Certificadora, ou opcionalmente usa a própria AC interna para lhe prover um certificado;
- **Transparência:** o site protegido resultante dá ao usuário final a impressão de ser uma coisa só; a transição entre as páginas geradas pelo ViaProxy e pela aplicação em si pode ser tornada praticamente imperceptível.

## ViaProxy e ViaCert: proteção em dobro, do cliente e do servidor

O ViaProxy e o ViaCert, apesar de serem funcionalmente autônomos, integram-se perfeitamente. Assim, sites que desejem ou requeiram maior proteção podem migrar instantaneamente para a tecnologia de certificação digital, beneficiando-se da rapidez, comodidade e da dupla proteção oferecida pela tecnologia Tempest tanto para o lado do cliente quanto para o lado do servidor.

# Casos de Sucesso

## O Site do Programa JuroZero da FINEP

Destaques:

- *Milhares de cópias do Tempest ViaCert distribuídas entre usuários de todo o país;*
- *Assinaturas digitais de propostas, pareceres e contratos diretamente no site web;*

O Programa Juro Zero (www.jurozero.finep.gov.br) foi criado com a finalidade de estimular o desenvolvimento das Micro e Pequenas Empresas inovadoras brasileiras nos aspectos gerenciais, comerciais, de processo ou de produtos/serviços viabilizando o acesso ao crédito por parte destas empresas, concedendo-lhes empréstimos a "juro zero". Foi lançado e é coordenado pela FINEP – Financiadora de Estudos e Projetos (www.finep.gov.br), empresa vinculada ao Ministério da Ciência e Tecnologia.

Para obter o empréstimo, uma empresa interessada se inscreve no site, que desde o princípio requer que o usuário possua um certificado digital eCNPJ, emitido por uma das Autoridades Certificadoras credenciadas pela Secretaria da Receita Federal. Utilizando-se dos recursos únicos do Tempest ViaCert, o site pode detectar quais certificados o usuário tem, excluindo desde já os que não aceita e mostrando apenas os que aceita.

O usuário então preenche o formulário-proposta, onde detalha os dados cadastrais da empresa, sua composição acionária, área de atuação, tipo de inovação que realiza, quanto dinheiro precisa (dentro dos limites previstos no Projeto) e como pretende aplicá-lo, entre vários outros quesitos. Essa proposta é assinada digitalmente e enviada, através do *workflow* interno do site, para os Parceiros Estratégicos, que realizam uma pré-avaliação da proposta e anexam seus pareceres, também assinados digitalmente. Os pré-aprovados são encaminhados para uma segunda rodada de avaliação pela FINEP, e os aprovados finais reafirmam seu interesse. Por fim, o contrato final é assinado digitalmente no próprio site pela empresa aprovada e ela já recebe o empréstimo no mês seguinte.

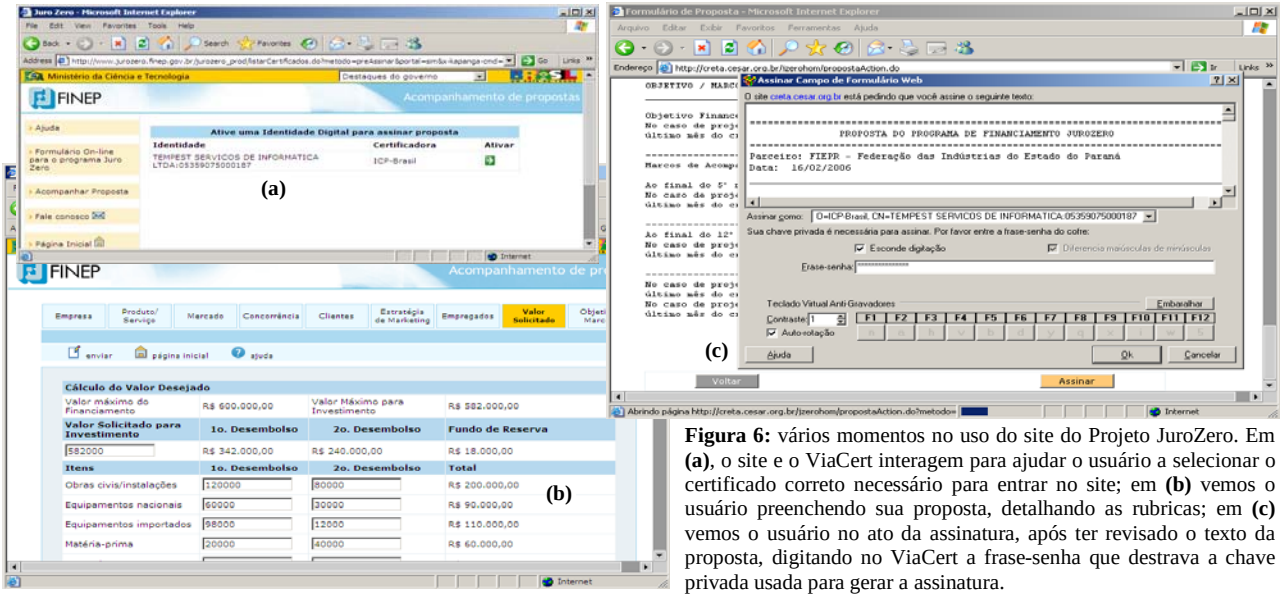


**Figura 6:** vários momentos no uso do site do Projeto JuroZero. Em **(a)**, o site e o ViaCert interagem para ajudar o usuário a selecionar o certificado correto necessário para entrar no site; em **(b)** vemos o usuário preenchendo sua proposta, detalhando as rubricas; em **(c)** vemos o usuário no ato da assinatura, após ter revisado o texto da proposta, digitando no ViaCert a frase-senha que destrava a chave privada usada para gerar a assinatura.

## Referências e Bibliografia Recomendada


1. Charles Leiserson, Thomas Cormen, Ronald Rivest & Clifford Stein, *Algoritmos: Teoria e Prática*, 2002, Ed. Campus, ISBN 8535209263

   - *Indicado para técnicos em informática e cientistas da computação interessados nos fundamentos matemáticos do algoritmo RSA, um dos mais amplamente adotados em aplicações de criptografia e um dos usados no Tempest ViaCert.*

2. William Stallings, *Cryptography and Network Security: Principles and Practice*, 4th edition, 2006, Prentice-Hall, ISBN 0-13-187316-4

   - *Referência indispensável para técnicos em informática que desejem ter uma visão ampla de como as técnicas de criptografia são aplicadas à segurança de redes de computadores. Provê um panorama geral de vários protocolos atualmente em uso, tais como o SSL/TLS e Kerberos, bem como um tratamento sobre certificados digitais X.509 e chaves PGP.*

3. Eric Rescorla, *SSL and TLS: Designing and Building Secure Systems*, 2000, Addison-Wesley, ISBN 0201615983

   - *Livro definitivo sobre a implementação dos protocolos SSL/TLS e como ele é agregado com o HTTP para resultar no HTTPS. Trata também de várias questões fundamentais para implementadores, tais como performance, integração com aplicações, etc.*

4. Marcos da Costa, *Validade jurídica e valor probante dos documentos eletrônicos*, 2003, I Fórum sobre Segurança, Privacidade e Certificação Digital, realizado pelo Instituto Nacional de Tecnologia da Informação, disponível em: `http://www.iti.br/twiki/pub/Forum/ArtigoD05/artigoD05-costa.rtf`

   - *Este artigo muito didático e acessível pode ser de grande interesse para gestores de TI e advogados, onde discute sob a ótica jurídica a inadequação do termo "validade jurídica do certificado digital" e estabelece o uso correto dos termos "eficácia probante". Um dos raros textos que corretamente prestigia a assinatura digital como protagonista e coloca o certificado digital como coadjuvante.*

5. Marcos da Costa & Augusto T. R. Marcacini, *Direito em Bits*, 2004, Ed. Fiuza, ISBN 8587035576

   - *Coletânea de artigos sobre vários aspectos do uso de criptografia no Direito e comentários às várias leis propostas ao longo dos anos para regulamentar a área. Muito relevante para advogados e gestores de TI em geral.*

# Glossário

**AC:** ➔ *veja:* autoridade certificadora.

**algoritmo de hash:** 1. procedimento matemático que cria um número de tamanho fixo a partir de um arquivo de tamanho arbitrário. 2. algoritmo de hash criptográfico. 🕮 *O cálculo dos dígitos verificadores do CPF é um algoritmo de hash muito conhecido, mas impróprio para uso em assinaturas digitais porque é fácil encontrar dois números de CPF que resultam nos mesmos dígitos verificadores.* ➔ *veja também:* colisão de *hash*, período seguro.

**algoritmo de hash criptográfico:** 1. algoritmo de hash especificamente projetado para que encontrar colisões, tanto intencional quanto não intencional, seja impraticável por requerer tempo e recursos computacionais absurdamente grandes. 🕮 *Os algoritmos de hash de qualidade criptográfica mais conhecidos são SHA1 e SHA256. Achava-se que o MD5 tinha qualidade criptográfica até que em 1998 os cientistas descobriram métodos viáveis de se encontrar colisões arbitrárias.*

**assinatura digital:** 1. número que atua como código de conferência, permitindo aferir se um documento digital é idêntico "bit-a-bit" a outro previamente assinado por um determinado signatário; 2. procedimento para geração desta assinatura, na forma de ações que o usuário precisa efetuar em um programa de computador para gerá-la; 3. procedimento matemático, normalmente executado por um programa de computador, para calcular a assinatura em função de uma chave privada e de um documento digital. 🕮 *A geração de uma assinatura digital é privilégio exclusivo dos detentores da chave privada; ao agregarmos assinaturas digitais aos documentos digitais, passa a ser fácil detectar qualquer tentativa de adulterá-lo.* ➔ *veja também:* algoritmos de *hash,* chave privada, Criptografia de Chaves Públicas.

**assinatura digital inválida:** 1. aquela cujo processo de conferência falhou, significando que o documento digital conferido não é idêntico ao assinado, ou foi assinado por uma chave privada que não corresponde à chave pública usada na conferência. 🕮 *"Sinto muito senhor, mas seu contrato digital não pode ser aceito porque a assinatura digital está inválida"; há quem chame uma assinatura digital inválida de "rasura digital".* ➔ *veja também:* assinatura digital, chave privada, chave pública.

**assinatura digital válida:** 1. aquela cujo processo de conferência teve sucesso, significando que o documento digital conferido é idêntico "bit a bit" ao que foi assinado e que foi assinado pela chave privada que corresponde à chave pública usada na conferência. 🕮 *"Mas por que eu não deveria aceitar esse documento? A assinatura digital nele está válida e tudo!?".* ➔ *veja também:* assinatura digital, chave privada, chave pública.

**autoridade certificadora:** 1. entidade especial a quem cabe emitir certificados digitais para titulares que possam satisfazer os critérios de suas Declarações de Práticas de Certificação. 🕮 *Para gerar sua identidade digital – informe-se junto a uma autoridade certificadora e siga seus procedimentos.* ➔ *veja também:* Declarações de Práticas de Certificação, entidade.

**autoridade certificadora intermediária:** 1. autoridades certificadoras que, na estrutura hierárquica, estão abaixo da autoridade certificadora raiz. 🕮 *Sem a autoridade certificadora intermediária não é possível completar o encadeamento de um certificado.* ➔ *veja também:* autoridade certificadora, autoridade certificadora raiz, encadeamento.

**autoridade certificadora raiz:** 1. autoridade certificadora especial, que, sob algum regime legal, técnico ou social, está no nível hierárquico mais alto e cujo certificado se presume conhecido por todos participantes, sejam eles autoridades certificadora ou entidades finais. 🕮 *Há quem*

*considere que o nascimento de uma Infra-estrutura de Chaves Públicas ocorre quando sua Autoridade Certificadora Raiz começa a operar*. ➔ *veja também:* autoridade certificadora, entidade final, Infra-estrutura de Chaves Públicas.

**CCP:** ➔ *veja*: Criptografia de Chaves Públicas.

**certificado digital**: 1. documento digital em formato padronizado que associa o nome de um titular a sua chave pública, tipicamente assinado por uma Autoridade Certificadora como prova de que dela garante a associação. 2. certificado digital que segue o padrão X.509. 🕮 *O certificado é algo como um cartão de visita: é do nosso interesse distribuí-lo amplamente, para que outras pessoas possam reconhecer nossas assinaturas digitais; é por causa do certificado digital que o ViaCert pode mostrar o nome dos titulares; se não fosse por eles, o que apareceria seria o número de centenas de dígitos que compõe a chave pública – e não teríamos a menor idéia de a que titular ele se refere.* ➔ *veja também:* autoridade certificadora, chave pública, titular, X.509.

**Certificate Revocation List**: ➔ *veja*: Lista de Certificados Revogados.

**certificação digital:** 1. nome genérico pelo qual são conhecidas um conjunto de tecnologias que viabilizam diversas formas de proteção para transações eletrônicas realizadas através de redes abertas que se baseiam no uso de criptografia de chaves públicas e certificados digitais; 2. freqüentemente usado para denotar alguma ICP que se baseie em certificados digitais que sigam ou se inspirem no padrão X.509. 🕮 *A utilização da certificação digital por empresas ou pessoas em geral tornará mais seguro o tráfego de informações pela Internet.* ➔ *veja também:* criptografia de chaves públicas, certificado digital, ICP, X.509.

**chave pública:** 1. um dos dois números associados a um titular em algum sistema de certificação digital e que se decide divulgá-lo para que possa através dele ser identificado. 🕮 *Em sistemas criptográficos seguros, a chave pública precisa ser um número muito longo, com centenas de dígitos; é por isso que ele fica guardado em um arquivo de computador, para que ninguém tenha que decorá-lo.* ➔ *veja também:* certificado digital, certificação digital.

**chave privada:** 1. um dos dois números associados a um titular em algum sistema de certificação digital e que lhe dá o poder de gerar assinaturas digitais. Para que esse poder seja exclusivo do titular, esse número fica em poder de um número limitado de detentores de sua confiança ou sob seu controle. 🕮 *"Pedro e eu somos detentores da chave privada da empresa onde trabalhamos, pois, somos responsáveis pela sua parte jurídica e financeira."; "Há quem defenda que, para o caso de pessoas físicas, o detentor deveria ser único: o próprio titular"* ➔ *veja também:* assinatura digital, certificação digital, detentor, titular.

**cliente:** 1. programa de computador que requisita um serviço a um servidor através da rede; 2. o computador onde está em execução um programa cliente; 3. o indivíduo que opera o computador e/ou programa que está atuando como cliente naquele momento. 🕮 N*avegadores são clientes web (Internet Explorer, Firefox, Mozilla); "o cliente não está conseguindo acessar a aplicação"; "meu cliente de e-mail (Outlook) está travando".* ➔ *veja também:* servidor.

**conferência de uma assinatura digital:** 1. resultado de um cálculo cujos procedimentos de realização são estudados pela CCP, que tem como ingredientes uma chave pública e um documento digital, dito "a ser conferido". 🕮 *Para que as assinaturas digitais possam realizar seu potencial de proteger transações eletrônicas, é essencial ter um programa de geração e conferência de assinaturas digitais que seja fácil e prático de usar (o ViaCert, por exemplo).* ➔ *veja também:* assinatura inválida, assinatura inválida, CCP, chave pública, documento digital.

**CPS:** 1. em inglês, "Certification Practice Statement". ➔ *veja*: Declaração de Práticas de Certificação.

**Criptografia de Chaves Públicas:** 1. ramo da Ciência da Computação com raízes na Matemática que estuda mecanismos de comunicação resistentes a ataques intencionais (interceptação e adulteração, principalmente); baseia-se na utilização de operações matemáticas com certos números especiais chamados par de chaves, uma pública e outra privada. 🕮 *Toda ICP é baseada em criptografia de chaves públicas.* ➔ *veja também*: chave pública, chave privada.

**CRL:** 1. em inglês, "Certificate Revocation List". ➔ *veja*: Lista de Certificados Revogados.

**Declarações de Práticas de Certificação**: 1. documentos publicados pelas autoridades certificadoras explicitando que procedimentos ela segue para se assegurar que os titulares são realmente conhecidos por aqueles nomes ou números de cadastro; e que eles detêm as chaves privadas correspondentes às chaves públicas. Neste documento também costumam constar às garantias que ela oferece, como lida em caso de falhas nos procedimentos, responsabilidades das partes e suas conexões com o regime normativo, legal ou institucional no qual está inserida. 🕮 *Consulte as Declarações de Práticas de Certificação de uma autoridade certificadora para entender os critérios exatos e o rigor utilizado na emissão de certificados digitais (algumas requerem a presença física do titular e cópias de seus documentos, conferem sua foto com a da sua cédula de identidade, entre outros requisitos; outras simplesmente verificam se o candidato consegue receber correio eletrônico no endereço que ele especificou).* ➔ *veja também*: autoridade certificadora, certificado digital, chave privada, chave pública, titular.

**detentor:** 1. o computador ou sistema computacional onde está armazenada uma determinada chave privada; 2. o indivíduo que controla este computador. 🕮 "*Pedro e eu somos detentores da chave privada da empresa onde trabalhamos, pois, somos responsáveis pela sua parte jurídica e financeira.*" ➔ *veja também*: chave privada, titular.

**documento digital:** 1. a representação de uma informação (textos, sons, imagens, filmes, etc.) em meios que possam ser armazenados e processados por computadores pessoais comuns; 2. em analogia com um documento em papel, o arquivo de computador onde fica armazenado algum texto, possivelmente acompanhado de imagens, tabelas, planilhas ou o que mais o programa aplicativo que o abre puder suportar. 🕮 *Distinguir cópia de original não faz sentido no caso de documentos digitais: toda cópia é 100% fiel e, portanto, indistinguível do original.*

**DPC:** *veja*: Declarações de Práticas de Certificação.

**entidade:** 1. pessoa física, jurídica ou um programa sendo executado em um determinado computador, identificável dentro do contexto técnico, institucional ou social onde está inserido, segundo algum padrão de nomenclatura. 🕮 S*ervidores web são entidades normalmente identificadas por seu nome DNS ou endereço IP*; *pessoas físicas provavelmente serão as entidades mais comuns na ICP-BR.* ➔ *veja também:* titular, detentor.

**entidade final:** 1. qualquer entidade em que o titular não seja uma autoridade certificadora. 🕮 *Servidores web, pessoas físicas e jurídicas em geral.* ➔ *veja também:* autoridade certificadora, titular.

**frase-senha:** senha preferivelmente longa ou composta de várias palavras, usada para proteger itens muito importantes, tais como chaves privadas, ou autorizar a execução de operações críticas, como a geração de assinaturas digitais. 🕮 *Toda vez que o ViaCert for assinar algum arquivo ou documento, ou precisarmos nos identificar, o ViaCert perguntará por sua frase-senha.* ➔ *veja também:* assinatura digital, chave privada.

**HTML (Hiper Text Markup Language):** 1. linguagem utilizada para criação de páginas para sites *web*. 🕮 *Os documentos HTML utilizam as extensões ".htm" ou ".html".* ➔ *veja também: web*.

**HTTPS (HyperText Transfer Protocol Secure):** 1. aprimoramento do protocolo HTTP que utiliza SSL; utilizado para criptografar todos os dados que transitarem através de uma rede (usualmente a Internet); possibilita a verificação da autenticidade do servidor e do cliente através de certificados digitais. 🕮 *Praticamente todos os servidores web modernos, tais como o Apache e o IIS (Microsoft Internet Information Services), já o suportam nativamente o HTTPS – bem como a maioria dos navegadores, tais como o Internet Explorer, o Mozilla ou o Firefox.* ➔ veja também: HTTP, SSL.

**HTTP (HyperText Transfer Protocol):** 1. em português, "Protocolo de Transferência de Hipertexto"; protocolo utilizado para transferência de dados através da *web* e comunicação entre cliente e servidor. ➔ veja também: *web*, cliente servidor.

**ICP:** ➔ *veja:* Infra-estrutura de Chaves Públicas.

**ICP-BR:** 1. infra-estrutura de chaves públicas brasileira, instituída com base na Medida Provisória 2200-2 de 24 de agosto de 2001. 🕮 *A ICP-BR exige que suas ACs realizem uma verificação rigorosa da identidade dos titulares, que devem comparecer pessoalmente às Autoridades de Registro para emitirem seus certificados digitais.* ➔ *veja também:* Infra-estrutura de Chaves Públicas.

**identidade digital:** 1. o conjunto composto pela chave privada e o certificado digital de um titular. 🕮 *Para poder assinar documentos digitalmente, você precisa antes de mais nada gerar sua identidade digital – informe-se junto a uma Autoridade Certificadora e siga seus procedimentos.* ➔ *veja também:* chave privada, certificado digital.

**Infra-estrutura de Chaves Públicas:** 1. conjunto de todos os participantes (titulares, detentores, Autoridades Certificadoras, etc.), infra-estrutura técnica (computadores e programas de computadores, normas técnicas) e instrumentos legais e/ou contratuais aos os quais os participantes escolheram aderir. 🕮 *Muitas ICPs se baseiam em certificados digitais que sigam ou se inspirem no padrão x.509.* ➔ *veja também:* Criptografia de Chaves Públicas.

**LCR:** ➔ *veja:* lista de certificados revogados.

**leitora de smartcards:** 1. dispositivo onde os *smartcards* são inseridos e que viabiliza sua comunicação com o computador principal. 🕮 *Alguns modelos de leitoras de smartcards se conectam ao computador pela interface serial, enquanto outras se ligam na porta USB.* ➔ *veja também:* smartcard.

**lista de certificados revogados:** 1. lista emitida periodicamente pelas autoridades certificadoras e contém um índice dos números de série dos certificados que foram revogados. 🕮 *A extensão padrão para arquivos que contém listas de certificados revogados é ".crl" (abreviatura de "Certificate Revocation List").* ➔ *veja também:* autoridade certificadora, certificado digital.

**navegador:** 1. software que possibilita o acesso a *sites web*. 🕮 *Os navegadores mais conhecidos são Internet Explorer, Firefox e Mozilla.* ➔ *veja também: web.*

**par de chaves:** 1. chaves geradas a partir de ingredientes e processos matemáticos no momento da emissão de uma identidade digital; consiste em uma chave pública e outra privada. 🕮 *Por serem números muito longos (mais de 200 dígitos), os pares de chaves quase sempre são armazenados e manipulados por computadores.* ➔ *veja também:* chave pública, chave privada, identidade digital.

**PKCS (Public-Key Cryptography Standards)**: conjunto de padrões técnicos relativos à criptografia de chaves públicas, criado e mantido pela empresa americana RSA Data Security

Inc. em conjunto com desenvolvedores de sistemas seguros do mundo todo, com o intuito de facilitar a adoção e promover a compatibilidade entre produtos de diferentes fabricantes. 🕮 *O ViaCert adere a vários desses PKCS, como o PKCS#7 e o PKCS#12.* ➔ *veja também:* CCP.

**proxy:** 1. software que intercepta as comunicações entre o cliente e o servidor para agregar-lhe algum tipo de serviço. 🕮 *Alguns proxies, por exemplo, fazem controle de acesso, isto é, pedem nome e senha para só permitir acesso à Internet a usuários cadastrados ou detectar/bloquear a propagação de vírus; outros proxies atuam como cache: eles "lembram" as páginas recentemente acessadas, de sorte que se você acessar algumas das que eles já têm, o proxy responde mais rápido do que o site original (e economiza uma ida-e-volta até a Internet); outros proxies ainda servem para auditoria e estatística: contabilizam quantas horas por dia os usuários passam online, que sites acessam, etc.*

**protocolo:** 1. conjunto de regras bem definidas para o diálogo entre dois computadores (tipicamente, um deles atuando como servidor e um ou mais atuando como clientes) para algum propósito específico. 🕮 *Os protocolos mais populares para se baixar mensagens da nossa caixa postal de correio eletrônico do servidor são o POP3 e o IMAP; a pedra fundamental da web é o protocolo HTTP.*

**PKI:** 1. em inglês, "Public Key Infrastructure". ➔ *veja*: Infra-estrutura de Chaves Públicas.

**rasura digital:** 1. termo informal dado a um documento cuja assinatura digital está inválida. 🕮 *Pode-se chamar de digitalmente rasurado aquele documento assinado cuja assinatura não confere.* ➔ *veja também*: assinatura digital válida, assinatura digital inválida.

**RFC:** ➔ *veja*: Request for Comments;

**Request for Comments:** 1. em Português, "Pedido de Comentários"; uma série de documentos que descrevem o funcionamento dos protocolos da Internet em detalhes técnicos suficientes para que possam ser reimplementados por diferentes grupos. Vários desses documentos são considerados padrões oficiais a serem seguidos. Cada RFC tem um número e trata de um assunto ou protocolo de rede específico. Por exemplo, a RFC principal que normatiza o protocolo HTTP é a RFC 2616; a especialização dos certificados X.509 e Listas de Certificados Revogados para uso na Internet é a RFC 3280. ➔ *veja*: http://www.rfc-editor.org

**servidor:** 1. programa de computador que oferece um serviço acessível remotamente em uma rede de computadores. 2. o computador onde um ou mais programas servidores estão em execução. 🕮 "*Este servidor web recebe centenas de transações bancárias por segundo de nossos correntistas pelo país afora*"; "*O servidor de correio eletrônico travou no último ataque do vírus*". ➔ *veja também:* cliente.

**smartcard:** 1. cartão de plástico do mesmo tamanho e formato de um cartão de crédito comum, mas que, ao invés de uma tarja magnética, contém um computador com processeador, memória e sistema operacional, mas sem vídeo nem teclado, miniaturizado no formato de uma pastilha quadrada pouco menor do que um confete de carnaval. A pastilha tem ranhuras que servem de contato elétrico, provendo comunicação com um computador convencional quando o cartão é inserido em uma leitora de smartcards . 🕮 *Como qualquer computador, o smartcard pode ser programado para fazer qualquer tipo de processamento de dados; existem vários tipos de smartcards para diferentes aplicações.* ➔ *veja também:* leitora de smartcards.

**SSL (Secure Socket Layer):** protocolo que possibilita a transmissão segura de dados entre clientes e servidores através de uma rede (normalmente a Internet); provê segurança para transações *web* através da utilização de autenticação, criptografia de dados e assinaturas digitais; foi desenvolvido pela Nestscape. 🕮 As *URLs que utilizam conexões SSL iniciam com "https" (ao invés de "http").*

**titular:** 1. a entidade que se convenciona: a) identificar por uma dada chave pública; b) ser tida como responsável pelos efeitos do uso da chave privada associada àquela chave pública. 🕮 *"O titular dessa chave pública não sou eu, mas sim a empresa em que trabalho; portanto, ela é que deve ser responsabilizada por esse contrato, e não eu!".* ➔ chave privada, chave pública.

**token:** combinação da pastilha-computador de um *smartcard* com a leitora em um único dispositivo; normalmente se conecta a uma das portas USB do computador principal; visualmente se assemelha a um *pendrive* e não a um cartão de crédito. 🕮 *A maior vantagem dos tokens é poderem ser ligados diretamente ao computador principal, sem a necessidade de uma leitora externa.* ➔ *veja também:* smartcard.

**URL (Uniform Resource Locator):** endereço de recurso ou arquivo disponível através da *web*. 🕮 http://www.tempest.com.br; ftp://ftp.tempest.com.br; https://ca.freeicp.org/. ➔ *veja também:* navegador, web.

**web:** 1. Termo usado para se referir à World Wide Web ("Teia Mundial", abreviada "WWW"), serviço baseado em hipertexto que permite a navegação entre as informações disponíveis nos computadores na Internet e que se baseia no protocolo HTTP. 🕮 *Precisamos de um navegador para acessar sites web.*

**webmail:** 1. Interface da *web* que possibilita a ler e escrever e-mails utilizando um navegador. 🕮 *"Quando estou viajando utilizo somente o webmail".* ➔ *veja também:* web, navegador.

**X.509:** padrão escolhido por várias entidades normativas e operativas, entre elas o ITU (*International Telecomunications Union*) e a ICP-BR como norma definidora do formato de certificados digitais. 🕮 *Certificados SSL são baseados no padrão X.509.*