CERTIFICAÇÃO DIGITAL: IMPORTÂNCIA E APLICABILIDADE

Tiago Lolato*
Evelacio Roque Kaufmann**

Resumo

Independente do ramo em que a organização atua, é fundamental manter políticas de segurança e alta confiabilidade das informações e recursos tecnológicos para garantir a continuidade dos negócios. A certificação digital é uma tecnologia que vem sendo aplicada no cenário corporativo para proporcionar segurança e agilidade nos processos de transações eletrônicas, com ampla aplicabilidade, na troca ou acesso das informações disponibilizadas de forma *on-line* ou na compra e venda de mercadoria por meio da internet. A aplicação desta tecnologia permite a economia de recursos como papel e principalmente o uso racional do tempo, recurso igualmente precioso no mundo dinâmico atual. Este artigo contextualiza as aplicabilidades da certificação digital nos cenários nacional e internacional, apresentando de forma geral as mudanças que esta nova tecnologia vem proporcionando aos negócios e às pessoas. Também são apresentados nos resultados do estudo as implicações relacionadas à segurança das informações, e como ela pode ser garantida pelo processo tecnológico da certificação digital.
Palavras-chave: Certificado digital. Segurança. Informação digital.

1 INTRODUÇÃO

O cenário empresarial passa constantemente por mudanças significativas, exigindo das organizações capacidade tecnológica para se manter no mercado. A opção de aderência a uma nova tecnologia pode gerar insegurança aos gestores, pois há risco de investirem valores significativos e não obterem o retorno esperado (CHEDE, 2004, p. 26).

A informação é um bem que agrega valor à organização, faz-se necessário o uso de recursos de Tecnologia da Informação (TI) de forma apropriada para a administração dos dados para permitir a busca de soluções que desencadeiam resultados satisfatórios com o menor custo possível (ALECRIM, 2011).

A gama de negócios realizados por meio da internet cresceu muito nos últimos anos, como o *e-commerce*, transações internacionais nos países do Mercosul, julgamento de processos judiciais digitais, entre várias outras áreas que também estão se utilizando da internet para agilizar seus processos e ganhar tempo, fazendo isso com segurança.

Para alcançar os resultados pretendidos durante o estudo, foram propostos alguns objetivos específicos:

a) apresentar a importância das informações para as pessoas e organizações por meio de levantamento bibliográfico;

b) realizar levantamento do estado da arte sobre a certificação digital no Brasil e em outros países do Mercosul;

c) fazer um comparativo dos padrões e modelos de certificação e apresentar como

* Graduando em Sistemas de Informação na Universidade do Oeste de Santa Catarina de São Miguel do Oeste; tiago_lolato@hotmail.com

** Mestre em Administração Estratégica de Negócios pela Universidade Nacional de Missiones; Especialista em Ciências da Computação pela Universidade Federal de Santa Catarina; Professor do Curso de Bacharelado em Sistemas de Informação na Universidade do Oeste de Santa Catarina de São Miguel do Oeste; Rua Oiapoc, 211, 89900-000, São Miguel do Oeste, SC; evelacio.kaufmann@unoesc.edu.br

funciona a estrutura das entidades certificadoras;

d) descrever quais as principais aplicabilidades para a utilização da certificação digital;

e) analisar aspectos legais da certificação digital, de que forma é amparada atualmente e quais as perspectivas futuras em termos de legislação;

f) realizar aplicações práticas e simulações relacionadas à segurança da informação e confiabilidade.

O certificado digital está cumprindo seu papel perante a necessidade de economia e agilidade, atualmente fatores críticos para organizações e pessoas, considerando que não é suficiente ser mais econômico ou mais rápido, deve-se atender aos padrões de segurança que o usuário necessita, ou seja, agilidade, economia e segurança. Com a tecnologia disponibilizada por meio do certificado digital, o consumidor consegue tudo isso sem sair de casa, sem enfrentar filas de banco ou de caixa de lojas, podendo, até mesmo, comprar de outros países sem a necessidade de sair de casa com dinheiro na mão, correndo o risco de ser assaltado ou de sofrer um acidente no trânsito cada vez mais crítico em todos os lugares.

2 ESTADO DA ARTE DA CERTIFICAÇÃO DIGITAL

A legislação vigente que delimita a utilização da certificação digital e assinatura eletrônica é recente se comparada ao início do termo assinatura digital que começou no ano de 1976, quando Whitfield Diffie e Martin Hellman, dois Matemáticos, publicaram um artigo descrevendo uma forma de enviar mensagens criptografadas por chave pública; dois anos mais tarde, Rivest, Adi Shamir e Leonard Adleman desenvolveram um sistema de assinatura digital.

Conforme Sá (2010, p. 59):

> Em 1976, em (Diffie e Hellman, 1976) Whitheld Diffie e Martin Hellman introduziram o conceito de criptografia de chave pública, em que a chave usada para decifrar é, de um ponto de vista computacional, praticamente impossível de obter conhecendo a chave usada para cifrar, que pode, portanto ser pública. Apesar de não apresentarem nenhuma proposta concreta, o artigo estimulou a procura de um tal sistema. Em 1978 Ronald Rivest, Adi Shamir e Leonard Adleman publicaram o primeiro sistema prático de chave pública, que pode ser usado para transmitir informação confidencial e também como um esquema de assinatura digital, que ficou conhecido pelas iniciais dos apelidos dos seus inventores: RSA.

No Brasil, o estudo para regulamentar a certificação digital teve seu início em 2001 com referência à Medida Provisória n. 2.200-2, de 24 de outubro de 2001, para que transações *on-line* pudessem ser mais ágeis, seguras e diminuir custos com armazenamento de dados, e para que os dados tivessem valor legal perante órgãos públicos. Iniciou com o ICP-Gov que atendia a órgãos públicos e logo se transformou em ICP-Brasil, atualmente a estrutura hierárquica de autoridades certificadoras ligadas ao Governo brasileiro. Para que a transação tenha validade jurídica no país, o certificado deve ser emitido por uma das atuais nove autoridades certificadoras credenciadas pela ICP-Brasil, que tem a competência de emitir, suspender, renovar ou revogar certificados dos níveis hierárquicos inferiores.

O Comitê Gestor (CG) é a entidade-chave que controla a certificação digital brasileira, responsável por diversas funções; é formado por diversos representantes do Governo e setor privado e é também assessorado pelo Comitê Técnico (Cotec).

A ICP-Brasil está dividida em subníveis de autoridade, possibilitando ter um controle de quem pode ser certificado; tudo o que é feito tem que passar por todos os níveis da ICP para conseguir o certificado digital. Os níveis da ICP são AC-Raiz, ACs e AR. No topo da hierarquia, está a Autoridade Certificadora Raiz (AC-Raiz), que no caso da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI), a AC-Raiz tem a responsabilidade de auditar as autoridades certificadoras ACs e AR que estão em níveis inferiores.

Segundo Ribeiro ([200-?]), a ICP-Brasil possui características de hierarquia e está subdividida em vários níveis:

> Uma das principais características da ICP-Brasil é sua estrutura hierárquica. No topo da estrutura encontra-se a Autoridade Certificadora Raiz (AC-Raiz) e, abaixo dela, as diversas entidades (ACs de primeiro e segundo nível e Autoridades de Registro). Na ICP-Brasil, a AC-Raiz é o ITI, que é responsável pelo credenciamento dos demais participantes da cadeia certificadora, pela emissão de seu próprio par de chaves e pela supervisão de todos os processos que envolvem a certificação.

AC-OAB ICP-Brasil ([200-?]) apresenta uma breve explicação do que se tratam as ACs e AR:

> [...] Vinculadas à ICP-Brasil estão as ACs – Autoridades Certificadoras, entidades públicas ou privadas que estabelecem previamente a identidade do futuro portador do Certificado Digital por meio dos documentos necessários e emitem o certificado. AR – Autoridade Registro é a entidade vinculada a uma Autoridade Certificadora, tendo como competência identificar e cadastrar usuários, de forma presencial, e encaminhar as solicitações de certificados à respectiva AC.

Várias novas ACs já estão em processo de cadastro tentando conseguir autorização para a emissão de certificados digitais, visto que a necessidade de certificado digital para as empresas é obrigatória; assim, o crescimento do volume de emissão de certificados digitais aumenta a cada ano, impulsionado pela exigência da Receita Federal na emissão das notas fiscais eletrônicas, pela Ordem dos Advogados do Brasil (OAB) que está efetuando a certificação de todos os advogados, entre outras situações. Este crescimento já era esperado. O volume de emissão e notas fiscais eletrônicas também já está sendo feito em larga escala já que grande parte das empresas de grande e médio porte está tendo que emitir notas fiscais eletrônicas.

Conforme Convergência Digital (2010):

> O número de certificados digitais emitidos na cadeia da Infraestrutura de Chaves Públicas brasileira – ICP-Brasil teve crescimento de 384% no último ano, ultrapassando a marca de um milhão e 250 mil certificados digitais [...]
> Para se ter uma ideia, o processo da Nota Fiscal eletrônica (e-NF), que teve início em 2008, atualmente, conta com quase 400 mil emissores, com um volume de 1 trilhão e 800 mil notas emitidas. Além da economia de papel, há a agilidade com que o processo entre as empresas e o fisco é realizado.

Uma pesquisa da IBM divulgada pelo *site* Convergência Digital (2011) mostrou que a maior demanda de compras *on-line* vem da América Latina e, entre os países, o Brasil é o que mais se destaca no volume destas compras.

Vários acordos com diversos países mostram que o Brasil se tornou referência com o modelo adotado para a certificação, o qual é controlado pelo Governo, mas cada país tem suas particularidades e normas; assim, surgem diferenças entre os padrões adotados por cada um. Um dos objetivos da certificação digital é de que se possa integrar um padrão de certificados, sendo este aceito em todo o mundo. Embora a certificação digital já esteja bastante difundida, ainda há muitas particularidades entre países a serem resolvidas até que se possa utilizar essa tecnologia para assinar documentos de outros países, e para que estes tenham validade jurídica.

Um projeto para a unificação de um padrão de certificado digital aceito internacionalmente já está sendo projetado entre Brasil e Portugal para que os certificados tenham validade e aceitação entre os dois países conve-

niados, sendo um primeiro passo para futuros novos convênios com outros países agregando mais valor, agilidade e confiança entre os países que aderirem ao convênio.

Conforme Santos (2009), em entrevista com Gerson Rolin, Coordenador do projeto Mercosul Digital, o convênio feito com o Governo de Portugal é um marco histórico no uso da certificação digital:

> Gerson Rolim, coordenador do projeto Mercosul Digital do Ministério da Ciência e Tecnologia no Brasil, considera o convênio assinado entre o ITI (Instituto Nacional de Tecnologia da Informação) e o CGRI (Centro de Gestão da Rede de Informática do Governo de Portugal) histórico porque não existe nenhum país que reconhece a identidade digital do outro por meio do uso de certificados digitais. "O arcabouço legal e jurídico já está consolidado no convênio de reconhecimento mútuo, mas as discussões para viabilizar essa tecnologia começam agora entre Brasil e Portugal", informa.

O projeto Mercosul Digital, iniciado no ano de 2009, está com sua implantação sendo feita nos quatro países abrangentes; os responsáveis do projeto pretendem alcançar o objetivo final até o ano de 2014 tendo aceitação entre os certificados dos quatro países, também tendo total controle e fiscalização de todos os processos efetuados entre eles, oferecendo mais segurança aos usuários que podem, então, fazer suas compras em outros países com mais tranquilidade e segurança, sabendo que terão a quem recorrer se ocorrer algum problema.

3 **METODOLOGIA**

O presente estudo consistiu em uma pesquisa bibliográfica abordando os conceitos relacionados à tecnologia de certificação digital, enfatizando sua aplicabilidade. O escopo do trabalho buscou abordar especificamente a aplicação e a segurança aplicadas à tecnologia utilizada para agilizar os processos que utilizam a certificação digital.

Para a escolha das ferramentas na realização de testes durante o estudo, foram observadas aquelas que atendessem aos padrões da ICP-Brasil e que garantissem a validade dos dados assinados digitalmente e criptografados. Foi utilizado o certificado digital para implementar alguns testes de validação e garantir a segurança empregada aos documentos digitais. Já na técnica de coleta de dados foram utilizados a pesquisa em referências científicas e materiais bibliográficos e eletrônicos. Também foram estudadas algumas ferramentas de assinatura digital com o intuito de escolher uma com as características desejadas para a realização dos testes e, posteriormente, foram realizados testes e observação para a posterior análise dos resultados obtidos.

Quanto aos recursos utilizados para realizar os testes práticos, foi utilizado um notebook com suporte USB para conectar a leitora de cartão. A validação dos testes foi realizada por uma leitora de cartão *Smart Card*, do modelo *Smart Card Gem Pc Twin*, conforme a Fotografia 1.

Fotografia 1 – Leitora de cartão *Smart Card Gem Pc Twin* utilizada para a leitura do *software* armazenado no *Smart Card*

Fonte: os autores.

O cartão com a identidade digital, utilizado nos testes práticos, é semelhante a um cartão de crédito convencional com *chip* (Fotografia 2), possui microprocessador e memória capaz de armazenar o *software* de certificação. Para efetuar sua leitura é necessária a utilização de uma leitora de cartão para o certificado digital.

Fotografia 2 – *Smart Card* AC-Caixa com *chip* para o armazenamento do *software* de certificação

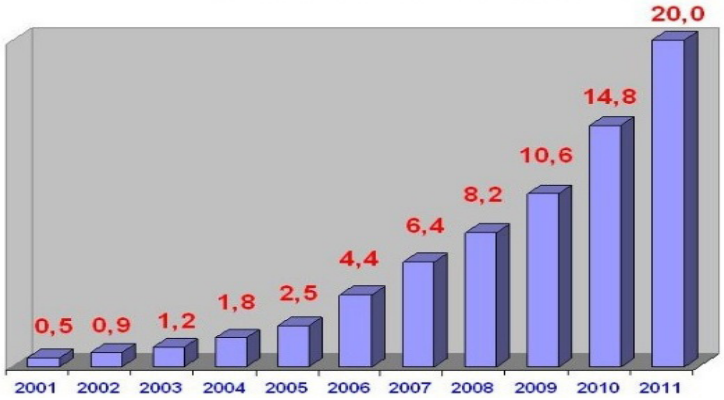
Fonte: os autores.

4 PRINCIPAIS APLICAÇÕES DA CERTIFICAÇÃO DIGITAL

Na era digital, tudo o que pode se economizar de tempo e recursos é um grande ganho para agilizar o funcionamento do sistema, entretanto, deve-se conciliar sempre a questão da segurança. Exige-se, atualmente, em quase todas as atividades corporativas, constante agilidade de execução e principalmente segurança no processo. No caso do *e-commerce*, há um vasto mercado envolvendo várias empresas, estimulando a concorrência, e como ela está sempre inovando na atualidade, quem for mais ágil e garantir melhor segurança é que fará o diferencial e terá maior competitividade.

Um exemplo dessa premissa é a estimativa do faturamento do *e-commerce* para o ano de 2011, que está estimado em 20 bilhões de reais, observada no Gráfico 1 que foi disponibilizado pelo eCommerceOrg ([200-?]). Desde o ano de 2001 até 2011 não houve quedas no faturamento anual do *e-commerce*.

Gráfico 1 – Faturamento do *e-commerce* no Brasil – Bilhões (2001-2011)



Fonte: Ecommerce Org (2008).

Apesar do valor estimado para o ano de 2011 ser de 20 bilhões de reais, esse valor ainda não contabiliza as vendas de carro, passagens aéreas e leilões que também são considerados *e-commerce*, ou seja, este número poderá ser ainda superior ao projetado.

Como o consumidor pode fazer compras sem ter que sair de casa, ele também pode pagar suas compras sem sair de casa, boletos, IPVA de veículos, conta de água, luz, telefone, consultar saldos em banco, entre outras diversas contas.

A implantação do certificado beneficiou não somente o *e-commerce*, mas abriu novas oportunidades para várias áreas de trabalho; um exemplo disso é a utilização do certificado digital para assinatura de documentos *on-line*, verificação de validade, técnicas criptográficas para manter informações sigilosas, possibilitando o acesso à informação de qualquer lugar que esteja conectado à internet. O certificado digital já está sendo utilizado em julgamentos e processos totalmente digitais.

Além do *e-commerce*, do poder judiciário e do Governo, o Instituto Nacional de Propriedade Industrial (INPI) também está convergindo para o lado da certificação digital; desde o dia 03 de outubro foi disponibilizado o e-Marcas que tem a função de coletar dados de novas marcas a serem registradas, o que anteriormente era feito por meio físico em papel, e hoje já pode ser entregue via internet diretamente ao INPI. Além do registro de marcas, também foi disponibilizado um sistema de patentes que utiliza certificado digital, chamado e-Patentes.

Até o fim de 2011 o INPI deve receber uma quantia de 150 mil pedidos de registro de marca, que estão sendo simplificados com a utilização da tecnologia de certificado digital; o usuário que está registrando a sua marca pode fazer a solicitação via internet, enviando os documentos necessários para o registro da sua marca diretamente ao INPI (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2011).

5 **TIPO DE SEGURANÇA**

O certificado digital possui oito tipos de certificados: quatro de assinatura e quatro de sigilo; os de assinatura classificam-se de A1 a A4 e têm a finalidade de assinar documentos digitalmente e em diversas transações *on-line*; já para a criptografia de arquivos, os certificados são classificados de S1 a S4, com a finalidade de embaralhar as informações de modo que ninguém consiga ter acesso a elas, a menos que possua as chaves pública e privada para criptografar e descriptografar os arquivos e obter esse acesso (RIBEIRO [200-?]).

Para garantir a segurança, são empregados dois tipos de criptografia. A simétrica utiliza uma mesma chave secreta para criptografar e descriptografar a informação, e a assimétrica utiliza um par de chaves criadas no mesmo momento chamadas de chave pública e chave privada. Os dois tipos de criptografia são diferenciados pela quantidade de chaves que possuem. A criptografia simétrica é composta em um algoritmo de criptografia que gera uma chave, utilizada tanto para criptografar a informação quanto para descriptografar; a criptografia simétrica requer um cuidado especial quanto à divulgação da chave, já que quem tem acesso a ela pode descriptografar a informação.

Na demonstração do Esquema 1, um destinatário possui a chave pública de Beto para criptografar o documento, e Beto possui a chave privada; as duas chaves são inversamente ligadas entre si já que são criadas no mesmo momento, então, partindo o texto original por meio de um mecanismo de criptografia, o destinatário utiliza a chave pública de Beto para cifrar o texto; após criptografado, o remetente envia o documento a Beto que possui sua chave privada à qual somente ele possui acesso, e utiliza-a para fazer o processo inverso da criptografia, fazendo com que o texto volte ao seu formato original e possa ser lido.

Esquema 1 – Criptografia Assimétrica

Fonte: Instituto Nacional de Tecnologia da Informação ([200-?]).

Para assinar um documento também são utilizados um par de chaves, pública e privada, assinatura feita pela chave pública e verificação de autenticidade feita pela chave privada. Conforme AC-OAB ICP-BRASIL ([200-?]), uma "[...] chave desempenha a função inversa da outra, ou seja, o que uma faz somente a outra chave pode desfazer. Por exemplo, a chave privada é usada para assinar o conteúdo de um documento enquanto a chave pública é usada para validar essa assinatura."

A principal diferença entre os certificados é a segurança empregada e o tipo de armazenamento, conforme Ribeiro ([200-?]) apresenta no Quadro 1:

Quadro 1 – Tipos de certificação digital

	Chave criptográfica			
Tipo de certificado	Tamanho (bits)	Processo de geração	Mídia armazenadora	Validade máxima (anos)
A1 e S2	1024	*Software*	Arquivo	1
A2 e S2	1024	*Software*	*Smart card* ou *token*, sem capacidade de geração de chave	2
A3 e S3	1024	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave	3
A4 e S4	2048	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave	3

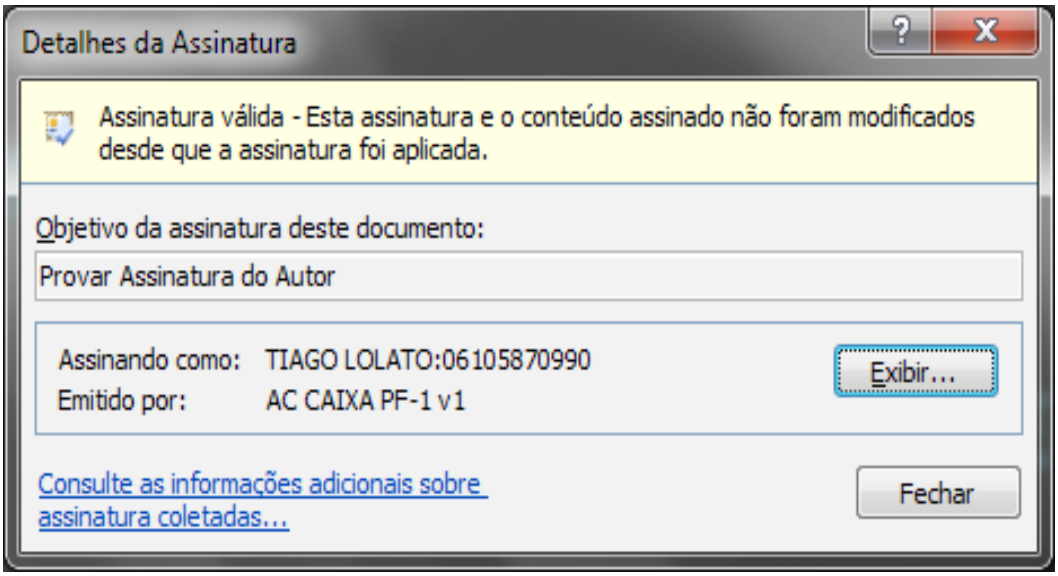
Fonte: Ribeiro ([200-?]).

6 APLICABILIDADES DA SEGURANÇA DIGITAL

Para as aplicações práticas de assinatura foi utilizado o software BrySigner versão 3.1.4.3, desenvolvido pela empresa Bry Tecnologia S.A., para assinar os documentos e verificar os dados do certificado, bem como se a assinatura é válida.

Na Tela 1, após ter devidamente assinado um documento, pode-se observar vários campos com informações importantes, como nome e CPF de quem assinou o documento, também o nome da autoridade de certificadora AC que, nesse caso, é a AC-Caixa e também traz um breve resumo do estado da assinatura no cabeçalho, provando, assim, que as informações não sofreram modificações posteriores à assinatura.

Tela 1 – Detalhes da assinatura

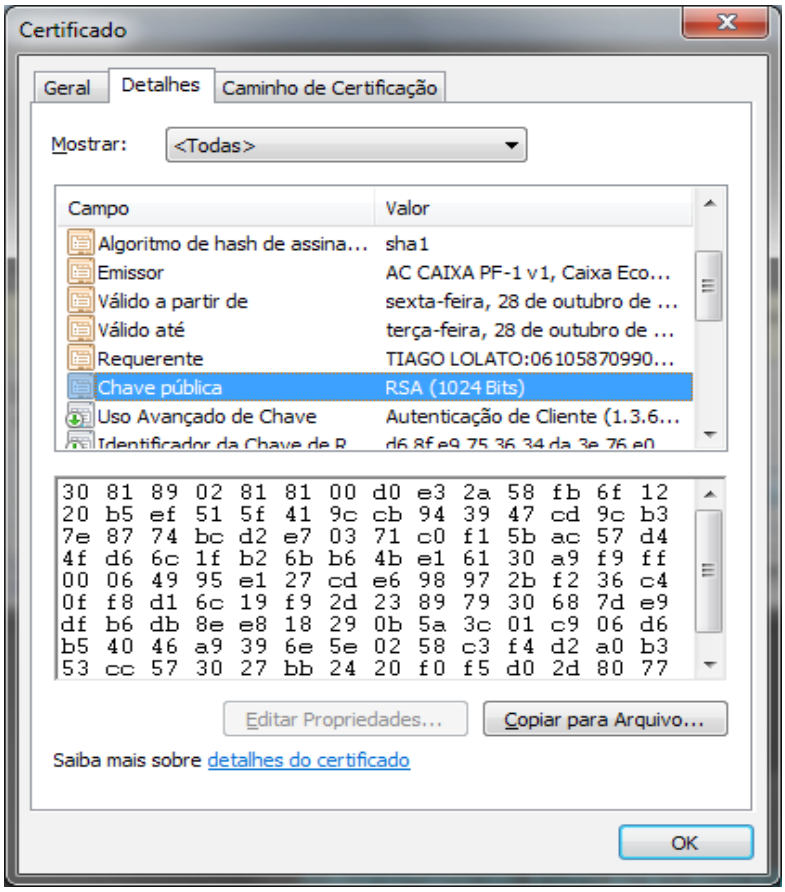


Fonte: os autores.

Clicando no botão Exibir da Tela 1, o *software* traz mais três abas com características do certificado utilizado para assinar o documento. A aba Geral apresenta informações como a data de início e a data de validade do certificado digital.

A aba Detalhes, que pode ser observada na Tela 2, contém o tipo de codificação *hash* para assinatura; o algoritmo utilizado neste certificado é o sha1, dado referente à validade do certificado, ao proprietário e também à chave pública RSA com a quantidade de *Bits* do modelo de certificado. O certificado utilizado é um *Smart Cart* do tipo A3 com 1024 *Bits*, a chave pública também pode ser visualizada em formato hexadecimal.

Tela 2 – Chave pública

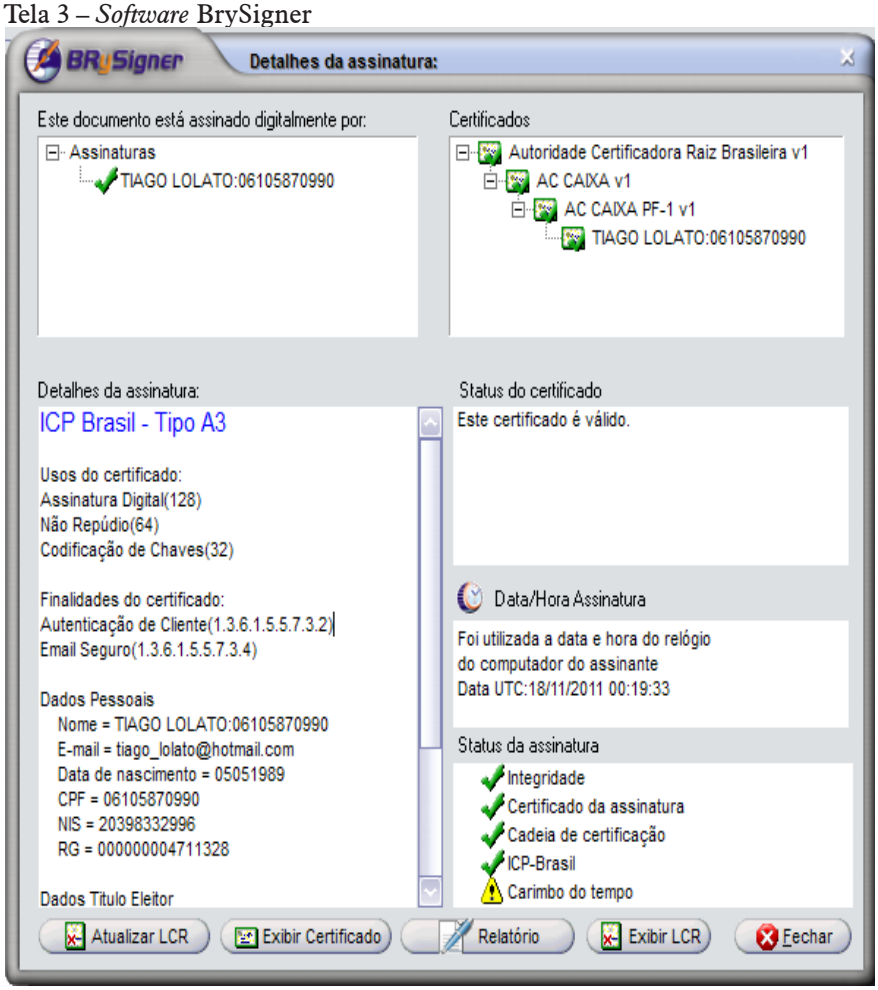


Fonte: os autores.

Na aba Caminho de Certificação, são exibidas informações referentes à hierarquia da cadeia de certificação, contendo no topo a AC-Raiz ICP-Brasil, a autoridade certificadora da caixa AC-Caixa, a AC-Caixa-PF, que indica que o certificado é de uma pessoa física, e por último, o proprietário do certificado digital.

Na Tela 3, o *software* BrySigner apresenta as informações do usuário que efetuou a assinatura; o campo Detalhes da assinatura apresenta o tipo de certificado utilizado, os dados pessoais do assinante, a hierarquia da certificação, o *status* do certificado e a data da assinatura.

Tela 3 – *Software* BrySigner

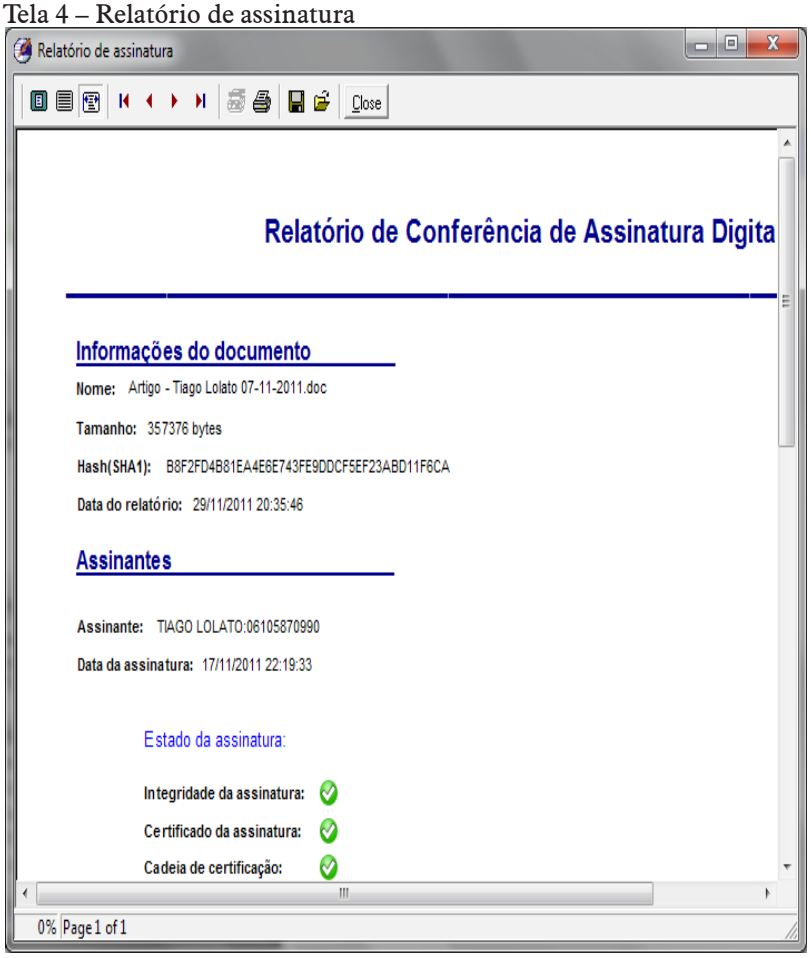


Fonte: os autores.

Ao clicar no botão Relatório da Tela 3, é exibido um relatório com todas as informações referentes ao documento e à assinatura, visualizadas na Tela 4, como nome do arquivo, tamanho do arquivo em *bytes*, um resumo *hash* do tipo SHA1 gerado por meio do tamanho do texto escrito no corpo do documento, informações sobre quem assinou o documento, data da assinatura e se a assinatura está válida.

A função *hash* é o resumo feito a partir do texto de um documento; o resumo pega cada espaço e qualquer outro caractere contido no documento e realiza o resumo atribuindo uma sequência de letras e números ao documento campo *hash* (SHA1) (Tela 4). Qualquer alteração feita ao documento, o resumo criptográfico *hash* é totalmente alterado.

Tela 4 – Relatório de assinatura



Fonte: o autor (2011).

O resumo criptográfico *hash* de cada documento e único, é como uma impressão digital, não possui outro resumo criptográfico igual para dois documentos com conteúdos diferentes.

7 CONCLUSÃO

Analisando a tecnologia empregada atualmente em todos os processos pessoais, organizacionais ou governamentais, tem-se a necessidade de implantar mais tecnologia a cada dia, em decorrência do grande número de crimes e problemas com compras *on-line* e fraudes contra o Governo que ocorrem com o uso da internet; busca-se a implementação de mecanismos e ferramentas que possam ajudar a diminuir estes problemas do cotidiano das organizações e dos usuários.

O grande avanço que está no mercado desde 2001 é o certificado digital, o qual, em termos de segurança, integridade e validade, é o que garante maior segurança em todas as transações feitas *on-line*, possibilitando uma maior segurança, tanto para quem está comprando quanto para quem está vendendo. Também para garantir segurança a quem troca informações, ou documento sigiloso *on-line*, garantindo que somente o destinatário terá acesso às informações e fornecendo a ele também a certeza de quem lhe enviou tal documento.

O crescimento econômico também deu um salto significativo desde 2001, ano do lançamento do modelo de certificado digital ICP-Brasil até o ano atual 2011; o faturamento para todo o setor do comércio que trabalha com *e-commerce* teve uma grande explosão nas vendas *on-line* em virtude de poder trabalhar *on-line* 24 horas por dia, sete dias por semana, oferecendo seus produtos de forma virtual para serem adquiridos em qualquer parte do mundo com segurança. Com isso, várias pessoas que antes saíam às ruas para fazer compras e pagar contas estão se adaptando à utilização da tecnologia para fazer essas tarefas com mais segurança. O crescimento das compras *on-line*

já é grande, mas ainda há resistência por parte de pessoas que ainda não fizeram, possivelmente, em razão do fator cultural de muitas famílias.

O certificado digital ajuda a encurtar caminhos e diminuir custos e tempo; hoje, vários processos judiciais e até julgamentos estão sendo feitos digitalmente, em decorrência da grande economia de recursos; os processos digitais podem ser acessados *on-line* a qualquer dia e julgados mais rapidamente, ajudando a desafogar os fóruns cheios de processos a serem julgados.

Várias opções de certificados estão disponíveis para o uso, sendo algumas pagas e outras grátis, ambas versões de certificados digitais são muito parecidas e utilizam praticamente a mesma estrutura de criptografia, diferenciando-se apenas pela garantia de segurança e validade jurídica dos certificados adquiridos a partir de uma autoridade certificadora. As opções grátis também podem ter validade jurídica desde que os envolvidos, destinatário e remetente, estejam cientes do processo executado entre eles.

Várias opções estão à disposição para diferentes níveis de segurança, podendo o usuário escolher e buscar a que mais se adapta à sua necessidade de segurança das informações e de utilização.

Digital certification: importance and applicability

Abstract

Regardless of the branch in which the organization operates, it is essential to maintain security and reliability policies of the information and technological resources to ensure business continuity. The digital certification is a technology that has been applied in the corporate setting to provide security and agility in the processes of electronic transactions, with wide applicability, whether in exchange or access of the information provided online, or in buying and selling merchandise through the internet. The application of this technology allows the saving of resources such as paper and mainly the rational use of time, a feature that is equally precious in today's dynamic world. This article analyzes the applicability of digital certification in national and international scene, presenting in general the changes that this new technology has been providing for business and for people. Also, it is presented in the results of the study the implications related to information security, and how it can be ensured by technological the digital certification process.
Keywords: Digital ertificate. Security. Digital information.

REFERÊNCIAS

AC-OAB ICP-BRASIL. **O certificado digital dos advogados**. ([200-?]). Disponível em: <http://www.oab.org.br/ac_oab/certificado.htm/>. Acesso em: 26 maio 2011.

ALECRIM, E. O que é tecnologia da informação (TI)? **Infowester**, 24 fev. 2011. Disponível em: <http://www.infowester.com/col150804.php>. Acesso em: 13 set. 2011.

CERTINEWS. **Mercosul digital vai criar certificação para comércio eletrônico**. 2011. Disponível em: </http://www.certisign.com.br/certinews/banco-de-noticias/2011/02/mercosul-digital-vai-criar-certificacao-para-comercio-eletronico/>. Acesso em: 09 set. 2011.

CHEDE, C. T. **Grid computing**: um novo paradigma computacional. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2004.

CONVERGÊNCIA DIGITAL. **Brasil exporta modelo de certificação digital**. 2011. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?amp=&infoid=25352 &sid=5/>. Acesso em: 30 set. 2011.

_____. **Certificação digital**: mais de um milhão emitidos em 2010. 2010. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid =24569&sid=16/>. Acesso em: 27 set. 2011.

_____. **Consumidor brasileiro busca novas tecnologias para compras online**. 2011. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27415 &sid=16&utm%5Fmedium=twitter&utm%5Fsource=twitterfeed/>. Acesso em: 21 set. 2011.

ECOMMERCE ORG.**Tudo sobre comércio eletrônico**. São Paulo, 2008. Disponível em: <http://www.e-commerce.org.br/index.php>. Acesso em: 26 maio 2011.

_____. **Vendas comércio eletrônico – Brasil**. ([200-?]). Disponível em: <http:// www.e-commerce.org.br/stats.php>. Acesso em: 20 set. 2011.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **O que é o RIC**. ([200-?]). Disponível em: <http://www.iti.gov.br/twiki/bin/ view/Main/Ric/>. Acesso em: 01 jun. 2011.

_____. **Registro de marcas utilizará certificação digital da ICP-Brasil**. 2011. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Noticias/PressRelease2011Sep29_142538/>. Acesso em: 01 nov. 2011.

RIBEIRO, G. **Como funciona a certificação digital**. ([200-?]). Disponível em: </http://informatica.hsw.uol.com.br/certificado-digital4.htm/>. Acesso em: 30 maio 2011.

SÁ, C. C. de; ROCHA, J. **Treze viagens pelo mundo da matemática**. Porto: Porto editorial, 2010.

SANTOS, C. **Mercosul digital cria software para ID**. 2009. Disponível em: <http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid= 4839&sid=42/>. Acesso em: 26 ago. 2011.