

## O Uso da Certificação Digital Como Meio Seguro de Identificação

Márcia Prante<sup>1</sup>

Universidade do Oeste de Santa Catarina (UNOESC)  
Rua Oiapoc, 211 – Bairro Agostini  
CEP 89900-000, São Miguel do Oeste – SC – Brasil.

Pós Graduação em Redes de Computadores

marciaprante@hotmail.com

**Abstract.** *In computer networks, to ensure the authenticity of electronic documents, these are digitally signed. This article highlights the use of digital certificates as a means of identification. He begins by outlining a general notion of encryption and digital signatures, explains the meaning of the word infrastructure and highlights its importance as answers by the use of digital certificates, since interoperability is essential to most infrastructure. The approach is made, first, with respect to ICP-Brazil and the use of digital certificates. Furthermore, it highlights the need and use of interoperable certificates for authentication and identification. Finally, it analyzes the relationship and the use of digital certificate to create a new civil identification securely.*

*Keywords: Signature. Digital Certificate. Civil Identity.*

**Resumo.** *Nas redes de computadores, para garantir a autenticidade de documentos eletrônicos, estes são assinados digitalmente. O presente artigo destaca uso de certificados digitais como meio de identificação. Principia por delinear uma noção geral de criptografia e de assinaturas digitais, explica o significado da palavra infraestrutura e destaca a sua importância, pois responde pelo uso dos certificados digitais, considerando que a interoperabilidade é essencial à generalidade das infraestruturas. A abordagem é feita, primeiramente, com relação à ICP-Brasil e o uso dos certificados digitais. Além disso, destaca a necessidade e uso de certificados interoperáveis para a autenticação e identificação. Por fim, analisa a relação e o uso do certificado digital na criação de um novo documento de identificação civil de forma segura.*

*Palavras chave: Assinatura. Certificado Digital. Identidade Civil*

---

<sup>1</sup> Professor Orientador: Sandro Silva de Oliveira

## **1. Introdução**

A necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade, que a internet oferece e a eficiência em todos os processos de negócio, estes significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos.

À medida que a internet torna-se cada vez mais presente em nossa vida, a necessidade de segurança eletrônica torna-se ainda mais crítica. Qualquer empresa engajada em atividades on-line deve avaliar e gerenciar os riscos da segurança eletrônica associada as suas atividades, desta forma a segurança deve ser contínua e evolutiva.

O grande problema discutido hoje quando se fala em era eletrônica e digital é a segurança, ou melhor, a falta dela. Este artigo tem por objetivo principal destacar as principais tecnologias que podem auxiliar em uma melhor proteção dos dados e das informações que são de caráter sigiloso.

A utilização eficaz de técnicas criptográficas está no núcleo de várias estratégias de segurança para o gerenciamento de riscos. Este artigo relata algumas tecnologias como criptografia para segurança eletrônica, assinatura e certificado digital para oferecer privacidade, segurança e integridade a um dos ativos mais preciosos de uma empresa ou pessoa: os dados.

O presente artigo trata dos temas criptografia, assinatura digital, ICP Brasil, a certificação digital tema central deste artigo e a interoperabilidade como meio de reconhecimento da veracidade de documentos, o que agilizará e dará segurança aos negócios, bem como a sua utilização na criação de vários documentos como, por exemplo, o do registro de identidade civil conforme veremos nos itens subsequentes deste artigo.

## **2. O uso da criptografia**

A criptografia é uma técnica muito antiga a qual tem a função de tornar ilegíveis informações de teor sigiloso, impedindo desta maneira que pessoas sem autorização tenham acesso a determinada informação. Percebe-se assim que a busca pela segurança da informação não é uma preocupação recente, desta forma faz necessário entender o que é o criptografia: Souza (2010, p.41) diz que a “criptografia pode ser definida como a técnica de escrever em códigos e transformar textos legíveis em ilegíveis e vice-versa”.

Segundo o Cert (2012, p.67), por meio do uso da criptografia é possível “proteger os dados sigilosos armazenados em seu computador, [...] proteger seus backups contra acesso indevido, [...] proteger as comunicações realizadas pela Internet, como os e-mails, transações bancárias e comerciais”.

O uso da criptografia ainda de acordo com o Cert (2012), possibilita que as propriedades importantes para a proteção da informação sejam alcançadas:

**Integridade:** proteger a informação contra alteração não autorizada.

**Autenticidade:** verificar se a entidade é realmente quem ela diz ser.

**Confidencialidade, Sigilo ou Privacidade:** proteger uma informação contra acesso não autorizado.

**Não-repúdio ou Irretratabilidade:** evitar que uma entidade possa negar que foi ela quem executou uma ação.

Como já dito a criptografia é bastante antiga e desde os tempos mais primórdios que a técnica da criptografia vem sendo utilizada para armazenar, transportar e ocultar informações. O passado da humanidade conforme Behrens (2005, p.22) foi permeado por civilizações que aplicaram o método da criptografia em diferentes períodos:

Um dos exemplos mais conhecidos, data de 475 a.C., quando os gregos de Esparta utilizaram o primeiro sistema criptográfico aplicado à mensagens militares, denominado como “ESCÍTALA”. Este sistema era composto por um bastão de madeira envolto por uma tira fina de pergaminho que apresentava a escrita da mensagem secreta. Ao ser enviada esta tira era solta da madeira original, resultando num emaranhado de letras cuja leitura só poderia ser possível se fosse enrolada num bastão de idêntico tamanho e espessura. Este foi o sistema precursor do método criptográfico de transposição.

Behrens (2005), destaca ainda outras formas de criptografia usados na antiguidade como o cifrador de César [...]. O autor cita que a Criptologia como ciência teve início entre os árabes, por volta de 600 d.C.. O mesmo diz ainda que os ocidentais apenas começaram a usar a criptografia na Idade Média, Ciência esta que continua se desenvolvendo até hoje.

A evolução da criptografia desenvolveu dois métodos para cifrar, a SIMÉTRICA e a ASSIMETRICA. A criptografia simétrica segundo Souza (2010, p. 42) “é um tipo de criptografia na qual a chave utilizada para cifrar a informação é mesma utilizada para decifrá-la”. Além de utilizar a mesma chave, a criptografia simétrica utiliza o mesmo algoritmo em ambos os lados. A criptografia simétrica é também chamada de criptografia de chaves privadas.

Já a criptografia assimétrica, conforme Souza (2010, p. 42) também pode ser chamada de criptografia de chaves públicas, por fazer a troca de chaves no processo:

O processo de troca de chaves consiste na adoção de duas chaves, uma privada e uma pública. A chave pública é disponibilizada pelo proprietário para todos que desejam se comunicar com ele e nesse processo não é necessário criar um canal seguro para a troca da chave. A chave privada deve ser de conhecimento único e

exclusivo do proprietário, portanto, somente ele deverá ter acesso a ela. A técnica de criptografia assimétrica garante que um texto cifrado com uma chave pública só poderá ser decifrado com a chave privada correspondente [...].

A criptografia assimétrica, é considerada um dos melhores sistemas de segurança segundo Behrens (2005), em virtude da chave privada ser de conhecimento apenas do seu titular [...] A vantagem do assimétrico é que para sua quebra há a necessidade de se arcar com um alto custo, bem como, com um elevado tempo. Essas dificuldades tornam “quase” impossíveis à execução de qualquer forma de interceptação e leitura dos documentos criptografados.

O método de criptografia assimétrica segundo Behrens (2005) tem como principal utilização a sua aplicação na assinatura digital, que tem por finalidade criar a possibilidade de assegurar um documento ou mensagem.

### **3. Assinatura digital**

Diversas iniciativas vêm sendo implementadas no decorrer dos últimos anos como forma de regular e atender demandas fomentadas pelo crescimento das transações online. Dentro dessa evolução, uma das ações em destaque é a Assinatura Digital.

Antes mesmo de se falar em assinatura digital, faz-se necessário compreender o significado do termo assinatura. Borba (2002, p.144) define assinatura como: “aposição do nome num documento como forma de confirmar autoria ou responsabilidade pelo que ele contém.” Nota-se que o indivíduo ao assinar está conferindo segurança a este documento.

Cert (2012) diz que a “assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada”.

A assinatura digital utiliza-se da criptografia assimétrica, baseando-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para cifrar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi cifrado com a chave privada, somente a chave pública correspondente pode decifrar, garantindo assim a autenticidade do documento. (CERT, 2012).

Para verificar se um documento foi ou não adulterado (integridade) utiliza-se se da função de Resumo de mensagem, também conhecido por *Hash*. Segundo Souza (2010), *Hash* é uma função matemática que age como se fosse uma impressão digital da informação a ser enviada, e não se pode obter a mensagem original a partir do *hash*, ou seja é unidirecional.

O principal objetivo da função *hash* é verificar se a mensagem sofreu algum tipo de alteração e a mudança de apenas um único bit na mensagem já irá gerar um *hash* totalmente diferente do anterior identificando assim que o documento foi adulterado.

Para que a assinatura digital seja caracterizada, conforme Souza (2012) ainda é necessário criptografar o próprio *hash*, como demonstrado na figura 1, pois sem criptografar o *hash* a mensagem poderia ser capturada na transmissão, gerado um novo *hash* anexado à mensagem alterada de forma que o receptor acreditaria na integridade da informação.



Figura 1: Funcionamento da Assinatura Digital  
 Fonte: Freund e Reiter (2008 apud SOUZA, 2010, p.47).

Utilizando-se dos procedimentos acima, o uso da assinatura digital possibilita garantir a autenticidade e a integridade no envio de uma informação. Dessa forma, a assinatura digital tem o mesmo valor que a assinatura manual. Qualquer assinatura digital tem o mesmo valor jurídico que teria se as partes tivessem se encontrado e assinado papéis a mão.

#### 4. ICP Brasil

O continuo avanço tecnológico e o uso crescente da internet, encurtou distancias e diminuiu o tempo de deslocamento para efetuar determinadas transações. Dessa forma, facilitou muito transações comerciais e bancárias. No entanto, da mesma forma que o mundo virtual nos oferece meios e facilidades, também permitiu o aparecimento de fraudes, na qual

demandou a necessidade da existência de mecanismos que dessem segurança para determinadas transações.

Diante da necessidade de segurança criou-se a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira), através da Medida Provisória 2.200-2, onde:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (BRASIL, 2001).

Conforme cita Alecrim (2009), é conveniente que cada nação conte com uma Infraestrutura de Chaves Públicas (ICP) ou, em inglês, Public Key Infrastructure (PKI), isto é, um conjunto de políticas, técnicas e procedimentos para que a certificação digital tenha amparo legal e forneça benefícios reais à sua população. O Brasil conta com a ICP-Brasil para essa finalidade.

A Alemanha foi o primeiro país da Europa, conforme Alecrim (2009), a editar uma lei específica sobre o tema:

A Aignaturgesetz, de 1º de agosto de 1997 introduziu as condições estruturais para a adoção das assinaturas eletrônicas [...] naquele país. [...] O legislador alemão previa a obrigatoriedade de os prestadores de serviços de certificação digital obterem uma licença perante o órgão público competente para que pudessem iniciar as suas atividades.

Nos Estados Unidos o desenvolvimento e a expansão das infraestruturas de chaves públicas segundo Menke (2011a), se deu de forma bastante desorganizada e hoje em dia são diversas as ICPs em funcionamento naquele país, com base tanto em iniciativas governamentais quanto em iniciativas privadas.

As vantagens de uma ICP nacional com a presença de uma entidade pública na posição de supervisão do sistema são inúmeras, ressalta Menke (2011a). A primeira é que proporciona uma uniformidade de padrões técnicos e políticas implementadas, facilitando a interoperabilidade entre os usuários finais de titulares de certificados. Isso significa que os usuários, em regra, poderão acessar as aplicações que demandem a utilização de certificados digitais para a sua identificação com o emprego de certificado emitido por qualquer uma das Autoridades Certificadoras que fazem parte da infraestrutura.

Conforme Menke (2011a), a uniformidade certamente vem em benefício do consumidor, uma vez que, a princípio, não necessitará adquirir diversos certificados digitais para comprovar a sua identidade no meio virtual e assinar digitalmente.

Menke (2011a), destaca ainda ser mais racional e de resultados melhores a implementação de uma ICP nacional. Outro aspecto é que, havendo uma ICP mais abrangente, como são a brasileira e a alemã, torna-se bem mais viável e atraente a celebração de acordos internacionais de reconhecimento recíproco de certificados digitais, o que possibilita transações eletrônicas internacionais mais seguras.

Percebe-se que é fundamental a existência de uma ICP (PKI), nacional ou abrangente, por questões de uniformidade e de segurança, já que se utiliza de chaves públicas. Mas afinal, qual é a função de um ICP? Nakamura e Geus (2007), descrevem as funções específicas de uma ICP como:

**Registro:** processo na qual uma entidade se registra a uma autoridade certificadora – CA [...]. **Inicialização:** é o processo no qual a entidade obtém os valores necessários para o início das comunicações com a PKI [...].

**Certificação:** é o processo em que a CA envia um certificado digital para a entidade que a solicitou e o coloca em um repositório [...]. **Recuperação do par de chaves:** [...] A PKI deve fornecer um sistema que permita a recuperação, sem apresentar riscos inaceitáveis de comprometimento da chave privada. **Geração de chaves:** dependendo da política da CA, o par de chaves pode ser gerado pelo próprio usuário em seu ambiente local ou pela CA. **Atualização de chaves:** todo par de chaves precisa ser atualizado regularmente [...]. **Certificação cruzada:** A certificação cruzada é necessária quando um certificado de uma CA é enviado a outra CA, [...] Essa interoperabilidade entre certificados é importante em um ambiente corporativo [...]. **Revogação:** [...] mudança de nome, [...], quebra no sigilo da chave privada. **Distribuição e publicação dos certificados e da notificação de revogação:** a distribuição dos certificados inclui sua transmissão a seu proprietário e sua publicação em um repositório [...].

Em se tratando da ICP-Brasil, quanto à estruturação, o que a caracteriza é a presença de uma entidade de direito público, a autarquia federal, Instituto Nacional de Tecnologia da Informação - ITI, no ápice da cadeia de certificação. O ITI é o responsável pela manutenção da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Como Autoridade Certificadora Raiz (AC-Raiz), controla outras políticas e regulamentações relacionadas à tecnologia no Brasil.

A ICP-Brasil é mantida e auditada pelo ITI, órgão público que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil, cujos membros, representantes dos poderes públicos, sociedade civil organizada e pesquisa acadêmica, são nomeados pelo Presidente da República. A principal linha de ação do ITI é a popularização da certificação digital ICP-Brasil e a inclusão digital, atuando sobre questões como sistemas criptográficos, hardware compatíveis com padrões abertos e universais, convergência digital de mídias, desmaterialização de processos, entre outras.

Conforme ITI (2012a), a ICP-Brasil é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também, tem o papel de

credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Compete à AC-Raiz (ITI) emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados. (ITI, 2012a).

Uma Autoridade Certificadora - AC, segundo ITI (2012a) é “uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais”. Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves.

Segundo ITI (2012a) é também função da AC “emitir listas de certificados revogados - LCR e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação – DPC”, a DPC deve ser pública, para permitir que as pessoas possam saber como foi emitido o certificado digital. Ainda estabelece e fazer cumprir, pelas Autoridades Registradoras a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação feita.

Uma AR - Autoridade de Registro, conforme ITI (2012a), “entidade responsável pela interface entre o usuário e a Autoridade Certificadora, vinculada a uma AC tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC”. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

Segundo o ITI (2012a) a estrutura da ICP-Brasil conta com dez Autoridades Certificadoras conforme pode ser visualizado na figura 2, sendo elas: “SERPRO - Serviço Federal de Processamento de Dados, Caixa Econômica Federal, Serasa Experian, Receita Federal do Brasil, Certisign, Imprensa Oficial do Estado de São Paulo, AC JUS, AC PR, Casa da Moeda Do Brasil, Valid Certificadora Digital”.

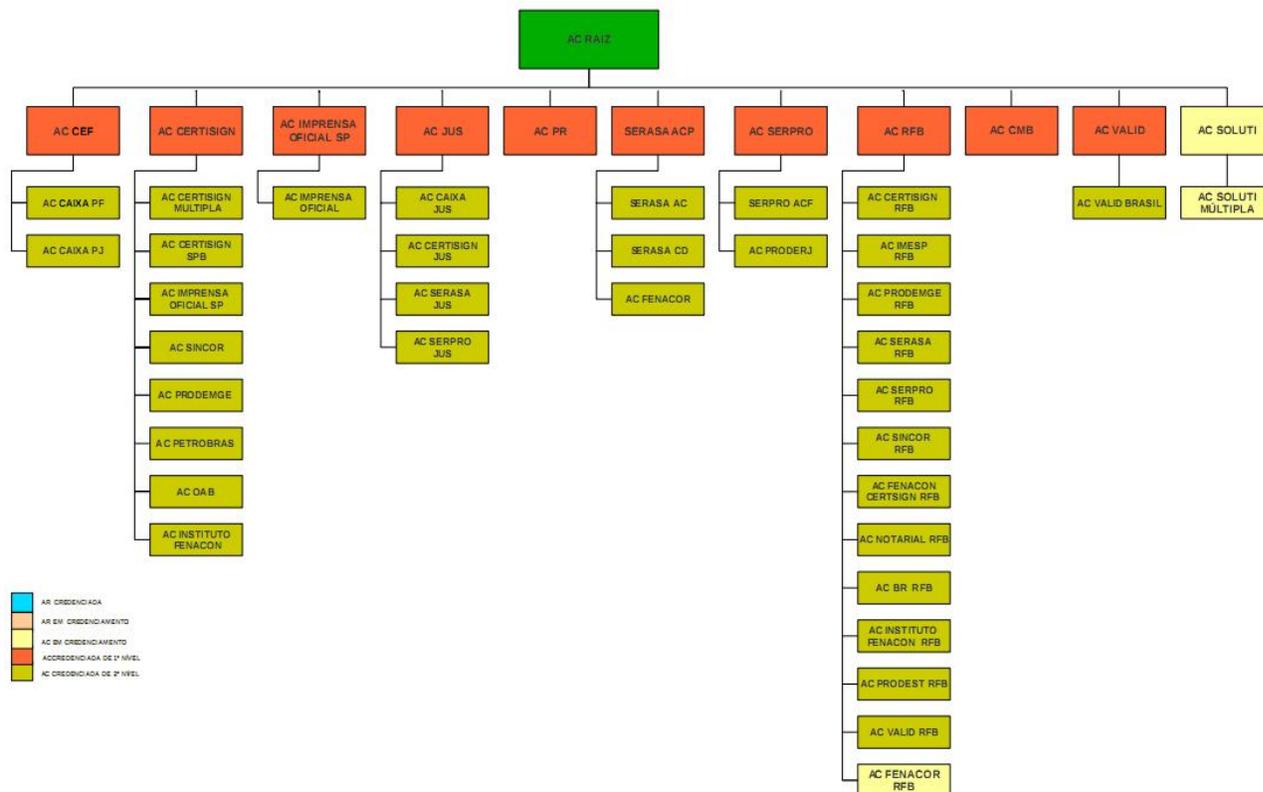


Figura 2: Estrutura da ICP Brasil

Fonte: ITI (2012c).

São essas instituições que devem ser procuradas por quem deseja obter certificado digital legalmente reconhecido no Brasil. Cada uma dessas entidades pode ter critérios distintos para a emissão de certificados, o que inclusive resulta em preços diferentes, portanto, é conveniente ao interessado saber qual AC é mais adequada às suas atividades.

A instituição da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, criada há onze anos, veio atender a necessidade da sociedade brasileira no quesito de segurança nas transações pelo meio virtual. Prova disso segundo ITI (2011), atualmente são emitidos um milhão de certificados por ano, “As Autoridades Certificadoras credenciadas de primeiro e segundo nível chegam hoje a 45. As Autoridades de Registro saltaram de apenas 12, em 2002, para 389 este ano. O mesmo ocorreu com as instalações técnicas físicas e de ARs lógicas, que chegaram a 885 e 1602”, respectivamente, no mês de março deste ano, conforme ITI (2011).

Em onze anos de existência, a ICP-Brasil atingiu os objetivos de criar um sistema nacional de certificação digital que abrange todo o território nacional e ter a interoperabilidade que permite o uso da mesma identidade eletrônica para diversas aplicações.

O Brasil, por meio da ICP-Brasil, deve estar preparado, segundo ITI (2011), as aplicações em certificação digital vão crescer cada vez mais, deve-se estar atento à evolução

tecnológica da ICP-Brasil, aos novos usos, à evolução dos algoritmos criptográficos e de todo o hardware envolvido no processo. “O desafio para o ITI hoje é estar no estado da arte dessa tecnologia”.

É graças à ICP-Brasil que as certificações digitais no país são amplamente aceitas e utilizadas, especialmente do ponto de vista legal. Em poucos anos de existência, a ICP-Brasil atingiu os objetivos de criar um sistema nacional de certificação digital que abrange todo o território nacional e ter a interoperabilidade que permite o uso da mesma identidade eletrônica para diversas aplicações.

## 5. Certificado digital

A certificação digital é uma ferramenta de segurança que permite ao cidadão brasileiro realizar transações, no meio eletrônico, que necessitem de segurança, como assinar contratos, obter informações sensíveis do governo e do setor privado, entre outros exemplos. O Brasil conta com um Sistema Nacional de Certificação Digital que é mantido pelo Instituto Nacional de Tecnologia da Informação.

O certificado digital da ICP-Brasil, segundo ITI (2012b), além de identificar o cidadão na internet, garante por meio da legislação atual, validade jurídica aos atos praticados com seu uso. A certificação digital permite que aplicações, como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas de forma segura e confiável.

Por meio de procedimentos lógicos e matemáticos, o certificado conforme ITI (2012b) é um documento eletrônico que assegura a integridade das informações e a autoria das transações. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

Segundo ITI (2012b), “o certificado equivale a uma carteira de identidade virtual ao permitir a identificação de uma pessoa no meio digital/eletrônico”. Ao enviar uma mensagem ou fazer alguma transação pela rede mundial de computadores usando um certificado, confere-se validade legal ao documento e identificação. Essa tecnologia confere validade jurídica ao documento assinado digitalmente de forma equivalente ao papel assinado de próprio punho.

Devido a interoperabilidade, segundo Burnett e Paine (2002) o formato de certificado digital mais aceito é o X.509, versão 3 da *International Telecommunications Union*.

Burnett e Paine (2002) destacam que todas as versões dos certificados X.509 contêm os seguintes campos: **Versão do certificado**, (versão 1, 2 ou 3), **Número de série do certificado**, campos este que contém um valor de número inteiro único, **Algoritmo de assinatura**, **Nome e assinatura do emissor** ou entidade que assinou o certificado,

**Validade**, no qual consta o período de validade do certificado, **Nome da pessoa ou entidade** a que o certificado se refere e a **Chave pública**, campo este que contém a chave pública do sujeito.

O ITI (2012b) complementa dizendo que um certificado digital contém os dados descritos anteriormente bem como e-mail, entre outras informações. Ao confrontar esses dados com as características do seu portador, pode-se saber se o mesmo é de fato a pessoa identificada.

Sincic, (2009), descreve o Certificado Digital, como sendo um arquivo de pouco mais de 1Kb que contém as chaves pública e privada. A chave pública é conhecida por todos os que se comunicam com o proprietário da chave, a chave privada só é conhecida do proprietário e da CA que a emitiu, desta forma o modelo de criptografia utilizado é assimétrico, o proprietário utiliza a chave privada para criptografar suas mensagens e a chave pública contém o algoritmo para descriptografar. O inverso na comunicação ocorre quando o destinatário envia para o proprietário utilizando a chave pública para criptografar, garantindo que apenas o proprietário conseguirá descriptografar, uma vez que ele é o único que tem a chave inversa, neste caso a privada. Sincic, (2009), destaca ainda que “o certificado contém um importante dado dentro dele chamado de “subject”, onde constam os dados de quem é o proprietário da chave e outros dados que a certificadora queira incluir”.

O ITI (2012b) descreve o procedimento para quem deseja obter um certificado digital. Deve-se em primeiro plano escolher uma Autoridade Certificadora (AC) da ICP-Brasil, posteriormente solicitar no próprio portal da internet da AC escolhida a emissão de certificado digital de pessoa física ou jurídica.

Para a emissão de um certificado digital O ITI (2012b) destaca que é necessário o solicitante ir pessoalmente a uma Autoridade de Registro (AR) da Autoridade Certificadora para validar os dados preenchidos na solicitação. Esse processo é chamado de validação presencial e será agendado diretamente com a AR que instruirá o solicitante sobre os documentos necessários, após este procedimento a AC e/ou AR notificará o cliente sobre os procedimentos para baixar o certificado e deverá prestar todo o suporte técnico quando solicitada pelo usuário. O ITI (2012b) ressalta ainda: “quando o certificado digital estiver perto do vencimento, este poderá ser renovado eletronicamente, uma única vez, sem a necessidade de uma nova validação presencial”.

Ao procurar informações para adquirir um certificado digital deve-se ficar atento a categoria de certificado que é mais conveniente para determinada atividade. Segundo Alecrim (2009) a ICP-Brasil oferece duas categorias de certificados digitais: “A e S, sendo que cada uma se divide em quatro tipos: A1, A2, A3 e A4; S1, S2, S3 e S4”. A categoria A é direcionada para fins de identificação e autenticação, enquanto que o tipo S é direcionado a atividades sigilosas.

Destaca-se as características que tornam as versões de ambas as categorias diferentes entre si, conforme Alecrim (2009): **A1 e S1**: a geração das chaves é feita por software; chaves de tamanho mínimo de 1024 bits; armazenamento em dispositivo de armazenamento (como um HD) e tem validade máxima de um ano. O certificado do tipo **A2 e S2**, a geração das chaves é feita por software; chaves de tamanho mínimo de 1024 bits, o armazenamento é

feito em cartão inteligente (com chip) ou token (dispositivo semelhante a um pendrive) e tem validade máxima de dois anos. No certificado do tipo **A3 e S3**, a geração das chaves é feita por hardware; chaves de tamanho mínimo de 1024 bits sendo que o armazenamento é feito em cartão inteligente ou token e a validade máxima é de três anos. Já no certificado do tipo **A4 e S4** a geração das chaves é feita por hardware com chaves de tamanho mínimo de 2048 bits onde o armazenamento é feito em cartão inteligente ou token e a validade máxima é de três anos.

Os certificados A1 e A3 segundo Alecrim (2009), são os mais utilizados, sendo que o A1 é geralmente armazenado no computador do solicitante, enquanto que o A3 é guardado em cartões inteligentes (*smartcards*) ou tokens protegidos por senha.

Segundo O ITI (2012b), a “AC [...] pode informar sobre aplicações, custos, formas de pagamento, equipamentos, documentos necessários e demais exigências. Além desses, há os do tipo T3 e S3, que também tem validade de até cinco anos”.

Além dos tipos de certificados citados anteriormente, Alecrim (2009) destaca ainda duas importantes iniciativas: o e-CPF e o e-CNPJ. O e-CPF é um certificado digital direcionado a pessoas físicas, sendo uma espécie de extensão do CPF, enquanto que o e-CNPJ é um certificado digital que se destina a empresas ou entidades, de igual forma, sendo um tipo de extensão do CNPJ.

Segundo Alecrim (2009) ao adquirir um e-CPF, uma pessoa tem acesso pela internet a diversos serviços, muitos dos quais até então disponíveis apenas em postos de atendimento de determinadas instituições. O e-CPF e o e-CNPJ estão disponíveis nos tipos A1 e A3.

É importante destacar que o e-CPF e o e-CNPJ não são gratuitos. Alecrim (2009), diz que sua aquisição deve ser feita em entidades conveniadas à Receita Federal e que os preços não são padronizados sendo que variam de acordo com a empresa e com o tipo de certificado.

O Brasil é provavelmente um dos países mais adiantados em relação à utilização de certificados digitais, vários bancos já utilizam chips com certificados digitais, nesses casos, a Autoridade Certificadora é o próprio banco, e por isso apenas os bancos emissores e seus clientes acreditam nesses certificados.

Mais que um avanço tecnológico e científico, a certificação digital é uma aplicação de caráter social, que permite maior segurança, redução de custos operacionais, aumento de produtividade, economiza tempo e diminui distâncias.

## **6. ICP, Certificado e interoperabilidade**

Como já definido anteriormente a ICP é uma infraestrutura e por se tratar de uma infraestrutura a interoperabilidade é explícita. Portanto, a interoperabilidade deve estar

presente e deve ser um atributo indispensável, sempre que o serviço fornecido tiver por escopo atingir a coletividade.

Interoperabilidade é definida pelo Comitê Executivo de Governo Eletrônico (2012) como sendo a “Habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, software e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados”.

No entender de Menke (2011b), foi acertada a posição adotada pelo Brasil sobre o modelo de infraestrutura de chaves públicas escolhido por meio da Medida Provisória nº 2.200 e regulações posteriores, pois desta forma “uma infraestrutura de segurança disseminada, uniforme, evita soluções díspares, isoladas, não interoperáveis” e foi essa a ideia que influenciou a criação da ICP-Brasil, justamente a de constituir uma infraestrutura para a coletividade, para toda a sociedade, tornando mais facilitada a comunicação entre os titulares de certificados digitais.

Há muito ainda por fazer para que consiga atingir a desejada interoperabilidade. Menke (2011b) destaca que a interoperabilidade “deve ser encarada como um desafio, algo em constante construção, e não como algo pronto e acabado, que tenha se esgotado com a simples edição do conjunto normativo mencionado”.

Menke (2011b) destaca que um dos desafios é à compatibilidade dos cartões inteligentes, leitoras, e softwares. “Há que se padronizar estes instrumentos, afim de que na prática se tenha a possibilidade de assinar digitalmente bem como verificar as assinaturas digitais a partir de qualquer equipamento.”

O que Menke (2011b) quer dizer é que não basta que os dispositivos de criação e de verificação das assinaturas funcionem aqui e agora. Da mesma forma, não basta que todos os indivíduos envolvidos na transação ou na comunicação utilizem o padrão do formato do certificado X.509. Menke (2011b) ainda destaca que “pretender que a interoperabilidade se resolva apenas a partir da utilização disseminada do padrão X.509 é, sem dúvida, analisar o problema de forma bastante superficial [...]”.

Para haver interoperabilidade no entender de Menke (2011b) “é necessário que todo o sistema tenha funcionado satisfatoriamente desde a primeira identificação do primeiro titular de certificado e que continue a funcionar, indefinidamente, de forma razoável.” Entende-se assim ser importante que os documentos básicos das autoridades certificadoras contenham um mínimo de similaridade quanto aos aspectos primordiais dos serviços, afim de que seja possível a “conversação”.

Para auxiliar nesta conversação o Comitê Executivo de Governo Eletrônico (2012) ressalta que criar políticas e especificações claramente definidas para interoperabilidade e gerenciamento de informações é fundamental.

A arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico, segundo o Comitê Executivo de Governo Eletrônico (2012) é concebida como uma estrutura básica

para a estratégia de governo eletrônico, aplicada inicialmente ao governo federal – Poder Executivo, não restringindo a participação, por adesão voluntária, de outros poderes e esferas de governo, a qual propicia uma melhor conexão do governo, tanto no âmbito interno como no contato com a sociedade e, em maior nível de abrangência, com o resto do mundo. Desta forma a arquitetura e-PING têm por finalidade ser o paradigma de interoperabilidade para o governo federal, inicialmente no âmbito do Poder Executivo, onde seu uso é obrigatório.

O Padrão de Interoperabilidade de Governo Eletrônico e-PING têm como foco de trabalho todos os assuntos que forem relevantes para garantir a interconectividade de sistemas, integração de dados, acesso a serviço de governo eletrônico e gerenciamento de conteúdo.

A implementação dos padrões de interoperabilidade, segundo o Comitê Executivo de Governo Eletrônico (2012) “deve priorizar o uso de software público e/ou software livre”, sendo que a aplicação da e-PING tem o objetivo de facilitar as interações do governo com a sociedade e que sejam realizadas de forma simples e direta, sem prejuízo da legislação vigente.

Outro termo destacado Menke (2011b) o qual pode significar interoperabilidade é a expressão “neutralidade tecnológica”. “O fato de um sistema ou de uma lei ser tecnologicamente neutra virou atributo de modernidade, de progresso, de se estar no caminho correto”.

O fato de um sistema ou de uma lei ser tecnologicamente neutra, conforme Menke (2011b) virou significado de modernidade e progresso, na qual se estaria no caminho correto da interoperabilidade. O autor ainda destaca que as manifestações escutadas em eventos técnicos e jurídicos da área de tecnologia da informação trilham a lógica que desemboca nas seguintes conclusões: “o que é tecnologicamente neutro é bom, o que não é tecnologicamente neutro é ruim”. E por assim ser, ainda nas palavras de Menke (2011b) “poucos param para pensar e avaliar se realmente a tão aclamada neutralidade tecnológica deve merecer mesmo esse status de dogma inabalável e indiscutível”.

Ser tecnologicamente neutro segundo Menke (2011b) é o atributo conferido principalmente às legislações, e significa não se privilegiar determinada técnica ou tecnologia em detrimento de outra. Uma segunda virtude seria a de que as legislações neutras teriam maior longevidade, não carecendo de alterações a todo o momento que as inovações fossem surgindo.

A neutralidade tecnológica ao invés de ajudar, pode atrapalhar na busca da indispensável interoperabilidade. Conforme a reflexão de Menke (2011b), a neutralidade tecnológica prega a maior abertura possível, e, ao assim proceder, acaba por transformar o que seria uma saudável tolerância e abertura, em vazio, que pode ser preenchido por qualquer coisa. E esse vazio prejudica justamente uma das características mais crucias de uma infraestrutura de chaves públicas: a interoperabilidade. Menke (2011b), ainda completa “se tudo for possível, pode ser que nada seja viável e realizável”.

Interoperabilidade e neutralidade tecnológica são expressões antagônicas, destaca Menke (2011b), onde uma delas for à finalidade, a outra certamente será deixada de lado, portanto a neutralidade tecnológica não pode ser vista como um significado indiscutível, pelo contrário, a neutralidade tecnológica deve ser observada na medida do possível e com cautela, para a finalidade de que não se estanque a pesquisa e a busca por novas alternativas de meios de identificação no ambiente virtual.

Para que se tenha interoperabilidade, de acordo com a reflexão de Menke (2011b) “algum tipo de escolha deve ser feito, caso o nosso intuito não seja o da institucionalização do caos.” Neste sentido a arquitetura e-PING (Padrão de Interoperabilidade de Governo Eletrônico), veio para estabelecer padrões de conexões e comunicação.

Como já foi visto a interoperabilidade é um atributo necessário de qualquer infraestrutura que pretenda atingir a coletividade, na qual os aparelhos ou equipamentos terão capacidade de comunicar-se entre si, independentemente de sua procedência ou do seu fabricante. Para que se conquiste essa tão desejada interoperabilidade, as pessoas e entidades devem estar engajadas num esforço contínuo, onde qualquer usuário possa simplesmente acoplar-se a ICP e dela fazer uso quando necessário, na qual sistemas, processos e culturas de uma organização sejam gerenciados e direcionados para maximizar oportunidades de troca e reuso de informações.

## **7. Registro Único de Identidade Civil**

A esfera digital tem sido o berço do desenvolvimento de múltiplas estratégias, com as mais variadas aplicações, e passo a passo caminha rumo ao amadurecimento de uma nova abordagem para muitos dos processos que hoje observamos e praticamos no mundo físico. A primeira, já em evidencia é a adoção do Registro de Identidade Civil (RIC), que oferecerá ao cidadão brasileiro uma identidade moderna e confiável tanto no mundo físico como no virtual.

O novo modelo de identificação pessoal, batizado como Registro de Identidade Civil ou, simplesmente, RIC, está prestes a ser regulamentado no Brasil. Segundo o ITI (2009) com esta inovação, informações importantes no dia-a-dia de qualquer cidadão, como RG, CPF, PIs/PAsEP, título de eleitor, assim como os dados da carteira de habilitação e de trabalho, serão reunidas em um único documento de identificação considerado mais robusto, além de ser mais conveniente de transportar, pois todas as informações estão em um único documento, sem ocupar muito espaço na carteira, mas destaca-se algo ainda mais importante que é a segurança que o novo sistema oferece. Ainda de acordo com ITI (2009) o RIC não deve substituir outros documentos, como CPF ou PIS, por exemplo, pois o governo optou por manter as bases próprias das instituições que deverão se comunicar com a base do Cadastro Nacional do RIC - CANRIC.

Pelo atual sistema em vigor, de acordo com o ITI (2011) um mesmo cidadão pode ter 27 diferentes números de carteira de identidade, um emitido em cada unidade da federação.

Outra questão crítica é o roubo de identidade. De posse de documentos falsos ou roubados, que estão à venda no mercado clandestino, um golpista pode abrir contas, alugar imóveis, fazer financiamentos, comprar carros e, até mesmo, abrir empresas. Com o RIC, a expectativa é por fim a essas situações, ou ao menos dificultá-las.

O ano de 1997 marcou o advento da era da documentação digital para os cidadãos brasileiros. O ITI (2009), destaca que em abril deste mesmo ano surgia a Lei nº 9.454, que passaria a instituir o número único de Registro de Identidade Civil. Já o ano de 2009 com a sanção da Lei nº 12.058 pode ser considerado como um marco, pois de acordo com o ITI (2011) essa legislação fez alterações à Lei 9.454, de 1997.

O Registro de Identidade Civil irá mudar, definitivamente, a forma como o cidadão brasileiro se identifica diante das instituições públicas e privadas, de acordo com o ITI (2009), colocará o Brasil em um novo patamar em termos de segurança e cidadania, coibindo fraudes e roubos de identidade, impossibilitando o cadastro duplo da mesma pessoa através de um número único de identificação válido para todo o País. “Pelo Projeto RIC, cada estado terá seu sistema e seu banco de dados e todos eles conectados ao Órgão Central”.

De acordo com o ITI (2009), o RIC agrega o que há de mais moderno em termos de segurança na identificação, pois devem ser incluídos dados básicos do cidadão, também o uso biometria e certificação digital no sistema, não há como adulterá-los, pois qualquer nova inclusão será automaticamente comparada com todas as outras previamente existentes, o que impede a alteração dos dados básicos identificadores do indivíduo, inclusive do número RIC. Ainda de acordo com o ITI (2009), “as alterações desses dados só serão possíveis com a existência de documentos que as embasarão, documentos esses que serão certificados digitalmente. Espera-se que o recadastramento de toda a população brasileira não ultrapasse o ano de 2017”.

O material utilizado na confecção do RIC conforme o ITI (2009) será o policarbonato (mesmo material do qual são fabricados os cartões de crédito) o qual possui uma durabilidade mínima de dez anos. Além disso, é resistente a torções, flexões e altas temperaturas, ajudando a preservar por longo tempo a integridade do documento. Os dados nele contidos como nome, filiação e sexo do cidadão são gravados a laser, modernas medidas de segurança, como tintas, fundos complexos e efeitos óticos especiais, também garantirão maior proteção às informações.

O ITI (2009), destaca que para habilitar a usar o número RIC, “o cidadão deve dirigir-se a um dos 4.375 institutos de identificação distribuídos em todo o país. O cadastro consiste na coleta da impressão digital, que será armazenada no órgão central, administrado pelo ministério da Justiça”. Os dados do cidadão serão pesquisados e confrontados no sistema AFIS, garantindo, assim, a unicidade do número emitido. O sistema AFIS (Automated Fingerprint Identification System), é uma poderosa ferramenta de coleta, armazenamento e comparação de impressões digitais, que passará a deter todas as informações necessárias ao RIC, sistema este que o governo federal adquiriu em 2004. O chip, contendo os dados



## 8. Considerações finais

O mundo em que vivemos evolui constantemente, com novas tecnologias trazendo diversos benefícios para as pessoas, como o uso de tecnologias sem fio, por exemplo, as pessoas ganham em produtividade, acessibilidade e desfrutam das facilidades obtidas com a mobilidade, porém como ocorre com tudo o que é novo, seja uma tecnologia ou um negócio, os riscos devem ser avaliados e minimizados.

O artigo abordou a importância da segurança, descrevendo como o uso da criptografia é fundamental, pois permitiu o uso de assinaturas digitais, bem como utilização de certificados digitais como meio seguro de autenticação, funcionando como uma espécie de documento de identidade.

Como visto no artigo, a ICP Brasil foi criada como órgão regulamentador com amparo legal, através Medida Provisória 2.200-2, sendo uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

O Brasil ao optar-se por um sistema de Infraestrutura de Chaves públicas, conclui-se que o mesmo seguiu o caminho correto, pois tem no ápice da cadeia de certificação uma entidade de direito público com a finalidade de credenciar e fiscalizar as operações das Autoridades Certificadoras que tencionem obter os níveis mais altos de segurança em suas operações.

Como já descrito anteriormente a ICP é uma infraestrutura e por se tratar de uma infraestrutura a interoperabilidade é explícita. Portanto, a interoperabilidade deve estar presente e deve ser um atributo indispensável.

Finalizando o artigo destaca-se a criação do Registro Único de Identidade Civil, o qual está prestes a ser regulamentado no Brasil, conforme visto, o RIC irá mudar definitivamente, a forma como o cidadão brasileiro se identifica diante das instituições públicas e privadas, colocando assim o Brasil em um novo patamar em termos de segurança e cidadania.

Conclui-se assim que a segurança é fundamental no momento em que vivemos, tanto para os negócios como em transações pessoais. Desta forma como já visto, o uso de criptografia, da assinatura digital e da certificação digital são essenciais, pois além de possibilitarem segurança ainda possibilitam a criação de novos documentos de identificação de forma segura.

## 9. Referências

ALECRIM, Emerson. **Entendendo a Certificação Digital**. 2009. Disponível em: <<http://www.infowester.com/assincertdigital.php>>. Acesso em: 26 jul. 2012.

BEHRENS, Fabiele. **A assinatura Eletrônica como requisito de validade dos negócios jurídicos e a inclusão digital na sociedade brasileira.** 2005. 138f. Dissertação (Mestrado em Direito Econômico e Social) - Pontifícia Universidade Católica do Paraná. 2005. Disponível em: [http://www.biblioteca.pucpr.br/tede/tde\\_arquivos/1/TDE-2005-10-07T063157Z-206/Publico/FabieleDto.pdf](http://www.biblioteca.pucpr.br/tede/tde_arquivos/1/TDE-2005-10-07T063157Z-206/Publico/FabieleDto.pdf)>. Acesso em: 10 ago. 2012.

BORBA, Francisco da Silva. **Dicionário de usos do Português do Brasil.** São Paulo: Ática, 2002.

BRASIL. Medida Provisória n. 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Presidência da República.** Brasília, DF, 24 de ago. de 2001. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/MPV/Antigas\\_2001/2200-2.htm](https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm)>. Acesso em: 13 set. 2012.

BURNET, Steve; PAINE, Stephen. **Criptografia e segurança: o guia oficial.** Rio de Janeiro: Elsevier, 2002.

CERT - CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet.** São Paulo, 2012.

COMITÊ EXECUTIVO DE GOVERNO ELETRÔNICO. **e-PING Padrões de Interoperabilidade de Governo Eletrônico.** 2012. <http://www.governoeletronico.gov.br/biblioteca/arquivos/documento-da-e-ping-versao-2012/view>>. Acesso em: 01 out. 2012.

ITI - Instituto Nacional de Tecnologia da Informação. A evolução da ICP-Brasil. **Revista Digital.** Ano 3, n. 4, p.5-11, 1º semestre, 2011. Disponível em: [http://www.iti.gov.br/images/publicacoes/revista-digital/revista\\_digital-2011-1.pdf](http://www.iti.gov.br/images/publicacoes/revista-digital/revista_digital-2011-1.pdf)>. Acesso em: 18 set. 2012.

\_\_\_\_\_. **Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).** 2012. Disponível em: <http://www.iti.gov.br/index.php/icp-brasil/o-que-e>>. Acesso em: 19 set. 2012.

\_\_\_\_\_. **O que é Certificado Digital**. 2012.

Disponível em: <<http://www.iti.gov.br/index.php/certificacao-digital/o-que-e>>. Acesso em: 24 set. 2012.

\_\_\_\_\_. Cidadania digital. **Revista Digital**. Ano 1, n. 2, p.18-21, 2º semestre, 2009.

Disponível em: <[http://www.iti.gov.br/images/publicacoes/revista-digital/revista\\_digital\\_1\\_semestre2009.pdf](http://www.iti.gov.br/images/publicacoes/revista-digital/revista_digital_1_semestre2009.pdf)>. Acesso em: 04 out. 2012.

\_\_\_\_\_. **Estrutura resumida das ACs**. 2012. Disponível em:

<[http://www.iti.gov.br/images/icp-brasil/estrutura/atualiza%C3%A7%C3%A3o14/Estrutura\\_da\\_ICP-Brasil\\_-\\_site.pdf](http://www.iti.gov.br/images/icp-brasil/estrutura/atualiza%C3%A7%C3%A3o14/Estrutura_da_ICP-Brasil_-_site.pdf)>. Acesso em: 17 out. 2012.

MENKE, Fabiano. Assinaturas Digitais, Certificados Digitais, Infra-Estrutura de Chaves Públicas Brasileira e a ICP Alemã. **Sistema Eletrônico de Editoração de Revistas**. 2011.

Disponível em:

<<http://www.buscalegis.ufsc.br/revistas/files/journals/2/articles/4429/public/4429-4422-1-PB.pdf>>. Acesso em: 15 set. 2012.

\_\_\_\_\_. **Considerações Sobre a Interoperabilidade Aplicada à Infra-Estrutura de Chaves Públicas**. 2011. Disponível em:

<<http://www.buscalegis.ufsc.br/revistas/files/anexos/19303-19304-1-PB.htm>>. Acesso em: 28 set. 2012.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

SINCIC, Marcelo. **Utilizando Certificados Digitais**. 2009. Disponível em:

<<http://msdn.microsoft.com/pt-br/library/ee923720.aspx>>. Acesso em: 21 set. 2012.

SOUZA, André Leopoldino de; **Segurança de rede**. Florianópolis: SENAI/SC, 2010.