Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Carlos Lúcio Corrêa de Barros Lampert

CERTIFICAÇÃO DIGITAL NO GOVERNO FEDERAL:
Como a Certificação Digital Irá Conferir Sigilo ao Documento Eletrônico?

Rio de janeiro

2008

Carlos Lúcio Corrêa de Barros Lampert

CERTIFICAÇÃO DIGITAL NO GOVERNO FEDERAL:
Como a Certificação Digital Irá Conferir Sigilo ao Documento Eletrônico?

Monografia apresentada para obtenção do título de especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil.

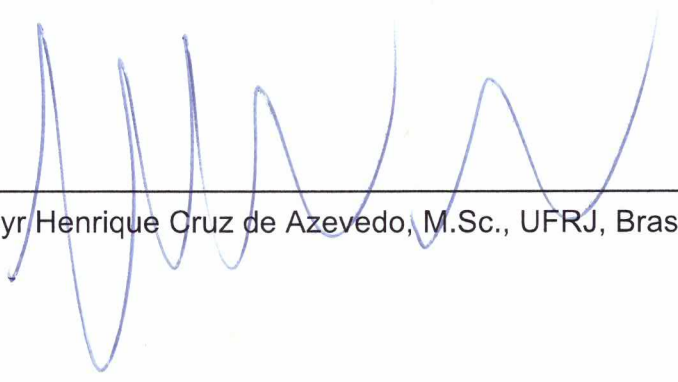
Rio de Janeiro
2008

Carlos Lúcio Corrêa de Barros Lampert

Certificação Digital no Governo Federal: Como a Certificação Digital Irá Conferir Sigilo ao Documento Eletrônico?

Monografia apresentada para obtenção do título de especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ

Aprovada em outubro de 2008.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil.

À minha esposa, que sempre me dá força para alcançar meus objetivos.

AGRADECIMENTOS

Ao meu orientador, aos amigos, colegas e todos que colaboraram de alguma forma para que este projeto se tornasse realidade.

RESUMO

LAMPERT, Carlos Lúcio Corrêa de Barros. **CERTIFICAÇÃO DIGITAL NO GOVERNO FEDERAL: como a certificação digital irá conferir sigilo ao documento eletrônico?** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

Com o advento da Internet e tecnologias que tratam meios físicos, digitalizando-os para seu trato no dia-a-dia, nos deparamos com inúmeros problemas. Os principais deles, a segurança e autenticidade do que se está tratando. Como ter certeza que determinado documento, arquivo ou usuário é realmente quem diz ser? Como ter certeza de que não é uma cópia ou mesmo uma farsa?

A Certificação Digital veio para resolver esse problema. Uma das maiores preocupações na utilização da Internet para realização de compras ou movimentações bancárias envolve a questão da segurança. A certificação digital assegura a integridade da identificação, ou seja, impede que uma pessoa se passe por outra para cometer fraudes. O segmento de negócios online entre empresas (business-to-business) é considerado um dos grandes beneficiados pela implementação dos certificados digitais, mas são nos serviços disponibilizados pelo Governo Federal, para a população, e na comunicação entre os órgãos da Federação que os ganhos serão ainda mais significativos.

A principal exigência do Governo Federal relaciona-se à compatibilidade dos certificados. A Medida Provisória 2.200-2 estabelece que todos os certificados emitidos no País deverão ser compatíveis com um código central, controlado pelo próprio Executivo. O Instituto Nacional de Tecnologia da Informação (ITI) é responsável pelo controle do padrão na emissão. As empresas que quiserem emitir certificados devem passar por uma auditoria do ITI, que analisará se a companhia está trabalhando com a Infra-estrutura de Chaves Públicas, ICP-Brasil, como se chama o código padrão do Governo.

Os órgãos públicos, em geral, encontram-se em um contexto onde a segurança das informações é crítica. Sendo detentores em sua maioria de equipamentos tecnológicos cada vez mais avançados, e de uma mão de obra especializada advinda dos concursos públicos, são o foco de desenvolvimento na área e desta pesquisa.

Este trabalho visa levantar as dificuldades e como os órgãos governamentais estão planejando conferir sigilo aos documentos digitalizados/digitais.

ABSTRACT

LAMPERT, Carlos Lúcio Corrêa de Barros. **CERTIFICAÇÃO DIGITAL NO GOVERNO FEDERAL: como a certificação digital irá conferir sigilo ao documento eletrônico?** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

With the advent of the Internet and technologies that deal with media, digitizing them for their deal from day to day, we face numerous problems. The most important are, the security and authenticity of what you're dealing with. How to make sure that particular document, file or user is who he says really is? How to make sure that it is not a copy or a fake?

The Digital Certification came to solve this problem. One of the biggest concerns in using the Internet to make purchases or bank transfers involves the issue of security. The certification ensures the integrity of identification, ie, prevents a person to pass for another to commit fraud. The segment of online business enterprises (business-to-business) is considered a major benefit from the implementation of digital certificates, but the services are provided by the Federal Government, to the public, and the communication between the body of the Federation that the profits will be even more significant.

The main requirement of the federal government is related to the compatibility of the licenses. The Provisional Measure 2200-2 provides that all certificates issued in the country should be compatible with a central code, controlled by the Executive. The National Institute of Information Technology (ITI) is responsible for controlling the pattern in the release. Companies that want to issue certificates must go through an audit of the ITI, which will examine whether the company is working with the Infrastructure Public Key, ICP-Brazil, as is called the code pattern of the government.

The public agencies in general are in a context where the security of information is critical. As holders mostly in equipment technology increasingly advanced, and a labor-specialized arising from public tenders, they are the focus of development in the area and this research.

This paper aims to raise what are the difficulties and how government agencies are planning to give secret documents scanned/digitalized.

LISTA DE FIGURAS

	Página
Figura 1 - Estrutura da ICP-Brasil	17
Figura 2 - Decifragem por Algoritmo	26
Figura 3 - Arquitetura Ponte	28
Figura 4 - Confidencialidade	29
Figura 5 - Autenticidade	30
Figura 6 - Assinatura Digital com Chave Pública	31
Figura 7 - Conferência da Assinatura Digital	32
Figura 8 - Linha do tempo do certificado e assinatura digital	44

LISTA DE TABELAS

	Página
Tabela 1 - Relação das Autoridades Certificadoras da ICP-Brasil	18
Tabela 2 - Comparação entre a plataforma Brasileira e a Americana.	27

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ITI	Instituto Nacional de Tecnologia da Informação
ICP	Infra-Estrutura de Chaves Públicas
CPF	Cadastro de Pessoa Física
CNPJ	Cadastro Nacional de Pessoa Jurídica
FEBRABAN	Federação Brasileira de Bancos
FINEP	Financiadora de Estudos e Projetos
Pro Uni	Programa Universidade para Todos
MEC	Ministério da Educação
CG	Comitê Gestor
CEPESC	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
AR	Autoridade de Registro
COTEC	Comissão Técnica Executiva
DOC-ICP-nn	Documentos em anexo da ICP
ADE-ICP	Adendos da ICP
MCT.nn	Manuais de Condutas Técnicas
PR	Presidência da República
LCR	Lista de Certificados Revogados
DPC	Declaração de Práticas de Certificação
MD5	Message-Digest algorithm 5
RSA	Acrônimo de Ron Rivest, Adi Shamir e Len Adleman
DES	Data Encryption Standard
OSI	Open Systems Interconnection
PBE	Password-Based Encryption
X.509	Padrão de Infraestrutura de Chave Pública
PEM	Privacy Enhancement Mail
SCT	Servidor de Carimbo de Tempo
PKCS	Public Key Cryptography Standards
ASN.1	Abstract Sintax Notation Number One
SPED	Sistema Público De Escrituração Digital – Sped
NF-e	Notas Fiscais Eletrônicas
ICMS	Imposto sobre Circulação de Mercadorias e Serviços
IPI	Imposto sobre Produtos Industrializados
ITA	Instituto Tecnológico da Aeronáutica
ABIN	Agência Brasileira de Inteligência

SUMÁRIO

	Página
1 INTRODUÇÃO	12
1.1 OBJETIVO	12
1.2 RELEVÂNCIA	12
2 REFERENCIAL TEÓRICO	14
2.1 VISÃO GERAL DA CERTIFICAÇÃO DIGITAL NO BRASIL	14
2.2 SIGILO EM DOCUMENTOS ELETRÔNICOS	15
2.3 IMPLANTAÇÃO NO GOVERNO FEDERAL	16
2.4 AUTORIDADES CERTIFICADORAS	17
3 METODOLOGIA DE PESQUISA	19
3.1 TIPO DE PESQUISA	19
3.2 SELEÇÃO DOS SUJEITOS	19
3.3 COLETA E ANÁLISE DOS DADOS	19
3.4 LIMITAÇÕES DO MÉTODO	20
4 CASOS DE USO	21
4.1 PROJETO JOÃO DE BARRO	21
4.2 MINISTÉRIO DA EDUCAÇÃO	22
4.3 SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL - SPED	23
5 TECNOLOGIAS	25
5.1 CRIPTOGRAFIAS	25
5.1.1 **Algoritmos Criptográficos de Chave Pública**	29
5.1.1.1 Confidencialidade	29
5.1.1.2 Autenticidade	30
5.2 ASSINATURA DIGITAL	31
5.3 CERTIFICADO DIGITAL	33
5.3.1 Public Key Cryptography Standards (PKCS)	35
5.3.1.1 PKCS#1: RSA Encryption Standard	35
5.3.1.2 PKCS#3: Diffie_Hellman Key Agreement Standard	36
5.3.1.3 PKCS#5: Password-Based Encryption Standard	37
5.3.1.4 PKCS#6: Extended-Certificate Syntax Standard	37
5.3.1.5 PKCS#7: Cryptographic Message Syntax Standard	38
5.3.1.6 PKCS#8: Private-Key Information Syntax Standard	38
5.3.1.7 PKCS#9: Selected Attribute Types	38
5.3.1.8 PKCS#10: Certification Request Syntax Standard	39
5.3.1.9 PKCS#12: Personal Information Exchange Syntax	39
5.3.1.10 PKCS#11,PKCS#13 e PKCS#15	40
5.3.2 Tipos de Certificações Digitais	40
5.3.3 Validade	43
6 NORMAS	46
6.1 ICP-BRASIL	46
6.1.1 Medida Provisória 2.200-2	46
6.1.2 Resolução do Comitê Gestor da ICP–BRASIL	46
6.1.3 Instrução Normativa AC-RAIZ	47
6.1.4 Documentos ICP-BRASIL	47
7 CONCLUSÃO	49
ANEXOS	50
REFERÊNCIAS	57

1 INTRODUÇÃO

1.1 OBJETIVO:

Este trabalho visa responder como a certificação digital irá conferir sigilo ao documento eletrônico, descrevendo a forma como o Governo Federal está propondo e implantando a certificação digital em serviços afetos ao público, buscando destacar alguns pontos críticos. Para isso, realiza um trabalho de investigação sobre os problemas na atribuição do sigilo a um documento eletrônico.

1.2 RELEVÂNCIA:

Muito se fala em reduzir a burocracia no serviço público brasileiro e uma das soluções possíveis é a utilização de tecnologia para agilizar e reduzir o custo das operações no geral. No entanto, a falta de segurança destas ações deixa os cidadãos temerosos e avessos a essas tecnologias. A solução para esse problema é a certificação digital de documentos eletrônicos. Por meio desse tipo de tecnologia a interação com os órgãos do governo, sem precisar sair de casa e enfrentar grandes filas nas repartições públicas, se torna possível. A segurança deixa de ser o grande vilão para se tornar o principal aliado destas operações e quem ganha com isso é o cidadão.

Algumas das realidades da utilização de certificação digital, e que estão contribuindo com a popularização cada vez maior da ferramenta, são os e-CPFs e e-CNPJs. Até o início de 2008 a Receita Federal emitiu mais de 500 mil certificações (e-CPFs e e-CNPJs). Dados preliminares da Receita Federal indicam que dos vinte

milhões e meio de contribuintes (98%) entregaram o Imposto de Renda por meio da Internet. Existe a previsão de emitir cerca de quatro milhões de certificados digitais até o ano de 2010 (dados publicados nos Boletins Digitais do ITI).

Em alguns programas do governo a certificação já é uma realidade. Uma das exigências da **Financiadora de Estudos e Projetos – FINEP**, para concorrer ao empréstimo do programa Juro Zero, é que as empresas precisam ter certificado digital emitido por uma Autoridade Certificadora. Já no **Programa Universidade para Todos – Pro Uni** do Ministério da Educação - MEC, a certificação digital é exigida na transação de informações com as instituições de ensino participantes.

A relevância do assunto foi tema em um dos artigos do Presidente do Instituto Nacional de Tecnologia da Informação, o ITI, Martini - 2005.

2 REFERENCIAL TEÓRICO

2.1 VISÃO GERAL DA CERTIFICAÇÃO DIGITAL NO BRASIL

O Certificado Digital é um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa uma entidade (pessoa, processo, servidor) a uma chave pública. Um certificado digital contém os dados de seu titular, tais como nome, correio eletrônico, CPF, chave pública, nome e assinatura da Autoridade Certificadora que o emitiu.

Na prática, o Certificado Digital funciona como uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em rede de computadores. O processo de certificação digital utiliza procedimentos lógicos e matemáticos para assegurar confidencialidade, integridade das informações e confirmação de autoria.

O Brasil montou sua infra-estrutura de chaves-públicas denominada ICP-Brasil. Trata-se de um conjunto de regras e normas baseadas em padrões públicos internacionais, que são definidas no país por um comitê gestor composto por representantes do governo e da sociedade civil.

O modelo adotado foi o de certificação com raiz única. O Instituto Nacional de Tecnologia da Informação - ITI está na ponta desse processo como Autoridade Certificadora Raiz, AC-Raiz, da Infra-Estrutura de Chaves Públicas Brasileira, ICP-Brasil. Cabe ao instituto credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

2.2 SIGILO EM DOCUMENTOS ELETRÔNICOS

O sigilo de documentos eletrônicos é essencial em aplicações que envolvam informações críticas, como comércio eletrônico, aplicações bancárias e documentos do governo. O surgimento de técnicas que permitem dar aos documentos eletrônicos os mesmos requisitos de segurança existentes nos documentos em papel tem auxiliado a disseminação de seu uso.

Estes requisitos são autenticidade, integridade, tempestividade, não repúdio e sigilo. O atendimento dos requisitos autenticidade e integridade são alcançados através do uso de assinaturas digitais. As autoridades de datação fornecem a referência temporal necessária para atender ao requisito tempestividade. O não repúdio, composto pela irrefutabilidade e irretratabilidade, tem sido amplamente discutido, tendo soluções desenvolvidas baseadas em software e hardware. O sigilo pode ser alcançado com o uso de criptografia.

O sigilo do documento eletrônico é obtido pela sua cifragem e o armazenamento seguro da chave de deciframento. A decifragem do documento depende diretamente da técnica de cifragem utilizada: se simétrica, é necessário o conhecimento da chave de sessão; se assimétrica, é necessária a posse da chave privada correspondente a chave pública usada na cifragem.

A perda da chave de decifragem impossibilita o acesso e inutiliza o documento cifrado. A gerência da chave de deciframento e do documento cifrado não é algo trivial.

2.3 IMPLANTAÇÃO NO GOVERNO FEDERAL

Como dito anteriormente, a ICP-Brasil utiliza o conceito de raiz única. Tendo o Instituto Nacional de Tecnologia da Informação – ITI – na ponta desse processo como Autoridade Certificadora Raiz, credenciando os demais participantes da cadeia, supervisionando e fazendo auditoria dos processos.

O Comitê Gestor, CG, da ICP-Brasil é designado pela Presidência da República para adotar as medidas necessárias ao funcionamento da Infra-estrutura de Chaves Públicas Brasileira. O art 3º do decreto 3872 de 18/07/2001, estabelece as competências do Comitê Gestor da ICP-Brasil. Sua composição foi estabelecida no art 2º do mesmo decreto.

O Comitê Gestor da ICP-Brasil conta com uma Comissão Técnica Executiva, COTEC, a quem cabe assistir e dar suporte técnico ao Comitê Gestor da ICP-Brasil, conforme especificado no art 4º do decreto 3872 de 18/07/2001 e uma Secretaria Executiva cuja competência está especificada no art 7º do mesmo decreto. Na Figura 1 podemos ver a atual estrutura da ICP-Brasil, criada pelo decreto citado.

A quantidade de entidades credenciadas na ICP-Brasil vem aumentando com freqüência, dada a percepção, pelos diversos setores, das inúmeras possibilidades de uso dos certificados digitais.

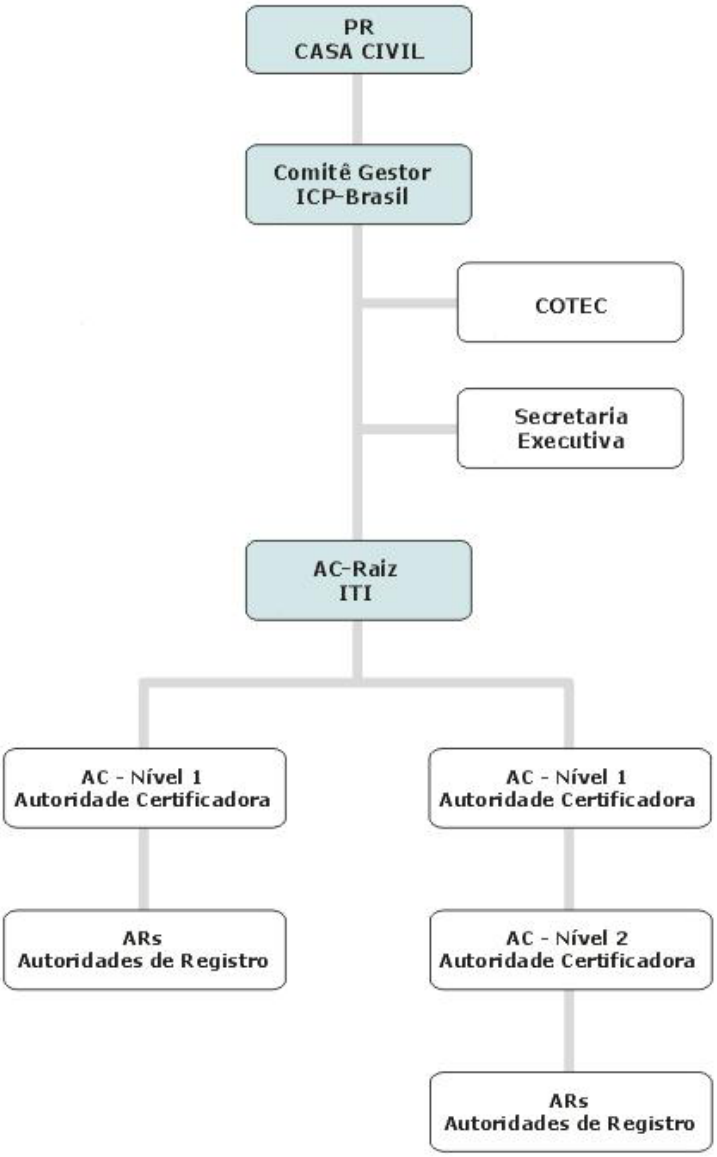


Figura 1 – Estrutura da ICP-Brasil

2.4 AUTORIDADES CERTIFICADORAS

O Governo Federal instituiu, através da Provisória 2.200-2 de 24 de agosto de 2001, a ICP-Brasil que cria o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz Brasileira e define as demais entidades que compõem sua estrutura. A partir dessa MP foram elaborados os regulamentos que regem as atividades das entidades integrantes da ICP-Brasil: as Resoluções do Comitê Gestor

da ICP-Brasil, as Instruções Normativas e outros documentos, que podem ser consultados em seu site. As Principais Autoridades Certificadoras da ICP-Brasil podem ser vistas na Tabela 1.

Tabela 1 - Relação das Autoridades Certificadoras da ICP-Brasil

Autoridade Certificadora do Serpro	www.serpro.gov.br	
Autoridade Certificadora CEF	icp.caixa.gov.br	
Autoridade Certificadora Serasa	www.certificadosdigitais.com.br	
Autoridade Certificadora da Receita Federal	www.receita.fazenda.gov.br	
Autoridade Certificadora Certisign	www.certisign.com.br	
Autoridade Certificadora da Presidência da República	thor.serpro.gov.br	
Autoridade Certificadora da Justiça	www.acjus.gov.br	
Autoridade Certificadora da Imprensa Oficial	www.imprensaoficial.com.br	

3 METODOLOGIA DE PESQUISA

3.1 TIPO DE PESQUISA

A pesquisa se baseia em procedimentos técnicos e teóricos sobre a implantação da certificação digital no governo federal.

Esta pesquisa tem como objetivo explorar e explicar as dificuldades encontradas em se adaptar às recomendações do governo federal para assegurar sigilo em documentos eletrônicos.

3.2 SELEÇÃO DOS SUJEITOS

Dados foram obtidos em entrevistas, pessoalmente, através de e-mails e telefonemas com os órgãos e representantes do governo envolvidos (Receita Federal, ITI), e também em participações no CERTFORUM, evento internacional de Certificação Digital promovido pelo ITI, nos anos de 2006 e 2007 em Brasília no Distrito Federal.

3.3 COLETA E ANÁLISE DOS DADOS

O resultado da pesquisa foi extraído através de comparações das experiências vividas por profissionais da área, nos diversos seguimentos do Governo Federal, o que possibilita uma nova visão para aplicações futuras.

Artigos, questionamentos e participação em eventos da área possibilitaram a coleta de um montante de informação suficiente para obter um conhecimento atualizado e prognóstico do assunto em pauta.

3.4 LIMITAÇÕES DO MÉTODO

A Certificação Digital ainda é pouco conhecida até mesmo entre os profissionais da área de Tecnologia da Informação. O estudo desta tecnologia, que cresce a cada dia, ainda é muito difícil de ser realizado, pois existem poucas implantações, informações e conhecimento técnico sobre o assunto.

4 CASOS DE USO

4.1 PROJETO JOÃO DE BARRO

Um bom exemplo de projeto nesta área, e que deve ter uma continuidade para que se torne uma “realidade brasileira”, é o Projeto João de Barro, uma parceria entre o ITI, Marinha do Brasil, FINEP, Universidade Federal de Santa Catarina, Instituto Tecnológico da Aeronáutica - ITA, Agência Brasileira de Inteligência – ABIN e o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC, focando a Criptologia Livre.

Este projeto visou criar um módulo criptográfico, software e hardware, para a emissão das chaves públicas e privadas da Autoridade Certificadora Raiz. O ITI, por ser a Autoridade Certificadora Raiz, está na base da ICP-Brasil. Viabilizando assim uma auditoria plena.

A idéia de sua origem foi nacionalizar a plataforma, deixando de usar a tecnologia estrangeira, desenvolvendo tecnologia própria e utilizando-se software livre. Os outros componentes do projeto também seguem essa lógica de nomes ligados ao Brasil e ao João de Barro.

Assim, o hardware criptográfico a ser desenvolvido para a ICP-Brasil foi batizado de AYTY, que em tupi-guarani significa ninho, numa alusão ao ninho do João de Barro.

O sistema operacional (software) a ser desenvolvido para rodar na plataforma aberta foi batizado de NHEENGATU, que é uma língua antiga utilizada pelos índios das tribos da costa brasileira e, curiosamente, foi a língua mais falada no Brasil até o século XVIII.

Até o início de 2008 já foram investidos mais de dez milhões de Reais, somando com toda a implantação física de sala cofre para prover qualidade e confiabilidade em sua operação. Em 28 de maio de 2008, segundo o Boletim Digital do ITI, o Comitê Gestor da ICP-Brasil autorizou o ITI a gerar o novo par de chaves da ICP-Brasil utilizando a plataforma João de Barro, e, assim, emitir o novo certificado da Autoridade Certificadora Raiz. O Comitê aprovou, também, a versão atualizada da Declaração de Práticas de Certificação (DPC) que estabelece os procedimentos que a própria Autoridade Certificadora Raiz deve adotar. A previsão é que até final deste ano toda a cadeia de certificação ICP-Brasil estará renovada, com a emissão dos certificados em uma plataforma desenvolvida com tecnologia totalmente nacional e plenamente auditável.

4.2 MINISTÉRIO DA EDUCAÇÃO

Até o ano de 2009 serão emitidos cerca de cinqüenta e seis mil certificados digitais para prefeitos, secretários e demais gestores da área da educação com o objetivo de ampliar a comunicação eletrônica com representantes municipais envolvidos na área. O projeto começou em julho de 2008 e já distribuiu 90 certificados digitais em municípios do Rio de Janeiro e Rio Grande do Sul.

O certificado digital, do tipo A3, será utilizado para envio e recebimento das informações de escolas para as Secretarias de Educação e órgãos relacionados. A redução de custos nestas comunicações possibilitará o investimento na melhoria dos profissionais de ensino, na infra-estrutura do ensino, ampliação da inclusão digital e combate ao analfabetismo.

O Ministério da Educação terá assim uma importante ferramenta para tomada de decisões, como por exemplo, onde serão feitos os investimentos e com que prioridade.

4.3 SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL - SPED

A Nota Fiscal Eletrônica, o Sped Contábil e o Sped Fiscal são subprojetos que compõem o Projeto Sped (Sistema Público de Escrituração Digital). O objetivo principal, segundo Carlos Sussumu Oda supervisor-geral do projeto Sped e Auditor Fiscal da Receita Federal do Brasil, é unificar as atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração comercial e fiscal dos empresários, mediante fluxo único e computadorizado de informações, por meio do uso da certificação digital.

Representa um novo ambiente de interação entre a Administração Pública e as empresas em geral, que abrange e promove a modernização dos processos que têm como premissa a padronização, racionalização e simplificação do cumprimento de obrigações acessórias.

Mais de cento e onze milhões de Notas Fiscais Eletrônicas (NF-e) já foram emitidas por mais de quinze mil estabelecimentos em todo o país, representando quase dois trilhões de Reais em operações comerciais. Pelos cálculos da Receita Federal, a operação diária está se aproximando da marca de um milhão de NF-e em dias úteis. Os estabelecimentos estão implantando o documento fiscal eletrônico e, assim, substituindo a emissão do documento fiscal em papel. Para isso é necessário obter certificado digital padrão ICP-Brasil para garantir validade jurídica na assinatura e transmissão do documento eletrônico.

A implantação da NF-e está relacionada às atividades de fiscalização sobre operações e prestações tributadas pelo Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e pelo Imposto sobre Produtos Industrializados (IPI). O início da obrigatoriedade de adoção da NF-e deu-se em abril de 2008 para indústrias e distribuidores de cigarros e combustíveis líquidos.

Dentre os benefícios esperados para as empresas, Carlos Sussumo Oda, em artigo publicado no Boletim Digital nº 119 do ITI, cita:

- simplificação e racionalização de obrigações acessórias, com o conseqüente aumento de competitividade entre as empresas brasileiras;
- redução dos custos em decorrência da dispensa de emissão e armazenamento de documentos em papel;
- possibilidade de troca de informações entre os próprios contribuintes a partir de um leiaute padrão (comércio eletrônico);
- otimização da logística operacional;
- simplificação do processo de faturamento;
- uniformização das informações que o contribuinte presta às diversas unidades federadas;
- simplificação e agilização dos procedimentos sujeitos ao controle da administração tributária; entre outros.

5 TECNOLOGIAS

5.1 CRIPTOGRAFIAS

A criptografia se constitui em um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação, tanto em relação a modificações não autorizadas, quanto a alteração de sua origem, sendo uma das técnicas que possibilitam o atendimento dos requisitos básicos de segurança da informação.

A confidencialidade de um documento - texto claro - será garantida quando ele for processado por um conjunto de operações, sendo transformado em um texto cifrado. O emissor do documento envia, então, o texto cifrado, que será reprocessado pelo receptor, transformando-o, novamente em texto claro, igual ao emitido.

O conjunto de regras que determina as transformações do texto claro é chamado de algoritmo (uma seqüência de operações) e o parâmetro que determina as condições da transformação é chamado de chave.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar.

Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

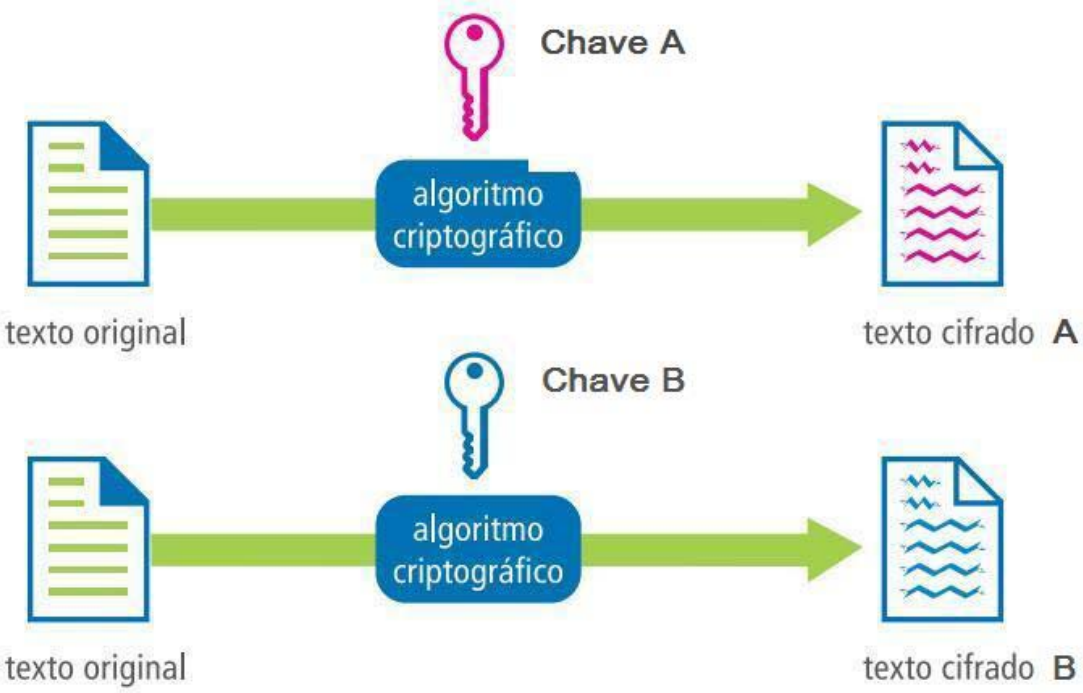


Figura 2 - Decifragem por Algoritmo

Atualmente existem dois tipos de criptografia: a simétrica e a de chave pública. A criptografia simétrica realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados.

O processo de compartilhar uma chave é conhecido como troca de chaves. A troca de chaves deve ser feita de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação cifrada.

Os algoritmos de chave pública operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja

revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente.

Inicialmente o Brasil adotou uma tecnologia estrangeira para a geração das chaves, baseando-se em uma estrutura já implantada nos Estados Unidos da América, por exemplo. Lá é utilizada a arquitetura Ponte que é um modelo de relacionamento entre Autoridades Certificadoras para conectar a Infra-estrutura de Chaves Públicas das organizações independentemente de sua arquitetura. Na tabela 2 estão destacadas as principais diferenças e na Figura 4 a representação básica de sua estrutura de aplicação:

Tabela 2 – Comparação entre a plataforma Brasileira e a Americana.

Descrição	**Modelo americano**	**Modelo brasileiro**
Arquitetura	Ponte.	Hierárquica.
Criptografia	Algoritmo tornado público.	Tecnologia nacional, tem sido mantida em sigilo.
Autoridades Certificadoras	Podem operar livremente. São reconhecidas por outras Autoridades Certificadoras por meio da Autoridade Certificadora ponte.	Devem possuir autorização do Comitê Gestor da ICP-Brasil para poderem operar.
Segurança	A segurança é inerente às Autoridades Certificadoras. Como elas são independentes, o comprometimento de uma não afeta as demais.	A chave raiz é um ponto de vulnerabilidade do sistema. Se sua segurança for corrompida, comprometer-se-á todo o sistema.

Descrição	Modelo americano	Modelo brasileiro
Privacidade	O serviço de inteligência do governo não tem como espionar as pessoas.	Como o governo é o administrador da chave raiz que usa algoritmo de criptografia nacional sigiloso, existe a possibilidade das mensagens virem a ser espionadas sem o conhecimento do autor.
Navegadores	As principais Autoridades Certificadoras já possuem suas chaves raiz embutidas nos navegadores em uso.	A chave raiz da ICP-Brasil será embutida nas próximas versões dos navegadores. Entretanto, para as pessoas que não atualizarem os seus softwares, será necessário baixar e instalar essa chave no navegador corrente. Isto é um ponto de vulnerabilidade porque alguém pode distribuir uma chave raiz falsa.

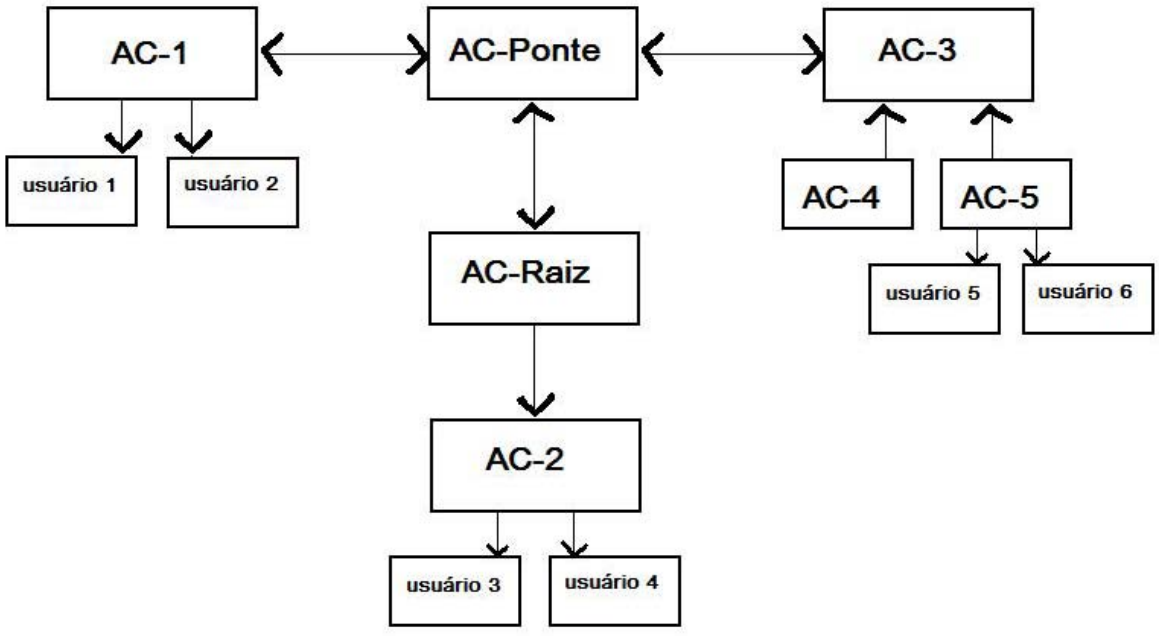


Figura 3 – Arquitetura Ponte

5.1.1 Algoritmos Criptográficos de Chave Pública

Os algoritmos criptográficos de chave pública permitem garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas.

5.1.1.1 Confidencialidade

O emissor que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela Internet.

Figura 4 - Confidencialidade

O sigilo é garantido já que somente o destinatário que possui a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais. Por exemplo, para Alice compartilhar uma informação de forma secreta com Beto, ela deve cifrar a informação usando a chave pública de

Beto. Somente Beto pode decifrar a informação, pois somente Beto possui a chave privada correspondente.

5.1.1.2 Autenticidade

No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade. O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação.

Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário.

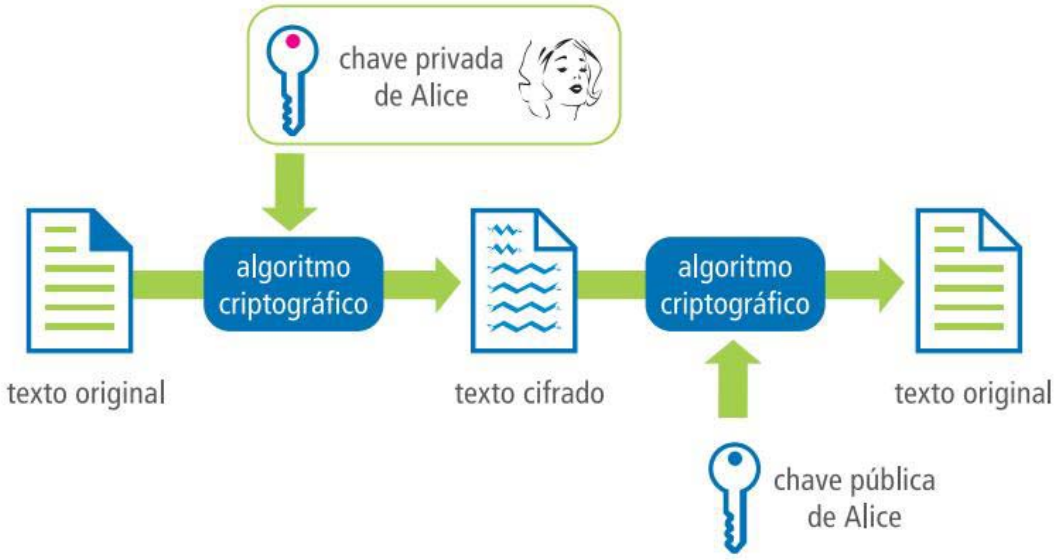


Figura 5 - Autenticidade

Assim, se Alice cifrar uma informação com sua chave privada e enviar para Beto, ele poderá decifrar esta informação, pois tem acesso à chave pública de Alice. Além disto, qualquer pessoa poderá decifrar a informação, uma vez que todos conhecem a chave pública de Alice.

Por outro lado, o fato de ser necessário o uso da chave privada de Alice para produzir o texto cifrado, caracteriza uma operação que somente Alice tem condições de realizar.

5.2 ASSINATURA DIGITAL

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de ‘hash’, é chamada de assinatura digital.

O resumo criptográfico é o resultado retornado por uma função de ‘hash’. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

Figura 6 - Assinatura Digital com Chave Pública

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia assimétrica são muito lentos.

A submissão de resumos criptográficos ao processo de cifragem com a chave privada reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que o documento em si. Assim, consomem um tempo baixo e uniforme, independente do tamanho do documento a ser assinado.

Na assinatura digital, o documento não sofre qualquer alteração e o 'hash' cifrado com a chave privada é anexado ao documento.

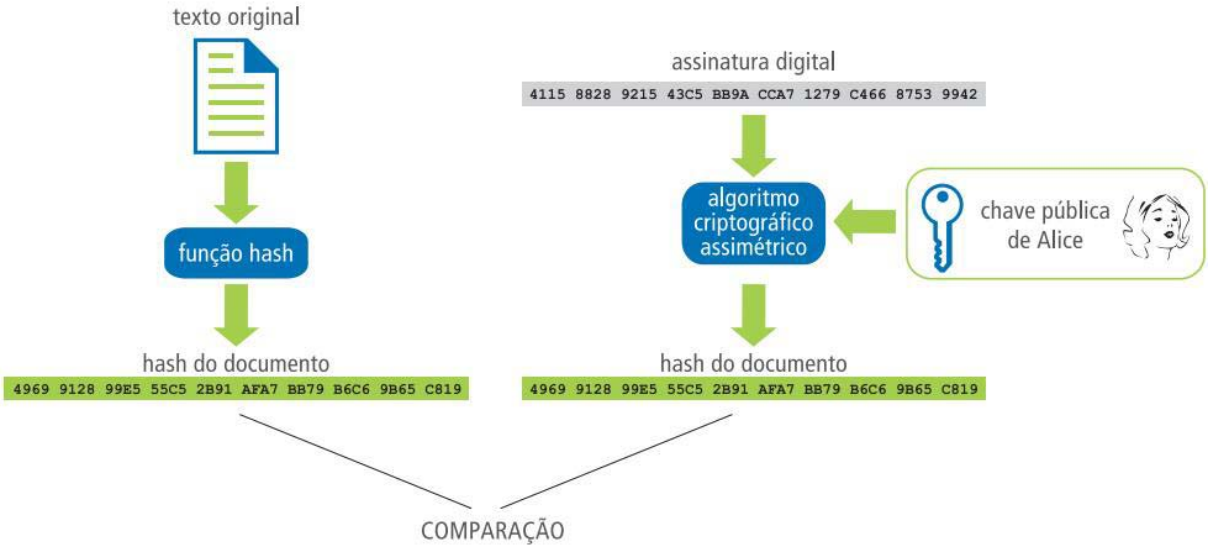


Figura 7 - Conferência da Assinatura Digital

Para comprovar uma assinatura digital é necessário inicialmente realizar duas operações: calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro.

Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.

5.3 CERTIFICADO DIGITAL

O certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos.

Um Certificado Digital normalmente apresenta as seguintes informações:

- Nome da pessoa ou entidade a ser associada à chave pública;
- Período de validade do certificado;
- Chave pública;
- Nome e assinatura da entidade que assinou o certificado; e
- Número de série.

Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet. Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor do banco.

E o cliente, ao solicitar um serviço, como, por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Serviços do governo estão sendo implantados para suportar transações eletrônicas utilizando certificação digital, visando proporcionar aos cidadãos benefícios como: agilidade nas transações, redução da burocracia, redução de custos, satisfação do usuário, entre outros.

Alguns casos de sucesso podem ser citados, como por exemplo:

- **GOVERNO FEDERAL** - O Presidente da República e Ministros têm utilizado certificados digitais na tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União. Um sistema faz o controle do fluxo dos documentos de forma automática, desde a origem dos mesmos até sua publicação e arquivamento.
- **ESTADO DE PERNANBUCO** - Foi o primeiro estado brasileiro a utilizar a Certificação Digital. A Secretaria de Fazenda de Pernambuco disponibilizou um conjunto de serviços pela Internet com base na certificação digital que proporcionou diversos benefícios como:
  - entrega de diversos documentos em uma única remessa;
  - redução drástica no volume de erros de cálculo involuntários;
  - apuração automática dos impostos;
  - minimização de substituições de documentos e redução de custos de escrituração e armazenamento de livros fiscais obrigatórios.
- **IMPRENSA OFICIAL DO ESTADO DE SÃO PAULO** - Implantou certificação digital de ponta a ponta em seu sistema que automatiza o ciclo de publicações na Internet, permitindo a eliminação das ligações interurbanas e dos constantes congestionamentos telefônicos em horários de pico, uma vez que se utiliza a Internet com garantias de sigilo e privacidade, além da obtenção de garantia de autoria por parte do autor das matérias.

5.3.1 Public Key Cryptography Standards (PKCS)

A empresa RSA Data Security, formada pelos inventores das técnicas RSA de criptografia de chave pública, tem um papel importante no mercado de normalização, e uma divisão no laboratório RSA mantém uma série de padrões denominados PKCS, muito importantes na implementação e na utilização da Infra-Estrutura de Chaves Públicas.

Os PKCS visam a preencher o vazio que existe nas normas internacionais relativas a formatos para transferência de dados que permitam a compatibilidade e a interoperabilidade entre aplicações que utilizem criptografia de chave pública. Existem doze padrões desse tipo: PKCS#1, #3, #5, #6, #7, #8, #9, #10, #11, #12, #13 e #15.

Os PKCS descrevem a sintaxe de mensagens de uma forma abstrata, utilizando o ASN.1, e não restringem a sua codificação.

5.3.1.1 PKCS#1: RSA Encryption Standard

Tem por objetivo servir de normalização para a utilização do algoritmo RSA nas seguintes aplicações:

- **Assinaturas digitais** - A informação a assinar é inicialmente reduzida a um valor de ‘hash’, utilizando um algoritmo de “message digest”, como o MD5 que é um algoritmo responsável por gerar um resumo de uma mensagem de tamanho fixo, que

seja único e inviolável. O resultado é, então, criptografado com a chave privada RSA.

- **Envelopes digitais** - A informação a proteger é criptografada com a chave de sessão, utilizando um algoritmo simétrico, como o DES. Posteriormente a chave de sessão é criptografada com a chave pública RSA.

O formato de uma mensagem contendo uma assinatura digital ou um envelope digital PKCS#1 está definido no PKCS#7, que será visto mais adiante. Essa norma também inclui uma sintaxe para chaves RSA que é compatível com as normas X.509 e Privacy Enhancement Mail - PEM. O padrão X.509 surgiu em 1988 com uma camada de autenticação recomendada para o padrão de diretório X.500, que pressupõe, como atributos de diretório, distribuição global e controle de acesso, ou seja, identificação positiva e distinguida para autorização e possível sigilo nos canais de acesso. Esses atributos fizeram com que ao longo do tempo o uso do X.509 migrasse definitivamente para infra-estrutura de Chaves Públicas e serviço de diretórios. O padrão PEM – Privacy Enhanced Mail – é um dos padrões da Internet para o envio de mensagens de correio eletrônico criptografadas. Assim, é possível interligar aplicações para Infra-Estrutura de Chaves Públicas baseadas no RSA utilizando essa norma.

5.3.1.2 PKCS#3: Diffie-Hellman Key Agreement Standard

Normaliza a utilização do protocolo de acordo com as chaves Diffie-Hellman no estabelecimento de chaves secretas ou de sessão. Destina-se a ser

incluído, no âmbito das camadas de rede e de transporte, numa versão futura do modelo OSI. Esse protocolo permite a dois usuários acordarem uma chave secreta, sobre um canal inseguro, sem trocarem informação que permita a um intruso obter essa mesma chave.

5.3.1.3 PKCS#5: Password-Based Encryption Standard

Descreve um método para criptografar um array de bytes utilizando uma chave secreta calculada com base em uma senha (Password-Based Encryption ou PBE).

Destina-se à proteção de chaves privadas em situações que exijam a sua transferência. Isso pode ser necessário, por exemplo, quando as chaves são geradas pela Autoridade Certificadora, e não pelo utilizador; ou quando ele necessita transferir a chave para outra máquina. A criptografia utilizada baseia-se no DES - Data Encryption Standard.

5.3.1.4 PKCS#6: Extended-Certificate Syntax Standard

Estende a definição de certificados X.509, permitindo a associação de outros atributos à entidade titular do certificado. O campo “Selected Attríbute Types” lista diversos atributos que podem ser incluídos num certificado X.509. Um exemplo de um atributo definido nesta norma é o endereço de correio eletrônico do titular, que é bastante utilizado.

5.3.1.5 PKCS#7: Cryptographic Message Syntax Standard

Define uma sintaxe para mensagens criptografadas, como assinaturas digitais e envelopes digitais. Essa sintaxe admite recursividade, como, por exemplo, pode haver uma assinatura digital de um envelope digital. No caso das assinaturas digitais, permite a associação de atributos de natureza arbitrária aos dados assinados.

Como caso particular dessa sintaxe é também definido um meio para distribuir certificados e Listas de Certificados Revogados. É compatível com o Privacy Enhanced Mail no sentido de que uma mensagem PKCS#7 pode ser convertida de e para mensagens Privacy Enhanced Mail, sem necessidade de operações para criptografar, bastando alterar o formato.

5.3.1.6 PKCS#8: Private-Key Information Syntax Standard

Define uma sintaxe para informações relativas a chaves privadas, tais como: o valor da chave, o algoritmo correspondente e um conjunto de atributos associados.

Define também uma sintaxe para chaves criptografadas, como exemplo, recorrendo às técnicas Password-Based Encryption definidas no PKCS#5.

5.3.1.7 PKCS#9: Selected Attribute Types

Lista alguns dos atributos que podem ser associados a uma chave privada. Como exemplo, temos a identificação de uma Autoridade Certificadora Raiz.

Desta forma, é possível inicializar o usuário com uma raiz para as suas relações de confiança.

O PKCS#9 lista diversos atributos que podem ser incluídos num certificado X.509. Um exemplo de um atributo definido nestas normas é o endereço de correio eletrônico do titular, que é bastante utilizado.

5.3.1.8 PKCS#10: Certification Request Syntax Standard

Define uma sintaxe para pedidos de certificação. Esse pedido inclui: os atributos de identificação do futuro titular do certificado; outros atributos, como o endereço da entidade que faz a requisição para que lhe seja enviado o certificado; a chave pública a incluir no certificado; uma assinatura digital do pedido que simultaneamente demonstra o conhecimento da chave privada e assegura a integridade da mensagem.

Pretende-se que um pedido desse tipo forneça à Autoridade Certificadora todas as informações necessárias para gerar o certificado. É importante observar que existem outros aspectos relevantes no processo de certificação, como, por exemplo, a prova de identidade que tem de ser fornecida pelo titular do certificado.

5.3.1.9 PKCS#12: Personal Information Exchange Syntax

Descreve uma sintaxe para a transferência de informação de identificação pessoal, incluindo chaves privadas, certificados, chaves secretas e extensões.

É uma norma muito útil, uma vez que é utilizada por diversas aplicações, como, por exemplo, Internet Explorer e Mozila para importar e exportar esse tipo de informação.

Suporta a transferência de informação pessoal em diferentes condições de manutenção da privacidade e integridade. Para um grau de segurança mais elevado prevê a utilização de assinaturas digitais e criptografias assimétricas para proteção da informação. Isto implica na utilização de certificados e pares de chaves associados às plataformas de origem e de destino, entre as quais se transfere a informação.

Para um nível de segurança intermediário, prevê a utilização do Password-Based Encryption para proteção dos segredos. Esta norma é uma extensão do PKCS#8 para transferência de informação de identificação pessoal.

5.3.1.10 PKCS#11,PKCS#13 e PKCS#15

As normas PKCS#11 e PKCS#15 referem-se à utilização de dispositivos portáteis em criptografia. A norma PKCS#13 está ainda em desenvolvimento e será dedicada às técnicas de criptografia baseadas em curvas elípticas.

5.3.2 Tipos de Certificações Digitais

Conforme já mencionado anteriormente, o Brasil adotou os padrões internacionais, utilizando diversos tipos de certificados, como por exemplo:

- CERTIFICADO DE ATRIBUTO – Estrutura de dados contendo um conjunto de atributos, características e informações, sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos no certificado são considerados válidos.
- CERTIFICADO DE AUTO-ASSINADO – Certificado assinado com a chave privada da própria entidade que o gerou. O único certificado auto-assinado da ICP-Brasil é o da Autoridade Certificadora Raiz.
- CERTIFICADO DE CALIBRAÇÃO – Documento emitido pelo Observatório Nacional, atestando que o equipamento usado para emitir carimbos de tempo (SCT – Servidor de Carimbo de Tempo) encontra-se dentro dos padrões de sincronismo esperados e está apto a entrar em funcionamento.
- CERTIFICADO DE ASSINATURA DIDIGTAL (A1, A2, A3 E A4) – São os certificados usados para confirmação da identidade na web, correio eletrônico, transações virtuais on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.
- CERTIFICADO DE SIGILO (S1, S2, S3 E S4) – São os certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.

- CERTIFICADO DO TIPO A1 E S1 - É o certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha cifrado por software. Sua validade máxima é de um ano, sendo a freqüência de publicação da Lista de Certificados Revogados no máximo de quarenta e oito horas e o prazo máximo admitido para conclusão do processo de revogação de setenta e duas horas.
- CERTIFICADO DO TIPO A2 E S2 – É o certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos, por senha. As chaves criptográficas têm no mínimo 1024bits. A validade máxima do certificado é de dois anos, sendo a freqüência de publicação da Lista de Certificados Revogados no máximo de trinta e seis horas e o prazo máximo admitido para conclusão do processo de revogação de cinqüenta e quatro horas.
- CERTIFICADO DO TIPO A3 E S3 – É o certificado em que a geração e o armazenamento das chaves criptográficas são feitos em Cartão Inteligente ou Token, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024bits. A validade máxima do certificado é de três anos, sendo a freqüência de publicação da Lista de Certificados Revogados no máximo de vinte e quatro horas, e o

prazo máximo admitido para conclusão do processo de revogação de trinta e seis horas.

- ❖ CERTIFICADO DO TIPO A4 E S4 – É o certificado em que a geração e o armazenamento das chaves criptográficas são feitas em Cartão Inteligente ou Token, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a freqüência de publicação da Lista de Certificados Revogados no máximo de doze horas, e o prazo máximo admitido para conclusão do processo de revogação de dezoito horas.

5.3.3 Validade

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. Após a assinatura, é possível, no entanto, conferi-las mesmo após o certificado expirar.

O certificado digital pode ser revogado antes do período definido para expirar. As solicitações de revogação devem ser encaminhadas à Autoridade Certificadora que emitiu o certificado ou para quem foi designada essa tarefa. As justificativas podem ser por diversos fatores como comprometimento da chave privada, alterações de dados do certificado ou qualquer outro motivo.

A Autoridade Certificadora, ao receber e analisar o pedido, adiciona o número de série do certificado a um documento assinado chamado Lista de Certificados Revogados (LCR) e a publica. O local de publicação das Listas de Certificados Revogados está declarado na Declaração de Práticas de Certificação da Autoridade Certificadora que emitiu o certificado, e em muitos casos o próprio certificado possui um campo com apontador para um endereço WEB que contém o arquivo com a Lista de Certificados Revogados.

As Listas de Certificados Revogados são publicadas de acordo com a periodicidade que cada Autoridade Certificadora definir. Essas listas são públicas e podem ser consultadas a qualquer momento para verificar se um certificado permanece válido ou não.

Após a revogação ou expiração do certificado todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas, se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado.

Mas como obter essa característica? Existem técnicas para atribuir a indicação de tempo a um documento, chamadas carimbo de tempo. Estes carimbos adicionam uma data e hora à assinatura, permitindo determinar quando o documento foi assinado, conforme demonstrado na Figura 8.

Figura 8 - Linha do tempo do certificado e assinatura digital

O usuário pode solicitar a renovação do certificado para a Autoridade Certificadora após sua perda de validade. Na solicitação, o usuário pode manter os dados do certificado e até mesmo o par de chaves, se a chave privada não tiver sido comprometida.

Mas, por que não emitir os certificados sem data final de validade? Porque a cada renovação da validade do certificado renova-se também a relação de confiança entre seu titular e a Autoridade Certificadora.

Essa renovação pode ser necessária para a substituição da chave privada por uma outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário.

Essas alterações têm como objetivo tornar mais robusta a segurança em relação às técnicas de certificação e às informações contidas no certificado.

6 NORMAS

6.1 ICP-BRASIL

6.1.1 Medida Provisória 2.200-2

A Medida Provisória 2.200-2 [02] foi publicada em 24.08.2001 e possui os seguintes pontos principais:

- Atribuição de valor legal às assinaturas digitais geradas com
- chave privada associada a certificado digital ICP-Brasil;
- Modelo com Autoridade Certificadora Raiz única;
- Exigência de identificação presencial do titular para obtenção do certificado; e
- Vinculação da identidade executora diretamente à Casa Civil da presidência da República, como forma de garantir apoio político e orçamentário a longo prazo.

6.1.2 Resolução do Comitê Gestor da ICP–Brasil

O Comitê Gestor da ICP-Brasil estabelece diretrizes técnicas para a formulação de políticas de certificados e regras operacionais das Autoridades Certificadoras e das Autoridades Registradoras e define níveis da cadeia de certificação.

Também atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil, garante aí compatibilidade e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Para emanar essas diretrizes e normas, utiliza-se de Resoluções que são analisadas pelos membros da Comissão Técnica e do Comitê Gestor e aprovados por esses últimos em reuniões específicas. Essas resoluções, publicadas no Diário Oficial da União, possuem numeração seqüencial.

6.1.3 Instrução Normativa AC-Raiz

A Resolução do Comitê Gestor de número 33, de 21.10.2004, concedeu à Autoridade Certificadora Raiz da ICP-Brasil a possibilidade de criar instruções normativas com o objetivo de suplementar as normas do Comitê Gestor.

Essa medida visou assegurar maior rapidez e objetividade às decisões da Autoridade Certificadora Raiz em relação à aplicação das normas do Comitê Gestor, situando-se na proximidade dos fatos, pessoas ou problemas a atender.

As instruções normativas também são publicadas no Diário Oficial da União e possuem numeração seqüencial, reiniciando-se a cada ano.

6.1.4 Documentos ICP-Brasil

Até abril de 2006 as resoluções e instruções normativas traziam, em seu próprio corpo, o conteúdo técnico a que se referiam.

Atualmente as resoluções são sucintas, limitando-se a aprovar documentos em anexo, esses sim contendo as diretrizes técnicas a serem observadas.

Tais documentos são conhecidos por DOC-ICP-nn. Possuem controle de versão e qualquer alteração deve sempre ser aprovada pelo Comitê Gestor da ICP-Brasil por meio de Resoluções.

Para cada alteração em um DOC-ICO-nn deve ser adotado um novo número de versão. Uma nova versão consiste num documento completo, contendo todo o texto da versão anterior mais as modificações aprovadas.

Caso necessário, tais documentos podem ser suplementados por outros, aprovados por meio de instruções normativas, aprovadas pela Autoridade Certificadora Raiz, que percebem a nomenclatura DOC-ICP-nn.mm.

Além disso, formulários, modelos e outros elementos que podem necessitar de alterações mais freqüentes, sem prejuízo ao conteúdo das normas, foram separados do corpo dos documentos, criando-se, para eles, a categoria de Adendos – ADE-ICP.

Foi necessário também criar uma categoria específica de documentos para o processo de homologação: os Manuais de Condutas Técnicas – MCT.nn, que detalham os requisitos técnicos que os dispositivos devem atender para receber o selo de homologação da ICP-Brasil; os materiais a depositar para análise; e a relação de testes que serão realizados no material.

7 CONCLUSÃO

Sem dúvida alguma os esforços do Governo Federal na implementação da certificação digital foram recompensados. O sigilo eletrônico hoje é uma realidade em diversas transações governamentais graças aos investimentos alocados em pesquisas e tecnologia.

O uso desses conhecimentos, descritos e analisados neste trabalho, foram de suma importância para a viabilidade de projetos tão importantes. Pensando num futuro próximo, precisamos de mais investimentos e mais informação, que já estão sendo planejados em diversos projetos a nível Brasil.

O Brasil começou o processo de maneira segura, através de uma tecnologia já conhecida (padrão americano) e alçou-se num projeto pioneiro para tornar o processo de certificação totalmente nacional, usando tecnologia nacional, um verdadeiro sucesso e realidade.

Um desafio ainda maior é vislumbrado para os próximos anos: a grande luta para que possamos disseminar a certificação digital para todas as camadas sociais a custo zero, sem burocracia e de fácil compreensão. É a verdadeira inclusão digital a serviço do progresso!

ANEXO

ANEXO A - MEDIDA PROVISÓRIA 2200-2

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 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.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

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.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

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

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos

signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente

ANEXO B - Decreto nº 3872

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

DECRETO Nº 3.872, DE 18 DE JULHO DE 2001.

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200, de 28 de junho de 2001,

DECRETA:

Art. 1º O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória nº 2.200, de 28 de junho de 2001, exerce a função de autoridade gestora de políticas (AGP) da referida Infra-Estrutura.

Art. 2º O CG ICP-Brasil, vinculado à Casa Civil da Presidência da República, é composto por onze membros, sendo quatro representantes da sociedade civil, integrantes de setores interessados e sete representantes dos seguintes órgãos, todos designados pelo Presidente da República:

I - Casa Civil da Presidência da República, que o coordenará;

II - Gabinete de Segurança Institucional da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Fazenda;

V - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI - Ministério do Planejamento, Orçamento e Gestão; e

VII - Ministério da Ciência e Tecnologia.

§ 1º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 2º A participação no CG ICP-Brasil é de relevante interesse público e não será remunerada.

§ 3º O CG ICP-Brasil terá uma Secretaria-Executiva.

§ 4º As decisões do CG ICP-Brasil serão aprovadas pela maioria absoluta de seus membros.

§ 5º Os membros do CG ICP-Brasil serão, em seus impedimentos, substituídos por suplentes designados na forma do **caput**.

§ 6º Poderão ser convidados a participar das reuniões do CG ICP-Brasil, a juízo do seu Coordenador ou do próprio Comitê, técnicos e especialistas de áreas afins.

Art. 3º Compete ao CG ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil;

II - estabelecer a política, os critérios e as normas para licenciamento das Autoridades Certificadoras - AC, das Autoridades de Registro - AR e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da Autoridade Certificadora Raiz - AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil, negociar e aprovar, observados os tratados, acordos e atos internacionais, acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 4º O CG ICP-Brasil será assistido e receberá suporte técnico da Comissão Técnica Executiva - COTEC, coordenada pelo Secretário-Executivo do Comitê Gestor, e integrada por representantes indicados pelos membros do CG ICP-Brasil e designados pelo Chefe da Casa Civil da Presidência da República.

§ 1º Serão convidados permanentes às reuniões da COTEC representantes:

I - do Ministério da Defesa;

II - do Ministério da Previdência e Assistência Social;

III - do Ministério da Saúde; e

IV - da Autoridade Certificadora Raiz - AC Raiz.

§ 2º Poderão ser convidados a participar das reuniões da COTEC, a juízo do seu Coordenador ou da própria Comissão, representantes de outros órgãos e entidades públicos.

§ 3º Compete à COTEC:

I - manifestar-se previamente sobre todas as matérias a serem apreciadas e decididas pelo CG ICP-Brasil;

II - preparar e encaminhar previamente aos membros do CG ICP-Brasil expediente contendo o posicionamento técnico dos órgãos e das entidades relacionados com as matérias que serão apreciadas e decididas; e

III - cumprir outras atribuições que lhe forem conferidas por delegação do CG ICP-Brasil.

§ 4º Os membros da COTEC serão, em seus impedimentos, substituídos por suplentes designados na forma do **caput**.

Art. 5º O CG ICP-Brasil estabelecerá a forma pela qual lhe será prestada assessoria pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC.

Art. 6º A Secretaria-Executiva do CG ICP-Brasil é chefiada por um Secretário-Executivo e integrada por assessores especiais e por pessoal técnico e administrativo.

§ 1º O Secretário-Executivo será designado por livre escolha do Presidente da República.

§ 2º A Secretaria-Executiva receberá da Casa Civil da Presidência da República o apoio necessário ao exercício de suas funções, inclusive no que se refere aos cargos de assessoria e ao apoio técnico e administrativo.

Art. 7º Compete à Secretaria-Executiva do CG ICP-Brasil:

I - prestar assistência direta e imediata ao Coordenador do Comitê Gestor;

II - preparar as reuniões do Comitê Gestor;

III - coordenar e acompanhar a implementação das deliberações e diretrizes fixadas pelo Comitê Gestor;

IV - coordenar os trabalhos da COTEC; e

V - cumprir outras atribuições que lhe forem conferidas por delegação do Comitê Gestor.

Art. 8º Este Decreto entra em vigor na data de sua publicação.

Brasília, 18 de julho de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Pedro Parente

REFERÊNCIAS

[1] Martini, R. da Silveira, Presidente do ITI. (Brasília, Brasil, janeiro de 2006).

[2] Módulo Security: em conformidade com a Norma Internacional de Segurança da Informação ISO 27001

[3] (http://www.modulo.com.br/empresa/site/modulo_interna_lernota.jsp?pidNota=604&pTipoNota=clipping&pMenuPai=5&pLinkMenu=abre_menu acessado em abril / 2008).

[4] O Instituto Nacional de Tecnologia da Informação – ITI: autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz, AC-Raiz, da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. (http://www.iti.gov.br/ acessado em abril / 2008).

[5] A ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileira – (https://www.icpbrasil.gov.br acessado em setembro/outubro de 2008).

[6] Eletronic Frontier Fundation (http://www.eff.org/ acessado em setembro de 2008).

[7] RSA (http://www.rsa.com/ acessado em setembro de 2008).

[8] SERPRO – (http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040226_08 acessado em setembro de 2008).