UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA PROPOSTA PARA A REGULAMENTAÇÃO DA CERTIFICAÇÃO DIGITAL NO BRASIL

VIVIANE REGINA LEMOS BERTOL

ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JR.

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.TD – 042/09

BRASÍLIA/DF: 07 - 2009

FICHA CATALOGRÁFICA

BERTOL, VIVIANE REGINA LEMOS

Uma Proposta para Regulamentação da Certificação Digital no Brasil [Distrito Federal] 2009. xvi, 105 p., 210 x 297 mm (ENE/FT/UnB, Doutor, Tese de Doutorado – Universidade de Brasília. Faculdade de Tecnologia.

Departamento de Engenharia Elétrica

1.Infraestrutura de chaves públicas 2.Assinatura Digital

3.Preservação de longo Prazo 4.Documento Eletrônico

I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

BERTOL, V. R. L. (2009). Uma Proposta para Regulamentação da Certificação Digital no Brasil. Tese de Doutorado em Engenharia Elétrica, Publicação PPGENE.TD-042/09 Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 120 p.

CESSÃO DE DIREITOS

AUTOR: Viviane Regina Lemos Bertol.

TÍTULO: Uma Proposta para Regulamentação da Certificação Digital no Brasil.

GRAU: Doutor ANO: 2009

_____

Viviane Regina Lemos Bertol
Rua Antônio José Thomaz da Costa nº 174, Campeche.
88063-610 Florianópolis – SC – Brasil.

AGRADECIMENTOS

Agradeço ao professor Rafael Timóteo de Sousa Jr. pela orientação e apoio.

Agradeço pela colaboração e incentivo a Renato da Silveira Martini, Maurício Augusto Coelho, Pedro Paulo Lemos Machado, Pedro Pinheiro Cardoso, Alexandre Menezes Ribeiro, Gilmar Belchior, Wilson Roberto Hirata, Ernandes Bezerra, Ângela Maia e demais colegas do Instituto Nacional de Tecnologia da Informação.

Agradeço também pelas contribuições e sugestões do prof. Ricardo Felipe Custódio, Nelson da Silva e Thiago Acordi Ramos, do Labsec/UFSC; Manuel Matos, da Câmara-e.net; Fabiano Menke, da Universidade de Kassel.

Dedicado a Silvio,
Débora, Sabrina,
Amália, Rubens
e Giovanna

RESUMO

UMA PROPOSTA PARA REGULAMENTAÇÃO DA CERTIFICAÇÃO DIGITAL NO BRASIL

Autora: Viviane Regina Lemos Bertol

Orientador: Rafael Timóteo de Sousa Júnior

Programa de Pós-graduação em Engenharia Elétrica

Brasília, julho de 2009

Neste trabalho são analisados os regulamentos da ICP-Brasil, com o objetivo de verificar se os documentos assinados digitalmente, no âmbito dessa infraestrutura, possuem as características técnicas necessárias e suficientes para serem úteis, efetivamente, como evidência legal, mesmo por longo prazo. São analisados os padrões internacionais que tratam de certificação e assinatura digital e a legislação de outros países e regiões, em especial da Comunidade Européia. São apontadas lacunas importantes na legislação brasileira, sendo a principal delas a ausência de regulamentação sobre armazenamento de documentos assinados digitalmente, processo que exige a adoção de uma série de atividades periódicas, como a revalidação das assinaturas, para preservar a eficácia dos documentos. Também foram detectadas lacunas na regulamentação que trata de revogação de certificados, de sistemas para geração e verificação das assinaturas digitais e de tipos e aplicabilidade dos certificados digitais. Para cada lacuna são recomendadas medidas que podem contribuir para saná-las, entre as quais estão a criação de novas entidades e de novos serviços na ICP-Brasil, a modificação de serviços já existentes, a alteração dos tipos de certificados utilizados na ICP-Brasil, a criação de manuais para orientar os usuários e a definição de novo processo para a homologação de sistemas usados na geração e verificação de assinaturas digitais.

ABSTRACT

A PROPOSAL FOR REGULATION OF DIGITAL CERTIFICATION IN BRAZIL

Author: Viviane Regina Lemos Bertol

Supervisor: Rafael Timóteo de Sousa Júnior

Programa de Pós-graduação em Engenharia Elétrica

Brasília, july of 2009

This work examined the regulation of ICP-Brazil, aiming to verify whether the digitally signed documents within this infrastructure, have the technical characteristics necessary and sufficient to be useful, indeed, as legal evidence, even for long term. We analyzed international standards for digital certification and digital signature and the legislation of other countries and regions, in particular the European Community. We pointed out important gaps in the Brazilian legislation, the main one being the lack of regulations on storing documents digitally signed, a process that requires the adoption of a series of regular activities such as revalidation of signatures to preserve the effectiveness of documents. We also found gaps in the regulations dealing with certificate revocation, systems for generation and verification of digital signatures and types and application of digital certificates. For each gap we recommended steps that can help to solve them. Among these recommendations, there is the creation of new entities and new services in the ICP-Brasil, the modification of existing services, the change of types of certificates used in ICP-Brasil, the creation of manuals to guide the users and the definition of a new process for the approval of systems used in generation and verification of digital signatures.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SÍMBOLOS, NOMENCLATURA E ABREVIAÇÕES

AA	Autoridade de Atributos
ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz
ACT	Autoridade de Carimbo do Tempo
ADE-ICP	Adendo ICP-Brasil
AENOR	*Associación Española de Normalización y Certificación*
ALADI	Associação Latino-Americana de Integração
AMN	Associação Mercosul de Normalização
ANSI	*American National Standards Institute*
APF	Administração Pública Federal
AR	Autoridade de Registro
BS	*British Standards*
CA	Certificado de Atributos
CAdES	*Advanced Electronic Signatures*
CC	*Common Criteria for Information Technology Security Evaluation*
CD	Certificado Digital
CDC	Código de Defesa do Consumidor
CEN	*European Committee for Standardization*
CEN TR	*CEN Technical Report*
CEN/ISSS	*European Committee for Standardization / Information Society Standardization System*
CENELEC	*Comité Europeén de Normalisation Eletrotechnique*
CEPESC	Centro de Pesquisas e Desenvolvimento para a Segurança das

	Comunicações
CG	Comitê Gestor
CMN	Comitê Mercosul de Normalização
CMS	*Cryptographic Message Syntax*
COBEI	Comitê Brasileiro de Eletricidade Industrial
COMPRAS-NET	Portal de Compras do Governo Federal
CONARQ	Conselho Nacional de Arquivos
COPANT	Comissão Panamericana de Normas Técnicas
COTEC	Comissão Técnica
CSM	Comitês Setoriais Mercosul
CT	Carimbo do Tempo
CWA	*CEN Workshop Agreements*
DCSSI	*Direction centrale de la sécurité des systèmes d'information*
DIN	*Deutsches Institut für Normung*
DN	*Distinguished Name*
DNA	Ácido Desoxirribonucleico
DOC-ICP	Documento ICP-Brasil
DPC	Declaração de Práticas de Certificação
DPCT	Declaração de Práticas de Certificação de Carimbos do Tempo
DSS	*Digital Secure Signature*
EAI	Empresa de Auditoria Independente
EESSI	*European Electronic Signature Standardization Initiative*
EN	*European Norms*
ENCAT	Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais
ESI	*Electronic Signatures and Infrastructures*
ETSI	Instituto Europeu de Normalização das Telecomunicações

ETSI ESI	*ETSI Electronic Signatures and Infrastructures*
ETSI SR	*ETSI Special Report*
ETSI TR	*ETSI Technical Report*
ETSI TS	*ETSI Technical Specification*
FIPS	*Federal Information Processing Standard*
GSI	Gabinete de Segurança Institucional
IBNORCA	*Instituto Boliviano de Normalización y Calidad*
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Pública Brasileira
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IN	Instrução Normativa
INN	*Instituto Nacional de Normalización* (do Chile)
InterPARES	*International Research on Permanent Authentic Records in Electronic Systems*
IPSec	*IP Security Protocol*
IPTV	*Internet Protocol Television*
IRAM	*Instituto Argentino de Normalización y Certificación*
ISO	*International Organization for Standardization*
ISO/IEC	*ISO / International Electrotechnical Commission*
ITI	Instituto Nacional de Tecnologia da Informação
ITU	*International Telecommunication Union*
IVA	Imposto sobre o Valor Agregado
LCR	Lista de Certificados Revogados
LEA	Laboratório de Ensaios e Auditoria
LPA	Lista de Políticas de Assinatura Aprovadas
MARE	Ministério da Administração Federal e Reforma do Estado

MCT	Manuais de Condutas Técnicas
MERCOSUL	Mercado Comum do Sul
MP	Medida Provisória
MSC	Módulos de Segurança Criptográfica
NASA	*National Aeronautics and Space Administration*
NBR	Norma Brasileira
NIST	*National Institute of Standards and Technology*
OASIS	*Organization for the Advancement of Structured Information Standards*
OCSP	*Online Certificate Status Protocol*
OID	Identificadores de Objeto
ONN	Organismos Nacionais de Normalização
PA	Política de Atributos
PC	Política de Certificação
PCT	Políticas de Carimbo do Tempo
PEM	*Privacy Enhanced Mail*
PIN	Número de Identificação Pessoal
PKI	*Public Key Infrastructure*
PKIX	*Public-Key Infrastructure (X.509)*
PL	Projeto de Lei
PROUNI	Programa Universidade para Todos
PSA	Prestadores de Serviços de Arquivamento de Longo Prazo
PSC	Prestador de Serviços de Certificação
PSS	Prestador de Serviços de Suporte
RFC	*Requests for Comments*
S/MIME	*Secure / Multipurpose Internet Mail Extensions*
SCC	*Standards Council of Canada*

SERPRO	Serviço Federal de Processamento de Dados
SGT-13	Subgrupo de Trabalho sobre Comércio Eletrônico do Mercosul
SIGA	Sistema de Gestão de Documentos de Arquivo
SINAR	Sistema Nacional de Arquivos
SPB	Sistema de Pagamentos Brasileiro
SSL	*Secure Sockets Layer*
TF	Titular Final de Certificado
TP	Terceira Parte
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
W3C	*World Wide Web Consortium*
WORM	*Write Once Read Many*
XML	*EXtensible Markup Language*

1 INTRODUÇÃO

O desenvolvimento de um país já não pode prescindir do desenvolvimento de uma economia digital forte, amparada em transações realizadas via Internet de forma rápida e segura. Por esse motivo, diversas organizações e governos estão criando infraestruturas de chaves públicas (ICP), como forma de solucionar os problemas de autenticação, integridade e sigilo enfrentados pelos sistemas de informação disponibilizados via Internet.

A certificação digital é uma grande oportunidade para atender necessidades de segurança relacionadas à identificação e para acelerar processos de negócio, uma vez que as assinaturas digitais agilizam o trâmite de fechamento de transações entre partes e conferem, em muitos países, validade legal a essas assinaturas.

Nem tudo é resolvido, todavia, quando se implanta uma ICP. Diversas questões permanecem em aberto e muitos problemas surgem quando se tenta migrar do modelo teórico para aplicações práticas, o que tem gerado intensos debates entre os especialistas em segurança da informação de todo o mundo. O modelo existente, portanto, não é adequado e suficiente para implementação em aplicações críticas, como as que lidam com valores financeiros, bens, contratos, informações sigilosas, entre outras.

No Brasil, embora já existissem iniciativas anteriores de utilização de certificados digitais, o grande desenvolvimento do tema deu-se em 2001, a partir da criação, pelo Governo Federal, da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), uma infraestrutura composta por técnicas, práticas e procedimentos a ser implementados pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

A ICP-Brasil teve um grande crescimento desde sua criação e as assinaturas digitais estão sendo amplamente utilizadas em inúmeras áreas de importância para o País, dado que possuem validade jurídica semelhante a assinaturas de punho.

Hoje, no País, diversos tribunais formam processos judiciais inteiros sem utilizar uma única folha de papel, baseando-se apenas em documentos eletrônicos assinados

digitalmente. Essa tecnologia é utilizada também para representar a vontade das partes em contratos e diversos tipos de documentos que implicam obrigações legais e financeiras.

Essa situação coloca o Brasil na dianteira em relação a muitos países, nos quais a certificação e a assinatura digital ainda são utilizadas de forma bastante restrita. Por outro lado, caso não sejam adotados os cuidados necessários, a utilização dessa tecnologia pode acarretar graves conseqüências, como a instalação de um "caos jurídico" em torno da validade de uma assinatura digital, no qual fique impossível definir qual das partes está com a razão.

As questões propostas neste trabalho são: com a atual regulamentação, os documentos assinados digitalmente no âmbito da ICP-Brasil reúnem as condições técnicas necessárias e suficientes para serem úteis como evidência legal? Estão garantidas a confiabilidade e a longevidade desses documentos? Estão eles aptos a atender às necessidades de uma sociedade que anseia por utilizar processos virtuais de forma semelhante aos processos em papel?

Nossa hipótese neste trabalho é a de que os regulamentos ainda não são suficientes e precisam ser progressivamente complementados. Essa hipótese foi formulada com base no conhecimento previamente adquirido sobre a regulamentação da ICP-Brasil e nos estudos realizados durante a elaboração dos regulamentos sobre assinatura digital, no ano de 2008, quando a autora atuava na AC-Raiz daquela ICP.

Foi realizada extensa pesquisa bibliográfica, em que ficou evidenciado o acerto da hipótese levantada, com a descoberta de diversos pontos em aberto na legislação brasileira. Foi possível perceber também a similitude das necessidades brasileiras, em relação a certificação e assinatura digital, com as da Comunidade Europeia, o que permitiu a comparação entre suas normas e regulamentos e ensejou a criação de um capítulo sobre o estado atual da certificação digital naquele bloco econômico.

1.1 JUSTIFICATIVA

Estima-se que até o momento tenham sido emitidos mais de um milhão de certificados digitais ICP-Brasil para pessoas físicas e jurídicas [BRASIL, 2007a].

Esses certificados estão sendo utilizados em variadas aplicações [ITI, 2009], tais como:

a) Sistema de Pagamentos Brasileiro (SPB);

b) automatização da prestação de informações fiscais à Receita Federal do Brasil;

c) nota fiscal eletrônica;

d) assinatura de documentos eletrônicos;

e) informatização do Poder Judiciário;

f) informatização de serviços cartoriais;

g) informatização de processos para abertura de empresas;

h) informatização de prontuários médico-odontológicos;

i) programas de Governo, como PROUNI;

j) autenticação dos servidores para acesso aos sistemas de diferentes órgãos federais, tais como da Receita Federal do Brasil;

k) automatização de procedimentos que exigem autorização de despesas, usando assinatura digital, como ocorre no Sistema de Controle de Diárias e Passagens do Governo Federal;

l) compras governamentais, por meio de pregão eletrônico e Compras-net.

Essa intensa utilização, se por um lado mostra a confiança que os agentes da sociedade depositam na ICP-Brasil, por outro lado traz uma enorme responsabilidade para todos os que trabalham em sua implementação e em especial aos entes públicos que criam e mantém os normativos que regem seu funcionamento.

Isso porque, caso não sejam tomados os cuidados necessários, inúmeros fatores podem comprometer a confiabilidade dos documentos assinados digitalmente, desde deficiências na regulamentação a problemas tecnológicos, passando ainda por falhas humanas, acidentais ou intencionais.

As gerações futuras dependerão cada vez mais de transações e documentos eletrônicos confiáveis, que possam reproduzir com segurança as características que hoje são encontradas nos documentos em papel. É necessário, portanto, que todos os aspectos que envolvem essa "virtualização" sejam previstos e regulamentados.

1.2 APRESENTAÇÃO DO TEMA

O presente trabalho se propõe a analisar os regulamentos da ICP-Brasil e, se necessário, apontar aqueles que devem ser criados ou alterados para que os documentos assinados digitalmente com chaves privadas associadas a certificados digitais ICP-Brasil reúnam condições técnicas necessárias e suficientes para serem úteis como evidência legal, mesmo no longo prazo.

Cumpre conhecer o papel das entidades que hoje atuam no cenário da ICP-Brasil e os regramentos a que se sujeitam. Cumpre, ainda, analisar a necessidade e viabilidade de criar outras entidades ou outras estruturas dentro da ICP-Brasil que venham a se integrar ao contexto atual, de forma a completar o conjunto de processos a serem executados para garantir a segurança dos documentos e transações eletrônicos, no longo prazo.

As declarações de práticas de certificação, as políticas de certificados e os demais regulamentos da ICP-Brasil estabelecem claramente os procedimentos e ações esperados das diferentes entidades que a compõem.

As autoridades certificadoras e as autoridades de registro devem manter evidências de que estão cumprindo os regulamentos, em especial no que diz respeito à guarda de suas chaves privadas, à verificação da identidade dos titulares de certificados e ao cumprimento das responsabilidades pecuniárias, em caso de danos aos usuários.

Os titulares de certificados, por sua vez, têm também responsabilidades, em especial quanto à geração, guarda e utilização de suas chaves privadas. As terceiras partes confiáveis devem executar adequadamente os processos de validação do *status* dos certificados e verificação dos limites para uso dos certificados.

Mesmo que se considere, hipoteticamente, que nenhuma falha venha a ocorrer e que todas as entidades que compõem atualmente a ICP-Brasil realizem os procedimentos a seu cargo de forma correta e segura, é preciso assegurar que sejam mitigados outros riscos que possam comprometer a confiabilidade das assinaturas digitais, em todas as fases do ciclo de vida do documento eletrônico assinado digitalmente, que compreende desde sua criação, verificação, armazenamento até a eventual revalidação.

Estarão os usuários (titulares de certificados e terceiras partes que confiam no certificado e no documento assinado) seguros, no momento da geração e verificação de uma assinatura digital? O titular do certificado desejava mesmo assinar digitalmente aquele documento? O sistema que utiliza realiza corretamente todos os processos necessários para verificar uma eventual revogação do certificado?

Depois de gerada a assinatura, o armazenamento do documento está sendo feito de forma a preservar suas características ao longo do tempo, já que esses documentos possuem, muitas vezes, uma vida muito maior do que as chaves criptográficas e as tecnologias empregadas na geração da assinatura digital?

Questões dessa natureza precisam ser respondidas de forma positiva e categórica, para que a credibilidade dos documentos assinados e da própria tecnologia de certificação digital seja preservada.

1.3 ESCOPO DO TRABALHO

É grande e complexa a diversidade de desafios e questões que envolvem as ICPs. A busca de respostas para esses desafios vem sendo empreendida por diferentes países e organizações. Todos esperam uma "solução consistente" que permita, finalmente, que a certificação digital atenda às expectativas das gerações atuais e futuras.

Este trabalho, todavia, não se propõe a sugerir soluções que sejam aplicáveis a qualquer ICP. Ele possui um escopo bastante definido: propor soluções para a ICP-Brasil, uma ICP com uma Autoridade Certificadora Raiz única, fortemente regulamentada pelo Governo Federal Brasileiro, que vem investindo recursos consideráveis na sua implantação [BRASIL, 2008d] e obteve a adesão e consenso da sociedade brasileira [ITI, 2009].

Mesmo dentro do contexto da ICP-Brasil, este trabalho está voltado especificamente para as questões relacionadas com assinatura digital, visto que um dos principais objetivos, ao criar-se a ICP-Brasil, foi conferir validade jurídica aos documentos assinados digitalmente, conforme expresso na Medida Provisória 2.200-2 [BRASIL, 2001b], principal alicerce legal dessa infraestrutura, como segue:

"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."* (sem grifo no original).

1.4 OBJETIVOS

Apresenta-se a seguir o objetivo geral e os objetivos específicos do estudo, de forma a melhor delimitar seu escopo.

1.4.1 Objetivo Geral

O objetivo deste trabalho é estudar a situação atual dos regulamentos sobre certificação digital na ICP-Brasil e, se necessário, propor adequações nesses regulamentos, de forma a permitir a criação, manuseio e recuperação de documentos assinados digitalmente que possam ser utilizados como evidência legal competente, no longo prazo.

1.4.2 Objetivos Específicos

Os objetivos específicos são:

a) estudar a ICP-Brasil, seus componentes, funcionamento e os regulamentos que se aplicam;

b) estudar os padrões internacionais e legislação de outros países sobre certificação e assinatura digital;

c) identificar as características esperadas das ICPs e dos documentos eletrônicos assinados digitalmente, para uso como evidência legal competente;

d) identificar e descrever os principais assuntos que precisam ser regulamentados na ICP-Brasil para possibilitar que os documentos eletrônicos assinados digitalmente sejam úteis como evidência legal competente;

e) propor a criação de novos regulamentos e alteração de alguns já existentes, contemplando os assuntos identificados no item anterior;

f) sugerir diretrizes para incorporação dos regulamentos propostos ao conjunto normativo atual da ICP-Brasil.

1.5 METODOLOGIA

A metodologia adotada compreendeu pesquisa bibliográfica, análise e comparação da legislação brasileira com a da Comunidade Europeia e calcou-se também, fortemente, na observação detalhada dos processos adotados na ICP-Brasil, durante os sete anos em que a autora trabalhou na AC-Raiz, inicialmente na Coordenação de Auditoria e Fiscalização e nos últimos três anos na Coordenação de Normalização e Pesquisa.

1.6 TRABALHOS RELACIONADOS

Estudos nessa área estão sendo conduzidos por outros países e blocos econômicos, em especial a Comunidade Europeia, que apresenta desenvolvimento similar ao brasileiro no que tange ao uso de certificação e assinatura digital, aplicadas às faturas eletrônicas e outros documentos de valor legal.

2 A ICP-BRASIL

2.1 INTRODUÇÃO

Neste capítulo são apresentadas as entidades que compõem a ICP-Brasil, descrevendo brevemente as funções de cada uma. Também se descreve o funcionamento da infraestrutura como um todo e os regulamentos sobre os quais se apoia. O objetivo é familiarizar o leitor com os termos mais utilizados e passar uma visão geral do ambiente abordado na tese.

2.2 ENTIDADES INTEGRANTES

As principais entidades integrantes da ICP-Brasil estão representadas na estrutura hierárquica apresentada na figura 2.1. O modelo detalhado encontra-se no Apêndice 1.

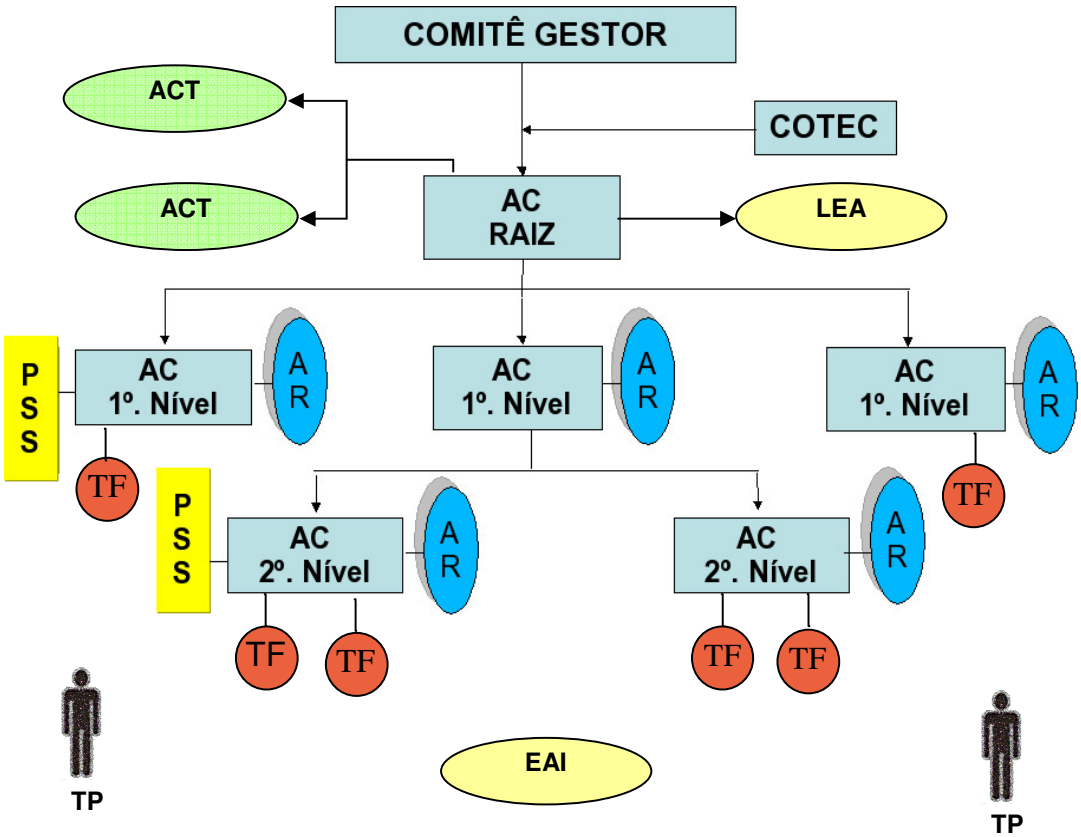

Figura 2.1: Organograma da ICP-BRASIL

2.2.1 Comitê Gestor

Composto por membros do Governo e da sociedade civil, tem por principal atribuição coordenar a implantação e o funcionamento da ICP-Brasil, além de estabelecer a política, os critérios e as normas para credenciamento das ACs, ARs e demais entidades que fazem parte da estrutura.

2.2.2 Comissão Técnica (COTEC)

Presta suporte técnico e assistência ao Comitê Gestor, sendo responsável por manifestar-se previamente sobre as matérias apreciadas e decididas pelo comitê Gestor. É convocada sempre que necessário, sendo que cada um de seus representantes é indicado por um dos membros do Comitê Gestor.

2.2.3 AC-Raiz

Primeira autoridade da cadeia de certificação, a AC-Raiz executa as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor.

Emite seus próprios certificados; emite, expede, distribui, revoga e gerencia os certificados das ACs de nível imediatamente subseqüente ao seu; gerencia sua lista de certificados revogados.

Também executa atividades de fiscalização e auditoria das entidades da ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

2.2.4 Autoridades Certificadoras (AC)

As autoridades certificadoras (ACs) são credenciadas para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Emitem, expedem, distribuem, revogam e gerenciam os certificados, bem como colocam à disposição dos usuários listas de certificados revogados e outras informações pertinentes e mantêm o registro de suas operações.

Na ICP-Brasil, configuram-se dois tipos de Autoridades Certificadoras: aquelas que estão diretamente subordinadas à AC-Raiz, e são conhecidas como ACs de 1º Nível, e aquelas que lhes são subordinadas, conhecidas como AC de 2º Nível, conforme representado na Figura 2.2.

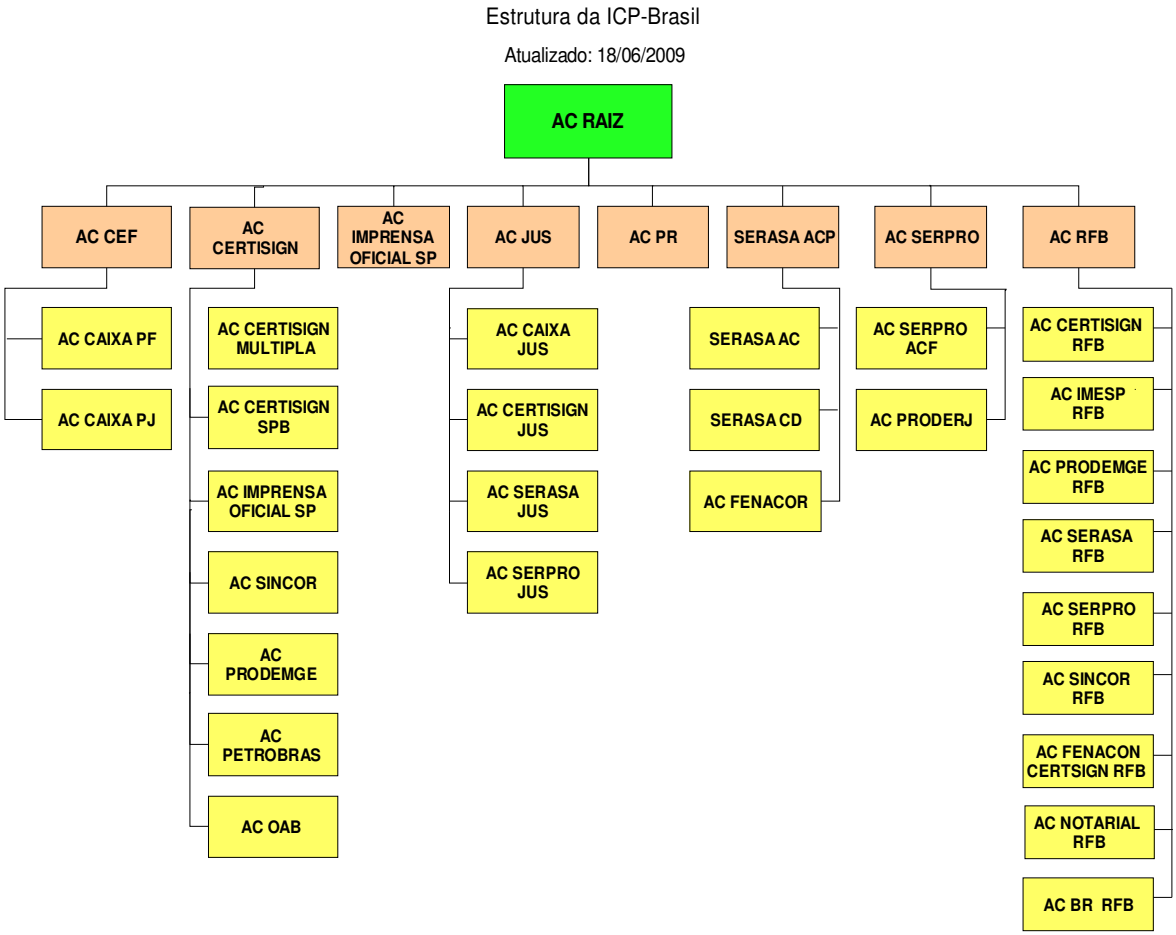

Figura 2.2 ACs credenciadas na ICP-Brasil em 18.06.2009 (fonte: [ITI, 2009a])

Uma AC de 1º Nível pode emitir certificados ou para titulares finais ou para ACs de 2º Nível. Conforme Figura 2.2, atualmente apenas duas ACs de 1º Nível (Presidência da República e Imprensa Oficial SP) emitem certificados para titulares finais. As demais 6 ACs de 1º Nível emitem certificados para outras ACs.

Essa configuração permite que uma AC de 1º Nível defina regras próprias (coerentes com as da ICP-Brasil, mas com algumas peculiaridades a mais) para os certificados que são emitidos na cadeia que lhe está subordinada. Ao mesmo tempo, exime a AC de 1º Nível de

emitir, ela própria, os certificados de titulares finais, processo bem mais trabalhoso do que emitir certificados de AC de 2º Nível.

2.2.5 Autoridades de Registro (AR)

As autoridades de registro (ARs) são entidades operacionalmente vinculadas a determinada AC. Compete-lhes identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às ACs e manter registros de suas operações.

2.2.6 Prestadores de Serviços de Suporte (PSS)

Os Prestadores de Serviços de Suporte (PSSs) são empresas contratadas por uma AC ou AR para realizar atividades de disponibilização de infraestrutura física e lógica e disponibilização de recursos humanos especializados.

2.2.7 Empresas de Auditoria Independente (EAI)

As empresas de auditoria independentes (EAIs) são entidades que, uma vez cadastradas junto à AC-Raiz, podem ser contratadas pelas autoridades certificadoras para realizar auditorias operacionais nas próprias ACs e nas entidades a elas subordinadas.

2.2.8 Laboratórios de Ensaio e Auditoria (LEA)

Os laboratórios de ensaios e auditoria (LEAs) são entidades formalmente vinculadas à AC Raiz, aptas a realizar os ensaios exigidos nas avaliações de conformidade e a emitir os correspondentes laudos de conformidade que embasarão a tomada de decisão, por parte da AC Raiz, quanto à homologação ou não de um dado sistema ou equipamento avaliado pelos LEAs.

2.2.9 Autoridades de Carimbo do Tempo (ACT)

As autoridades de carimbo do tempo (ACTs) são entidades responsáveis pela operação dos equipamentos que, conectados à Rede de Carimbo do Tempo da ICP-Brasil, geram carimbos e os assinam em nome da ACT.

2.2.10 Titulares Finais (TF)

Os titulares finais (TFs) são as entidades, pessoa física ou jurídica, para as quais são emitidos certificados digitais. O titular do certificado é responsável pela chave privada correspondente à chave pública contida no certificado e pode utilizar tanto uma quanto a outra.

2.2.11 Terceiras Partes (TP)

As terceiras partes (TPs) são quaisquer pessoas físicas ou jurídicas que confiam no teor, validade e aplicabilidade dos certificados digitais, dos carimbos do tempo e demais documentos assinados digitalmente no âmbito da ICP-Brasil.

2.3 VISÃO GERAL DO FUNCIONAMENTO DA ICP-BRASIL

Para explanar o funcionamento da ICP-Brasil, adota-se como ponto inicial a AC Raiz. Ela foi a primeira autoridade certificadora a ser criada e emitiu seu próprio certificado em novembro de 2001, estando a partir de então habilitada a assinar certificados para as demais ACs da cadeia, mas não para titulares finais.

As ACs, ARs, ACTs e PSSs, para operarem na ICP-Brasil, devem solicitar credenciamento à AC-Raiz, e precisam demonstrar que se encontram aptas a prestar os serviços pretendidos, submetendo-se a auditoria pré-operacional que analisa a segurança do ambiente físico, dos sistemas informáticos que utilizam e das pessoas que executam atividades-chave na entidade. Auditorias operacionais são realizadas anualmente nessas entidades, com vistas a confirmar se elas continuam operando de acordo com os regulamentos da ICP-Brasil.

As ACs e ACTs, além dos documentos administrativos, devem apresentar sua declaração de práticas de certificação (DPC) ou declaração de práticas de carimbo do tempo (DPCT), conforme o caso, que estabelece os principais procedimentos adotados na consecução de suas atividades. Essas declarações são usadas em quase todas as ICPs no mundo. Servem tanto para informar ao público sobre os procedimentos adotados pela entidade, como para sua responsabilização legal, em caso de eventual descumprimento dessas práticas, que venham a causar prejuízos aos titulares de certificados ou a terceiros.

Além disso, ACs e ACTs devem publicar suas políticas de certificados (PCs) ou políticas de carimbo do tempo (PCTs). Esses documentos detalham o formato e outras particularidades dos certificados e carimbos do tempo emitidos pelas entidades. As PCs devem ser consultadas pelos titulares de certificados e pelas terceiras partes para verificar se o formato do certificado atende às suas necessidades e expectativas. As PCTs devem ser consultadas pelos solicitantes de carimbos de tempo e pelas terceiras partes, com o mesmo propósito.

Tal é a importância das DPCs, DPCTs, PCs e PCTs que qualquer alteração em um desses documentos deve ser previamente aprovada pela AC-Raiz, que publica no Diário Oficial da União o resumo criptográfico de cada versão aprovada.

Uma AC, para ser credenciada, deve também indicar uma ou mais ARs que irão trabalhar como uma interface entre a AC e o titular final, realizando a identificação presencial desse e alimentando o sistema da AC com informações que irão culminar com a emissão ou rejeição do pedido de certificado.

Os certificados ICP-Brasil podem ser emitidos para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações. Para certificados para pessoas jurídicas, equipamentos ou aplicações, sempre deve ser designada uma pessoa física como responsável pelo uso da chave privada correspondente.

Cada certificado possui prazo de validade definido (variando de 1 a 3 anos), mas a revogação de um certificado antes da data de expiração prevista pode ocorrer em situações como perda da chave privada, alterações nos dados do certificado etc.

Os certificados digitais ICP-Brasil podem ser de dois tipos: certificados de assinatura e certificados de sigilo. Os de sigilo são usados para cifrar e decifrar documentos e os de assinatura para autenticação em sistemas e assinatura digital de documentos.

Um documento assinado digitalmente pode ser apresentado à terceira parte, que pode ou não confiar no teor do documento, dependendo de vários fatores, sendo um deles a confiança depositada no certificado da AC-Raiz. Para validar a assinatura digital, a terceira

parte utiliza também os demais certificados da cadeia de certificação, ou seja, os certificados das ACs de 1º Nível e de 2º Nível (se for o caso).

Tanto o titular final como a terceira parte podem, a qualquer momento, solicitar a uma autoridade de carimbo do tempo um carimbo que atesta a existência do documento em determinada data e hora, mecanismo vital para assinaturas digitais que devem ser validadas após a expiração do certificado digital associado à chave privada usada para assinatura.

Para aumentar a segurança dos procedimentos realizados, foi criado processo de homologação dos diversos dispositivos seguros de criação ou verificação das assinaturas digitais realizadas no âmbito da ICP-Brasil. Os interessados solicitam a homologação do dispositivo à AC-Raiz, entregando também os materiais e a documentação exigida. Os ensaios são executados pelo Laboratório de Ensaios e Auditoria, que ao final envia à AC-Raiz laudo, utilizado para decidir pela homologação ou não do dispositivo.

A AC-Raiz publica no Diário Oficial da União informação sobre os eventos relevantes ocorridos em sua esfera: credenciamento e descredenciamento de entidades, geração de certificados para si própria e para ACs diretamente subordinadas, alteração nas Declarações de Práticas de entidades, homologação de dispositivo criptográfico etc.

As ACs e ACTs publicam em seu sítio suas declarações de práticas (DPC e DPCT), políticas de certificados (PC), políticas de carimbo do tempo (PCTs) e outras informações relevantes.

2.4 REGULAMENTOS

A implantação da Infraestrutura de Chaves Públicas Brasileira teve seus primórdios em 1988, com a criação da Câmara Técnica dos Serviços de Rede do Poder Executivo Federal [BRASIL, 1998], órgão colegiado, diretamente subordinado ao Secretário de Logística e Tecnologia da Informação da Secretaria de Estado de Administração e do Patrimônio, instituída pela Portaria MARE 3.132, de 26-10-1998, e que tinha por finalidade:

- Planejar, organizar e acompanhar a implantação de serviços de rede, visando a racionalização de recursos no âmbito da Administração Pública Federal (APF);
- Propor critérios e parâmetros com vistas a promover a uniformização de conceitos e de procedimentos para os serviços de rede no âmbito da APF;
- Elaborar sistemáticas de avaliação e de auditoria sobre o desempenho e os resultados dos serviços de rede propostos, no âmbito da APF.

Entre os grupos de trabalho constituídos naquele colegiado, estava o de Segurança da Informação, que tinha por objetivos:

- Apresentar um conjunto de recomendações mínimas para a implementação, no âmbito da Rede Governo, de uma Política de Segurança;
- Apresentar uma proposta para adoção de Infraestrutura de Chaves Públicas, com seus mecanismos, ferramentas e aplicações associadas;
- Analisar a possibilidade de uso de padrões comerciais de segurança criptográfica disponíveis no mercado tais como: S/MIME, SSL, IPSec, entre outros

Participaram desse grupo: Ministério dos Transportes, Ministério da Marinha, Ministério da Aeronáutica, Ministério do Exército, Ministério da Ciência e da Tecnologia, Ministério da Agricultura, Ministério do Planejamento, Orçamento e Gestão, Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC) e Serviço Federal de Processamento de Dados (SERPRO).

A partir de então iniciaram-se os trabalhos que culminaram na criação da ICP-Brasil em 24.08.2001, com a publicação da MP 2.200-2 [BRASIL, 2001b].

A Casa Civil Presidência da República coordenou as atividades necessárias à implantação no País da tecnologia de certificação digital, inovadora àquela época. Foram criados grupos de trabalho compostos por especialistas e pesquisadores de diferentes órgãos do Governo e de empresas privadas. Surgiram assim as primeiras Resoluções da ICP-Brasil, de números 01 a 08, que pavimentaram o caminho para a criação de toda a infraestrutura que se seguiu.

Atualmente, a criação de regulamentos é feita pelo Comitê Gestor, que é o órgão encarregado de aprovar, por meio de Resoluções, os documentos que regem a ICP-Brasil. O Comitê Gestor pode valer-se do apoio da Comissão Técnica para analisar questões específicas, que demandem aprofundamento técnico.

A AC-Raiz trabalha na proposição de assuntos e na elaboração de documentos que são levados ao Comitê Gestor para avaliação e aprovação. Essa atividade é feita por meio de pesquisa, grupos de trabalho e interação com Universidades e órgãos normativos, como a ABNT. A AC-Raiz também pode, por meio de Instruções Normativas, suplementar regulamentos emanados nas Resoluções.

As demais entidades que compõem a ICP-Brasil devem obedecer aos regulamentos e eventualmente podem colaborar na sua elaboração, participando de grupos de trabalho ou oferecendo contribuições em consultas públicas sobre temas que estejam sendo normalizados

Os regulamentos sobre os quais se alicerça a ICP-Brasil são:

a) Medida Provisória 2.200-2 [BRASIL, 2001b];

b) decretos;

c) resoluções do Comitê Gestor da ICP-Brasil;

d) instruções normativas da AC Raiz;

e) documentos complementares.

2.4.1 MP 2.200-2

A Medida Provisória 2.200-2 [BRASIL, 2001b] é o principal marco legal da ICP-Brasil. Publicada em 24.08.2001 tem força de lei, mesmo não tendo sido analisada no Congresso Nacional, haja vista que o mecanismo de "caducidade" das MPs não analisadas somente foi instituído pela Emenda Constitucional 32, de 11.09.2001.

Os principais pontos da MP 2.200-2 são:

a) atribuição de valor legal às assinaturas digitais geradas com chave privada associada a certificado digital ICP-Brasil;

b) modelo com Autoridade Certificadora Raiz única;

c) exigência de identificação presencial do titular, para obtenção do certificado;

d) vinculação da entidade executora diretamente à Casa Civil da Presidência da República, como forma de garantir apoio político e orçamentário a longo prazo.

Na redação da MP-2200-2 foi adotada uma abordagem minimalista, visto que ela apenas cria a ICP-Brasil e confere valor legal às assinaturas geradas em seu âmbito, sem descer a pormenores técnicos sobre a implementação da estrutura, tarefa essa deixada em aberto para ser abordada nos demais documentos.

Encontra-se em análise no Congresso Nacional o Projeto de Lei 7316/2002, que irá substituir a MP 2.200-2 quando aprovado. O texto do PL traz uma abordagem mais próxima daquela utilizada na União Europeia, na medida em que detalha conceitos e processos, como os de acreditação de prestadores de serviços de certificação e de geração de assinaturas digitais. O texto mais atualizado do PL é o substitutivo datado de 25.09.2007 [BRASIL, 2007].

2.4.2 Decretos

Vários decretos presidenciais tratam da regulamentação da ICP-Brasil, sendo os principais:

- **DECRETO Nº 3.505** [BRASIL, 2000], que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- **DECRETO Nº 3.872** [BRASIL, 2001], que dispõe sobre o Comitê Gestor da InfraEstrutura de Chaves Públicas Brasileira – CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências;
- **DECRETO Nº 3.996** [BRASIL, 2001a], que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- **DECRETO Nº 4.414** [BRASIL, 2002], que altera o Decreto no 3.996, de 31 de Outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- **DECRETO Nº 4.689** [BRASIL, 2003], que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências;

- **DECRETO Nº 5.420** [BRASIL, 2005], que dispõe sobre o remanejamento de cargos em comissão;
- **DECRETO Nº 6.605** [BRASIL, 2008f], que dispõe sobre o Comitê Gestor da InfraEstrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

2.4.3 Resoluções do Comitê Gestor da ICP-Brasil

O Comitê Gestor estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das ACs e das ARs e define níveis da cadeia de certificação. Também atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil, garante sua 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 COTEC e do Comitê Gestor e aprovadas por esses últimos em reuniões específicas.

Essas resoluções, publicadas no Diário Oficial da União, possuem numeração consecutiva.

2.4.4 Instruções Normativas da AC-Raiz

A Resolução do Comitê Gestor de número 33 [BRASIL, 2004a] concedeu à AC-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 AC-Raiz em relação à aplicação das normas do Comitê Gestor, situando-as 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.

2.4.5 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-ICP-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 AC Raiz, que recebem 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 apartados 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: são 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 o rol de testes que serão realizados no material.

A tabela 2.1 explica a estrutura normativa e a relação entre os diferentes tipos de documentos:

Tabela 2.1 – Estrutura Normativa da ICP-Brasil

Código	*Tipo de Documento*	*Forma de Aprovação*
DOC-ICP-nn	Documento da ICP-Brasil	Resolução do CG da ICP-Brasil
DOC-ICP-nn.mm	Documento da ICP-Brasil vinculado ao DOC-ICP-nn	Instrução Normativa da AC-Raiz
ADE-ICP-nn.a	Adendo (formulário, modelo de documento, termo etc.) vinculado ao documento DOC-ICP-nn	Publicação no sítio iti.gov.br
ADE-ICP-nn.mm.a	Adendo (formulário, modelo de documento, termo etc.) vinculado ao documento DOC-ICP-nn.mm	Publicação no sítio iti.gov.br
MCT – Vol. nn	Manual de Condutas Técnicas para os processos de homologação	Publicação no sítio iti.gov.br

Onde "nn" e "mm" variam de 01 a 99 e "a" varia de A até Z

Fonte: Estrutura Normativa da ICP-Brasil [ITI, 2008].

Os regulamentos da ICP-Brasil compreendem um conjunto de documentos criados e/ou alterados ao longo dos anos, em função das necessidades apresentadas pela infraestrutura. Atualmente, esse conjunto compreende 15 documentos principais e 13 documentos complementares. A tabela 2.2 relaciona esses documentos agrupados pela autora deste trabalho de acordo com o assunto principal sobre o qual tratam:

Tabela 2.2 – Documentos ICP-Brasil agrupados por assunto

Código do documento	**Nome do documento**
Formato e conteúdo dos certificados digitais e das LCR	
DOC-ICP-04	Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil

Código do documento	Nome do documento
DOC-ICP-04.01	Atribuição de OID na ICP-Brasil
Credenciamento e funcionamento das entidades da ICP-Brasil	
DOC-ICP-01	Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil
DOC-ICP-01.01	Padrões e Algoritmos Criptográficos na ICP-Brasil
DOC-ICP-02	Política de Segurança da ICP-Brasil
DOC-ICP-03	Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil
DOC-ICP-03.01	Características Mínimas de Segurança para as ARs da ICP-Brasil
DOC-ICP-05	Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil
DOC-ICP-05.01	Procedimentos de Identificação de Servidores do Serviço Exterior Brasileiro em Missão Permanente no Exterior
DOC-ICP-06	Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil
DOC-ICP-07	Diretrizes para Sincronização de Freqüência e do Tempo na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil
Fiscalização e auditoria das entidades credenciadas	
DOC-ICP-08	Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP-Brasil
DOC-ICP-09	Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil
Processo de homologação de dispositivos criptográficos	
DOC-ICP-10	Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil
DOC-ICP-10.01	Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil
DOC-ICP-10.02	Estrutura Normativa Técnica e Níveis de Segurança de Homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da

Código do documento	Nome do documento
	ICP-Brasil
DOC-ICP-10.03	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (*smartcards*), leitoras de cartões inteligentes e *tokens* criptográficos no âmbito da ICP-Brasil
DOC-ICP-10.04	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Softwares de Assinatura Digital, Sigilo e Autenticação no Âmbito da ICP-Brasil
DOC-ICP-10.05	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil
DOC-ICP-10.06	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Softwares de Bibliotecas Criptográficas e Softwares Provedores de Serviços Criptográficos no Âmbito da ICP-Brasil
Carimbo do Tempo	
DOC-ICP-11	Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil
DOC-ICP-12	Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil
DOC-ICP-13	Requisitos Mínimos para as Políticas de Carimbo do Tempo na ICP-Brasil
DOC-ICP-14	Procedimentos para Auditoria do Tempo na ICP-Brasil
Assinatura Digital	
DOC-ICP-15	Visão Geral Sobre Assinaturas Digitais na ICP-Brasil
DOC-ICP-15.01	Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP -Brasil
DOC-ICP-15.02	Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil
DOC-ICP-15.03	Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil

Fonte: Legislação ICP-Brasil [ITI, 2009b]

Todos os regulamentos da ICP-Brasil, bem como a relação completa das entidades credenciadas, podem ser obtidos no sítio da AC-Raiz: http://www.iti.gov.br.

2.5 CONCLUSÃO

Foram apresentadas as entidades componentes da ICP-Brasil, os regulamentos que se aplicam a essa infraestrutura e uma visão geral do seu funcionamento. A partir dessa visão, pode-se traçar um paralelo entre os regulamentos brasileiros e os europeus, que serão estudados no próximo capítulo.

3 PADRÕES, NORMAS E REGULAMENTOS SOBRE CERTIFICAÇÃO E ASSINATURA DIGITAL

3.1 INTRODUÇÃO

Neste capítulo são apresentados conceitos sobre padrões, normas e regulamentos, visando clarificar o significado de cada um desses termos, que muitas vezes são usados, erroneamente, como sinônimos. A seguir, apresentam-se os principais órgãos de normalização e os padrões internacionais que tratam de certificação, assinatura digital e assuntos correlatos. Por fim, estuda-se o processo adotado pela Comunidade Europeia para criar os regulamentos necessários à adoção da assinatura digital pelos países-membros.

3.2 CONCEITOS SOBRE PADRONIZAÇÃO, NORMALIZAÇÃO E REGULAMENTAÇÃO

Para que se possa ter compreensão clara dos aspectos que envolvem a regulamentação na ICP-Brasil, cumpre compreender com clareza os principais termos usados no processo de normalização, utilizando os conceitos obtidos no sítio da Associação Brasileira de Normas Técnicas [ABNT, 2008].

3.2.1 Normalização

Normalização é a "atividade que estabelece, em relação a problemas existentes ou potenciais, prescrições destinadas à utilização comum e repetitiva, com vistas à obtenção do grau ótimo de ordem, em um dado contexto."

Entre os objetivos da normalização, tem-se:

- simplificar e reduzir procedimentos para elaboração de produtos e realização de serviços;
- reduzir a crescente variedade de produtos e procedimentos, bem como seus custos, proporcionando ao consumidor e ao fabricante melhores condições de mercado;

- proporcionar informações mais eficientes para o fabricante e o consumidor, melhorando a confiabilidade das relações comerciais e de serviços;
- disponibilizar à sociedade meios eficientes para aferir a qualidade de produtos e serviços;
- facilitar o intercâmbio comercial, evitando a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países.

3.2.2 Padrão

Aquilo que serve de base ou norma para avaliação de qualidade ou quantidade.

3.2.3 Norma

Documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto.

3.2.4 Regulamento

Documento que contém regra de caráter obrigatório e que é adotado por uma autoridade.

3.2.5 Regulamento Técnico

Regulamento que estabelece requisitos técnicos, seja diretamente, seja pela referência ou incorporação do conteúdo de uma norma, de uma especificação técnica ou de um código de prática. Um regulamento técnico pode ser complementado por diretrizes técnicas, estabelecendo alguns meios para obtenção da conformidade com os requisitos do regulamento, isto é, alguma prescrição julgada satisfatória para obter conformidade.

O processo de regulamentação técnica é o meio pelo qual os governos estabelecem os requisitos de cumprimento compulsório relacionados principalmente à saúde, segurança, meio ambiente, defesa do consumidor e prevenção de práticas enganosas de comércio.

3.2.6 Norma Mandatória

Norma cuja aplicação é obrigatória em virtude de uma lei geral, ou de referência exclusiva em um regulamento.

3.2.7 Documento Normativo

Documento que estabelece regras, diretrizes ou características para atividades ou seus resultados. "Documento Normativo" é um termo genérico que engloba documentos como normas, especificações técnicas, códigos de prática e regulamentos. Os termos para diferentes tipos de documentos normativos são definidos considerando cada documento e seu conteúdo como uma entidade única.

3.2.8 Organismos de Normalização

De forma sistematizada, a normalização é executada por organismos que contam com a participação de todas as partes interessadas (produtores, consumidores, universidades, laboratórios, centros de pesquisas e governo). Um organismo de normalização pode ser oficial ou independente, mas em qualquer dos casos tem como principal função a elaboração, aprovação e divulgação de normas, que devem ser colocadas à disposição do público.

3.2.8.1 Organismos nacionais de normalização

Um organismo nacional de normalização é aquele reconhecido oficialmente para executar o processo de normalização em nível nacional. Nessa condição, ele é indicado para ser membro da correspondente organização regional e internacional de normalização.

São exemplos de organismos nacionais de normalização reconhecidos em seus respectivos países [ABNT, 2008];

- Alemanha – *Deutsches Institut für Normung (DIN);*
- Argentina – *Instituto Argentino de Normalización y Certificación (IRAM)*;
- Canadá – *Standards Council of Canada (SCC)*;
- Espanha – *Associación Española de Normalización y Certificación (AENOR).*

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica. Fundada em 1940, a ABNT é uma entidade privada, sem fins lucrativos e representa o País nas entidades internacionais: ISO (International Organization for Standardization), IEC (International Electrotechnical Commission); e nas entidades de normalização regional COPANT (Comissão Panamericana de Normas Técnicas) e a AMN (Associação Mercosul de Normalização) [ABNT, 2008].

3.2.8.2 Organismos regionais de normalização

Um organismo regional de normalização congrega organismos nacionais de normalização reconhecidos pelos países situados em uma mesma área geográfica, política ou econômica.

São exemplos de organizações regionais de normalização [ABNT, 2008]:

- *Comité Europeén de Normalisation (CEN)*, organismo que promove a harmonização voluntária de normas técnicas na Europa;
- *Comité Europeén de Normalisation Eletrotechnique (CENELEC)*, associação civil, integrada por organismos nacionais no âmbito europeu, que opera exclusivamente no campo eletrotécnico;
- Comissão Pan-Americana de Normas Técnicas (COPANT), associação civil que congrega os países das três Américas e os organismos nacionais de normalização da Espanha (AENOR), França (AFNOR), Itália (UNI) e Portugal (IPQ).

O Mercosul possui uma associação oficial de normalização instituída por tratado, em outubro de 1991 [ABNT, 2008]. O Comitê MERCOSUL de Normalização (CMN) é uma associação civil sem fins lucrativos, não governamental, reconhecida pela Resolução Nº 2/92 do Grupo Mercado Comum. A partir de 2000 o Comitê passou a se chamar Associação Mercosul de Normalização e se transformou no único organismo responsável pela gestão da normalização voluntária no âmbito do Mercosul.

A Associação é formada pelos Organismos Nacionais de Normalização (ONN) dos países membros, que são:

- *Instituto Argentino de Normalización y Certificación* – Argentina;
- *Instituto Nacional de Tecnología y Normalización* – Paraguai;
- Associação Brasileira de Normas Técnicas – Brasil;
- *Instituto Uruguayo de Normas Técnicas* – Uruguai;

Outros Organismos Nacionais de Normalização que integram a AMN como membros associados são:

- INN - *Instituto Nacional de Normalización*, do Chile;
- IBNORCA - *Instituto Boliviano de Normalización y Calidad,* da Bolívia.

A AMN desenvolve suas atividades de normalização por intermédio de Comitês Setoriais Mercosul (CSM), que estabelecem os programas setoriais de normalização e conduzem o processo de elaboração e harmonização de normas para posterior aprovação da AMN.

Entre os CSM existentes, o que guarda mais relação com o assunto Documento Eletrônico e Assinatura Digital é o Comitê Setorial Mercosul de Segurança da Informação, que publicou, até o momento, as seguintes normas: [ABNT, 2008]

- Norma: NM ISO/IEC 27001:2008 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos (ISO/IEC 27001:2005, IDT);
- Norma: NM ISO/IEC 27002:2008 - Tecnologia da informação - Código de boas práticas para a gestão da segurança da informação (ISO/IEC 27002:2005, IDT).

Essas normas não tratam de documentos eletrônicos e assinaturas digitais, embora já se observe a necessidade de criar normas sobre tais assuntos no âmbito do Mercosul. Exemplo disso são os trabalhos conduzidos no âmbito da Associação Latino-Americana de Integração (ALADI), com o objetivo de substituir os Certificados de Origem das mercadorias que circulam entre as fronteiras do Mercosul por documentos eletrônicos assinados digitalmente.

3.2.8.3 Organismos internacionais de normalização

Nas organizações internacionais de normalização a participação é aberta a todos os organismos nacionais de normalização. Entre as principais organizações internacionais de normalização podem ser citadas [ABNT, 2008]:

- *International Organization for Standardization (ISO)*, organização não governamental integrada por organismos nacionais de normalização de 157 países, contando com um representante por país; a ABNT é a representante do Brasil [ISO, 2008];

- *International Electrotechnical Commission (IEC)*, federação mundial integrada por 68 organismos nacionais de normalização, contando com um representante por país, atuando especificamente na normalização internacional no campo da eletricidade e, eletrônica; o representante brasileiro é a ABNT, que conta com o Comitê Brasileiro de Eletricidade Industrial (COBEI) para sua representação [IEC, 2008];

- *O International Telecomunication Union (ITU)* [ITU, 2008], entidade sediada em Genebra na Suíça, responsável por definir normas e padrões de telecomunicações, de forma a permitir a interoperabilidade de todos os sistemas de telecomunicações a nível mundial. Foi criado em 1865, em Paris, com o nome de *Internacional Télegraph Union*. Nasceu para controlar as conexões entre redes de telégrafos locais, mas atualmente seus padrões abrangem desde funcionalidades de rede básica e de banda larga até a próxima geração de serviços, como televisão sobre IP. Trata-se, na verdade, da organização internacional mais antiga do mundo. Devido a essa longevidade e a seu *status* como agência especializada da ONU, obtido em 1947, os padrões promovidos pelo ITU são respeitados e reconhecidos por outras organizações que publicam especificações técnicas similares. Desde o seu início o ITU tem sido uma organização intergovernamental formada por parceria público-privada. Atualmente possui a adesão de 191 países (Estados-Membros) e de mais de 700 empresas do setor público e privado, bem como de entidades internacionais e regionais de telecomunicações.

3.2.8.4 Organismos de Normalização Independentes

Além das organizações de normalização oficiais, existem organizações de normalização independentes que desenvolvem e publicam normas e padrões técnicos para uso internacional, algumas delas trabalhando em contextos especializados, como o IETF, o W3C ou o IEEE.

Geralmente a participação nessas organizações é aberta a peritos de todo o mundo, que atuam individualmente ou como representantes de indústrias ou corporações.

Em geral, o trabalho técnico dessas organizações é feito em grupos de trabalho, que são organizados por assunto em várias áreas. Grande parte das atividades é realizada remotamente, através de listas de discussão e outras ferramentas online de apoio. Reuniões presenciais são realizadas periodicamente.

O *Internet Engineering Task Force (IETF)* é uma grande comunidade internacional aberta, formada por projetistas de rede, operadores, vendedores e pesquisadores preocupados com a evolução da arquitetura e o bom funcionamento da Internet. Dentre os grupos de trabalho do IETF, o que mais guarda relação com o tema em estudo é o PKIX, criado em 1995 com o objetivo de desenvolver padrões Internet para dar suporte a ICPs baseadas em certificados X.509 [IETF, 2008b].

Outro organismo de normalização independente que se destaca na área de normalização e tem tido vasta atuação no desenvolvimento de padrões para assinaturas digitais é o Instituto Europeu de Normalização das Telecomunicações (ETSI), um organismo sem fins lucrativos, que congrega 62 países e províncias dentro e fora da Europa e é oficialmente responsável pela criação de padrões para tecnologias da informação e comunicação na Comunidade Europeia [ETSI, 2008].

3.3 PADRÕES SOBRE CERTIFICAÇÃO E ASSINATURA DIGITAL

Os diferentes organismos de normalização produziram inúmeros padrões ou propostas de padrões sobre o tema deste trabalho. Relacionam-se a seguir alguns deles, que foram ou podem vir a ser utilizados como referência para os regulamentos da ICP-Brasil.

3.3.1 Documentos do ETSI

Os comitês técnicos do ETSI, atuando em suas áreas específicas, criam e mantêm diversos tipos de documentos, dentre os quais se destacam [ETSI, 2008b]:

- *ETSI Standard (ES)* – usado quando o documento contém requisitos normativos e é necessário submetê-lo a todos os associados ETSI para aprovação;

- *Special Report (SR)* - usado para vários propósitos, inclusive disponibilizar ao público informações não produzidas dentro de um comitê técnico. SRs são também usados para documentos "virtuais", isto é, aqueles que são gerados dinamicamente por meio de uma consulta a uma base de dados na web. Um SR é publicado pelo comitê técnico responsável por aquele tema;

- *ETSI Technical Specification (TS)* - usado quando o documento contém requisitos normativos e quando é essencial sua validação ou manutenção em curto prazo; ele é aprovado pelo comitê que gerou a minuta;

- *ETSI Technical Report (TR)* - usado quando o documento contém principalmente elementos informativos; é aprovado pelo comitê que gerou a minuta.

O comitê técnico *Electronic Signatures and Infrastructures (ESI)* vem trabalhando na criação de padrões ETSI para assinatura digital que permitam a implantação dessa tecnologia na Comunidade Europeia, em consonância com a Diretiva 93/1999 [EUROPA, 1999]. Para tanto, atua em cooperação com o *European Electronic Signature Standardization Initiative (EESSI)* e o *European Committee for Standardization* (CEN) [ETSI, 2008a].

Sempre que possível, o comitê utiliza especificações já existentes do ITU, ISO e IETF, detalhando e suplementando tais especificações, se necessário.

A atualização de vários documentos ETSI relacionados com assinatura digital tem ocorrido com freqüência, o que demonstra o esforço que vem sendo realizado pelos países europeus para adoção dessa tecnologia. Um exemplo é o documento ETSI TS 101733 *Electronic Signatures and Infrastructures (ESI) - CMS Advanced Electronic Signatures (CAdES)*

[ETSI, 2007a], que hoje serve como referência a outros organismos de normalização no campo das assinaturas digitais. Ele foi criado em dezembro de 2000 e já teve 7 atualizações, sendo a última datada de julho de 2008.

3.3.2 Documentos do CEN

Como um dos principais organismos de normalização europeus, o CEN publica diversos tipos de documentos: padrões europeus (EN), Especificações Técnicas (CEN TS) e Relatórios Técnicos (CEN TR), o CEN elabora os *Workshop Agreements* (CWA), documentos produzidos a partir de reuniões que visam eliminar a distância entre a indústria, que produz padrões de fato com participação limitada das partes interessadas, e o processo formal de normalização europeu, que produz padrões através de consenso, com autorização dos membros do CEN [CEN, 2008].

Para o presente trabalho, interessam-nos os documentos que dizem respeito a ICPs e assinaturas digitais, desenvolvidos em cooperação com o ETSI e o EESSI, detalhando os requisitos técnicos que devem ser observados pelos fabricantes de equipamentos e sistemas para uso em assinatura digital no âmbito da União Europeia.

3.3.3 Documentos do ITU-T

Os principais produtos do ITU-T são as Recomendações (ITU-T Recs) São padrões que definem como as redes de telecomunicação operam e interagem. As Recomendações ITU-T possuem um *status* não mandatório, até que sejam adotados pelas leis nacionais. Entretanto, os níveis de aderência são altos, devido à aplicabilidade internacional e à alta qualidade garantida pelo secretariado do ITU-T e à participação de membros das companhias mais famosas e administrações globais [ITU-T, 2009].

Existem mais de 3000 recomendações em vigor em tópicos que vão da definição do serviço até a arquitetura de rede e segurança, desde banda larga DSL até sistemas de transmissão ótica de gigabits/s, incluindo a nova geração de redes (NGN) e assuntos relacionados a IP, todos eles componentes fundamentais das tecnologias de informação e comunicação atuais.

As recomendações são organizadas em séries, identificadas por letras do alfabeto. A série X trata de redes de dados, sistemas de comunicação abertos e segurança. É dentro dessa série que se encontram as recomendações mais ligadas a certificação e assinatura digital, e em especial o padrão ITU-T X.509 [ITU, 1997].

O padrão X.509 foi inicialmente publicado em 1998. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Ele assume um sistema hierárquico restrito de Autoridades Certificadoras para emitir certificados. O sistema X.509 nunca foi completamente implementado e o grupo de trabalho IETF/PKIX adotou o padrão para uso na Internet, definindo um perfil para certificados digitais e LCRs na RFC 5280.

Várias outras séries de recomendações do ITU-T utilizam-se dos mecanismos de segurança oferecidos pelos certificados e assinaturas digitais, como é o caso das recomendações da série H, que tratam de sistemas de audiovisual e multimídia, como TV a cabo e TV Digital. Nessas recomendações, a certificação digital é uma das opções a serem utilizadas para controlar o acesso aos serviços.

3.3.4 Documentos do IETF

Os documentos do IETF mais conhecidos são as *Requests for Comments* (RFCs) [IETF, 2008]. As RFCs, ao contrário do que alguns imaginam, não são padrões a serem seguidos de forma compulsória, sob pena de prejudicar a interoperabilidade e mesmo a credibilidade de um projeto. Na verdade, muitas das RFC são apenas textos colocados em discussão na comunidade da Internet, os quais nunca chegarão a ser (e nem pretendem ser) efetivamente um padrão IETF.

As RFCs podem ter uma das seguintes classificações [IETF, 2008a]:

a) padrão proposto;

b) minuta de padrão;

c) padrão;

d) experimental;

e) informativo;

f) histórico;

g) melhores práticas;

h) desconhecido.

Somente as classificações “padrão proposto”, “minuta de padrão” e “padrão” fazem parte do processo de padronização do IETF. As demais classificações indicam que a RFC não está no processo para se tornar um padrão, tendo por objetivo apenas atender ao que está previsto na designação da classificação. Para chegar a ser um “padrão”, uma RFC deve passar pelos estágios de “padrão proposto” e depois “minuta de padrão”. Esse processo pode levar anos ou mesmo pode não se concluir nunca.

As RFCs que tratam de infraestruturas de chaves públicas, assinaturas digitais e temas correlatos não chegaram a atingir o *status* de padrão IETF. Um exemplo dessa situação pode ser observado na série de RFCs que tratam dos perfis para certificados X.509 v3 e para listas de certificados revogados X.509 v2 para uso na Internet, mostradas na tabela 3.1. Desde a criação da versão inicial (RFC2459) [HOUSLEY, 1999] até a versão atual (RFC5280) [HOUSLEY, 2008], esses documentos tiveram apenas a classificação “padrão proposto”

Tabela 3.1 – Evolução das RFCs sobre formato de certificado

Número	Título	Data	Classificação
RFC5280 Torna obsoletas: RFC3280, RFC4325, RFC4630	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	Mai 2008	PADRÃO PROPOSTO
RFC4630 Tornada obsoleta por: RFC5280 Atualiza: RFC3280	*Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	Ago 2006	PADRÃO PROPOSTO
RFC4325 Tornada obsoleta por: RFC5280 Atualiza: RFC3280	*Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension*	Dez 2005	PADRÃO PROPOSTO
RFC3280 Torna obsoleta: RFC2459 Tornada obsoleta por: RFC5280 Atualizada por: RFC4325 e RFC4630	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*	Abr 2002	PADRÃO PROPOSTO
RFC2459 Tornada obsoleta por: RFC3280	*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*	Jan 1999	PADRÃO PROPOSTO

Fonte: www.ietf.org [IETF, 2008]

É preciso, portanto, tomar cuidado com as implementações que tomem por base exclusivamente as propostas das RFCs, sem considerar outros documentos ou as necessidades específicas da ICP que está sendo modelada.

3.3.5 Documentos da ABNT

NBR ISO/IEC 17799:2005 [ABNT, 2005] - Tecnologia de Informação / Técnicas de Segurança / Código de prática para a gestão da segurança da informação. A NBR 17799, lançada em agosto de 2005, é a versão brasileira da norma amplamente utilizada pela comunidade internacional para a gestão de segurança de informações. Ela se aplica à segurança da informação em sentido amplo. Fornece os melhores procedimentos, diretrizes e princípios gerais de implementação, manutenção e gestão da segurança de dados em qualquer organização, produzindo e utilizando informação em qualquer formato.

A versão original da ISO/IEC 17799 foi publicada em 2000, e por sua vez era uma cópia fiel do padrão britânico (BS) 7799-1:1999, que serviu como referência para a criação do DOC-ICP-02 [BRASIL, 2008], que trata da Política de Segurança a ser observada por todas as entidades componentes da ICP-Brasil.

NBR 11.515/NB 1334 [ABNT, 1990] - Critérios de Segurança Física Relativos ao Armazenamento de Dados - Essa norma deve ser observada pelas autoridades certificadoras e prestadores de serviços de suporte, conforme consta no DOC-ICP-05 [BRASIL, 2008e].

3.3.6 Outros Documentos

Padrão FIPS 140-2 [EUA, 2005] - *Federal Information Processing Standard* é um padrão que descreve os requisitos do Governo Americano que devem ser seguidos pelos fabricantes de produtos de tecnologia da informação voltados para utilização com informações sensíveis. O padrão foi publicado pelo *National Institute of Standards and Technology* (NIST) e adotado pelo Governo Canadense e pela comunidade financeira, através do *American National Standards Institute* (ANSI).

ISO 15408 [ISO/IEC, 2005] - *Common Criteria for Information Technology Security Evaluation,* conhecido como *Common Criteria* ou CC é um padrão internacional que não

define uma lista de requisitos que os produtos de segurança devem conter, mas descreve uma plataforma padrão, que pode ser adotada pelos usuários de sistemas e equipamentos para especificar suas necessidades de segurança, pelos fabricantes e desenvolvedores para implementar os seus produtos e pelos laboratórios de avaliação para determinar se esses produtos realmente possuem as características de segurança que dizem possuir.

ISO 14721 [ISO/IEC, 2003] – O *Open Archive Information System (OAIS)* – especifica um modelo de referência para um sistema de arquivamento aberto. O propósito dessa ISO 14721:2003 é estabelecer um sistema de arquivamento da informação, tanto digitalizada como física, com um esquema organizacional composto de pessoas que aceitam a responsabilidade de preservar informação e torná-la disponivel para uma comunidade designada. O modelo OAIS descrito na ISO 14721:2003 pode ser aplicado a qualquer arquivo. É especialmente aplicável a organizações com a responsabilidade de disponibilizar a informação por longo tempo. Isso inclui organizações com outras responsabilidades, tais como processamento e resposta a necessidades programáticas.

3.4 REGULAMENTAÇÃO EUROPÉIA SOBRE ASSINATURA DIGITAL

3.4.1 Histórico

Para fomentar o amplo desenvolvimento da Assinatura Digital na Comunidade Europeia, a Comissão e o Parlamento Europeu adotaram a Diretiva 93/1999 para Assinaturas Eletrônicas [EUROPA, 1999].[1]

Na União Europeia, os Estados Membros são obrigados, pelo Tratado de Roma, a implementar as Diretivas da União Euopéia nas legislações nacionais. Os Estados-membros que não o fizerem serão culpáveis pelo dano que causarem e, além disso, poderão ser forçados pela Corte de Justiça Europeia a implementar as Diretivas.

A Diretiva 93/1999 tinha de ser implementada nas legislações nacionais antes de 18 de julho de 2001. Quase todos os estados-membros efetivamente o fizeram, alguns de forma mais ampla do que outros, mas mesmo assim restaram diversas questão em aberto, como:

- interoperabilidade europeia;
- coordenação da supervisão europeia;
- esquemas de acreditação;
- autoridade-raiz europeia;
- sustentabilidade do modelo de negócios.

Iniciou-se então um esforço conjunto para solucionar essas questões, sendo que os padrões EESSI *(European Electronic Signature Standardisation Initiative)* foram o primeiro passo importante para isso.

O EESSI foi criado em 1999 para coordenar a atividade de padronização para dar suporte à implementação da Diretiva 93/1999. As atividades de padronização foram realizadas pelos

[1] A Diretiva 93/1999 procurou ser abrangente, usando o termo "assinatura eletrônica", que engloba várias tecnologias, inclusive a assinatura digital. Na prática, todavia, a regulamentação europeia está voltada para a tecnologia de assinatura digital.

grupos de trabalho CEN/ISSS e ETSI TC SEC/ESI. As referências aos padrões foram publicadas no Jornal Oficial da Comunidade Europeia em julho de 2003. Esses padrões são parte de um conjunto maior definido pelo EESSI e incluído em seu programa de trabalho. O EESSI completou seu mandato e foi encerrado em outubro de 2004, ficando a manutenção dos documentos e a criação de novos padrões diretamente a cargo do CEN e do ETSI.

Nesse meio tempo a Comissão Europeia continuou trabalhando na elaboração do arcabouço legal necessário à implantação da assinatura digital na Europa, ESTANDO OS principais regulamentos relacionados a seguir.

3.4.2 Diretiva 93/1999

Este é o principal marco regulatório europeu sobre o assunto. Entre os pontos relevantes da Diretiva 93/1999 [EUROPA,1999] pode-se destacar:

- Relevância legal: assinaturas avançadas, criadas com um Dispositivo Seguro de Criação de Assinaturas e com um Certificado Qualificado são iguais a assinaturas manuscritas. Para outras assinaturas, em princípio, não se pode negar relevância legal.
- Auto-regulação: o legislador define os objetivos. Os técnicos se auto-regulamentam, definindo as formas de atingir os objetivos, respeitando os padrões internacionais.
- Neutralidade tecnológica: a Lei não deve inibir a inovação nem impedir a competição.
- Proteção da privacidade: as assinaturas eletrônicas não devem facilitar *data mining*. A liberdade no uso de pseudônimos é garantida como direito individual.
- Acreditação voluntária: não existe licenciamento, a acreditação dos prestadores de serviços de certificação (PSC) é voluntária, mas é obrigatória a supervisão por cada Estado-membro dos PSC que estejam sediados em seu país.
- Proteção ao consumidor: os PSC assumem responsabilidades sobre o serviço de certificação. A tecnologia é transparente para os usuários, cabendo aos Estados-

membros designar entidades para avaliar a conformidade dos dispositivos seguros de criação de assinaturas com os requisitos constantes na diretiva.

- Não-discriminação: o legislador nacional não pode discriminar assinaturas que venham de outros Estados-membros.
- Reconhecimento Internacional: um certificado emitido por PSC de país que não pertença à Comunidade Europeia deve ser aceito, desde que atendidas determinadas condições.

O artigo quinto da Diretiva afirma:

> *"1. Os Estados-Membros assegurarão que as assinaturas eletrônicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas:*
>
> *a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e*
>
> *b) São admissíveis como meio de prova para efeitos processuais."* [EUROPA,1999]

Fica patente, assim, que na Comunidade Europeia, para obter o que é chamado no Brasil de "presunção de validade jurídica", não basta que a assinatura tenha sido criada com base em certificado qualificado, mas é preciso que tenha sido utilizado um "**dispositivo seguro para criação de assinaturas",** que é aquele que atende aos requisitos elencados no Anexo III da Diretiva:

> *"1. Dispositivos seguros para criação de assinaturas precisam, por meios técnicos e procedimentais apropriados, assegurar pelo menos que:*
>
> *(a) os dados usados para geração de assinatura podem ocorrer praticamente uma única vez, e seu sigilo é razoavelmente assegurado;*
>
> *(b) os dados usados para criação da assinatura não podem, com uma razoável certeza, ser deduzidos e a assinatura está protegida contra falsificações usando a tecnologia atualmente disponível;*

(c) os dados usados para criação da assinatura podem proteger o assinante legítimo contra o uso de outros.

2. Dispositivos seguros para criação de assinaturas não devem alterar os dados a serem assinados ou evitar que esses dados sejam apresentados ao assinante antes do processo de assinatura." [EUROPA,1999]

3.4.3 Diretiva 709/2000

Para permitir a implementação da Diretiva 93/1999 foi necessário complementá-la com outros regramentos.

A Diretiva 709/2000 [EUROPA, 2000] é um deles. Tem por objetivo "*estabelecer os critérios a seguir pelos Estados-Membros quando designarem as entidades nacionais responsáveis pelas avaliações da conformidade dos dispositivos de criação de assinaturas seguras*." Aborda questões como capacidade técnica do laboratório e de seu pessoal, independência, imparcialidade, confidencialidade no trato das informações, contratação de seguro etc.

3.4.4 Diretiva 115/2001

Um grande incentivo para a utilização de assinaturas digitais na Europa foi dado com a publicação da Diretiva 115/2001 [EUROPA, 2001], que trata do imposto sobre o valor agregado (IVA), buscando simplificar, modernizar e harmonizar as condições aplicáveis à faturação. Esse imposto é de extrema relevância para os países-membros pois responde por percentual relevante da arrecadação tributária de cada país.

A legislação anterior sobre IVA, datada de 1977, deixava muitos pontos em aberto e não previa novas tecnologias, como o uso de faturas eletrônicas. A Diretiva 115/2001 visou corrigir essa situação:

"Por conseguinte, para assegurar o bom funcionamento do mercado interno, afigura-se necessário estabelecer, a nível comunitário, para efeitos de imposto sobre o valor acrescentado, uma lista harmonizada de menções que devem obrigatoriamente figurar nas facturas, bem como algumas regras comuns de recurso à ***faturação eletrônica*** *e à* ***armazenagem eletrônica das faturas****, assim*

como à auto-faturação e à subcontratação das operações de faturação." (sem grifo no original) [EUROPA, 2001]

Para tanto, deve ser possível garantir autoria e integridade das faturas eletrônicas, o que pode ser feito por outros meios, mas principalmente pelo uso de assinaturas digitais criadas em conformidade com a Diretiva 93/1999.

Um ponto a observar na Diretiva 115/2001 é a preocupação com a guarda dos documentos, o que levou à criação de padrões ETSI que tratam do armazenamento de documentos assinados digitalmente.

3.4.5 Decisão 511/2003

A Decisão 511/2003 [EUROPA, 2003], que está parcialmente transcrita a seguir, regulamenta as normas que definem os requisitos para os produtos seguros de assinatura eletrônica, constantes nos Anexos II e III da Diretiva 93/1999.

"A COMISSÃO DAS COMUNIDADES EUROPEIAS, [....]

Tendo em conta a Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999, relativa a um quadro comunitário para as assinaturas eletrônicas e, nomeadamente, o nº 5 do seu artigo 3º,

Considerando o seguinte:

(1) O anexo II, alínea f), e o anexo III da Diretiva 1999/93/ /CE estabelecem os requisitos para os produtos seguros de assinatura eletrônica. [....]

ADOTOU A PRESENTE DECISÃO:

Artigo 1º Os números de referência das normas geralmente reconhecidas para produtos de assinatura eletrônica são estabelecidos no anexo [....].

ANEXO

A. Lista das normas geralmente reconhecidas para produtos de assinatura eletrônica que permitem presumir a conformidade com o requisito do anexo II, alínea f), da Diretiva 1999/93/CE.

— CWA 14167-1 (Março de 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements

— CWA 14167-2 (Março de 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)

B. Lista das normas geralmente reconhecidas para produtos de assinatura eletrônica que permitem aos Estados-Membros de presumir a conformidade com os requisitos do anexo III da Diretiva 1999/93/CE.

— CWA 14169 (Março de 2002): secure signature-creation devices"

3.4.6 Decisão 717/2007

Em 2007 a Comissão Europeia publicou a decisão 717/2007 [EUROPA, 2007], para criar um grupo de trabalho, com mandato até 2009, visando a atender aos seguintes objetivos (sem grifo no original):

*"a) **Identificar lacunas no quadro normativo de faturação eletrônica**, a nível comunitário e nacional, que possam impedir a economia comunitária de explorar todas as suas potencialidades;*

b) Identificar as necessidades das empresas em matéria de faturação eletrônica para efeitos do quadro atinente e garantir a sua validação pelos principais interessados (3);

*c) Identificar os dados pertinentes em matéria de faturação eletrônica, em especial para estabelecer uma associação entre a fatura e, no mínimo, os processos de aquisição e de pagamento, bem como as questões relacionadas com o imposto sobre o valor acrescentado, **a autenticação e a integridade e as exigências em matéria de arquivo e armazenamento de dados e, ainda, com a necessidade de garantir a validação destes elementos pelos principais interessados**;*

*d) **Propor as responsabilidades que devem ser atribuídas aos organismos de normalização, bem como um calendário para a elaboração de normas comuns**, com base nas necessidades das empresas e nas exigências em matéria de dados das partes interessadas, a fim de apoiar um quadro europeu de faturação eletrônica;*

e) Propor o quadro europeu de faturação eletrônica. No âmbito deste quadro, instituir-se-á uma estrutura conceitual comum que tenha em conta normas e necessidades das empresas, e propor-se-ão soluções que facilitem a prestação de serviços de faturação eletrônica de uma forma aberta e interoperável em toda a Europa." (sem grifo no original) [EUROPA, 2007].

O trabalho de regulamentação sobre a assinatura digital e armazenamento seguro de faturas eletrônicas encontra-se em andamento na Comunidade Europeia, já tendo sido elaborados diversos padrões pelo ETSI e CEN para apoiar esse processo, conforme se pode observar no Anexo.

3.4.7 Transposição da Diretiva Europeia para Legislação dos Países-Membros

Como já citado, os países da Comunidade Europeia tiveram de transcrever para suas leis a Diretiva Europeia 93/1999 e decisões correlatas da Comissão.

Para exemplificar esse processo, tome-se o caso francês, relatado pelo governo daquele país em documento intitulado *Signature Electronique – Point de Situation* [FRANÇA, 2004], segundo o qual a transposição da Diretiva Europeia para a legislação francesa aconteceu em várias etapas:

***"Lei n º 2000-230 de 13 de Março de 2000**: adaptação do direito de prova às tecnologias da informação e relativa à assinatura eletrônica. Essa Lei inclui no Código Civil francês o artigo 1316-4, que define assinatura e coloca equivalência entre assinatura eletrônica e assinatura manuscrita sob certas condições: "A confiabilidade deste método é presumida, até prova em contrário, uma vez que a assinatura eletrônica tenha sido criada, a identidade do signatário assegurada e a integridade do ato garantida, dentro de condições estabelecidas pelo Conselho de Estado." (Artigo 1316-4 do Código Civil).*

***Decreto n º 2001-272 de 30 de Março de 2001**: sobre a aplicação do artigo 1316-4 do Código Civil e sobre a assinatura eletrônica, na redação dada pelo Decreto nº 2002-535 de 18 Abril de 2002. Esse decreto descreve as condições sob as quais o processo de assinatura eletrônica é considerado confiável e define os requisitos para dispositivos seguros de criação de assinaturas;*

Decreto n º 2002-535 de 18 de Abril de 2002*: sobre a avaliação e certificação da segurança oferecida pelos produtos e sistemas de tecnologia da informação. Esse decreto estabelece as regras para a certificação de produtos de segurança e notadamente de dispositivos seguros de criação de assinaturas. Estabelece que a avaliação dos dispositivos para certificação deve acontecer num centro de uma avaliação aprovado pelo Governo francês. Esses centros procedem às avaliações segundo um dos critérios: ITSEC (cada vez menos utilizados) ou padrão 15408 (também chamado de "Common Criteria").*

Lei n º 2004-575 de 21 de junho de 2004*: para a confiança na economia digital, notadamente o seu artigo 33 que especifica o regime de responsabilidade dos provedores de serviços de certificação eletrônica que emitem certificados eletrônicos qualificados.*

Lei n º 2004-801 de 6 de agosto de 2004*: sobre a proteção das pessoas físicas quanto ao tratamento de dados pessoais e que altera da Lei n º 78-17 de 6 de janeiro de 1978, relativa à informática, aos arquivos e às liberdades, que transpõe, no seu artigo 5º, o artigo 8 º da Diretiva sobre a Proteção de Dados (novo Artigo 33 º da Lei de 6 de janeiro de 1978).*

Ordem de 26 de julho de 2004*: sobre o reconhecimento das qualificações dos prestadores de serviço de certificação eletrônica e à acreditação dos organismos que exercem a sua avaliação, anunciada no Decreto 2001-272. Esse decreto define o esquema francês de qualificação de Prestador de Serviços de Certificação. Os PSC se submetem voluntariamente para essa avaliação, a fim de receber um atestado de qualificação. Um provedor sem atestado de qualificação pode, porém, declarar que emite certificados qualificados se ele acredita que cumpra as exigências do artigo 6 do Decreto."*

Outros regulamentos detalhando os assuntos contidos nas leis e decretos são expedidos pela Direção Central de Segurança de Sistemas de Informação *(Direction centrale de la sécurité des systèmes d'information - DCSSI),* que desempenha um conjunto de tarefas que, no Brasil, se equivalem às realizadas pela AC-Raiz da ICP-Brasil, pelo Gabinete de Segurança Institucional (GSI) e pela Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento.

O DCSSI está ligado ao Secretariado Geral da Defesa Nacional e é o centro focal do estado francês para a segurança dos sistemas de informação. Traça as diretrizes que devem ser seguidas pelos órgãos de governo sobre procedimentos de segurança da informação e uso de tecnologias seguras. Com relação a certificação, assinatura digital e arquivamento de documentos eletrônicos, aquele órgão expediu diversos regulamentos, entre os quais citamos:

Documentos sobre arquivamento eletrônico - Elaborados em conjunto com a Direção Central dos Arquivos da França, do Ministério da Cultura e da Comunicação e a Direção Central para Modernização do Estado, do Ministério da Economia, Finanças e Indústria.

- Arquivamento Eletrônico Seguro – Ganhos jurídicos;
- Arquivamento Eletrônico Seguro – O estado da arte;
- Arquivamento Eletrônico Seguro - Apresentação dos elementos que devem ser considerados em um projeto de arquivamento eletrônico seguro e dos documentos necessários para concretizá-lo;
- Arquivamento Eletrônico Seguro - Caderno de encargos para um sistema de arquivamento eletrônico (esfera pública).

Documentos sobre certificação digital

- Política de certificados – indivíduo - para certificados qualificados com utilização de dispositivos seguros de criação de assinaturas;
- Política de certificados – empresa - para certificados qualificados com utilização de dispositivos seguros de criação de assinaturas;
- Guia de Auditoria de PSC.

Documentos sobre homologação de dispositivos de segurança

- Regras relativas à qualificação de produtos de segurança pelo DCSSI;
- Materiais necessários à análise dos mecanismos criptográficos;
- Procedimento: Manutenção da confiança – continuidade da segurança;
- Procedimento: Utilização da marca “Certificação de Segurança TI”;

- Procedimento: Certificação de conformidade dos módulos criptográficos dos PSC;
- Procedimento: Certificação de conformidade dos dispositivos de criação de assinatura eletrônica;
- Procedimento: Certificação de segurança de primeiro nível das tecnologias da informação;
- Procedimento: Aprovação dos centros de avaliação em vista da certificação da segurança de primeiro nível;
- Acordos de Reconhecimento Mútuo assinados pelo DCSSI para reconhecimento de certificação de produtos de segurança;
- Catálogo de produtos de segurança homologados pelo DCSSI para construção de arquiteturas seguras.

3.4.8 Resultados Obtidos na Comunidade Europeia

A Comunidade Europeia e os estados-membros vêm realizando esforços consideráveis para implantar a assinatura digital em seus regramentos. Mesmo assim, na maior parte dos países europeus a certificação digital continua sendo utilizada principalmente para projetos de governo eletrônico e serviços de *e-banking*. [FOKUS, 2006].

Diversas pesquisas foram realizadas para tentar determinar as causas disso. Uma delas foi empreendida pelo OASIS PKI TC [OASIS, 2003], cujo resultado está na Figura 3.1:

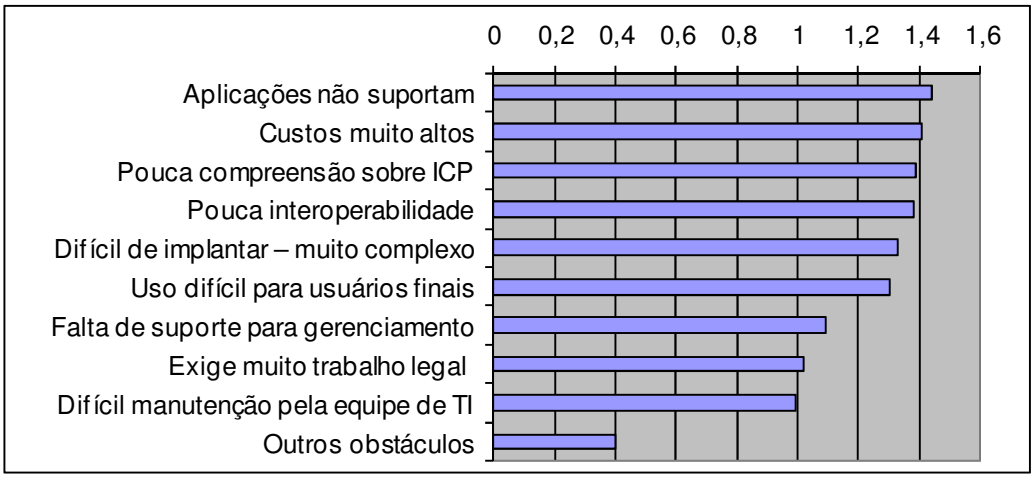

Figura 3.1 - Pesquisa OASIS TC PKI sobre obstáculos a ICP (Fonte: [OASIS, 2003])

Outra pesquisa foi conduzida pela própria Comissão Europeia, que publicou o resultado no Relatório 120/2006 [EUROPA, 2006].

> *"A utilização das assinaturas eletrônicas qualificadas tem sido muito inferior ao que se esperava, estando o mercado, atualmente, pouco desenvolvido [...].*
>
> *A principal razão do arranque lento do mercado é de natureza econômica: os fornecedores de serviços estão pouco motivados para desenvolverem assinaturas eletrônicas multiaplicações, preferindo oferecer soluções para os seus próprios serviços, como as desenvolvidas pelo sector bancário. Esta situação atrasa o processo de desenvolvimento de soluções interoperáveis. A falta de aplicações, como, por exemplo, soluções globais para arquivos eletrônicos, pode igualmente impedir o desenvolvimento de assinaturas eletrônicas polivalentes, que pressupõe a obtenção de uma massa crítica de utilizadores e de utilizações.*
>
> *No entanto, algumas aplicações poderão vir a provocar o crescimento do mercado. A utilização das assinaturas eletrônicas nos serviços de administração pública em linha já atingiu um volume apreciável, podendo, no futuro, tornar-se um importante elemento catalisador [...].*
>
> *A Comissão continuará a incentivar o desenvolvimento de serviços e aplicações de assinatura eletrônica e monitorizará o mercado. Para além do apoio fornecido através das atividades de administração pública em linha, será dada especial atenção à interoperabilidade e à utilização transfronteiras das assinaturas eletrônicas. A Comissão incentivará o avanço dos trabalhos de normalização para promover a interoperabilidade e a utilização de todos os tipos de tecnologias para a assinatura eletrônica qualificada no mercado interno."* (tradução nossa)

Também o trabalho *Study on PKI and Certificate Usage in Europe 2006* [FOKUS, 2006] descreve os progressos na introdução de serviços baseados em ICP nos diferentes países da Comunidade Europeia e analisa com detalhes a utilização de certificados, *smartcards* e assinaturas digitais, bem como as estratégias de penetração e impacto dessas tecnologias na sociedade:

> *"A principal conclusão obtida a partir da comparação dos países é que as assinaturas eletrônicas não são ainda extensamente utilizadas, não obstante as diferentes estratégias de penetração (por exemplo:* ***certificados a custo zero****,*

facilidades no processo de registro, assinaturas por dispositivos móveis ou USB) em diferentes países." (sem grifo no original)

Para Genghini [GENGHINI, 2005] essas pesquisas deixam claro, também, que:

- a aceitação social da certificação e assinatura digital é baixa: seu uso ocorre apenas se for obrigatório;
- a tecnologia é difícil de usar e mesmo de compreender;
- não permite ao signatário ter certeza de que aquilo que está assinando é aquilo que lhe está sendo mostrado na tela;
- os dispositivos seguros de criação de assinaturas são usados apenas se forem obrigatórios ou se forem significativamente mais baratos do que outras opções;
- existem expectativas erradas em relação àquilo que as assinaturas digitais qualificadas podem fazer;
- falta um modelo de negócios bem-sucedido para as entidades envolvidas com certificação digital;
- a única estória de sucesso é a autenticação de dados de origem.

Segundo Dumortier [DUMORTIER, 2003] já foram mapeadas as questões a serem resolvidas para permitir o uso mais extensivo e a aceitação das assinaturas eletrônicas na Europa. Também já foram identificadas as atividades que devem ser empreendidas pela Comissão Europeia nesse sentido. Segue um breve resumo dessas questões:

•" Não existe demanda de mercado natural para Certificados Qualificados e serviços relacionados. A maior aplicação na Europa para assinaturas eletrônicas está geralmente relacionada a aplicações de e-banking em ambientes fechados, e assim fora do escopo da Diretiva. Dentro do escopo da Diretiva muito poucas aplicações estão em uso hoje e elas são quase todas limitadas a e-gov.

• Muitos prestadores de serviços de aplicação acreditam, falsamente, que suas aplicações precisam utilizar assinaturas eletrônicas qualificadas como um patamar mínimo, para estar em acordo com legislação, o que conduz a custos e complexidade desnecessários.

• A falta de interoperabilidade, tanto em nível nacional como transnacional é um grande obstáculo para a aceitação pelo mercado e para a proliferação de assinaturas eletrônicas.

• Em parte porque a Diretiva Europeia atualmente define requisitos muito altos para os dispositivos seguros de criação de assinaturas digitais, tais dispositivos raramente encontram aceitação no mercado.

• O ambiente regulatório da Diretiva Europeia 93/1999 inclui regras bastante detalhadas para os provedores de certificados, mas não faz o mesmo para outras categorias de provedores de serviços de certificação. „(tradução nossa).

3.5 CONCLUSÃO

A regulamentação sobre assinaturas e certificados digitais é um processo complexo, que demanda grande esforço, passando desde o desenvolvimento de normas e padrões, realizado por organismos de normalização, oficiais ou independentes, até a incorporação desses padrões na legislação dos países que se dispõem a adotá-los.

Foi estudado o caso da Comunidade Europeia, que se empenha há uma década no processo de implantação da assinatura digital em documentos e transações, mas que ainda hoje não tem o uso de assinatura digital plenamente disseminado nos diversos países que a integram. Pesquisas realizadas para compreender o motivo dessa utilização inicipiente apontam como principais causas a falta de aplicações que suportem assinatura digital, os altos custos e a complexidade na implementação, gerenciamento e utilização dessa tecnologia, entre outras.

Do trabalho realizado, depreende-se que as dificuldades na implantação das tecnologias de certificação e assinatura digital na Europa decorrem também das diferenças na implementação das disposições contidas nas diretivas, em cada país. O formato das assinaturas digitais, por exemplo, foi implementado com pequenas diferenças em cada país, mesmo tendo sido regulamentado por meio dos documentos ETSI, já que aqueles documentos facultam a utilização ou não de determinados requisitos, bem como permitem mais de uma forma de preenchimento desses requisitos.

Isso tem obrigado a Comunidade Europeia a realizar estudos comparativos e expedir novos regulamentos, visando a harmonização dos procedimentos em todos os países membros. O Brasil leva vantagem em relação àquele bloco econômico, na medida em que a legislação sobre certificação e assinatura digital, em nosso País, possui abrangência nacional.

4 ASSINATURAS DIGITAIS E SUA UTILIZAÇÃO COMO EVIDÊNCIA LEGAL

4.1 INTRODUÇÃO

Neste capítulo faz-se uma breve explanação sobre o que é uma assinatura digital e os processos que a envolvem. Relacionam-se ainda questões relevantes sobre documentos assinados digitalmente e sua utilização como evidência legal.

4.2 O PROCESSO DE ASSINATURA DIGITAL

A tecnologia da assinatura digital faz uso de um par de chaves assimétricas: a chave privada e a chave pública. A chave privada serve para gerar uma assinatura digital e/ou para decifrar informações criptografadas. A chave privada deve permanecer secreta, enquanto a chave pública é publicada. A chave pública é usada para verificar uma assinatura digital e / ou cifrar informações confidenciais. As chaves privadas e públicas não podem ser derivadas uma da outra. Na ICP-Brasil esse par de chaves é obrigatoriamente criado pelo próprio titular, embora em outras ICPs isso possa ser realizado por outras entidades, como a autoridade certificadora.

Assinar um documento eletrônico com uma assinatura digital é um processo de dois passos: o arquivo de computador que contém o documento eletrônico é primeiramente submetido a um algoritmo de embaralhamento com perda, o que produz um valor conhecido por *hash* ou resumo criptográfico. Na segunda etapa, esse *hash* é então cifrado com a chave privada do signatário. O resultado dessa operação é a assinatura digital, que se constitui em um objeto digital separado do documento eletrônico em si, mas que fica associado a ele, para futura validação.

O documento eletrônico, juntamente com a assinatura digital, é apresentado para a terceira parte, que confirma sua validade ao decifrar a assinatura digital com a chave pública do signatário, obtida no certificado digital. O resultado da decifração é o valor *hash* do documento eletrônico, conforme gerado pelo signatário. A seguir, a terceira parte realiza, ela própria, um novo cálculo do valor *hash* do documento e o compara com o valor *hash* que recebeu junto com o documento. Se forem iguais, significa que o documento

eletrônico está íntegro e que é possível identificar o signatário por meio do certificado digital. Caso contrário, a assinatura digital é inválida.

Uma assinatura digital tem, em teoria, três funções:

- autenticação: a assinatura digital foi criada com a chave privada do remetente;
- integridade: a prova de que o documento não foi modificado após ter sido assinado;
- "não-repúdio": o signatário não pode negar que ele tenha assinado o documento.

Por si só, uma assinatura digital não diz nada sobre a verdadeira identidade do signatário. Para a verificação de uma assinatura digital, a ligação entre o signatário e sua chave pública deve ser evidenciada a partir de um certificado digital. Na ICP-Brasil, o certificado digital deve ser criado por uma autoridade certificadora credenciada, o que lhe confere um alto grau de confiabilidade.

O certificado digital contém a chave pública e informações sobre a identidade do titular do certificado (proprietário da chave), o período de validade, o algoritmo de assinatura, o número de série do certificado e o nome da autoridade certificadora, entre outras informações. Os certificados digitais têm um prazo de validade limitado, mas também podem ser revogados antes do término desse período. O titular do certificado pode pedir a revogação do certificado em diversas situações, como roubo ou perda da chave privada, alteração nas informações contidas no certificado etc.

Para permitir que se verifique a confiabilidade dos certificados de titulares finais, eles são assinados com a chave privada da autoridade certificadora. Para verificar se a assinatura realizada pela autoridade certificadora é válida, deve-se obter sua chave pública. Essa chave pública, por sua vez, está contida num certificado digital, emitido por outra autoridade certificadora de nível mais alto, que o assina digitalmente. Esse processo se repete até chegar-se a um certificado auto-assinado, emitido por uma AC considerada confiável.

Assim, para a verificação de uma assinatura digital, é necessária a validação de toda uma cadeia de entidades. Não é suficiente apenas arquivar o documento e a assinatura digital, se se deseja validar um documento eletrônico assinado digitalmente, no futuro. Isso significa que, além dos processos de assinatura, é necessário realizar ações complementares, tais

como obter de carimbos de tempo para confirmar o momento da assinatura, anexar todos os certificados da cadeia e as respectivas LCRs etc.

Documentos assinados digitalmente têm, muitas vezes, uma vida muito maior do que as chaves criptográficas e as tecnologias empregadas na geração da assinatura digital. Isso ocorre porque a validade das chaves é intencionalmente curta, uma vez que elas podem ser comprometidas ou podem, futuramente, ser descobertos métodos de criptoanálise que permitam descobrir com facilidade a chave privada, a partir da chave pública correspondente [STAPLETON, 2005].

Uma escritura digital de compra e venda de imóveis, por exemplo, precisará durar por dezenas de anos, ao passo que os certificados e as chaves privadas usadas para assiná-la serão válidos por poucos anos, dependendo da legislação de cada país. Como verificar, daqui a uma dezena de anos, se o certificado digital correspondente à chave privada que assinou o documento não estava expirado ou revogado, no momento da assinatura? Ou ainda, como precisar o momento em que foi realizada a assinatura?

Para tentar solucionar essas questões, podem ser utilizados carimbos do tempo, que registrem data e hora no resumo criptográfico (*hash)* do documento digital e/ou da assinatura digital. Essa medida, todavia, remete de volta à questão inicial, uma vez que o carimbo do tempo é, ele mesmo, um conjunto de dados assinado digitalmente. Como provar, daqui a dezenas de anos, que a chave privada da Autoridade de Carimbo do Tempo não foi comprometida, ou que o carimbo não foi forjado, de alguma maneira, dada a evolução tecnológica dos computadores e o avanço na solução de problemas matemáticos hoje insolúveis?

A compreensão de arquivos digitais depende também dos formatos e tipos de mídia em que foram gravados, bem como da existência de equipamentos ou emuladores que permitam sua leitura. Isso implica que devem ser adotados procedimentos para migrar esses arquivos para formatos e mídias adequadas, conforme os antigos se tornem obsoletos.

4.3 CARACTERÍSTICAS ESPERADAS DAS ICPS E DAS ASSINATURAS DIGITAIS

Uma ICP, ao fornecer certificados que podem ser utilizados para assinar digitalmente documentos eletrônicos com validade jurídica, deve prover confiabilidade e segurança em todos os processos, tanto os que envolvem o ciclo de vida do certificado digital como os que dizem respeito ao ciclo de vida da assinatura digital. Deve também prover rastreabilidade e auditoria dos processos executados, de forma a possibilitar a realização de perícias técnicas, em caso de eventuais disputas judiciais.

Essas características são fundamentais para que as assinaturas sejam usadas como evidência legal e implicam a adoção de um grande número de cuidados pelos executores das diversas atividades que compõem aqueles processos.

As etapas que dizem respeito ao ciclo de vida dos certificados digitais na ICP-Brasil estão previstas e regulamentadas no DOC-ICP-05 [BRASIL, 2008e]. São elas:

a) **Solicitação** - processo no qual é acessado o sistema da AC e preenchido formulário específico de solicitação de certificado digital;
b) **Validação** – processo no qual o solicitante do certificado comparece a uma instalação técnica de AR e apresenta seus documentos de identidade a dois agentes de registro, que o identificam e validam sua solicitação no sistema da AC;
c) **Emissão** – processo no qual o solicitante, utilizando uma senha especial, recebida na AR, comanda a emissão do seu certificado e o instala em seu computador ou dispositivo criptográfico;
d) **Revogação** – processo no qual um certificado já emitido é revogado pelo próprio titular ou pela AR, em função de solicitação motivada.

Já o ciclo de vida de uma assinatura digital compreende os seguintes processos, segundo o DOC-ICP-15 [BRASIL, 2009a]:

a) **Criação** - processo de criação de um resumo criptográfico logicamente associado a um conteúdo digital e a chave criptográfica privada do signatário;
b) **Verificação Inicial** - processo de verificação quanto à validade de uma ou mais assinaturas digitais logicamente associadas a um conteúdo digital;

c) **Armazenamento** – processo que trata da guarda da assinatura digital. Compreende, pelo menos, cuidados para conversão dos dados para mídias mais atuais, sempre que necessário;
d) **Revalidação** – processo que estende a validade do documento assinado, por meio da reassinatura dos documentos ou da aposição de carimbos do tempo, quando da expiração ou revogação dos certificados utilizados para gerar ou revalidar as assinaturas, ou ainda quando do enfraquecimento dos algoritmos ou tamanhos de chave utilizados.

Para Blanchette [BLANCHETTE , 2006], existe ainda mais uma etapa do ciclo de vida da assinatura digital: a **Verificação Final** ou **Litígio**, na qual o documento é apresentado como evidência para um juiz e a assinatura é novamente verificada, para se obter informações sobre a identidade do signatário e a integridade do documento. Embora se espere que a etapa de Verificação Final raramente venha a ocorrer, ela é o principal ponto a ser considerado no processo de arquivamento. Questões importantes surgem em função do tempo significativo que pode decorrer entre a etapa de Verificação Inicial e a etapa de Verificação Final. A Verificação Inicial pode ocorrer segundos, minutos ou dias depois da etapa de Criação, ao passo que a Verificação Final pode acontecer anos depois da Criação da assinatura e já no contexto de um documento arquivado.

As etapas relativas ao ciclo de vida do certificado estão adequadamente mapeadas e os principais riscos estão controlados por meio de diversos mecanismos de segurança, como:

a) dupla validação obrigatória para realização de operações críticas, como as que envolvem a identificação presencial dos titulares de certificados e a operação do sistema de certificação;
b) ferramentas de segurança física, como segmentação de ambientes, controle de acesso físico, monitoração permanente etc;
c) ferramentas de segurança lógica e de rede, como cartões criptográficos para ativar sistemas, gravação de *logs* das atividades importantes, uso de criptografia nas comunicações com os servidores das ACs, proteção de redes com *firewalls* etc.

Para assegurar que esses controles estejam operacionais e ofereçam a segurança esperada às ACs, ARs, ACTs e deamis entidades integrantes da ICP-Brasil, são realizadas auditorias periódicas por Empresas de Auditoria Independente, cujos resultados são repassados à AC-

Raiz da ICP-Brasil, que pode, ainda, realizar fiscalizações em qualquer das entidades, sempre que julgar necessário.

Na figura 4.1 pode-se visualizar um desenho esquemático dos processos do ciclo de vida do certificado digital, em que estão assinalados os pontos onde podem ocorrer ataques e representados alguns dos controles utilizados para mitigar o risco.

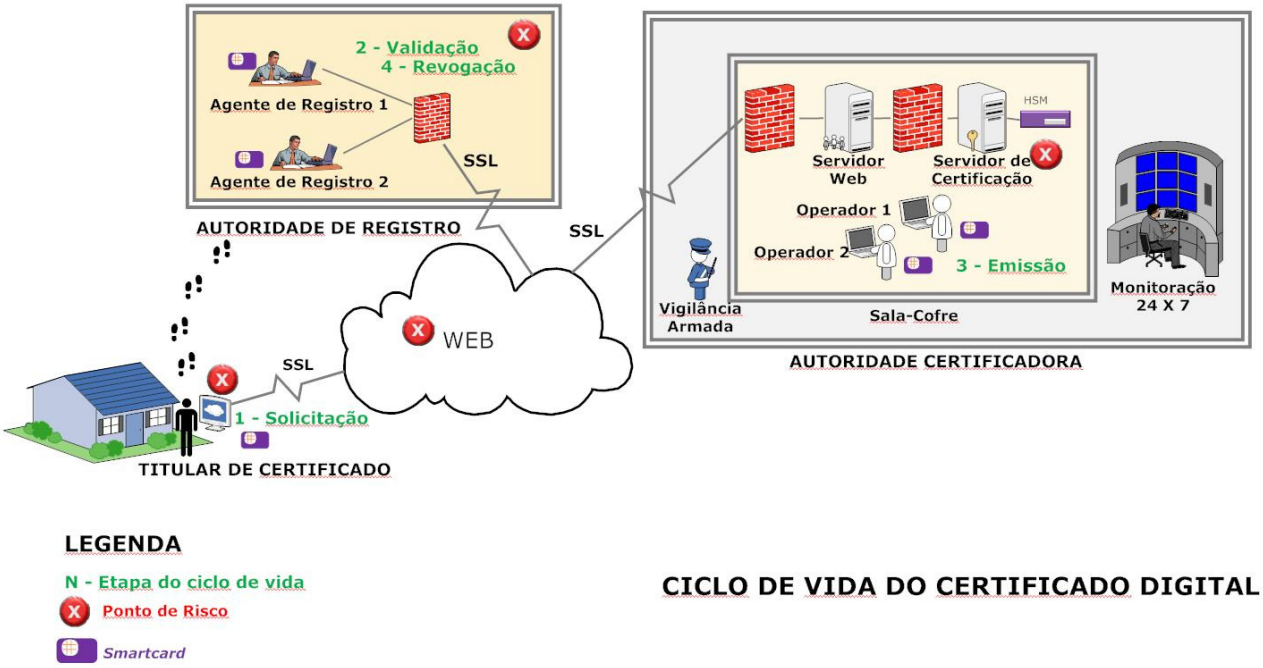

Figura 4.1: Ciclo de vida dos certificados digitais ICP-BRASIL

Já as etapas do ciclo de vida da assinatura digital ocorrem, normalmente, em ambientes sobre os quais a AC-Raiz possui pouco ou nenhum controle. Elas estão representadas na figura 4.2. A Criação de uma assinatura digital de um documento eletrônico pode ser criada em ambiente físico e lógico desprotegido, com a utilização de aplicativo não homologado. O mesmo ocorre com a Verificação Inicial, o Armazenamento e a Verificação Final.

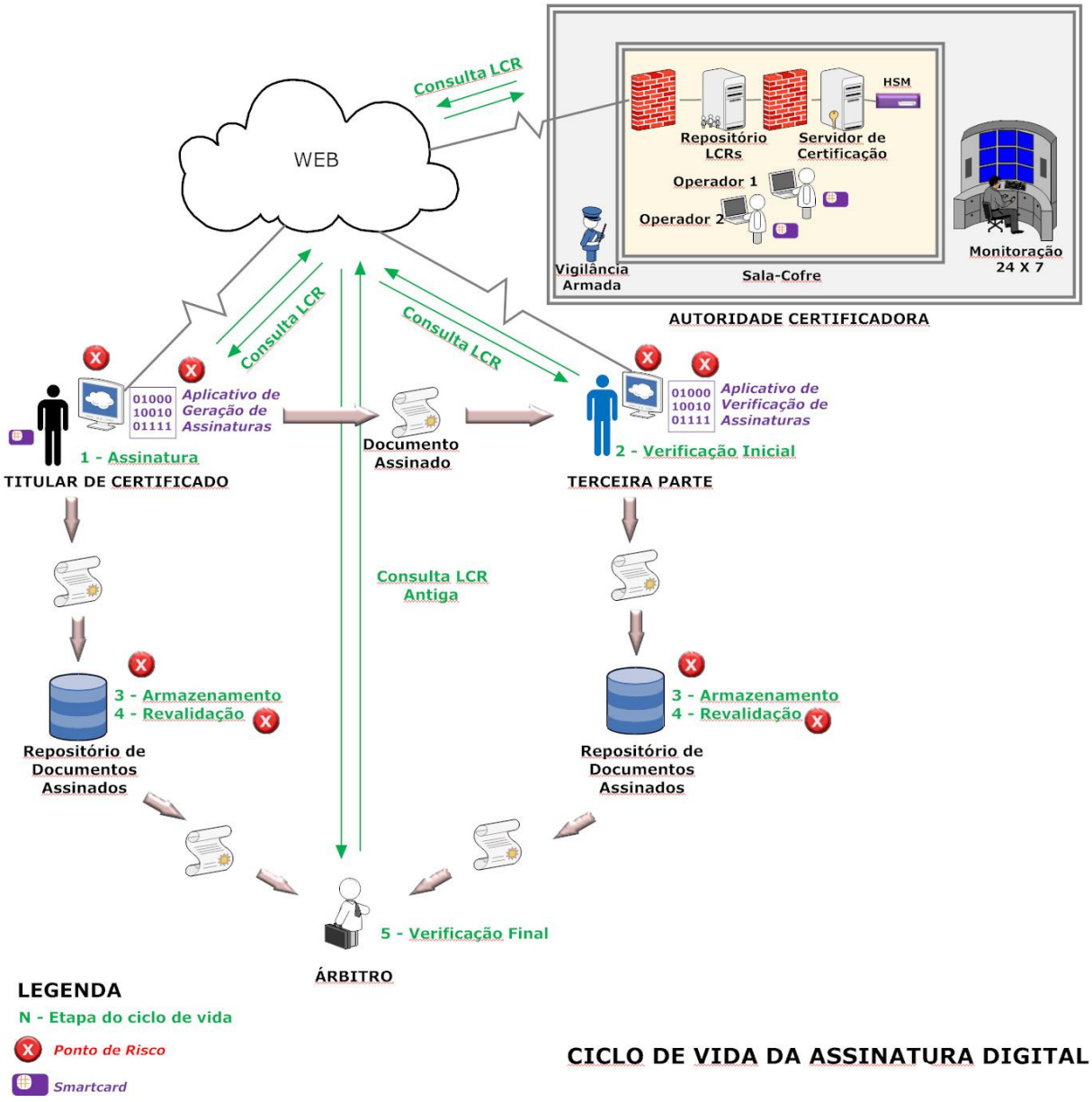

Figura 4.2: Ciclo de vida das assinaturas digitais ICP-BRASIL

Os procedimentos a serem executados em cada uma das etapas acima precisam estar claramente definidos e levar em consideração aspectos de segurança e auditabilidade [FERNANDES, 2001].

Para ilustrar a importância desse assunto, cita-se Lynch et al. [LYNCH, 1997], que faz uma inusitada mas ilustrativa comparação entre o Ácido Desoxirribonucleico (DNA) e a assinatura digital como elementos a serem utilizados como evidência legal em disputas jurídicas.

O DNA era considerado uma prova irrefutável de autoria de um crime, até 1995, ano em que O. J. Simpson, famoso ex-jogador de futebol americano, acusado de matar a esposa, foi inocentado no julgamento, mesmo tendo sido encontradas amostras de sangue com seu DNA na cena do crime.

A defesa baseou-se no fato de que as amostras de DNA foram coletadas por policiais sem a presença de testemunhas; os policiais ficaram com as amostras durante todo o dia e somente à noite as encaminharam para análise no laboratório, sendo que essa análise também não foi acompanhada por testemunhas nem por outros requisitos formais.

> "*Conforme três sociologistas explicaram: seguindo as amostras a partir da cena do crime até o laboratório, e então do laboratório até o tribunal, percebe-se que uma impressão digital genética somente pode ser útil como testemunha competente se (e apenas se) a sucessão de transações que compreendem a coleta, transporte, preservação, digitalização e análise da amostra forem, elas próprias, atestadas por testemunhas, certificadas e devidamente registradas por autoridades competentes. Para ser considerada como tal, a confiança contida na assinatura automática (o código de barras genético) precisa ser acompanhada, rodeada por uma série completa de registros burocráticos: assinaturas feitas à mão em formulários, códigos de barra verdadeiros afixados em sacolas contendo as amostras etc.*
>
> *Foram esses registros que foram sucessivamente contestados durante o caso Simpson, porque, como os arquivistas sabem há muito tempo, nenhuma evidência é auto-compreensível. O mesmo princípio se aplica aos registros eletrônicos: para que possam ser uma "testemunha competente" de um fato jurídico (compromisso de uma obrigação assumida), um documento eletrônico precisa ser acompanhado por registros de todas as operações que são susceptíveis de lhe ocorrer: criação, modificação, anotações, assinatura, conversão, transmissão, etc. De outra forma, assinaturas digitais seriam inábeis para atestar em si e por si mesmas sobre a identidade e a integridade de um documento, pois, para serem efetivas, precisam ainda ser acompanhadas por vários registros que atestem sua própria identidade e integridade como evidência – certificados de chaves públicas, listas de revogação, cadeias de certificados, trilhas de auditoria, resumos criptográficos, etc.*
>
> *A lição aqui é que o critério para autenticidade eletrônica não será estabelecido por uma bala de prata. Assim como as assinaturas foram, elas mesmas, uma*

novidade tecnológica em torno da qual as práticas sociais gradualmente convergiram, o valor de evidência de documentos eletrônicos irá emergir do lento e gradual envolvimento de grupos sociais com os vários meios técnicos que suportam a alegação de autenticidade. Embora a legislação possa oferecer uma rica janela de trabalho para suportar esse envolvimento, esforços para obrigar ao uso de regras precisas são, no mínimo, ainda prematuros." [LYNCH, 1997]

4.4 CONCLUSÃO

Foram apresentadas neste capítulo noções básicas sobre assinaturas digitais e a importância de cercá-las de processos seguros, desde a geração dos certificados até o arquivamento dos documentos assinados digitalmente. Todos esses processos devem ser realizados de forma a permitir rastreabilidade e auditoria, com o objetivo de conferir às assinaturas digitais condições técnicas necessárias e suficientes para serem úteis como evidência legal.

5 PRINCIPAIS DESAFIOS NA ICP-BRASIL

5.1 INTRODUÇÃO

Neste capítulo relacionam-se questões sobre assinatura digital de documentos eletrônicos que, na visão da autora, ainda não estão tratadas de forma adequada na ICP-Brasil e que podem comprometer a utilização desses documentos como evidência legal competente.

Foi utilizada, para elaborar essa relação, a experiência obtida durante os sete anos de trabalho na AC-Raiz da ICP-Brasil, inicialmente na área de Auditoria, como responsável pela avaliação das entidades que se credenciavam no sistema e depois na área de Normalização e Pesquisa, como responsável pelo estudo e proposição de novos regulamentos e de alterações em regulamentos já existentes.

Todas as questões aqui levantadas baseiam-se na legislação publicada até 20.06.2009. Foram desconsiderados, portanto, eventuais estudos internos que possam estar em andamento na AC-Raiz e que não ainda tenham sido aprovados pelo Comitê Gestor da ICP-Brasil e publicados no Diário Oficial da União e no sítio www.iti.gov.br [ITI, 2009b].

5.2 PONTOS QUE NECESSITAM DE ADEQUAÇÃO NA ICP-BRASIL

5.2.1 Revogação de Certificados

A utilização de uma chave privada para realizar assinaturas fora do período de validade do certificado associado implica a não-aceitação da assinatura como evidência legal. Assim, saber se um certificado estava ou não revogado no momento em que a assinatura digital foi realizada é um dos pontos-chave que devem estar adequadamente tratados numa ICP.

Para verificar a situação do certificado digital quanto à revogação são utilizados dois mecanismos: as Listas de Certificados Revogados (LCRs) [HOUSLEY, 2008] e as consultas usando o *Online Certificate Status Protocol* (OCSP) [MYERS, 1999].

As LCRs funcionam pela publicação, em algum repositório, de uma relação de certificados que não estão mais válidos e devem ser rejeitados pela pessoa ou aplicação que estiver realizando a validação. Essa relação pode ter tamanho variável, chegando muitas vezes a

vários *megabytes*. Já as consultas OCSP baseiam-se no envio de uma consulta ao servidor, na qual são informados dados do certificado cuja validade se deseja verificar. O servidor emite uma resposta assinada com sua chave privada, informando a situação do certificado.

Cada uma dessas tecnologias possui pontos fortes e fracos. As LCRs apresentam diversos problemas, mas destaca-se aqui o fato de que elas trazem informação defasada, pois relacionam as revogações que ocorreram no período anterior a sua geração e publicação [GUTMAN, 2002]. Isso gera dificuldades quando se trabalha com aplicações críticas, que na maior parte das vezes, necessitam de informação atualizada e imediata. Já a versão de OCSP mais utilizada, que é a proposta na RFC 2560 [MYERS, 1999], apresenta semântica confusa e baseia suas respostas em LCRs, o que significa que herda delas diversos problemas, como a defasagem das informações e a exclusão dos certificados revogados que tenham expirado.

Na ICP-Brasil, embora algumas ACs disponibilizem serviço OCSP, a principal forma de validação de *status* de certificados é através de LCRs. O DOC-ICP-05 [BRASIL, 2008e] define que cada AC deve gerar uma nova versão de LCR a cada 6 horas e publicá-la em repositório com disponibilidade de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana).

Em tese, para aplicações não críticas, esse serviço seria suficiente para permitir a validação de uma assinatura digital, mesmo bem depois do instante de sua criação. Bastaria verificar se o certificado associado à chave privada consta ou não da LCR mais recente emitida pela AC. Caso negativo, a assinatura seria válida. Caso positivo, seria necessário ainda comparar o momento em que a assinatura foi realizada (constante no carimbo do tempo associado à assinatura) com o momento em que o certificado foi revogado (constante na LCR), o que permitira verificar se a assinatura deu-se antes ou depois da revogação.

Ocorre que, para evitar que as LCRs fiquem muito longas, as ACs da ICP-Brasil excluem delas os certificados revogados, após sua expiração. Esse procedimento, previsto na seção 5 da RFC 5280 [HOUSLEY, 2008], permite diminuir o tamanho da LCR, o que confere maior agilidade na sua importação para um sistema local. Todavia, fragiliza a automação dos processos de validação do *status* de certificados, pois para validar uma assinatura

digital, cujo certificado correspondente já tenha expirado, será preciso consultar a LCR emitida logo depois do momento provável da assinatura.

O DOC-ICP-05 [BRASIL, 2008e] no item 6.1.3, define que as ACs da ICP-Brasil devem guardar, permanentemente, todas as LCRs emitidas ao longo de sua existência, para verificações futuras, mas não faz referência alguma à disponibilização dessas LCRs.

Com isso, caso as informações sobre o *status* dos certificados que compõem a cadeia de certificação não tenham sido capturadas no momento da geração da assinatura digital, ou pelo menos antes da expiração do certificado do titular, validar uma assinatura digital na ICP-Brasil será uma tarefa bastante difícil. Além disso, como para validar um certificado é preciso fazê-lo igualmente para os demais certificados da cadeia de certificação, essa complexidade aumenta ainda mais.

Uma possível solução para o problema seria a disponibilização obrigatória, por todas as ACs, de serviço OCSP, mas essa tecnologia, da forma como vem sendo utilizada na ICP-Brasil, também tem suas deficiências, como visto.

5.2.2 Preservação de Documentos Assinados Digitalmente

Um dos principais desafios com que se depara ao lidar com documentos assinados digitalmente diz respeito à sua preservação por longo prazo. Essa preocupação extrapola o âmbito da certificação digital, visto que se aplica a todos os documentos eletrônicos, sejam eles assinados digitalmente ou não.

No meio acadêmico internacional, diversos autores já estudam o problema. Ansper, Buldas e Willemson [ANSPER, 2001] propõem, para validação de assinaturas a longo prazo, a utilização de protocolo baseado em cadeias de *hashes*, que prescinde da utilização de notários ou terceiras partes confiáveis para garantir a validade das assinaturas.

Já Gritzalis e Lekkas [GRITZALIS, 2004] questionam o método de cadeia de *hashes*, dada a dificuldade em fazer-se a conferência, num futuro distante, de todas as assinaturas apostas pelas autoridades de carimbo tempo, dado que essas podem nem mais existir, ou não ser mais confiáveis, na época da validação da assinatura. Além disso, citam as dificuldades que podem ocorrer em função das diferentes tecnologias e equipamentos

usados ao longo do tempo, para geração e validação dos carimbos e assinaturas. Sugerem um esquema de Notarização Cumulativa, que, apesar de facilitar a validação das assinaturas, traz implícita a necessidade de que haja confiança nos notários por parte dos usuários da ICP.

Maniatis e Baker [MANIATIS, 2002] propõem, ao invés do uso de notarização, a utilização de mecanismos de carimbo do tempo combinados com um Serviço de Arquivamento de Chaves, que guardaria em repositório seguro as chaves das Autoridades Certificadoras da ICP. Periodicamente, seus arquivos seriam carimbados por uma Autoridade de Carimbo de Tempo, como forma de provar aos usuários a existência dos certificados da AC, em dado instante de tempo. Com isso, entendem que ficaria assegurada a validação dos certificados emitidos, com a preservação da cadeia de certificação. Poderiam também ser arquivados nesse repositório seguro documentos, certificados digitais, trilhas de auditoria e demais arquivos com dados de grande valor.

No âmbito da ICP-Brasil, ainda não existem diretrizes sobre o caminho a adotar, embora já existam milhões de documentos assinados digitalmente. Os bancos brasileiros, por exemplo, utilizam desde 2004, para contratos de câmbio, um formato de assinatura que segue diretriz específica para esse tipo de documento, emanada pelo Banco Central do Brasil [BRASIL, 2004]. Milhares de empresas brasileiras emitem notas fiscais seguindo o padrão de assinatura definido em 2006 pelo ENCAT - Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais [BRASIL, 2009c], já tendo sido produzidas mais de 3 milhões de notas fiscais. O Poder Judiciário brasileiro, por outro lado, vem informatizando o processo judiciário com a utilização de certificação digital, já tendo gerado milhões de documentos com assinaturas digitais ICP-Brasil. Em todos esses casos, a conservação dos documentos assinados deve extrapolar o prazo de validade do certificado digital correspondente.

Somente em dezembro de 2008 foram aprovados regulamentos sobre assinaturas digitais no âmbito da ICP-Brasil, que definem *"as diretrizes técnicas a serem adotadas para que os processos de geração e verificação de assinaturas digitais sejam realizados de forma padronizada e com requisitos de segurança suficientes para garantir, a médio e longo prazos, a recuperação das assinaturas e documentos eletrônicos, bem como a determinação de sua autoria e integridade"* DOC-ICP-15 [BRASIL, 2009a]. Uma

importante lacuna nesses regulamentos é que não definem o tratamento a ser dado aos milhões de documentos assinados antes da sua publicação e que provavelmente se encontram fora do padrão ali definido.

Finalmente, não se observa em nenhum documento da ICP-Brasil orientação sobre como armazenar os documentos assinados digitalmente, tarefa essa bastante complexa. Envolve não apenas as questões relacionadas com o arquivamento de documentos eletrônicos (migração de dados e metadados para novas mídias, sistemas operacionais e sistemas aplicativos; migração de representações e formatos de arquivos etc.) [THOMAZ, 2003], como também questões específicas relacionadas à certificação digital, [LUPOVICI, 2000] como:

a) foram arquivadas, juntamente com o documento eletrônico assinado, todas as informações necessárias para comprovar se os certificados estavam válidos no instante da assinatura?
b) caso negativo, é possível obter essas informações no momento da verificação? de que forma?
c) como proceder em caso de descoberta de fraquezas nos parâmetros criptográficos usados, que ensejem a falsificação de assinaturas digitais?
d) como proceder em caso de expiração ou revogação dos certificados dos usuários e das ACs e ACTs envolvidas?

Além de oferecer resposta todas essas questões, os responsáveis pelo armazenamento dos documentos eletrônicos assinados digitalmente devem preocupar-se em registrar todos os procedimentos realizados, de forma que seja possível provar a integridade do documento ao longo do tempo, para que ele mantenha sua capacidade de servir como evidência legal.

Muitas das pessoas ou entidades brasileiras que hoje estão de posse de documentos eletrônicos assinados digitalmente desconhecem a maneira correta de armazená-los e não há, na ICP-Brasil, definição de processos e estruturas visando à preservação adequada desses documentos no longo prazo.

Outra questão relevante é que, para verificar assinaturas digitais será necessário reconstruir de forma correta o caminho de certificação e obter informações adicionais [LEKKAS, 2007], [ALEMNEH, 2002]; é necessário, portanto, dispor de LCRs, certificados digitais da

AC, da ACT e respectivas PC, DPC, PCT, DPCT etc. Hoje a maior parte desses arquivos encontra-se na guarda das entidades que os geraram, o que pode dificultar sua recuperação a médio e longo prazo, caso não sejam realizados os procedimentos de arquivamento adequados.

Algumas ACs podem ter dificuldade de manter disponíveis até mesmo os dados mais básicos, como os certificados digitais e LCRs emitidos, por utilizarem sistemas de certificação com restrições operacionais e deficiências diversas.

Outro exemplo ocorre com as políticas de certificados (PCs), documentos que definem, entre outras coisas, as aplicações para as quais os certificados definidos pela PC são adequados e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados. Hoje, pela regulamentação da ICP-Brasil, cada AC pode alterar suas PCs quando julgar necessário, desde que submeta à AC-Raiz as novas versões desses documentos antes de publicá-los em seus repositórios. Não existem referências, porém, sobre o que fazer com as versões anteriores, que deveriam ser guardadas permanentemente, de forma segura, para evitar futuras alegações de que uma assinatura digital tenha sido realizada em desacordo com a PC aplicável à época.

Todas essas questões podem dificultar a verificação se certificado digital era válido em determinado momento do passado, o que é especialmente danoso para os casos de certificados usados em carimbos do tempo, que são utilizados, muitas vezes, como forma de garantir a validade das assinaturas digitais [ILIADIS, 2003].

5.2.3 Sistemas para Geração e Verificação das Assinaturas Digitais

Para que documentos assinados digitalmente apresentem as condições técnicas necessárias e suficientes para serem úteis como evidência legal, é preciso que todos os processos relacionados com sua criação e verificação sejam realizados de forma segura. Esses processos envolvem, em maior ou menor grau, a utilização de sistemas e equipamentos criptográficos, que devem ter seu funcionamento avaliado e, de preferência, certificado por um organismo confiável, para garantir aos usuários a segurança de suas chaves privadas.

Uma solução para garantir que os sistemas estejam seguros e adequados à regulamentação brasileira seria submetê-los ao processo de homologação ICP-Brasil, criado em outubro de

2004, com a publicação do DOC-ICP-10 [BRASIL, 2004a], que estabelece as regras e os procedimentos gerais que devem ser observados nos processos de homologação de sistemas e equipamentos para uso na ICP-Brasil. Nesse modelo, os fabricantes não pagam pela homologação, ficando esses custos a cargo do Governo Federal, que contrata Laboratórios de Ensaio e Auditoria (LEAs) para realização das análises. A especificação dos requisitos técnicos que esses sistemas e equipamentos devem atender é realizada pela AC-Raiz e publicada nos Manuais de Condutas Técnicas (MCTs).

Para equipamentos, esse modelo tem obtido relativo sucesso, na medida em que já existem dispositivos homologados e que, obrigatoriamente, a partir de 31.12.2010, todos os equipamentos criptográficos para uso na ICP-Brasil deverão ter sido previamente homologados, conforme DOC-ICP-01.01 [BRASIL, 2009].

A situação é diferente, porém no que tange aos sistemas utilizados para geração e verificação de assinaturas digitais. Percebe-se que muitas aplicações que utilizam certificação digital não estão aptas a lidar de forma adequada com os certificados e as informações de revogação. Mesmo softwares de grandes fabricantes tratam de forma errada os bits configurados nos certificados. É comum, por exemplo, que certificados de sigilo sejam usados para realizar assinaturas. A interpretação e o tratamento das extensões críticas ou não críticas varia de um software para outro. Muitos aplicativos não estão configurados para trabalhar corretamente com campos importantes dos certificados, como aqueles que tratam das restrições de uso aplicáveis.

Um erro que pode acarretar graves conseqüências é a validação incorreta do caminho de certificação. O processo de validação depende de vários fatores, entre os quais a utilização, interpretação e processamento correto de diversos campos dos certificados, como "*basicConstraints*", "*policyConstraints*", "*nameConstraints*", "*authorityKeyIdentifier*", "*subjectKeyIdentifier*", "*keyUsage*". Muitos desenvolvedores desconsideram esses campos em suas aplicações, o que pode gerar vários problemas, até mesmo a aceitação de certificados completamente inválidos.

Na ICP-Brasil vivenciam-se esses problemas não apenas nos sistemas operacionais, navegadores e outros programas de grandes fabricantes, mas também naqueles desenvolvidos especificamente para a realidade brasileira, como softwares de assinatura e

outros aplicativos específicos, como os que tratam de nota fiscal eletrônica, por exemplo. Em todos eles, a não implementação adequada de rotinas para tratamento da certificação digital pode comprometer a segurança e confiabilidade dos processos executados.

No caso específico, o documento que traz as especificações dos sistemas para geração e verificação de assinaturas digitais é o Manual de Condutas Técnicas 4 (MCT-4) [BRASIL, 2007d], cuja versão mais atual foi publicada em 2007, antes, portanto, da publicação do DOC-ICP-15 [BRASIL, 2009a], que regulamenta as assinaturas digitais no âmbito da ICP-Brasil. Além de não estar ajustado à regulamentação atual sobre assinatura digital na ICP-Brasil, o MCT-4 mostra outras deficiências, se comparado, por exemplo, com o padrão utilizado na Comunidade Europeia, constante dos documentos *CWA 14170 Security requirements for signature creation applications* [CEN, 2004] e *CWA 14171 General guidelines for electronic signature verification* [CEN, 2004a]. Entre elas podem ser citadas a inexistência de requisitos para autenticação biométrica do titular para acesso à sua chave privada, a não previsão de assinatura digital em ambientes distribuídos etc.

O principal problema, porém, é que a homologação de sistemas para uso na ICP-Brasil ainda é facultativa e até o momento nenhum sistema foi homologado, segundo o sítio www.iti.gov.br [ITI, 2009c], mesmo passados cinco anos da implantação do processo de homologação.

Entende-se o receio das autoridades da ICP-Brasil em exigir que todos os sistemas e aplicativos sejam homologados, haja vista que o processo pode ser demorado e caro, impactando de forma indesejada o preço e conseqüente utilização de dispositivos homologados. Além disso, uma vez homologado o dispositivo, é difícil que se mantenham estáticos seus componentes, o que pode gerar a necessidade de constante reavaliação pelos laboratórios, com mais custos e delongas. Isso é mais verdadeiro ainda para os softwares, haja vista a dinâmica natural dos sistemas informatizados. Por outro lado, deixando-se a situação como está, expõe-se os usuários a riscos significativos e compromete-se a credibilidade das assinaturas geradas.

5.2.4 Tipo e Aplicabilidade dos Certificados Digitais

Na ICP-Brasil conforme DOC-ICP-04 [BRASIL, 2008d] estão regulamentados apenas dois tipos de certificados para titular final: certificados de sigilo e de assinatura. Esses últimos são usados tanto para assinatura digital, propriamente dita, como para processos de autenticação do titular em servidores e aplicativos. Ocorre que esses servidores podem estar instalados em ambientes que não são controlados pelo titular. Exemplo disso se observa nas organizações que exigem que o funcionário se autentique com certificado digital para acessar suas áreas de trabalho, em computadores controlados por terceiros, como os administradores de sistemas e de redes. Com isso, gera-se um risco ao titular do certificado, pois a mesma chave privada usada para autenticação pode ser usada para assinar documentos de cunho legal e financeiro.

É preciso considerar, ainda, que existem quatro tipos de certificados de assinatura na ICP-Brasil: A1, A2, A3 e A4. As chaves privadas associadas aos certificados do tipo A1 e A2 são geradas e/ou armazenadas em software e as do tipo A3 e A4 são geradas e armazenadas em hardware criptográfico. Mesmo oferecendo níveis de segurança bastante distintos, qualquer desses certificados pode, em tese, ser utilizado para assinar qualquer tipo de documento, ficando essa definição na dependência apenas do gestor do aplicativo. Com isso, os titulares de certificados do tipo A1 e A2 ficam ainda mais expostos ao risco de captura de sua chave privada para utilização em transações as mais diversas.

Outro fator que traz insegurança aos titulares de certificados ICP-Brasil é que a regulamentação atual não lhes permite estabelecer limite de valores para as transações, documentos e contratos a serem assinados com a chave privada associada ao certificado. Na Comunidade Europeia, ao contrário, essa possibilidade está prevista na própria diretiva 93/1999.

Para as pessoas jurídicas, os certificados ICP-Brasil apresentam ainda deficiências importantes, que dificultam sua utilização nos processos de negócios. Uma empresa pode ter vários certificados de assinatura, cada um deles indicando uma pessoa física responsável pela guarda e uso da chave privada correspondente, conforme DOC-ICP-05 [BRASIL, 2008e]. Ocorre que não é possível estabelecer, no certificado digital, segregação

de funções e limitação de poderes para os responsáveis. Assim, cada um deles pode assinar, em nome da empresa, documentos de qualquer tipo e valor. Pior ainda: muitas vezes, por falta de conhecimento dos empresários e por necessidade operacional, as chaves privadas acabam em poder do contador ou de terceiros que prestam serviços para a empresa, como emissão de notas fiscais eletrônicas, expondo ainda mais a empresa ao risco de utilização indevida da chave. Além dos problemas de segurança, isso dificulta a automação dos processos de negócios, em que existem fluxos pré-definidos de atividades, com segregação das partes executantes e os sistemas devem analisar as assinaturas digitais e sua relação com o documento, ou seja, identificar se o documento admite uma assinatura digital de uma pessoa e qual o papel dela no processo.

Vê-se, assim, que os tipos e aplicabilidade dos certificados ICP-Brasil não atendem as atuais necessidades da sociedade e podem ensejar, no futuro, alegações de que algum documento foi assinado sem a expressa vontade e consentimento do titular do certificado ou do responsável legal pela chave privada.

5.2.5 Estrutura para Pesquisa, Normalização e Regulamentação

É grande o esforço que uma ICP demanda em pesquisa, normalização e regulamentação. Trata-se de trabalho complexo, que envolve especialistas de diferentes áreas e necessita de extensas pesquisas, algumas das quais devem ser realizadas em laboratórios especializados.

No cenário internacional, a solução foi criar grupos de trabalho ou comitês permanentes para atender de forma satisfatória à demanda pela elaboração de normas e padrões. Na Europa, por exemplo, CEN e ETSI atuam de forma integrada para produzir com rapidez os padrões necessários para a implantação da assinatura e da fatura digital, contando, nesse processo, com uma estrutura vigorosa e com a colaboração de especialistas de diversos países.

Viu-se que há inúmeros pontos na ICP-Brasil que ainda necessitam ser regulamentados, mas a capacidade de produção desses regulamentos ainda é extremamente limitada em função do contingenciamento de recursos financeiros e humanos. Na AC-Raiz a equipe responsável por essa tarefa é composta de um único técnico e duas auxiliares administrativas. Essa situação concorreu para que regulamentos importantes somente

fossem elaborados muitos anos depois da criação da ICP-Brasil, como foi o caso da regulamentação da estrutura para emissão de carimbos do tempo, aprovada em 2008, e a regulamentação dos formatos de assinatura digital, aprovada em 2009. Mantidas as condições atuais, a elaboração dos regulamentos necessários para complementar a estrutura somente ocorrerá em prazo muito longo.

Outras entidades que poderiam contribuir nesse processo não se mostram interessadas. A ABNT, por exemplo, não possui nenhum Comitê ou Comissão de Estudos Especiais dedicado à criação de padrões sobre documentos eletrônicos e assinatura digital. Tampouco se percebe no Mercosul um esforço maior de regulamentação dos assuntos técnicos atinentes à certificação digital, estando seus esforços voltados à regulamentação de aspectos jurídicos, como é o caso das resoluções elaboradas pelo Grupo de Trabalho 13, que tratam do reconhecimento mútuo de certificados digitais e assinaturas eletrônicas entre os países do bloco [MERCOSUL, 2006].

Com isso, tem-se um importante gargalo para o atendimento das necessidades de regulamentação brasileiras. Os documentos assinados digitalmente, até que se complementem os regulamentos, podem vir a ter sua eficácia como evidência legal contestada.

5.3 CONCLUSÃO

O presente capítulo evidenciou deficiências importantes nos regulamentos atuais da ICP-Brasil, que podem dificultar a criação de documentos assinados digitalmente com as características técnicas adequadas para servir como evidência legal. Estão relacionadas à revogação de certificados, preservação de documentos assinados digitalmente, sistemas para geração e verificação das assinaturas digitais e tipo e aplicabilidade dos certificados digitais ICP-Brasil.

Também mostrou que a estrutura para pesquisa, normalização e regulamentação, atualmente existente na ICP-Brasil, é insuficiente para produzir, rapidamente, as alterações necessárias nesses regulamentos.

6. ADEQUAÇÕES PROPOSTAS PARA A ICP-BRASIL

6.1 INTRODUÇÃO

Foram relacionados no Capítulo 5 os principais desafios a serem equacionados para prover as condições técnicas necessárias para que os documentos eletrônicos assinados digitalmente no âmbito da ICP-Brasil sejam utilizados como evidência legal competente. Neste capítulo propõe-se um conjunto de medidas que podem auxiliar a equacionar tais desafios,

Entendendo que uma abordagem genérica poderia comprometer os resultados esperados do trabalho [VESSEY, 1998], optou-se por propor medidas que se aplicam especificamente à ICP-Brasil e que visam solucionar apenas questões técnicas relacionadas com documentos eletrônicos assinados digitalmente e sua utilização como evidência legal, conforme proposto em [BERTOL, 2009].

6.2 ADEQUAÇÕES PROPOSTAS

6.2.1 Revogação de certificados

6.2.1.1 Implantação Obrigatória de Serviço de Validação Online do *Status* dos Certificados

Para eliminar a situação que se vivencia hoje na ICP-Brasil, com a defasagem das informações de revogação, todas as ACs (exceto a Raiz) devem oferecer obrigatoriamente, um serviço online de validação de *status* de certificados, que pesquise a base de dados de certificados emitidos e forneça uma resposta binária, ou seja:

a) o certificado é válido: consta da lista de certificados emitidos pela AC e não está revogado; ou

b) o certificado não é válido: não consta da lista de certificados emitidos pela AC ou está revogado.

Esse modelo de serviço de verificação online é diferente do que está proposto na RFC 2560 [MYERS, 1999], mas equipara-se ao que vem sendo usado em países da Comunidade Europeia, como a Alemanha, conforme Menke [MENKE, 2008].

Embora obrigue os desenvolvedores de aplicativos a fazer alterações em seus sistemas e as ACs a alterarem seus processos, essa medida, tem vários pontos positivos:

a) elimina os inconvenientes apresentados pelas LCRs e serviço OCSP tradicional, de fornecer informação defasada e/ou incompleta;

b) permite que a certificação digital seja usada de forma mais intensa para processos críticos, como transações financeiras;

c) diminui a carga na rede, por evitar a baixa de LCRs.

Na regulamentação desse novo serviço devem ser igualmente tratados pontos importantes a ele relacionados, como a inclusão, nos certificados de titulares finais, da extensão *AuthorityInfoAccess,* que indica como acessar informações e serviços da AC emitente do certificado, entre eles o serviço OCSP.

A emissão de LCRs pelas ACs, por outro lado, seria facultativa, podendo ser realizada em periodicidade mais longa (por exemplo, a cada mês), apenas para fins de consulta histórica.

Essa medida ensejará alterações no DOC-ICP-04 [BRASIL, 2008d] e DOC-ICP-05 [BRASIL, 2008e], que tratam dos requisitos mínimos a serem observados pelas ACs da ICP-Brasil na criação de suas políticas de certificados e declarações de práticas de certificação.

6.2.1.2 Regulamentação do fornecimento de LCRs antigas

Independentemente da adoção da medida anterior, é necessário que o fornecimento de LCRs antigas seja regulamentado, para permitir a validação das assinaturas digitais realizadas com chaves associadas a certificados já expirados. Esses regulamentos devem definir, pelo menos: como solicitar uma LCR antiga, qual prazo máximo a AC possui para disponibilizá-la, se pode cobrar por esse serviço, quanto pode cobrar etc.

Com essas informações, os usuários poderão traçar suas estratégias para obter os dados de validação. Por exemplo, grandes instituições poderão optar por montar sua própria base de dados de LCRs antigas, para consulta sem custos ou prazos adicionais. Já usuários de menor porte poderão preferir a consulta à AC, quando necessitarem desse tipo de informação.

6.2.2 Preservação de Documentos Assinados Digitalmente

6.2.2.1 Regulamentação do serviço de arquivamento de documentos assinados

Uma medida prioritária para a ICP-Brasil é a regulamentação dos procedimentos a serem adotados para arquivamento de documentos assinados digitalmente, assunto que não é tratado em nenhum dos documentos da ICP-Brasil. Para a criação desses novos regulamentos é importante o envolvimento do Arquivo Nacional, que poderá contribuir na definição das políticas e práticas arquivísticas a serem observadas, considerando ainda as necessidades dos usuários dessas informações no futuro [DOYLE, 2007].

Entre essas práticas, segundo [ANSPER, 2001], [POREKAR, 2009], temos:

a) carimbos do tempo emitidos por Autoridades de Carimbo do Tempo confiáveis;
b) concatenação de valores de *hashes* criptográficos;
c) apresentação de evidências para grupos de documentos digitais;
d) cadeias de carimbos do tempo de arquivamento.

Nessa regulamentação, deve ser prevista a criação de uma nova categoria de entidade: o Prestador de Serviços de Arquivamento (PSA), responsável pela guarda de forma confiável de documentos assinados digitalmente no longo prazo. Os objetivos primários de um PSA são dar suporte ao não-repúdio da existência de dados, integridade e origem [BLAZIC, 2007].

Esse tipo de entidade já existe na Comunidade Europeia, que, premida pela necessidade de arquivar os documentos relativos a faturas eletrônicas assinadas digitalmente, criou em 2007 o padrão ETSI TS 102573 *Policy requirements for trust service providers signing and/or storing data for digital accounting* [ETSI, 2007b].

A utilização dos serviços do PSA seria facultativa: grandes usuários, que tenham milhares de documentos para armazenar, poderiam criar em seu próprio ambiente as condições para isso, desde que atendessem os requisitos para arquivamento definidos. Usuários menores, ou todos aqueles que não desejassem despender recursos com a criação de ambiente próprio, utilizariam os serviços de um PSA.

Pontos relevantes dessa proposta foram apresentados em [BERTOL, 2009a].

6.2.2.2 Criação de Repositório Seguro de Informações Críticas

Foi destacada a importância em guardar informações complementares para validar assinaturas digitais no futuro, como LCRs, certificados digitais de AC e diferentes versões de PC, DPC, PCT, DPCT etc. Hoje essas informações estão armazenadas nas diferentes ACs e ACTs, o que pode dificultar sua recuperação, no futuro.

A proposta é que a AC-Raiz brasileira crie um repositório seguro com essas informações (ou designe um Prestador de Serviços para isso), de forma a garantir sua preservação e disponibilidade adequada.

6.2.2.3 Criação de manuais orientando os usuários sobre o tratamento do legado

Conforme Resolução 62 do CG da ICP-Brasil, de 09.01.2009 [BRASIL, 2009a], a definição dos critérios para validação dos documentos assinados digitalmente usando certificados ICP-Brasil em formatos não padronizados foi deixada a cargo das partes interessadas. Como essa definição pode ser complicada, especialmente para usuários leigos que não disponham de estrutura organizacional para apoiá-los, cabe à AC-Raiz criar um Guia, orientando-os sobre as formas como pode ser realizada a validação e sobre os consequentes procedimentos a que os documentos assinados devem ser submetidos, em cada caso.

6.2.2.4 Inclusão de orientações sobre arquivamento a longo prazo de documentos assinados digitalmente nos termos de titularidade

No momento em que recebe o certificado digital, o titular assina e recebe uma cópia do Termo de Titularidade, documento no qual constam seus dados de identificação e uma relação resumida de seus deveres como titular de um certificado ICP-Brasil. A minuta desse termo está estabelecida em adendo do DOC-ICP-05 [BRASIL, 2008e] e deve ser adotada por todas as ACs credenciadas.

Propõe-se que sejam incluídas nesse documento orientações sobre os procedimentos que o titular deve adotar em relação aos documentos assinados digitalmente, com vistas a manter as características adequadas para utilização como evidência legal, no futuro.

Essa medida vem ao encontro do disposto no Código de Defesa do Consumidor, que garante ao consumidor o direito à informação e estabelece ao fornecedor o dever de informar [PAULA, 2003].

6.2.3 Sistemas para Geração e Verificação das Assinaturas Digitais

6.2.3.1 Regulamentação do Processo de Validação de Certificados e Assinaturas Digitais

A regulamentação do processo de validação de certificados e assinaturas digitais é necessária para evitar a implementação incorreta desse processo nas aplicações, o que pode gerar conseqüências indesejadas, como a aceitação de certificados inválidos ou revogados ou a validação de assinaturas sem as características esperadas.

Nenhum dos documentos da ICP-Brasil trata do assunto, motivo pelo qual deverá ser criado novo conjunto de documentos, incorporando essa proposta.

6.2.3.2 Regulamentação do Serviço de Validação de Certificados e Assinaturas Digitais

Mesmo com a regulamentação do processo de validação de certificados e assinaturas digitais, usuários e desenvolvedores podem preferir delegar essa atividade a entidades especializadas. Propõe-se, por isso, a criação de Prestadores de Serviço de Verificação (PSV), entidades credenciadas na ICP-Brasil para realizar os processos de criação de caminhos de certificação e validação do *status* de certificados. Esses prestadores também poderiam validar até mesmo as assinaturas digitais como um todo, e não apenas o caminho de certificação, simplificando essa atividade para usuários finais e aliviando as aplicações para que possam se concentrar nas atividades-fim a que se destinam.

Essa solução se assemelha à proposta na RFC5055 [FREEMAN, 2007], que define um protocolo que permite a um cliente delegar a um servidor a criação do caminho de certificação e a validação dos certificados.

6.2.3.3 Implantação de Declaração de Conformidade para Sistemas

Viu-se a importância de oferecer aos usuários sistemas para geração e verificação de assinaturas seguros e alinhados com os regulamentos da ICP-Brasil. A garantia de que esses dispositivos atendem a tais características poderia ser obtida pela homologação junto a laboratórios especializados, mas essa alternativa encareceria os produtos e inibiria o lançamento de novas versões.

Para solucionar essa questão, propõe-se estratégia semelhante à adotada na Alemanha [ALEMANHA, 2001], [ALEMANHA, 2001a]: os fabricantes de produtos para assinaturas digitais devem fornecer declaração pública de que seus produtos estão em conformidade com os requisitos de segurança estabelecidos nos regulamentos da ICP-Brasil. Uma cópia escrita deve ser depositada na AC-Raiz, que publicaria no seu sítio a lista desses dispositivos "declarados confiáveis", para conhecimento dos titulares de certificados e terceiras partes.

Com isso, o fabricante assume sua parcela de responsabilidade caso um dispositivo por ele produzido venha a causar prejuízos a terceiros, facilitando assim sua imputação legal e ensejando que seja mais consciencioso com relação aos produtos ofertados.

6.2.4 Tipos e Aplicabilidade dos Certificados Digitais

6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de Atributos

Para solucionar os pontos levantados no item 5.2.4, relacionados com as dificuldades de utilização de certificados digitais por pessoas jurídicas, a recomendação é que seja criada, na ICP-Brasil, uma infraestrutura voltada para emissão de certificados de atributo. Um certificado de atributo é uma estrutura de dados contendo um conjunto de atributos para uma entidade final e alguma outra informação. Essa estrutura é assinada digitalmente por uma entidade confiável. O certificado de atributo não possui chave pública: é utilizado em conjunto com um certificado de chave pública, adicionando atributos ao detentor desse certificado. Assim os atributos constantes no certificado de atributo podem ser alterados ou mesmo revogados sem que isso implique a revogação do certificado de chave pública.

Os certificados de atributos podem ser usados para diversas finalidades, como:

a) identificação de profissionais que pertencem a determinada categoria;
b) identificação e definição de cargos/hierarquias de funcionários e servidores de empresas ou órgãos públicos;
c) identificação de pessoas que fazem jus a determinado direito (ex.: bolsa-família;)
d) restrição de acesso de determinados usuários à aplicações;
e) delegação de poderes (procuração).

Os padrões internacionais que tratam dessa matéria são a RFC 3281 *An Internet Attribute Certificate* [HOUSLEY, 2002], a RFC 4476 *Attribute Certificate Policies Extension* [FRANCIS, 2006] e o documento ETSI TR 102 044 *Electronic Signatures and Infrastructures (ESI); Requirements and role for attribute certificates* [ETSI, 2002].

Neles está prevista a criação de dois tipos de entidades: a autoridade designadora de atributos e a autoridade emissora de atributos. A primeira possui autoridade sobre determinado atributo, podendo designar quem poderá obter um certificado com aquele atributo (por exemplo, um conselho de classe pode designar quais são os profissionais habilitados a exercer a profissão). Já a autoridade emissora realiza a emissão do certificado de atributo, em condições semelhantes às utilizadas para emissão de certificados digitais: ambientes com requisitos elevados para segurança física, lógica e de pessoal etc.

Para a ICP-Brasil, além de definir as entidades que irão compor essa nova infraesturutura, é preciso detalhar suas funções, regras de acreditação e funcionamento, tipos de dispositivos a utilizar, procedimentos a serem observados pelos agentes de registro para validação dos atributos, forma e condições de revogação de atributos etc., o que exigirá a criação de um novo conjunto de documentos.

6.2.4.3 Alteração nos certificados ICP-Brasil

Viu-se que os tipos de certificados atualmente disponíveis na ICP-Brasil não atendem adequadamente às necessidades dos titulares, trazendo mesmo riscos de segurança aos seus usuários.

Propõe-se, assim, a criação de um novo tipo de certificado: o certificado de autenticação, que se destina apenas a permitir ao titular acesso a sistemas diversos, não podendo ser utilizado para assinatura digital de documentos. As chaves criptográficas desse tipo de certificado podem estar armazenadas em software ou em hardware criptográfico, visto que seu uso restrito não ensejará graves prejuízos, em caso de captura por terceiros.

Esse tipo de certificado é usado em países como Portugal [PORTUGAL, 2006] e Bélgica, que incorporam em seus documentos de identidade certificados digitais de assinatura e de autenticação, armazenados em áreas distintas dos cartões inteligentes. Isso permite que o certificado de autenticação seja utilizado em variados ambientes, como serviços médicos, escolas etc (o que propicia às autoridades a obtenção de dados para programas sociais), preservando a segurança da chave privada de assinatura.

Na regulamentação que tratará desse assunto, deve ser prevista ainda a possibilidade de inclusão de limites de valores nos certificados de assinatura, caso o titular assim deseje.

6.2.5 Estrutura para Pesquisa, Normalização e Regulamentação

6.2.5.1 Criação de Organismo de Normalização Independente

Viu-se que grande parte dos regulamentos da ICP-Brasil requer atualização periódica, ao passo que existem diversos assuntos que ainda não foram regulamentados. Mantendo-se as condições atuais, nas quais um único técnico, na AC-Raiz, está encarregado de criar e atualizar todos esses documentos, observa-se um gargalo importante nessa área, que pode comprometer a segurança de toda a infraestrutura.

Assim, entende-se que a ICP-Brasil deve fomentar a criação de uma entidade de normalização independente, seja no âmbito brasileiro, seja no âmbito do Mercosul, capaz de produzir em tempo hábil os padrões necessários. Esse organismo, a exemplo dos existentes em outros países e regiões, contaria com a colaboração de técnicos de órgãos governamentais e empresas privadas, que atuariam em conjunto para elaboração de padrões, que poderiam abranger outros temas, além de certificação e assinatura digital. Tais padrões, depois de avaliados pela AC-Raiz e pelo Comitê-Gestor, poderiam então ser incorporados aos regulamentos da ICP-Brasil.

É importante enfatizar que o ONI proposto não concorrerá com o Comitê Gestor da ICP-Brasil ou com a AC-Raiz na criação de regulamentos, visto que essa é uma atribuição exclusiva daqueles órgãos. O ONI trabalhará na criação de normas, que somente se transformarão em regulamentos se aprovados pelos órgãos competentes.

6.3 INCLUSÃO DAS ADEQUAÇÕES PROPOSTAS NOS REGULAMENTOS

As medidas acima propostas ensejarão grandes modificações no conjunto de documentos ICP-Brasil. Para que para sejam mantidas a unidade e coerência desse conjunto, propõe-se que se observem as seguintes diretrizes:

a) para criação de um novo tipo de entidade:

1. criar documento Visão Geral do serviço a ser prestado pelas entidades;
2. alterar o documento que trata das regras para credenciamento (DOC-ICP-03) [BRASIL, 2008a], para incluir os requisitos legais que devem ser observados pelas entidades;
3. criar documentos contendo os Requisitos Mínimos para as Declarações de Práticas das entidades, definindo os procedimentos gerais e cuidados de segurança a serem adotados para execução dos serviços;
4. criar documentos contendo os Requisitos Mínimos para as Políticas de Serviços das entidades, definindo os diferentes serviços prestados (por exemplo, uma entidade pode emitir diferentes tipos de certificados de atributos, sendo necessária uma Política de Atributos para cada um deles);
5. alterar os documentos da ICP-Brasil que tratam de auditoria (DOC-ICP-08 [BRASIL, 2008b] e de fiscalização (DOC-ICP-09 [BRASIL, 2008c], para incluir as novas entidades.

b) para criação de novos serviços e produtos, ou alterações em serviços e produtos já existentes, oferecidos por entidades já credenciadas:

1. alterar, se necessário, o documento que contém os Requisitos Mínimos para as Declarações de Práticas das entidades que executarão os serviços;
2. criar / alterar documento contendo os Requisitos Mínimos para as Políticas de Serviços das entidades;

c) criação de novos documentos ICP-Brasil que não se enquadrem nas categorias anteriores: analisar caso a caso.

Aplicando essas diretrizes, foram incorporadas as medidas propostas neste capítulo aos regulamentos apresentados na Tabela 2.2. O resultado obtido está expresso na tabela 6.1, onde estão relacionados todos os documentos (já existentes ou novos) com a recomendação que motivou sua modificação ou criação.

Tabela 6.1 – Regulamentos da ICP-Brasil com as adequações propostas

Código / Nome do documento		**Recomendação**
Formato dos certificados digitais e das LCR		
DOC-ICP-04	Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil	6.2.4.3 Alteração nos certificados ICP-Brasil
DOC-ICP-04.01	Atribuição de OID na ICP-Brasil	6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de Atributos
Credenciamento e funcionamento das entidades da ICP-Brasil		
DOC-ICP-01	Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil	6.2.2.2 Criação de Repositório Seguro de Informações Críticas
DOC-ICP-01.01	Padrões e Algoritmos Criptográficos na ICP-Brasil	SEM MODIFICAÇÕES
DOC-ICP-02	Política de Segurança da ICP-Brasil	SEM MODIFICAÇÕES
DOC-ICP-03	Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil	6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de Atributos 6.2.2.1 Regulamentação do serviço de arquivamento de documentos assinados
DOC-ICP-03.01	Características Mínimas de Segurança para as ARs da ICP-Brasil	SEM MODIFICAÇÕES

Código / Nome do documento			Recomendação
DOC-ICP-05	Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil		6.2.1.1 Implantação Obrigatória de Serviço de Validação Online do Status dos Certificados 6.2.1.2 Regulamentação do fornecimento de LCRs antigas
DOC-ICP-05.01	Procedimentos de Identificação de Servidores do Serviço Exterior Brasileiro em Missão Permanente no Exterior		SEM MODIFICAÇÕES
ADE-ICP-05.A	Modelo de Termo de titularidade		6.2.2.4 Inclusão de orientações sobre arquivamento a longo prazo
DOC-ICP-06	Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-07	Diretrizes para Sincronização de Freqüência e do Tempo na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil		SEM MODIFICAÇÕES
Fiscalização e auditoria das entidades credenciadas			
DOC-ICP-08	Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP-Brasil		6.2.2.1 Regulamentação do serviço de arquivamento de documentos assinados 6.2.3.2 Regulamentação do Serviço de Validação de Certificados e Assinaturas Digitais 6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de Atributos
DOC-ICP-09	Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil		6.2.2.1 Regulamentação do serviço de arquivamento de documentos assinados 6.2.3.2 Regulamentação do Serviço de Validação de Certificados e Assinaturas Digitais 6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de

Código / Nome do documento			Recomendação
			Atributos
Processo de homologação de dispositivos criptográficos			
DOC-ICP-10	Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP-Brasil		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas
DOC-ICP-10.01	Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas
DOC-ICP-10.02	Estrutura Normativa Técnica e Níveis de Segurança de Homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas
DOC-ICP-10.03	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (Smart Cards), leitoras de cartões inteligentes e tokens criptográficos no âmbito da ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-10.04	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Softwares de Assinatura Digital, Sigilo e Autenticação no Âmbito da ICP-Brasil		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas
DOC-ICP-10.05	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-10.06	Padrões e Procedimentos técnicos a serem observados nos processos de homologação de Softwares de Bibliotecas Criptográficas e Softwares Provedores de Serviços		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas

Código / Nome do documento			Recomendação
	Criptográficos no Âmbito da ICP-Brasil		
ADE-ICP-10.nn	Modelo de Declaração de Conformidade de Sistema para uso na ICP-Brasil		6.2.3.3 Implantação de Declaração de Conformidade para Sistemas
Carimbo do Tempo			
DOC-ICP-11	Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-12	Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-13	Requisitos Mínimos para as Políticas de Carimbo do Tempo na ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-14	Procedimentos para Auditoria do Tempo na ICP-Brasil		SEM MODIFICAÇÕES
Assinatura Digital			
DOC-ICP-15	Visão Geral Sobre Assinaturas Digitais na ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-15.01	Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP -Brasil		SEM MODIFICAÇÕES
DOC-ICP-15.02	Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-15.03	Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil		SEM MODIFICAÇÕES
DOC-ICP-15.04	Guia para tratamento de documentos assinados digitalmente fora do padrão ICP-Brasil		6.2.2.3 Criação de manuais orientando os usuários sobre o tratamento do legado
Certificados de Atributo			
DOC-ICP-16	Visão Geral Sobre Certificados de Atributos na ICP-Brasil		

Código / Nome do documento			Recomendação
DOC-ICP-17	Requisitos Mínimos para as Declarações de Práticas das Autoridades de Atributos da ICP-Brasil		6.2.4.1 Criação de Infraestrutura para Emissão de Certificados de Atributos
DOC-ICP-18	Requisitos Mínimos para as Políticas de Certificação de Atributos da ICP-Brasil		
DOC-ICP-19	Requisitos Mínimos para as Declarações de Práticas das Autoridades Designadoras de Atributos da ICP-Brasil		
DOC-ICP-20	Requisitos Mínimos para as Declarações de Práticas das Autoridades Designadoras de Atributos da ICP-Brasil		
Serviços de Arquivamento de Documentos			
DOC-ICP-21	Visão Geral Sobre Arquivamento de Longo Prazo na ICP-Brasil		6.2.2.1 Regulamentação do serviço de arquivamento de documentos assinados
DOC-ICP-22	Requisitos Mínimos para as Declarações de Práticas das Autoridades de Arquivamento de Longo Prazo da ICP-Brasil		
DOC-ICP-23	Requisitos Mínimos para as Políticas de Arquivamento da ICP-Brasil		
Orientações aos Desenvolvedores			
DOC-ICP-24	Procedimentos para validação de certificados na ICP-Brasil		6.2.3.1 Regulamentação do Processo de Validação de Certificados e Assinaturas Digitais
Serviços de Verificação de Certificados e Assinaturas Digitais			
DOC-ICP-25	Visão Geral Sobre o Serviço de Verificação de Certificados e Assinaturas Digitais		

Código / Nome do documento			Recomendação
DOC-ICP-26	Requisitos Mínimos para as Declarações de Práticas dos Prestadores de Serviços de Verificação de Certificados e Assinaturas Digitais		6.2.3.2 Regulamentação do Serviço de Validação de Certificados e Assinaturas Digitais
DOC-ICP-27	Requisitos Mínimos para as Políticas de Verificação de Certificados e Assinaturas Digitais		

OBS: A recomendação 6.2.5.1 – Criação de Organismo de Normalização Independente não se reflete nessa tabela, tendo em vista que a proposta é que esse organismo seja constituído como entidade externa à ICP-Brasil.

6.4 INCLUSÃO DAS ADEQUAÇÕES PROPOSTAS NA ESTRUTURA

As medidas propostas ensejarão também modificações na estrutura da ICP-Brasil, estudada no Capítulo 2. A nova configuração, incorporando as alterações, está retratada no Apêndice 2.

6.5 CONCLUSÃO

Neste capítulo são apresentadas propostas de alterações nos regulamentos ICP-Brasil, que compreendem:

a) criação de novas entidades: prestadores de serviços de arquivamento, prestadores de serviços de validação de certificados e assinaturas, autoridades designadoras de atributos, autoridades emissoras de atributos;

b) criação de novos serviços e produtos: validação online do *status* de certificados, fornecimento de LCRs antigas, repositório seguro de informações críticas, certificados de autenticação;

c) alterações nos certificados ICP-Brasil: inclusão de limites de valores nos certificados de assinatura;

d) criação de novos documentos ICP-Brasil: declaração de conformidade para sistemas, manuais orientando sobre o tratamento do legado.

Foi também proposto que a ICP-Brasil fomente a criação de um organismo de normalização independente, nacional ou no âmbito do Mercosul, capaz de produzir de forma rápida padrões e normas que sirvam de subsídios à elaboração dos regulamentos aqui propostos e de outros que se mostrem necessários.

Por fim, sugerem-se diretrizes para realizar as alterações sem perder a coerência e unidade dos documentos ICP-Brasil e aplicam-se essas diretrizes, criando tabela que expressa quais documentos devem ser alterados ou criados, e por qual motivo.

7 CONCLUSÕES

7.1 CONCLUSÕES GERAIS

O desenvolvimento alcançado pela ICP-Brasil levou o País a ocupar um papel de destaque em nível mundial na área de certificação digital, documento eletrônico e assinatura digital. Já forma criados milhões de documentos assinados digitalmente, que *"presumem-se verdadeiros em relação aos signatários*", conforme Medida Provisória 2.200-2 [BRASIL, 2001b], que instituiu a ICP-Brasil,

O objetivo deste trabalho foi estudar a situação atual dos regulamentos da ICP-Brasil para verificar se contemplam os aspectos relevantes para conferir a esses documentos as características técnicas necessárias e suficientes para serem úteis, efetivamente, como evidência legal, mesmo por longo prazo.

Partiu-se da hipótese de que os regulamentos atuais não são suficientes. Para confirmá-la, analisaram-se os padrões internacionais que tratam do assunto e a legislação de outros países e blocos econômicos, em especial a Comunidade Europeia, que possui grande similaridade com o Brasil no que diz respeito à utilização de certificação e assinaturas digitais. Percebe-se, todavia, naquela região, um esforço maior de regulamentação, que passa pela criação de padrões diversos, por organismos independentes, até a implementação desses padrões nas legislações nacionais.

Também utilizou-se, para analisar os regulamentos brasileiros, a experiência obtida em sete anos de trabalho na AC-Raiz da ICP-Brasil, o que permitiu apontar lacunas na legislação que necessitam ser sanadas. A principal delas diz respeito ao armazenamento de documentos assinados digitalmente, que exige a adoção de uma série de procedimentos periódicos, como a revalidação das assinaturas, para preservar a eficácia dos documentos. Esse assunto não é regulamentado em nosso País e muitos usuários desconhecem a necessidade de executar tais procedimentos. Mesmo que soubessem dessa necessidade, muitos não teriam condições de fazê-lo. Por esse motivo, recomenda-se a criação de regulamentos sobre esse assunto e a criação de um novo tipo de entidade na ICP-Brasil, voltada para a prestação de serviços de armazenamento dos documentos assinados digitalmente.

Também foram detectadas lacunas na regulamentação que trata da revogação de certificados, sistemas para geração e verificação das assinaturas digitais, e nos tipos e aplicabilidade dos certificados digitais.

Recomendou-se, para cada uma, medidas que podem contribuir para saná-las. Entre tais medidas estão a criação de novas entidades e de novos serviços na ICP-Brasil, a modificação de serviços já existentes, a alteração dos tipos de certificados utilizados na ICP-Brasil, a criação de manuais e documentos para orientar os usuários e a definição de novo processo para a homologação de sistemas.

Conhecendo a estrutura interna da AC-Raiz, também foi possível apontar a dificuldade em realizar as adequações necessárias com o contingente reduzido de pessoal hoje dedicado à criação de regulamentos para a ICP-Brasil, o que levou à proposta de criação de um organismo de normalização independente, que possa atuar com tempestividade nessa tarefa.

Por fim, foram definidas diretrizes para a incorporação dos novos regulamentos ao conjunto já existente, objetivando manter sua unidade e coerência. Utilizando essas diretrizes, foi elaborada tabela apontando quais documentos devem ser alterados ou criados, e qual a recomendação motivou sua modificação ou criação.

Este trabalho mostra que nossa hipótese é verdadeira, na medida em que aponta diversos assuntos que ainda carecem de regulamentação na ICP-Brasil para que as assinaturas digitais reúnam condições técnicas necessárias e suficientes para servirem como evidência legal competente.

Como contribuição, realizou-se levantamento e análise crítica da regulamentação da ICP-Brasil, levantamento de padrões e regulamentos internacionais (cerca de 10 países) e comparação com o cenário brasileiro, identificação de 5 questões principais que necessitam de ação corretiva e proposição e descrição de 16 ações corretivas.

Com base nas observações realizadas durante a pesquisa bibliográfica, em que se observou como outros países utilizam a certificação digital, entende-se que os trabalhos futuros na área podem compreender:

- detalhamento dos assuntos cuja regulamentação está sendo proposta, com vistas a subsidiar a elaboração dos regulamentos brasileiros;
- análise de lacunas na regulamentação brasileira com relação a outros pontos relevantes, como proteção de dados pessoais;
- utilização da certificação digital em carteira de identificação;
- detalhamento do funcionamento de organismos de normalização independentes.

Percebeu-se ainda a necessidade de contar com um modelo para construção de ICPs, que possa expressar de forma esquemática seus diversos componentes e a maneira como se interrelacionam. Não foi possível encontrar esse tipo de modelo na bibliografia consultada, assim entende-se que a proposição de um modelo para essa finalidade seria um trabalho importante para subsidiar estudos sobre ICPs.

REFERÊNCIAS

ABNT. (1990). Associação Brasileira de Normas Técnicas. *NBR 11515. Critérios de segurança física relativos ao armazenamento de dados*.

ABNT. (2005). Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002. *Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação* (CONTEÚDO TÉCNICO IDÊNTICO AO DA ABNT NBR ISO/IEC 17799/2005).

ABNT. (2008). Associação Brasileira de Normas Técnicas. *Manual da Normalização.* Disponível em: <http://www. http://www.abnt.org.br>. Acesso em: 21 jul. 2008.

ALEKSEJ, B.; TOMA, K.; BORKA, J. (2007). *Long-term trusted preservation service using service interaction protocol and evidence records.* Computer Standards & Interfaces archive, v. 29, e. 3, p. 398-412, Slovenia.

ALEMANHA (2001). German Bundestag. *Law Governing Framework Conditions for Electronic Signatures (Signatures Law - SigG)* (Federal Law Gazette I, p. 876, of 16 May 2001). Disponível em: <http://www.bundesnetzagentur.de/media/archive/3612.pdf>.

ALEMANHA (2001a). German Bundestag. *Ordinance on Electronic Signatures (Signatures Ordinance – SigV).* Novembro 2001. Disponível em: <http://www.bundesnetzagentur.de/media/archive/3613.pdf>.

ALEMNEH, D.; HASTINGS, S.; HARTMAN, C. (2002). *A metadata approach to preservation of digital resources: The University of North Texas Libraries' experience*, First Monday Journal, v. 7, n. 8. Agosto 2002.

ANSPER, A. et al. (2001). *Efficient long-term validation of digital signatures,* in Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), p. 402-415, Korea.

BERTOL, V.; SOUSA, R.; PEOTTA, L. (2009). *Um Modelo Para As Normas Sobre Certificação Digital No Brasil.* VI Conferência Internacional de Perícias em Crimes

Cibernéticos. Natal, Brasil, 2009.

BERTOL, V.; SOUSA, R.; CUSTÓDIO, R. (2009a). *Propostas para apoiar a preservação documental de longo prazo na ICP-Brasil.* V Ibero-American Congress on Information Security *CIBSI'09.* Montevideu, Uruguai, 2009.

BLAZIC, A.; KLOBUCAR, T.; JERMAN, B. (2007). *Long-term trusted preservation service using service interaction protocol and evidence records.* Computer Standards & Interfaces, v. 29, e. 3, p. 398-412. Março 2007.

BLANCHETTE, J. (2006). *The digital signature dilemma - Le dilemme de la signature numérique.* Annales des Télécommunications. Maio/Junho 2006.

BRASIL. (1998). Ministério do Planejamento, Orçamento e Gestão. *Câmara Técnica dos Serviços de Redes.* Disponível em: <http://www.redegoverno.gov.br/projetos/rede.asp>. Acesso em 15.05.2009.

BRASIL. (2000). Poder Executivo. *Decreto n. 3.505*, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>.

BRASIL. (2001). Poder Executivo. *Decreto nº 3.872*, de 18 de Julho de 2001. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/Quadro_2001.htm>.

BRASIL. (2001a). Poder Executivo. *Decreto n. 3.996*, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>

BRASIL. (2001b). Poder Executivo. *Medida Provisória nº 2.200-2*, de 24 de agosto de 2001. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil/mpv/Antigas 2001/2200-2.htm>.

BRASIL. (2002). Poder Executivo. *Decreto Nº 4.414*, de 07 de outubro de 2002. Altera o Decreto Nº 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de

serviços de certificação digital no âmbito da Administração Pública Federal. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4414.htm>

BRASIL. (2003). *Decreto nº 4.689*, de 07 de maio de 2003. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências. Poder Executivo, Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/D4689.htm>.

BRASIL. (2004). Banco Central do Brasil. *Carta Circular 3.134. Procedimentos e padrões técnicos para uso de assinatura digital em contratos de câmbio*. Disponível em: <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=104062827>.

BRASIL. (2004a). Comitê Gestor da ICP-Brasil. *Resolução N° 33, de 21 de outubro de 2004 – Delega à AC Raiz da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências*. Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2005). Poder Executivo. *Decreto Nº 5.420,* de 13 de abril de 2005. Dispõe sobre o remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, altera o Anexo II ao Decreto nº 4.689, de 7 de maio de 2003, o art. 2o e o caput do art. 8o do Anexo I e o Anexo II ao Decreto nº 5.135, de 7 de julho de 2004 e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-006/2005/Decreto/D5420.htm>

BRASIL. (2007). Câmara dos Deputados. *Projeto de Lei 7316/2002. Substitutivo de 25.09.2007*. Brasília, DF. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=369788>.

BRASIL. (2007a). Receita Federal do Brasil. Coordenação de Imprensa**.** *Receita deverá habilitar Instituto para emitir certificado digital*. Disponível em: <https://www.receita.fazenda.gov.br/AutomaticoSRFsinot/2007/06/08/2007_06_08_16_25_26_69279287.htm>. Acesso em: 19 maio 2009.

BRASIL. (2007d). Instituto Nacional de Tecnologia da Informação. *Manual de*

Condutas Técnicas 4 - Volume I - Requisitos, Materiais e Documentos Técnicos para Homologação de Softwares de Assinatura Digital no Âmbito da ICP-Brasil. versão 2.0. São Paulo, 22 de novembro de 2007. Disponível em http://www.iti.gov.br/twiki/pub/Homologacao/Documentos/MCT4_Vol.I.pdf

BRASIL. (2008). Comitê Gestor da ICP-Brasil. *Resolução N° 51, de 28 de Novembro de 2008 – Altera a Política de Segurança da ICP-Brasil (DOC-ICP-02)*. Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008a). Comitê Gestor da ICP-Brasil. *Resolução N° 52, de 28 de Novembro de 2008 – Altera os Critérios e Procedimentos para Credenciamento na ICP-Brasil (DOC-ICP-03)*. Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008b). Comitê Gestor da ICP-Brasil. *Resolução N° 56, de 28 de Novembro de 2008 – Altera os Critérios e Procedimentos para Realização de Auditorias nas Entidades Integrantes da ICP-Brasil (DOC-ICP-08).* Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008c). Comitê Gestor da ICP-Brasil. *Resolução N° 57, de 18 de Abril de 2006 – Altera os Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil (DOC-ICP-09).* Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008d). Comitê Gestor da ICP-Brasil. *Resolução N° 53, de 28 de Novembro de 2008 – Altera os Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (DOC-ICP-04)*. Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008e). Comitê Gestor da ICP-Brasil. *Resolução N° 54, de 28 de Novembro de 2008 – Altera os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil (DOC-ICP-05)*. Infraestrutura de Chaves Públicas Brasileira. Disponível em:

<http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2008f). Poder Executivo. *Decreto Nº 6.605,* de 14 de outubro de 2008. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira -CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-010/2008/Decreto/D6605.htm>

BRASIL. (2008g). Presidência da República. Casa Civil. Secretaria de Controle Interno. Coordenação-Geral de Auditoria. *Relatório de Auditoria 016/2008*. Disponível em <http://www.iti.gov.br/twiki/pub/Main/PrestacaoContasAnuais/0800569.pdf>

BRASIL. (2009). Comitê Gestor da ICP-Brasil. *Padrões e Algoritmos Criptográficos da Infra-Estrutura de Chaves Públicas Brasileira (DOC ICP-01.01)***.** Versão 2.0. Brasília. ICP-BRASIL. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2009a). Comitê Gestor da ICP-Brasil. *Resolução N° 62 de 09 de janeiro de 2009. Aprova a versão 1.0 do documento Visão Geral sobre Assinaturas Digitais na ICP-Brasil (DOC-ICP-15).* Infraestrutura de Chaves Públicas Brasileira. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Legislacao>.

BRASIL. (2009b). Instituto Nacional de Tecnologia da Informação. *Processos de Homologação. Concedidas.* Disponível em: <http://www.iti.gov.br/twiki/bin/view/Homologacao/Concedidas>.

BRASIL. (2009c).Ministério da Fazenda. *Portal Nacional da Nota Fiscal Eletrônica.* Disponível em: <http://www.nfe.fazenda.gov.br/portal/>

CEN (2004). European Committee for Standardization. C*WA 14170 Security requirements for signature creation applications.* Maio 2004. Disponível em <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf>

CEN. (2004a). European Committee for Standardization. *CWA 14171 General guidelines for electronic signature verification.* Maio 2004. Disponível em: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf>

CEN. (2008). European Committee for Standardization. *Standards and drafts.* Disponível em: <http://www.cen.eu/cenorm/standards_drafts/index.asp>

DIAS, J.; CUSTÓDIO, R.; DE ROLT, C. (2003). *Assinatura Confiável de Documentos,* In: Workshop em Segurança de Sistemas Computacionais - WSeg-2003. v.1. p.103 – 112. Natal.

DOYLE, J.; VIKTOR, H.; PAQUET, E. (2007). *Long term digital preservation - An end user's perspective,* Sch. of Inf. Technol. & Eng., Ottawa, Univ., Ottawa, ON - Digital Information Management, 2007. ICDIM '07. 2nd International Conference on, v. 1, p. 146 – 151. Lyon, Outubro 2007.

DUMORTIER, J. et al. (2003). *The Legal and Market Aspects of Electronic Signatures, Study for the European Commission* - DG Information Society. Disponível em: <http://www.secorvo.de/publikationen/electronic-signatures-dumortier-kelm-2004.pdf>

ETSI. (2002). European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates. ETSI TR 102 044.* Dezembro 2002. Disponível em: <http://www.etsi.org/WebSite/Standards/Standard.aspx>.

ETSI. (2007). European Telecomunications Standards Institute. *CMS Advanced Eletronic Signatures (CadES). ETSI TR 102 733.* Disponível em <http://www.etsi.org/WebSite/Standards/Standard.aspx>.

ETSI. (2007b). European Telecommunications Standards Institute. *Policy requirements for trust service providers signing and/or storing data for digital accounting. ETSI TS 102 573.* Disponível em: <http://www.etsi.org/WebSite/Standards/Standard.aspx>.

ETSI. (2008). European Telecommunications Standards Institute. *ETSI Standards.* http://portal.etsi.org/esi/el-sign.asp. Disponível em: <http://www.etsi.org/WebSite/Standards/Standard.aspx>.

ETSI. (2008a). European Telecommunications Standards Institute. *MANDATE 290* .

Standardization mandate addressed to CEN, CENELEC and ETSI in the field of Information Society Standardization. Disponível em: <http://www.etsi.org/website/document/aboutetsi/ec_mandates/m290.pdf>

ETSI. (2008b). European Telecommunications Standards Institute. *ETSI deliverable types.* Disponível em: <http://www.etsi.org/WebSite/Standards/ETSIDeliverables.aspx>

EUA. (2005). Department of Commerce. National Institute of Standards and Technology, Information Technology Laboratory. *FIPS 140-2. Security Requirements for Cryptographic Modules***.** US Government Printing Office. Washington, 2005. Disponível em: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

EUROPA. (1999). Parlamento Europeu. Comissão das Comunidades Europeias. *Diretiva 1999/93/CE de 13 de Dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas.* Jornal Oficial da União Européia. 19 de janeiro de 2000.

EUROPA. (2000). Comissão das Comunidades Europeias. *Decisão 2000/709/CE da Comissão de 6 de Novembro de 2000 sobre os critérios mínimos a ter em conta pelos Estados-Membros ao designarem as entidades previstas no n.o 4 do artigo 3.o da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho relativa a um quadro comunitário para as assinaturas eletrônicas*. Jornal Oficial da União Europeia. 16 de novembro de 2000.

EUROPA. (2001). Conselho da União Europeia. *Diretiva 2001/115/CE do Conselho de 20 de Dezembro de 2001 que altera a Diretiva 77/388/CEE tendo em vista simplificar, modernizar e harmonizar as condições aplicáveis à faturação em matéria de imposto sobre o valor acrescentado.* Jornal Oficial da União Européia. 17 de janeiro de 2002.

EUROPA. (2003). Comissão das Comunidades Europeias. *Decisão 511/2003 sobre a publicação dos números de referência das normas geralmente reconhecidas para produtos de assinatura eletrônica, nos termos da Diretiva 1999/93/CE do Parlamento Europeu e do Conselho*. Jornal Oficial da União Europeia. 14 de julho

de 2003.

EUROPA. (2006). Comissão das Comunidades Europeias. *COM 120/2006 - Relatório sobre o funcionamento da Diretiva 1999/93/CE relativa a um quadro legal comunitário para as assinaturas eletrônicas.* Bruxelas.

EUROPA. (2007). Comissão das Comunidades Europeias. *Decisão 717/2007 da Comissão Europeia, de 31 de Outubro de 2007 que institui um grupo de peritos em faturação eletrônica.* Jornal Oficial da União Europeia. 01 de novembro de 2007.

FERNANDES, A. (2001). *Risking Trust in a public key infrastructure: Old techniques of managing risk applied to new technology.* Decision Support Systems, p. 303-322, v. 31, 2001.

FOKUS. (2006). Fraunhofer Institute. *Study PKI and Certificate Usage in Europe 2006*. Disponível em: <http://www.ecom.jp/report/Study_on_PKI_2006_in_EUROPE-FINAL.pdf>.

FRANÇA. (2004). Secrétariat Général de La Défense National. *Signature Electronique – Point de Situation. Memento. Version 0.94. 25.08.2004.* Disponível em: <http://www.ssi.gouv.fr/site_documents/sigelec/signature-memento-v0.94.pdf>.

FRANCIS, C.; PINKAS, D. (2006). *RFC 4476 - Attribute Certificate (AC) Policies Extension.* Internet Engineering Task Force. Disponível em: <http://www.ietf.org/rfc/rfc4476.txt>.

FREEMAN, T. et al. (2007). *RFC 5055 - Server-Based Certificate Validation Protocol (SCVP).* Internet Engineering Task Force. Disponível em: <http://www.ietf.org/rfc/rfc5055.txt>.

GENGHINI, R. (2005) *PKI Deployment in Europe*. Apresentação. Disponível em: <http://www.etsi.org/WebSite/document/Workshop/Security2007/Security2007S7_1_Output_Report.pdf>

GRITZALIS, D.; LEKKAS, D. (2004). *Cumulative Notarization for Long-term Preservation of Digital Signatures*, Computers & Security, v. 23, e. 5, p. 413-424. Julho 2004.

GUTMAN, P. (2002). *PKI: It's Not Dead, Just Resting.* IEEE Computer. Agosto 2002.

HOUSLEY, R. et al. (1999). *RFC 2459 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.* Internet Engineering Task Force. 1999. Disponível em: <http://www.ietf.org/rfc/rfc2459.txt>.

HOUSLEY, R.; FARRELL, S. (2002). *RFC 3281 - An Internet Attribute Certificate Profile for Authorization.* Internet Engineering Task Force. Disponível em: <http://www.ietf.org/rfc/rfc3281.txt>.

HOUSLEY, R. et al. (2008). *RFC 5280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.* Internet Engineering Task Force. Disponível em: <http://www.ietf.org/rfc/rfc5280.txt>.

IEC. (2008). International Electrotechnical Commission. *About the IEC.* Disponível em <http://www.iec.ch/helpline/sitetree/about>.

IETF. (2008). Internet Engineering Task Force. *Request for Comments. Disponível em:* <http://www.ietf.org/rfc.html>.

IETF. (2008a). Internet Engineering Task Force. *The Internet Standards Process -- Revision 3.* Disponível em: <ftp://ftp.rfc-editor.org/in-notes/bcp/bcp9.txt>

IETF. (2008b). Internet Engineering Task Force. *Public-Key Infrastructure (X.509) (pkix).* Disponível em: <http://www.ietf.org/html.charters/pkix-charter.html>

ITU-T. (2009). International Telecommunication Union. ITU-T Recommendations. Disponível em: < http://www.itu.int/ITU-T/publications/recs.html>

ILIADIS, J. et al. (2003). *Towards a framework for evaluating certificate status information mechanisms.* Computer Communications, p. 1839-1850, v. 26, n. 16. 2003.

ISO (2008). International Organization for Standardization. *About ISO*. Disponível em: <http://www.iso.org/iso/about.htm>

ISO/IEC. (2003). International Organization for Standardization / International

Electrotechnical Commission. *ISO 14721:2003 - Space data and information transfer systems - Open archival information system - Reference model.* Genève, Switzerland. ISO/IEC.

ISO/IEC. (2005). International Organization for Standardization / International Electrotechnical Commission. *ISO 15408:2005 - Common Criteria for Information Technology Security Evaluation.* Genève, Switzerland. ISO/IEC.

ITI. (2008). Instituto Nacional de Tecnologia da Informação. *Estrutura Normativa da ICP-Brasil. Versão 1.5, de 24.10.2008.* Disponível em: <www.iti.gov.br>.

ITI. (2009). Instituto Nacional de Tecnologia da Informação. *Revista Digital*, ano 1, nº. 1. 1º semestre 2009. Disponível em: <http://www.icpbrasil.gov.br/twiki/pub/Certificacao/CartilhasCd/Digital.pdf>

ITI. (2009a). Instituto Nacional de Tecnologia da Informação. *Estrutura da ICP-Brasil. Posição em 18.06.2009*. Disponível em: http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_da_ICP-Brasil_-_site.pdf. Acesso em 20.06.2009

ITI. (2009b). Instituto Nacional de Tecnologia da Informação. *Legislação da ICP-Brasil.* Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao_da_ICP-Brasil_-_site.pdf>

ITI. (2009c). Instituto Nacional de Tecnologia da Informação. *Processos de Homologação. Concedidas.* Disponível em: <http://www.iti.gov.br/twiki/bin/view/Homologacao/Concedidas>

ITU. (1997). International Telecommunication Union. *Recommendation X.509/ISO/IEC 9594-8*: *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. Disponível em: <http://www.itu.int/rec/T-REC-X.509-199708-S/e>.

ITU. (2008). International Telecommunication Union. *About ITU.* Disponível em: <http://www.itu.int/net/about/index.aspx>.

LEKKAS, D. (2003). *Establishing and managing trust within the Public Key*

Infrastructure, Computer Communications, p. 1815-1825, v. 26, n. 16

LEKKAS, D.; GRITZALIS, D. (2007). *Long-term verifiability of the electronic healthcare records' authenticity,* International Journal of Medical Informatics, Volume 76, Issues 5-6, "Virtual Biomedical Universities and E-Learning" and "Secure eHealth: Managing Risk to Patient Data" - E-Learning and Secure eHealth Double S.I., p. 442-448. Maio-Junho 2007.

LUPOVICI, C.; MASANES, J. (2000). *Metadata for long-term preservation*. Biblioteque Nationale de France, NEDLIB Consortium. Diponível em: http://nedlib.kb.nl/results/D4.2/D4.2.htm

LYNCH, M.; McNALLY R.; DALY, P. (1997). *Le tribunal: fragile espace de la preuve*. La Recherche, 300, p. 112-115.

MANIATIS, P.; BAKER, M. (2002). *Enabling the Archival Storage of Signed Documents*, in Proc. of the FAST 2002 Conference on File and Storage Technologies, p. 31-45. USA.

MARTINI, R. (2008). *Tecnologia e Cidadania Digital*. S. Paulo. BRASPORT.

MCINTOSH, M.; AUSTEL P. (2005). *XML Signature Element Wrapping Attacks and Counterneasures* - Proceedings of the 2005 workshop on Secure web services SWS '05. ACM Press.

MENKE, F. (2008). *Die elektronische Signatur im deutschen und brasilianischen Recht: Eine rechtsvergleichende Studie* (A assinatura eletrônica no direito alemão e brasileiro - um estudo comparado). Defendida perante a Universidade de Kassel, dezembro de 2008, pendente de publicação.

MERCOSUL. (2006). *RES. Nº 34/06 - Diretivas para a celebração de acordos de reconhecimento mútuo de assinaturas eletrônicas avançadas no âmbito do Mercosul*. Disponível em: <www.mercosur.int/msweb/SM/Normas/Resoluciones/PT/2006/GMC_2006_RES_034_PT_Directrices.pdf. >.

MYERS, M. et al. (1999). *RFC 2560 - X.509 Internet Public Key Infrastructure Online*

Certificate Status Protocol – OCSP. Internet Engineering Task Force. Disponível em: <http://www.ietf.org/rfc/rfc2560.txt>.

OASIS. (2003). Organization for the Advancement of Structured Information Standards. *Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage.* Disponível em: <http://www.oasisopen.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf>

PAULA, M.; WACKERHAGEN, C. (2003). *A desobrigação do cumprimento do contrato de consumo por ofensa ao direito de informação*. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=4036>.

POREKAR, J. et al. (2009). *Patterns for Long Term Trusted Archiving*. Digital Society, 2009. ICDS '09. Third International Conference on, p. 241 – 246. Cancun, Mexico, Fevereiro 2009.

PORTUGAL. (2006). Serviço de Certificação Eletrônica do Estado. *Política de Certificados da SCEE e Requisitos Mínimos de Segurança*. Disponível em: <http://www.scee.gov.pt>.

STAPLETON, J.; DOYLE, P.; ESQUIRE, S. (2005). *The digital signature paradox,* Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, p. 456 – 457.

THOMAZ, K. (2003). *I Congresso de Tecnologias para Gestão de Dados e Metadados do Cone Sul*. Disponível em: <http://conged.deinfo.uepg.br >.

VESSEY, I.; GLASS, R. (1998). *Strong vs. Weak Approaches to Systems Developmen*t, Communications of the ACM, v.41, n. 4, p.99.

APÊNDICES

1 - ICP-BRASIL – ESTRUTURA HIERÁRQUICA – SITUAÇÃO ATUAL

2 - ICP-BRASIL – ESTRUTURA HIERÁRQUICA – SITUAÇÃO PROPOSTA