Ministério da Justiça

Termo de Cooperação/Projeto:

**Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto**

Documento:

# RT Diagnóstico da Situação Atual da Certificação Digital no Brasil

Data de Emissão:

**01/09/2015**

Elaborado por:

**Universidade de Brasília – UnB**
**Centro de Apoio ao Desenvolvimento Tecnológico – CDT**
**Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB**

**MINISTÉRIO DA JUSTIÇA**

**José Eduardo Cardozo**
Ministro

**Marivaldo de Castro Pereira**
Secretário Executivo

**Helvio Pereira Peixoto**
Coordenador Suplente do Comitê Gestor do SINRIC

EQUIPE TÉCNICA

**Ana Maria da Consolação Gomes Lindgren**
**Andréa Benoliel de Lima**
**Celso Pereira Salgado**
**Delluiz Simões de Brito**
**Elaine Fabiano Tocantins**
**Fernando Saliba**
**Fernando Teodoro Filho**
**Guilherme Braz Carneiro**
**Joaquim de Oliveira Machado**
**José Alberto Sousa Torres**
**Marcelo Martins Villar**
**Raphael Fernandes de Magalhães Pimenta**
**Rodrigo Borges Nogueira**
**Rodrigo Gurgel Fernandes Távora**
**Sara Lais Rahal Lenharo**

**UNIVERSIDADE DE BRASÍLIA**

**Ivan Marques Toledo Camargo**
Reitor

**Paulo Anselmo Ziani Suarez**
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

**Rafael Timóteo de Sousa Júnior**
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA

**Flávio Elias Gomes de Deus (Pesquisador Sênior)**
**William Ferreira Giozza (Pesquisador Sênior)**
**Ademir Agustinho de Rezende Lourenço**
**Adriana Nunes Pinheiro**
**Alysson Fernandes de Chantal**
**Andréia Campos Santana**
**Antônio Claudio Pimenta Ribeiro**
**Carolinne Januária de Souza Martins**
**Daniela Carina Pena Pascual**
**Danielle Ramos da Silva**
**Diogenes Ferreira Reis Fustinoni**
**Fábio Lúcio Lopes Mendonça**
**Fábio Mesquita Buiati**
**Glaidson Menegazzo Verzeletti**
**Heverson Soares de Brito**
**Johnatan Santos de Oliveira**
**Kelly Santos de Oliveira Bezerra**
**Luciano Pereira dos Anjos**
**Luciene Pereira de Cerqueira Kaipper**
**Luiz Antônio de Souto Evaristo**
**Luiz Claudio Ferreira**
**Marco Schaffer**
**Marcos Vinicius Vieira da Silva**
**Pedro Augusto Oliveira de Paula**
**Roberto Mariano de Oliveira Soares**
**Sergio Luiz Teixeira Camargo**
**Soleni Guimarães Alves**
**Suzane Lais De Freitas**
**Valério Aymoré Martins**
**Vera Lopes de Assis**
**Wladimir Rodrigues da Fonseca**

# HISTÓRICO DE REVISÕES

| Data | Versão | Descrição |
|---|---|---|
| 07/10/2013 | 0.1 | Versão inicial. |
| 22/10/2013 | 0.2 | Revisão de texto e forma. |
| 30/10/2013 | 0.3 | Alteração do documento e inclusão dos conceitos sobre criptografia. |
| 04/11/2013 | 0.4 | Revisão do texto. |
| 09/12/2013 | 0.5 | Alteração do documento, inclusão dos tipos de certificados. |
| 22/12/2013 | 0.6 | Alteração do documento, revisão dos tipos de certificados. |
| 06/01/2014 | 0.7 | Alteração do documento e inclusão dos serviços. |
| 14/01/2014 | 0.8 | Revisão do texto. |
| 26/01/2014 | 0.9 | Alteração do documento e revisão dos serviços. |
| 29/03/2014 | 1.0 | Revisão do documento. |
| 29/04/2014 | 1.1 | Reestruturação do relatório. |
| 20/05/2014 | 1.2 | Reestruturação do relatório. |
| 08.06.2014 | 1.3 | Revisão do documento. |
| 06.07.2014 | 1.4 | Revisão do documento. |
| 08.08.2014 | 1.5 | Introdução do Sumário Executivo. |
| 09.09.2014 | 1.6 | Atributos dos formatos da assinatura digital ICP-Brasil. |
| 10.07.2015 | 1.7 | Reestruturação do relatório. |
| 01.09.2015 | 1.8 | Revisão do documento |

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

# SUMÁRIO

# 1. GLOSSÁRIO

**Acesso:** é o estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações para a transferência de dados e a ativação de processos computacionais.

**Algoritmo:** é uma série de etapas necessárias para completar uma tarefa, procedimento ou fórmula na solução de um problema.

**Algoritmo Assimétrico:** é um algoritmo de criptografia que combina uma chave pública (de conhecimento público) e outra privada (sigilosa) necessárias à realização de muitas operações, incluindo criptografia e assinaturas digitais.

**Algoritmo Criptográfico:** processo matemático especificamente definido para cifrar e decifrar mensagens e informações, normalmente com a utilização de chaves.

**Assinatura digital:** é a transformação matemática de uma mensagem por meio da utilização de uma função matemática e da criptografia assimétrica do resultado desta com a chave privada da entidade assinante.

**Assinatura eletrônica:** é o resultado de um processamento eletrônico de dados que permite comprovar a autoria e integridade de um documento eletrônico.

**Atributo**: é uma propriedade do usuário distinta, mensurável, física ou abstrata.

**Autenticação:** é o processo que confirma a identidade de uma pessoa ou entidade, ou para garantir a fonte de uma mensagem.

**Autenticidade da origem:** garante a identidade de quem está enviando a mensagem.

**Autoridade Certificadora (AC):** entidade que emite certificados digitais.

**Autoridade de Registro (AR):** é uma entidade ligada diretamente a uma AC, de forma física ou remota, sendo seu braço operacional. É responsável pelo recebimento, validação e encaminhamento de solicitações de emissão ou revogação de certificados digitais.

**Autorização:** é a obtenção de direitos, incluindo a habilidade de acessar uma informação especial ou recurso de maneira específica.

**Biometria:** é a ciência que utiliza propriedades físicas e biológicas únicas e exclusivas para identificar indivíduos, gerando assim, identificações biométricas, tais como impressões digitais, escaneamento de retina e reconhecimento de voz.

**Certificado Digital**: um documento eletrônico que é emitido por uma autoridade de

certificado (CA) e contém o nome do usuário, a data de expiração, uma cópia da chave pública do usuário, e a assinatura digital pela emissora do certificado, tal que o receptor possa verificar se o certificado é válido. O certificado digital liga a verificação da assinatura a uma pessoa, confirmando sua identidade.

**Chave Criptográfica:** espécie de codificação ou valor numérico usado com um algoritmo criptográfico para transformar, validar, autenticar, cifrar e decifrar dados.

**Chave privada:** é a chave de propriedade e uso do usuário, correlacionada a uma chave pública. Juntas, compõem o par de chaves criptografadas do certificado digital. É mantida em segredo pelo seu dono e usada no sentido de criar assinaturas para cifrar e decifrar mensagens com a sua chave pública correspondente.

**Chave pública:** é uma das chaves criptografadas que compõe o certificado digital. É amplamente divulgada e usada para verificar a assinatura digital criada com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens.

**Cifração:** é o processo que transforma uma mensagem ou um texto original em um conjunto de caracteres incompreensível aplicando algoritmos criptográficos apropriados.

**Cifrar:** é o processo que transforma dados ou informação em uma forma ininteligível usando um algoritmo criptográfico e uma chave criptográfica.

**Controle de acesso:** é a garantia de que o conteúdo da mensagem somente será acessado por pessoas autorizadas.

**Credencial**: é uma informação criada pelo usuário com o objetivo de atestar a integridade e autenticidade dos atributos do usuário.

**Decifrar:** é o processo que transforma dados previamente cifrados e ininteligíveis de volta à sua forma legível**.**

**Declaração de Práticas de Certificação (DPC):** é o documento que contém as práticas e atividades que uma AC implementa para emitir certificados digitais. É a declaração da entidade certificadora a respeito dos detalhes de seu sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

**Disponibilidade:** é a garantia que uma informação estará disponível para acesso no momento desejado.

**Documento Digital:** é uma unidade de registro de informações codificada por meio de dígitos binários.

**Documento eletrônico:** é uma unidade de registro de informações acessível por meio de um equipamento eletrônico.

**eID**: é qualquer *hardware* ou *software*, ou combinação destes, que contenha credenciais geradas para uma entidade específica para provar sua identidade, podendo possuir várias formas como dados contidos em um *smart card* ou em um telefone móvel.

**Emissor**: entidade que valida um ou mais atributos do usuário por meio da emissão de uma credencial para o usuário.

**Função Resumo:** é transformação matemática de uma sequência de bits (mensagem) de tamanho arbitrário para uma sequência de bits de tamanho fixo menor, gerando como resultado um resumo criptográfico ou *hash.*

***Hash:*** é o resultado da aplicação de algoritmos sobre uma sequência de bits (mensagem) de tamanho arbitrário. É muito difícil encontrar o mesmo *hash* para duas mensagens.

**Identificação**: é um processo que fornece evidência (ex.: credenciais, documentos), dentro de um nível de segurança, para uma autoridade de identidade, e valida essa informação de forma que a entidade seja reconhecida dentro de certo contexto como uma referência única ou que a caracterize através de uma informação adicional.

**Infraestrutura de chave pública** (*Public Key Infrastructure* - PKI): um conjunto de sistemas para gerenciamento de pares de chaves privadas e públicas, que usuários e sistemas possam usar para autenticar, assinar documentos e enviar mensagens privadas entre si. É um tipo de “infraestrutura de confiança”. Em uma PKI, a autoridade certificadora possui a confiança de um ou mais usuários para criar e assinar certificados de chave pública.

**Integridade:** é a garantia de que o conteúdo da mensagem não foi alterado durante sua transmissão do remetente para o destinatário.

**Irretratabilidade e não repúdio:** é a garantia de que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gera gerar.

**Irretratabilidade:** mecanismo para garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.

**Mídia armazenadora:** base física (*hardware*) ou lógica (*software*) utilizada para registrar

informações e/ou exportá-las para outras mídias.

**Número de série do certificado:** valor que identifica de forma unívoca um certificado emitido por uma Autoridade Certificadora.

**Número primo:** característica dos números utilizados nas operações dos algoritmos assimétricos. Um inteiro p > 1 é primo se e só se p é divisível apenas por 1 e por p. O conjunto C dos primos é infinito (SOUZA, 2006).

**Política de certificação (PC):** documento que descreve os requisitos, procedimentos e nível de segurança adotados para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital.

**Privacidade:** é o impedimento de pessoas não autorizadas ao acesso do conteúdo da mensagem, garantindo que apenas a origem e o destino tenham o conhecimento dela.

**Provedor de serviço**: papel assumido por uma entidade do sistema, que provê serviços ao usuário, usualmente consiste em uma aplicação ou serviço *web*.

**Rastreabilidade:** relacionamento do resultado de uma medição de sincronismo com um valor de referência previamente estabelecido como padrão. A rastreabilidade se evidencia por intermédio de uma sequência contínua de medidas, devidamente registradas e armazenadas e permite a verificação, direta ou indireta, do relacionamento entre o tempo informado e a fonte confiável de tempo.

**Sigilo:** é a condição na qual os dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas.

***Smart Card***: consiste em um cartão portátil contendo circuito integrado (ICC), podendo prover identificação, autenticação, armazenamento e processamento de aplicações.

**Terceira parte:** parte que age confiante no teor, validade e aplicabilidade do certificado digital emitido por uma autoridade certificadora. Também se configura como pessoa ou instituição que age com total independência de fabricantes, desenvolvedores, representantes comerciais, prestadores de serviços de certificação digital e de potenciais compradores de sistemas e equipamentos de certificação digital.

**Vulnerabilidade:** é a fragilidade de uma máquina, programa ou sistema que pode ser explorada por um agressor com o objetivo de ter acesso ao sistema.

# 2. SUMÁRIO EXECUTIVO

O Registro de Identidade Civil (RIC) foi concebido com alguns valores, tais como: ser um instrumento de inclusão social e de garantia de direitos; ser confiável, seguro e prático para a sua utilização; ser transparente no uso e proteger os dados pessoais; universalizar o acesso à identificação civil; e ter eficiência e excelência na implementação, execução e gestão do projeto. Tomando por base os valores que dizem a respeito da confiabilidade, segurança, praticidade, transparência e proteção dos dados pessoais e contextualizando o cenário atual de imersão no mundo digital, é natural prever a aplicação da tecnologia de certificação digital para fins de autenticação segura do registro civil, razão pelo qual se faz necessário a elaboração do presente estudo do diagnóstico da certificação digital no Brasil.

O presente relatório inicia-se abordando o estudo da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), visando permitir uma melhor compreensão de como a certificação digital é estruturada no Brasil. Nesse tópico são abordadas as instituições que compõem a ICP-Brasil e suas respectivas responsabilidades. A instituição principal desta cadeia é a Autoridade Certificadora Raiz (AC-Raiz), cujo exercício é feito pelo Instituto Nacional da Tecnologia da Informação (ITI) (ITI, 2015). As demais instituições são as Autoridades Certificadoras (AC) de primeiro e segundo nível, as Autoridades de Registro (AR), os Prestadores de Serviço de Suporte (PSS), as Empresas de Auditoria Independente (EAI), os Laboratórios de Ensaio e Auditoria (LEA) e as Autoridades de Carimbo de Tempo (ACT) (Bertol, 2009).

O relatório avança com o estudo das normas técnicas a respeito da certificação digital, avaliando nesse quesito as normas estabelecidas pelo ITI. Este instituto estabeleceu 10 tipos de certificados digitais, sendo 6 relacionados com a assinatura digital (tipos A1, A2, A3, A4, T3 e T4) e 4 com sigilo (S1, S2, S3 e S4) (ITI, 2014). Os tipos de certificados A1 e S1 estão associados aos requisitos menos rigorosos, tendo um tempo de validade menor, enquanto os tipos A4 e S4 aos requisitos mais rigorosos, e, consequentemente, tem tempo de validade maior. É importante ressaltar que os certificados de assinatura no âmbito do ICP-Brasil acumulam a função de assinatura de documentos e autenticação em sistemas, o que não é interessante uma vez que o titular do certificado pode se equivocar e assinar um documento pensando se tratar de um processo de autenticação. Além disso, estudos mostram que um certificado A3 ICP-Brasil tem um custo mínimo avaliado de R$ 185,00

para pessoa física, o que o torna inviável para o RIC. Para o RIC é recomendável o uso de um certificado gratuito com função exclusiva de autenticação, tal como proposto em (Bertol, 2009) e, opcionalmente, um certificado para fins de assinatura pago pelo titular, se este o desejar.

Todos os certificados emitidos no âmbito da ICP-Brasil devem estar em conformidade com o formato definido pelo padrão ITU X.509 (ISO/IEC 9594-8) (ITI, 2014). O padrão ITU X.509 prevê a utilização de pseudônimos nos certificados para reduzir o comprometimento da privacidade do titular, o que seria interessante para a adoção de dois certificados com função de autenticação (o primeiro com identificação do titular e o segundo com pseudônimo) e, ainda, outro certificado com função de assinatura com a identificação do titular, uma vez que o certificado com pseudônimo pode agregar o anonimato com o objetivo de proteger os dados pessoais do titular do certificado. No entanto, o uso de pseudônimos não é previsto na normatização da ITI, o que vai em direção contrária, já que DOC-ICP-04 determina que o nome do titular do certificado deve constar no campo "*Subject*" (ITI, 2014).

Os algoritmos de criptografia assimétrica permitidos pelo ITI são o RSA e o ECC-*Brainpool* (conforme RFC 5639), com tamanhos de chave de 2048 bits e 4096 bits para o RSA, e 256 bits e 512 bits para o ECC-*Brainpool* (ITI, 2014). Os algoritmos de *hash* definidos para utilização nos certificados da ICP-Brasil são o SHA-256 e SHA-512 (ITI, 2014). Os algoritmos de criptografia simétrica previstos pelo ITI para a guarda da chave privada da entidade titular e *backup* são o 3-DES com 112 bits e o AES com 128 ou 256 bits (ITI, 2014). Todos os algoritmos mencionados são utilizados no âmbito da ICP-Brasil nos processos que envolvem os certificados digitais, como a criação/verificação de assinaturas digitais. Dos algoritmos citados destaca-se o ECC-*Brainpool*, uma vez que com uma chave criptográfica ECC de tamanho relativamente pequeno é possível ter o mesmo padrão de segurança que uma chave de maior tamanho do algoritmo RSA. Por exemplo, utilizando o ECC-*Brainpool* com uma chave de 512 bits o padrão de segurança é equivalente ao uso de RSA com uma chave de 15360 bits (Gupta, Gupta, & Chang, 2002). Algumas implicações quanto ao tamanho menor da chave ECC são listadas: uma chave menor leva a uma redução da memória necessária para armazenamento da chave pública no certificado digital, o que é recomendável para o armazenamento deste num documento de registro civil; o menor tamanho implica também uma menor exigência de processamento criptográfico e menor tempo de geração de chaves em comparação ao RSA (Rankal &

Effing, 2003), característica adequada para uso em *smart cards;* como o nível de segurança com uma chave ECC é alto, o tempo de validade do certificado pode ser maior, o que é visto na regulamentação da ITI, a qual considera que um certificado digital com chave ECC de 512 bits tem validade de 11 anos (ITI, 2014). Embora recomenda-se o uso de ECC para o RIC, um estudo aprofundado deve ser realizado para avaliar o tamanho de chave ECC com vista à adequação de certificados ICP-Brasil aos requisitos ICAO.

O ITI define os formatos, padrões, perfis e políticas de assinatura digital no âmbito da ICP-Brasil. Admite-se cinco formatos de assinatura digital na ICP-Brasil, listados a seguir: Assinatura Digital com Referência Básica (AD-RB), Assinatura Digital com Referência de Tempo (AD-RT), Assinatura Digital com Referências para Validação (AD-RV), Assinatura Digital com Referências Completas (AD-RC) e Assinatura Digital com Referências para Arquivamento (AD-RA) (ITI, 2012). O formato AD-RB é o formato de assinatura mais simples e básico, enquanto o AD-RA é um formato bastante completo, com carimbo de tempo que pode ser realizado periodicamente, para fins de armazenamento de longo prazo. Na ICP-Brasil (ITI, 2012) permite-se o uso de dois padrões para representação de assinaturas digitais: CAdES (CMS *Advanced Electronic Signature*) (ETSI, 2008) e XAdES (XML-*Dsig Advanced Electronic Signature*) (ETSI, 2004). Ambos padrões são equivalentes e tem por finalidade a padronização de formatos de assinaturas, os quais incluem formatos para assinaturas de longo prazo. Apesar da equivalência, o padrão XAdES carrega as vantagens da linguagem XML, como a possibilidade de criação de *tags* de modo arbitrário, e também pode assinar partes de um documento, o que não é possível no padrão CAdES. Os padrões CAdES e XAdES disponibilizam uma diversificada gama de atributos ou propriedades que permitem incorporar às assinaturas digitais informações com os mais diferentes objetivos, havendo assim a necessidade de definir um subconjunto desses atributos ou propriedades para maximizar a interoperabilidade das assinaturas digitais. Essa seleção de opções é chamada de perfil. Para a ICP-Brasil foi definido um perfil de assinatura para uso geral, baseado em ambos padrões, que sintetiza os principais atributos e propriedades a serem utilizados nas assinaturas digitais (ITI, 2012), permitindo-se ainda a criação de outros perfis para uso em segmentos específicos de atividade. O ITI também orienta quanto ao formato e a estrutura usada para a criação de uma política de assinatura, bem como define 10 políticas de assinatura padrão para facilitar o seu uso a usuários finais (ITI, 2012). Política de assinatura trata-se do conjunto de regras que formaliza os processos

de criação e verificação de uma assinatura digital e define as bases para que a assinatura digital possa ser considerada válida (ITI, 2012). Os detalhes do processo de criação e verificação de uma assinatura digital no âmbito do ICP-Brasil estão relacionados em (ITI, 2012).

Para um melhor cumprimento do escopo do estudo, procurou-se fazer um levantamento das regras de negócio que envolvem a certificação digital. Para o uso de certificação digital no RIC é necessário um debate junto ao ITI e ao Comitê da ICP-Brasil sobre a interpretação da obrigatoriedade de uso da ICP-Brasil para serviços de certificação digital no RIC, pois se por um lado a Medida Provisória N° 2.200-2 (Brasil, Medida Provisória N 2.200-2, 2001) indica que não seria necessário usar uma AC integrante da ICP-Brasil, por outro lado, o Decreto N° 3.996 (Brasil, DECRETO Nº 3.996, 2001) sinaliza que a questão não é tão simples. Adicionalmente deve-se levar em conta que os documentos eletrônicos produzidos com os certificados digitais do âmbito da ICP-Brasil são presumidos verdadeiros (Brasil, Medida Provisória N 2.200-2, 2001) e são considerados documentos públicos (Guelfi, 2007), uma vez que são oriundos de Pessoa Jurídica de Direito Público. Em termos de custo de implantação de uma AC de 1º nível, a Administração Direta da União é dispensada do pagamento das tarifas de emissão de certificado e auditoria pré-operacional pela AC-Raiz da ICP-Brasil (ITI, 2008), de forma que o custo se restringe à aquisição de equipamentos e serviços necessários para implantar uma AC e na apólice de contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro. O processo de credenciamento de uma AC na ICP-Brasil implica no atendimento de alguns critérios pelo candidato (ITI, 2014), tais como: ser órgão ou entidade de direito público ou pessoa jurídica de direito privado, atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica, ter instalações operacionais e recursos de segurança física e lógica ou contratar PSS que as possua, etc.

Apresenta-se também as ACs Públicas que poderiam ser parceiras do projeto RIC, analisando os certificados atuais emitidos, a criptografia assimétrica, as aplicações. Observou-se que praticamente todas as ACs utilizam a criptografia assimétrica RSA e emitem certificados para fins de autenticação/assinatura e algumas para sigilo de dados. Destaca-se a Autoridade Certificadora do Ministério das Relações Exteriores (AC-MRE), credenciada recentemente junto à ICP-Brasil, a qual utilizará em seus certificados digitais a criptografia de curvas elípticas (ECC-*Brainpool*) para a emissão de passaportes, opção

bastante interessante para utilizar no RIC, conforme já mencionado anteriormente.

O relatório avança com a compilação dos processos de certificação ao redor do mundo. Nesse estudo é visto que é comum o emprego de métodos de autenticação baseados em certificados digitais emitidos dentro de uma ICP em eID's de vários países. O padrão de certificado mais comumente adotado é o XAdES, em função das vantagens já mencionadas. O algoritmo criptográfico assimétrico empregado nos certificados digitais varia de acordo com o país em questão, sendo o RSA o algoritmo de uso mais comum com chaves que variam de 1024 a 2048 bits. Entretanto, existem países que adotam criptossistemas baseados em curvas elípticas como a Áustria, a Alemanha e a Estônia (nesse último país o ECC é suportado, mas não ativado).

O relatório é concluído reforçando as recomendações acima mencionadas para a adoção no RIC e adicionando algumas observações, tais como: a adoção de certificados digitais com fins exclusivos de autenticação nos registros de identificação civil segue a tendência vista em outros países ao redor do mundo; o uso de criptossistemas baseados em curvas elípticas provê maior eficiência, tem chaves menores e grau de segurança elevado, o que o torna adequado para o uso em *smart cards*; o uso da ICP-Brasil para a emissão de certificados traz algumas vantagens, como a presunção de veracidade dos documentos assinados, além de usar padrões já adotados em outros países, como o padrão XAdES para as assinaturas digitais, a previsão de uma cadeia de certificados com ECC-*Brainpoo*l permitindo certificados com longa duração, porém o uso da ICP-Brasil carece de algumas adequações nas normas para permitir o certificado para fins de autenticação, o uso do certificado ICAO para outras aplicações e também o uso de pseudônimos.

# 3. ICP-BRASIL e o Instituto Nacional de Tecnologia

A Medida Provisória 2.200/2001, de 24 de agosto de 2001, instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Brasil, Medida Provisória N 2.200-2, 2001). A ICP-Brasil configura-se como uma cadeia hierárquica e de confiança para viabilizar a emissão de certificados digitais, operando por meio do modelo de certificação com raiz única (ITI, 2015). Cabe à ICP-Brasil garantir autenticidade, integridade e validade jurídica de documentos eletrônicos (que utilizam certificados digitais) e a realização de transações eletrônicas seguras (Brasil, Medida Provisória N 2.200-2, 2001). A ICP-Brasil é mantida e auditada pelo Instituto Nacional de Tecnologia da Informação (ITI), entidade líder da cadeia de certificação digital da ICP-Brasil e também a primeira autoridade certificadora de toda a cadeia de certificação da ICP-Brasil – a autoridade certificadora raiz (AC raiz) (ITI, 2015).

## 3.1 Infraestrutura do ICP-Brasil

A ICP-Brasil é composta por um conjunto de instituições com responsabilidades distintas que operam conforme as resoluções do Comitê Gestor, instruções normativas e outros documentos emitidos pela AC-Raiz. Para melhor compreensão do funcionamento e das entidades que a compõem é apresentado na figura 1 um modelo resumido de sua estrutura hierárquica:

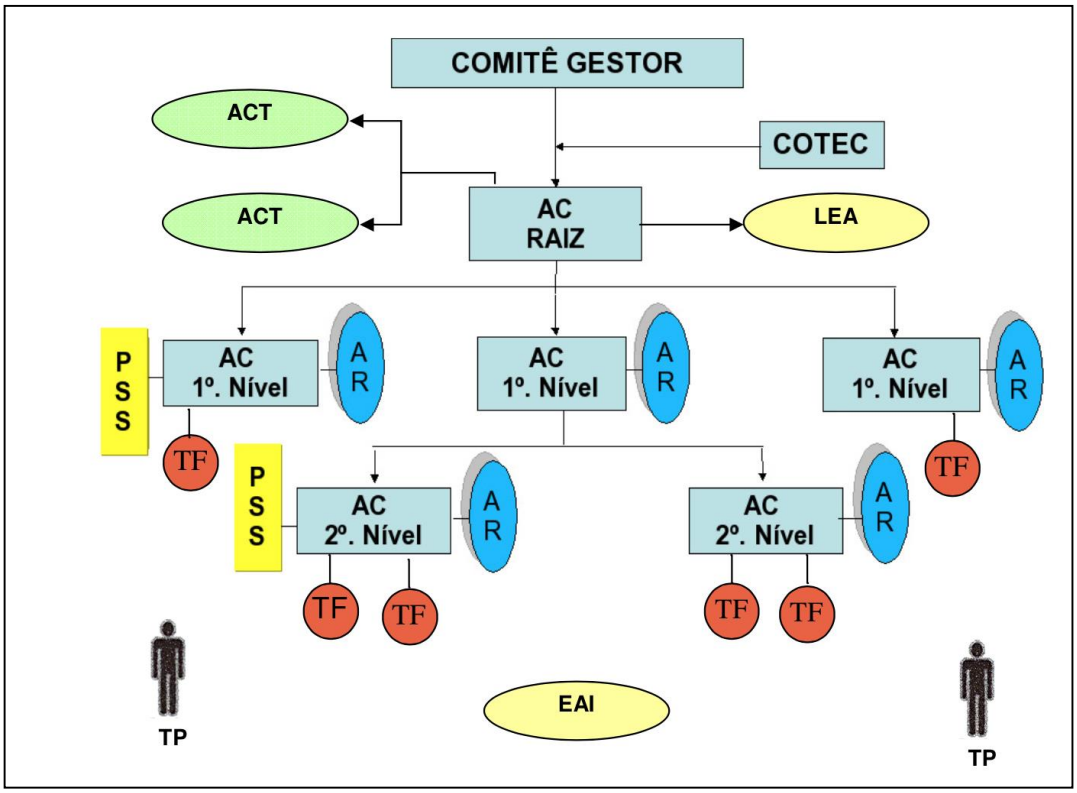


**Figura 1 – Organograma da estrutura hierárquica da ICP-Brasil (Fonte: Adaptado de (Bertol, 2009)).**

### 3.1.1 Comitê Gestor

Estabelece as regras de funcionamento da ICP-Brasil. É composto por membros do Governo e da sociedade civil. O Comitê Gestor exerce a função de autoridade gestora de políticas (AGP) da ICP-Brasil (BRASIL, 2008).

### 3.1.2 Comissão Técnica (COTEC)

Comissão que assessora o Comitê Gestor sobre matérias de natureza técnica, sempre quando solicitado. Cabe ainda à COTEC preparar e encaminhar previamente aos membros do Comitê Gestor um expediente contendo o posicionamento técnico dos órgãos e das entidades relacionados com as matérias que serão apreciadas e decididas. A COTEC é integrada por um representante indicado por cada membro do Comitê Gestor (BRASIL, 2008).

### 3.1.3 Autoridade Raiz (AC-Raiz)

A autoridade raiz (AC-Raiz) representa o primeiro nível da estrutura hierárquica da cadeia de certificação e é exercida pelo ITI. A AC-Raiz é o orgão responsável por executar as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, cabendo-lhe ainda o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e auditar os processos.

A AC-Raiz tem poder para emitir seus próprios certificados (Bertol, 2009), bem como emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, além de ser responsável pela emissão de sua própria lista de certificados revogados (LCR) (ITI, 2015). Cabe ainda à AC-Raiz fiscalizar e auditar as autoridades certificadoras (de primeiro e segundo nível), autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil, quanto à sua atuação dentro das conformidades das diretrizes e normas técnicas estabelecidas pelo Comitê Gestor (ITI, 2015).

### 3.1.4 Autoridades Certificadoras (AC)

As autoridades certificadoras (AC) são entidades públicas ou privadas credenciadas para emitir, distribuir, renovar, revogar e gerenciar certificados digitais de autoridades certificadoras e titulares finais. No âmbito da ICP-Brasil, há ACs de primeiro e segundo nível. As de primeiro nível são subordinadas diretamente à AC-Raiz e são responsáveis por emitir e publicar lista de certificados revogados (LCR) em seu âmbito de atuação. Podem ainda emitir os certificados digitais usados nos equipamentos e sistemas das Autoridades de Carimbo de Tempo (ACT) e da Entidade de Auditoria de Tempo (EAT), no âmbito da estrutura da ICP-Brasil (ITI, 2015).

Atualmente, são treze Autoridades Certificadoras de primeiro nível credenciadas na ICP-Brasil: Caixa Econômica Federal (AC-CEF), Certisign (AC-Certisign), Imprensa Oficial do estado de São Paulo (AC-Imprensa Oficial), Poder Judiciário (AC-JUS), Presidência da República (AC-PR), Serasa Experiam (Serasa ACP), Serviço Federal de Processamento de Dados – SERPRO (AC-SERPRO), Receita Federal do Brasil (AC-RFB), Casa da Moeda

do Brasil (AC-CMB), Valid (AC-Valid), Soluti (AC-Soluti), Digital Sign (AC-Digital Sign ACP), Boa Vista (AC-Boa Vista).

As ACs de segundo nível são subordinadas às ACs de primeiro nível, e suas responsabilidades são as de emitir, distribuir, renovar, revogar e gerenciar certificados digitais dos titulares finais. Essas ACs criam e assinam digitalmente o certificado do assinante atestando que o dono do certificado possui a chave privada correspondente à chave pública divulgada no referido certificado. Cabe também à AC de segundo nível emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Ainda estabelece e faz cumprir as políticas de segurança necessárias para garantir a autenticidade da identificação realizada pelas Autoridades de Registro (AR) a ela vinculadas.

Normalmente, as ACs de 1º nível emitem certificados digitais para as ACs de 2º nível, e estas emitem certificados para titulares finais. No entanto, há ACs de 1º nível que emitem certificados para titulares finais, como as autoridades certificadoras da Presidência da República (AC-PR), da Casa da Moeda do Brasil (AC-CMB) e do Ministério de Relações Exteriores (AC-MRE). Tais ACs não emitem, atualmente, certificados para ACs de 2º nível. A Figura 2~~Figura 2~~~~Figura 2~~ apresenta uma estrutura simplificada das ACs da ICP-Brasil.

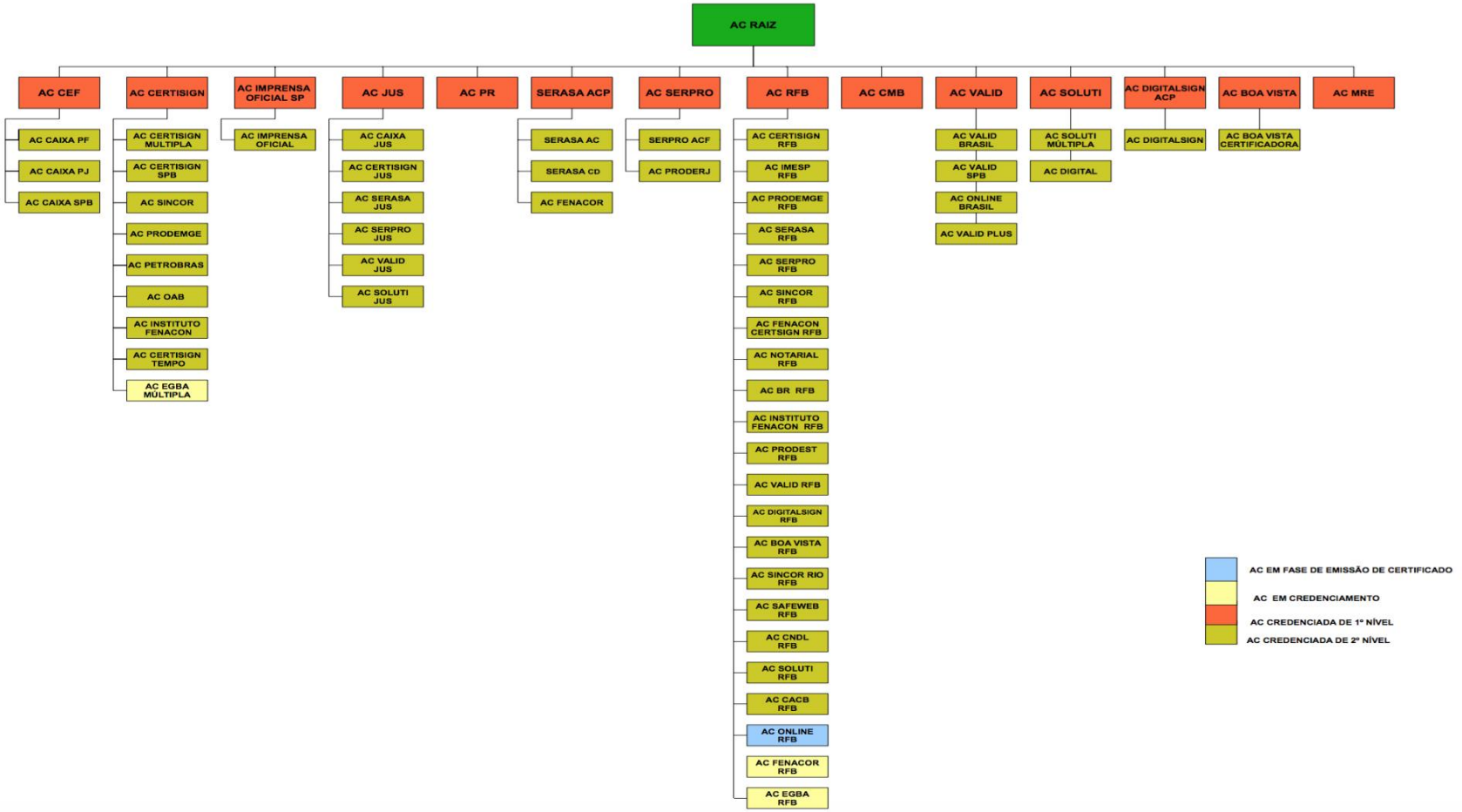

**Figura 2 – Estrutura simplificada das ACs que compõem a ICP-Brasil. (Fonte: Adaptado de (ITI, 2015), atualizado em 03/07/2015).**

### 3.1.5 Autoridades de Registro (AR)

As autoridades de registro (AR) são organizações privadas ou públicas e podem ser consideradas como os braços operacionais das Autoridades Certificadoras (AC). São responsáveis pela interface entre o usuário e a Autoridade Certificadora a elas vinculada. As ARs têm por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes (ITI, 2015). Cabe às ARs manterem registros de suas operações (Bertol, 2009).

### 3.1.6 Prestadores de Serviço de Suporte (PSS)

As Prestadoras de Serviço de Suporte (PSS) são empresas especializadas, dotadas de sede administrativa, instalações operacionais e recursos de segurança física e lógica, contratadas por uma autoridade certificadora (AC), autoridade de registro (AR) ou autoridade de carimbo de tempo (ACT) para prestarem serviços de infraestrutura de tecnologia da informação e lógica e recursos humanos especializados, conforme as políticas de certificação (PC) e declaração de práticas de certificação (DPC) destas empresas (Bertol, 2009).

### 3.1.7 Empresas de Auditoria Independente (EAI)

As empresas de auditoria independente (EAI) são organizações cadastradas pela AC-Raiz, para realizarem serviços de auditoria em todos os Prestadores de Serviço de Certificação (PSC), seja Autoridade Certificadora (AC), Autoridade de Carimbo do Tempo (ACT), Autoridade de Registro (AR) ou Prestador de Serviço de Suporte (PSS) (ITI, 2015).

As auditorias são do tipo pré-operacionais (realizadas antes de um PSC iniciar suas atividades no âmbito da ICP-Brasil) e operacionais (realizadas uma vez por ano a partir do primeiro ano civil após o cadastramento do PSC pela ICP-Brasil, objetivando a manutenção do credenciamento do PSC) (ITI, 2015).

### 3.1.8 Laboratório de Ensaio de Auditoria (LEA)

Os Laboratórios de Ensaio e Auditoria (LEA) são entidades vinculadas à AC-Raiz, devidamente equipados com tecnologia apropriada e profissionais de alto gabarito, para realizar ensaios destinados a avaliar a conformidade, em termos de equipamentos e aplicações, de software e hardware utilizados no sistema de certificação digital da ICP-Brasil (Bertol, 2009). Após os testes, o LEA emite laudos e pareceres técnicos que visam subsidiar a decisão da AC-Raiz quanto à homologação dos equipamentos e sistemas para operarem na cadeia de certificação digital da ICP-Brasil (ITI, 2015).

### 3.1.9 Autoridades de Certificadora de Tempo (ACT)

A autoridade de carimbo de tempo (ACT) são entidades responsáveis pela operação dos equipamentos conectados à rede de carimbo de tempo da ICP-Brasil e tem a função de emitir um carimbo de tempo e assinar documentos (Bertol, 2009). O carimbo do tempo corresponde a um conjunto de atributos fornecidos pela ACT que, associado a uma assinatura digital, atesta a questão temporal de uma transação e seu conteúdo (ITI, 2015). Na prática, ocorre a produção de um documento criptografado com aplicação dos atributos ano, mês, dia, hora, minuto e segundo atestados na forma da assinatura realizada com certificado digital, comprovando assim a sua autenticidade (ITI, 2015).

### 3.1.10 Titulares Finais (TF)

Os titulares finais são pessoas físicas ou jurídicas proprietárias de certificados digitais emitidos pelas autoridades certificadoras. Sendo o titular pessoa física, será responsável pela geração dos pares de chaves criptográficas e, caso seja pessoa jurídica, deverá indicar por meio de seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado (Bertol, 2009).

### 3.1.11 Terceiras Partes (TP)

As terceiras partes (TPs) correspondem a quaisquer pessoas físicas ou jurídicas que confiam no teor, validade e aplicabilidade dos certificados digitais, dos carimbos do tempo e demais documentos assinados digitalmente pelas entidades que compõem a ICP-Brasil (Bertol, 2009).

## 3.2 Estrutura das normas técnicas da ITI

Visando normatizar e criar diretrizes técnicas para o uso do certificado digital no âmbito do ICP-Brasil, a ITI criou uma série de documentos, instruções normativas e manuais técnicos. Foi criado uma estrutura para organizar e regular os documentos da ITI, conforme apresentado na Tabela 1~~Tabela 1~~~~Tabela 1~~ a seguir:

**Tabela 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-xx – VOL.nn | Manual de Condutas Técnicas para os processos de homologação. | Publicação no sítio iti.gov.br |

**Onde “nn”, “mm” e “xx” variam de 01 a 99 e “a” varia de A até Z**
**Fonte:** Estrutura Normativa da ICP-Brasil (ITI, 2010).

As normas da ICP-Brasil, organizadas de acordo com a estrutura normativa apresentada, contém todo o arcabouço técnico criado ou alterado pela ITI conforme as necessidades demandadas pela infraestrutura. A Tabela 2~~Tabela 2~~~~Tabela 2~~ apresenta a relação atual dos documentos da ICP-Brasil, agrupados por assunto sobre o qual tratam:

**Tabela 2 – Documentos ICP-Brasil agrupados por assunto**

| Código do documento | Nome do documento |
|---|---|
| **Formato e conteúdo dos certificados digitais** | |
| DOC-ICP-04 | Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil |
| DOC-ICP-04.01 | Atribuição de OID (*Objetc Identifiers*) 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 | Credenciamento das Entidades Integrantes da ICP-Brasil |
| DOC-ICP-03.01 | Características Mínimas de Segurança para as AR 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 Frequência e de Tempo na Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil |
| DOC-ICP-10.07 | Critérios e Procedimentos para Credenciamento de Laboratórios de Ensaios e Auditoria integrantes da 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 para homologação na 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 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 |
| DOC-ICP-10.08 | Padrões e Procedimentos Técnicos a serem observados nos processos de homologação de Equipamentos Criptográficos Não Contemplados em Manual de Conduta Técnica Específicos |
| **Carimbo de 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 da ICP-Brasil |
| DOC-ICP-14 | Procedimentos para Auditoria do Tempo da 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 das Políticas de Assinatura Digital na ICP-Brasil |
| **Certificado de Atributo** | |
| DOC-ICP-16 | Visão Geral sobre Certificado de Atributo para a ICP-Brasil |
| DOC-ICP-16.01 | Perfil de Uso Geral e Requisitos para Geração e Verificação de Certificados de Atributo na ICP-Brasil |

**Fontes:** Uma proposta de Regulamentação da Certificação Digital no Brasil (Bertol, 2009); Documentos Principais ICP-Brasil (ITI, n.d.).

# 4. Certificação Digital e normas técnicas do ITI

No presente tópico será apresentado um estudo das normas técnicas do ITI, tendo

por intuito levantar as questões técnicas relativas ao funcionamento do certificado digital, como os padrões adotados, os algoritmos criptográficos, tamanhos de chaves criptográficas, os protocolos de assinatura digital, etc. O ponto de partida para o referido estudo são os documentos normativos da ICP-Brasil, sendo complementados sempre que for necessário para o aprofundamento e compreensão das questões técnicas abordadas.

## 4.1 Certificado Digital

A criptografia assimétrica se baseia na utilização de duas chaves criptográficas correlacionadas, geradas a partir de funções matemáticas de tal forma que: se uma chave é utilizada para o processo de cifração de uma mensagem, a decifração desta só será possível com a utilização da outra chave correspondente (Stallings, 2005). As chaves criptográficas são chamadas de chave privada e chave pública. A chave privada corresponde à chave secreta que deve ser mantida com o dono do par de chaves. A chave pública é de livre divulgação para todas as entidades que possam interagir com o dono e o seu conhecimento não permite "descobrir" a chave privada correspondente. Dessa forma, as mensagens cifradas pelo dono das chaves com a sua chave privada têm caráter público, uma vez que todas as entidades que tiverem a chave pública podem decifrá-las. Porém, devido à correspondência entre as chaves pública e privada, todas as entidades terão certeza que a mensagem cifrada se originou do dono do par de chaves e também não foi alterada, visto que só este teria a chave privada corresponde para criar a mensagem cifrada. Analogamente, se uma mensagem for cifrada por uma dessas entidades com a chave pública do dono, pode-se afirmar que somente o dono teria a capacidade de decifrar a mensagem.

Com tais características a utilização da criptografia assimétrica demonstrou-se bastante interessante para promover confidencialidade, integridade, autenticação e não-repúdio, conforme a chave empregada na cifração. Porém, a criptografia assimétrica por si só esbarra no seguinte problema: como distribuir de maneira confiável a chave pública gerada pelo dono às entidades relacionadas. Assim, foi proposto a *Public Key Infraestructure* (PKI), ou Infraestrutura de Chave Pública (ICP), cujo intuito é assegurar que as chaves públicas sejam compartilhadas de forma segura

e eficiente.

A função de uma ICP é distribuir chaves públicas por meio dos certificados digitais, os quais correspondem a documentos eletrônicos que contém as chaves públicas a serem divulgadas. O funcionamento de uma ICP, pode ser explicado de forma simplificada da seguinte forma:

Suponha que Bob gere um par de chaves assimétricas, a chave privada e a chave pública, e, queira trocar mensagens com Alice. Bob solicita a uma Autoridade Certificadora (AC), que ambos Alice e Bob confiem, a criação do certificado digital.

A AC recebe a chave pública de Bob, por um meio seguro, procedendo com a criação do certificado digital. O certificado digital, além da chave pública de Bob, contém informações pessoais de Bob (o seu nome, endereço, etc.), dados de controle do certificado (número de série, data de validade, algoritmos criptográficos, etc.) e uma assinatura digital do conteúdo do certificado. A assinatura da AC é o que dará a Alice a segurança de que a o certificado digital é válido, e, consequentemente, a chave pública divulgada é verdadeira.

Bob recebe o certificado da AC, e, de posse deste, pode divulgar a Alice. Ao receber o certificado digital de Bob, Alice pode aferir sua autenticidade verificando a assinatura digital da AC, de forma que uma vez verificado, Alice pode utilizar a chave pública contida no certificado para se comunicar com Bob.

Em outras palavras, a correspondência entre a chave pública e a chave privada é o que dá a característica de identidade do certificado digital, o que por sua vez é atestado pela assinatura digital da AC. A AC funciona como uma espécie de cartório digital em que os usuários confiam. Dessa forma, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite identificação segura e inequívoca do titular da mensagem ou transação feita em meios eletrônicos, como a Web (ITI, n.d.).

O ITI estabeleceu 10 tipos de certificados digitais para usuários finais da ICP-Brasil, sendo 6 relacionados com a assinatura digital e 4 com sigilo (ITI, 2014). Os tipos de certificados A1 e S1 estão associados aos requisitos menos rigorosos, tendo um tempo de validade menor, enquanto os tipos A4 e S4 aos requisitos mais rigorosos, e, consequentemente, tem tempo de validade maior.

**Tabela 3 – Tipos de Certificados do ICP-Brasil**

| Tipo de Certificado | Observações |
|---|---|

| | |
|---|---|
| **A1** | Destinados à assinatura digital. Podem ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações. São associados a diferentes requisitos de segurança, onde que o tipo A1 é associado a requisitos menos rigorosos e o A4 a requisitos mais rigorosos. |
| **A2** | |
| **A3** | |
| **A4** | |
| **T3** | Destinados à assinatura digital. Somente podem ser emitidos para equipamentos de Carimbo de Tempo. Associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas |
| **T4** | |
| **S1** | Destinados à sigilo. Podem ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações. Associados a diferentes requisitos de segurança, onde que o tipo A1 é associado a requisitos menos rigorosos e o A4 a requisitos mais rigorosos. |
| **S2** | |
| **S3** | |
| **S4** | |

**Fonte:** DOC-ICP-04 – Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (ITI, 2014).

### 4.1.1 Formato dos certificados digitais

Todos os certificados emitidos no âmbito da ICP-Brasil devem estar em conformidade com o formato definido pelo padrão ITU X.509, versão 3 (ISO/IEC 9594-8) (ITI, 2014). O padrão X.509 é um padrão internacional reconhecido para a infraestrutura de chave pública, definida pela ITU-T. O X.509 define a estrutura do certificado digital, especificando os campos necessários para que este esteja completo e operacional. A Figura 3~~Figura 3~~~~Figura 3~~ apresenta a estrutura de um certificado X.509 ressaltando as diferenças em cada versão. A seguir são relacionados os campos de um certificado X.509 básico:

- **Versão** – indica qual a versão X.509 se aplica ao certificado. A versão indica quais os dados o certificado deve incluir.
- **Número serial** – é o número que identifica o certificado digital e o distingue dos demais certificados.
- **Informação do algoritmo** – informa o algoritmo utilizado pelo emissor para assinar o certificado digital.
- **Nome do emissor** – informa o nome da entidade emissora (AC) do certificado.
- **Período de validade do certificado** – informa a data de início e data de fim em que o certificado é considerado válido.
- **Nome do sujeito** – informa o nome do dono do par de chaves para o qual o

certificado foi criado.

- **Informação de chave pública do sujeito** – é a chave pública divulgada no certificado digital. Pode-se considerar que é o coração do certificado digital.
- **Extensões** – campo opcional que pode ser utilizado para armazenar e divulgar informação sobre as políticas de certificação da AC.
- **Assinatura** – é onde a AC emissora assina o conteúdo do certificado digital, atestando a sua veracidade.

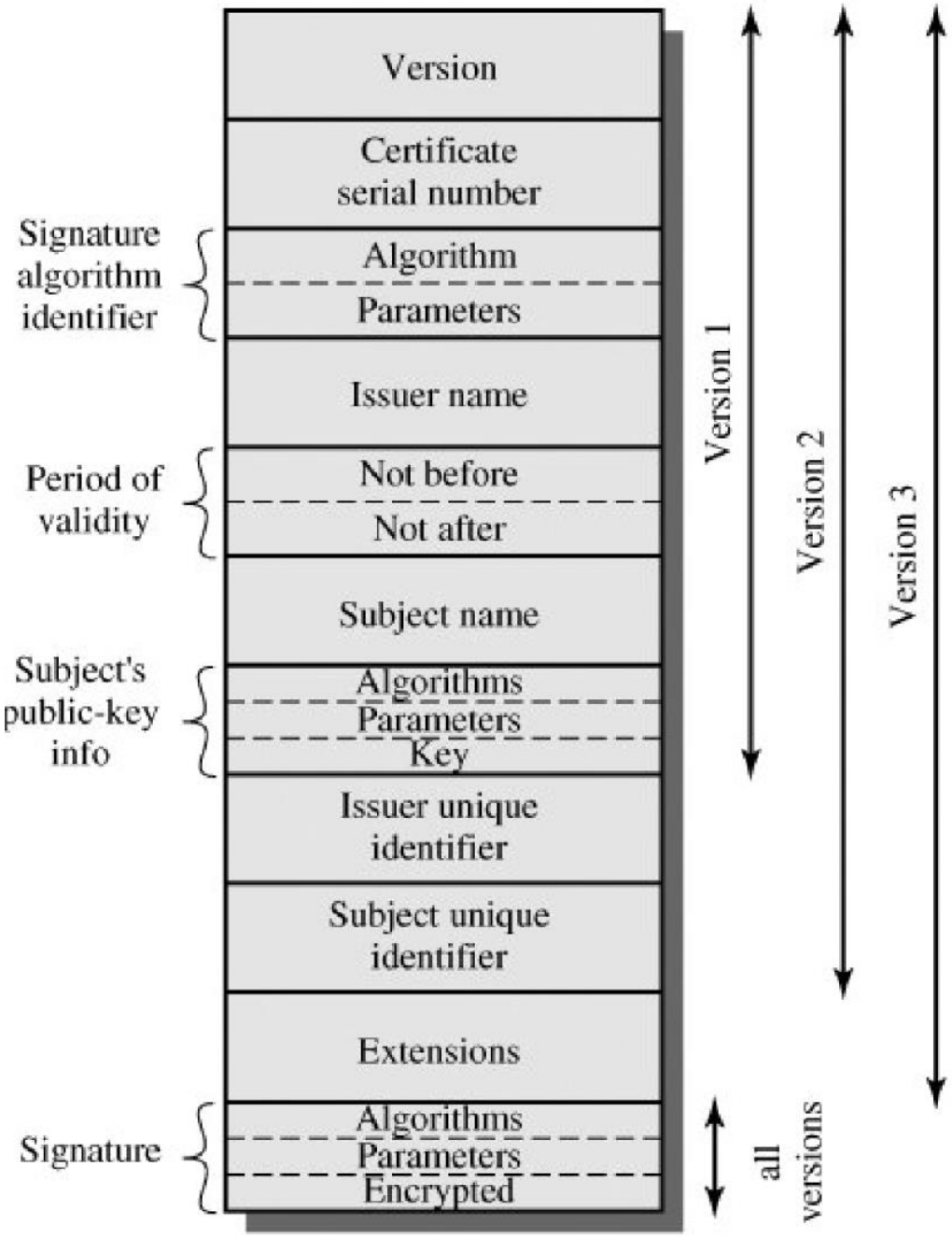

**Figura 3 – Estrutura de um certificado X.509 (Fonte: (Stallings, 2005)).**

Os campos constantes na estrutura de um certificado digital são referenciados por meio de *Objetc Identifiers* (OID). O OID consiste em séries numéricas separadas por pontos. O conjunto de números e pontos representa um arco, com os seus sub-arcos ou um objeto final na árvore de OID. Cada arco tem um significado. Por exemplo, tomando-se o OID 2.6.76.1 pode-se extrair as seguintes informações:

- **2.** – arco *join-iso-itu-t.* Esse arco é usado para identificar padrões comuns à ISO e ITU-T.
- **2.6.** – arco utilizado para identificar a atribuição para países.
- **2.6.76.** – arco utilizado para identificar o Brasil.
- **2.6.76.1** – arco utilizado para identificar a ICP-Brasil.

Além de definir o padrão X.509 para o formato dos certificados digitais em seu âmbito, a ICP-Brasil definiu também as extensões, seguindo as especificações da RFC 5280 (IETF, 2008), a seguir como obrigatórias (ITI, 2014):

- **"*Authority Key Identifier*", não crítica**[1]: o campo *keyIdentifier* deve conter o *hash* SHA-1 da chave pública da AC;
- **"*Key Usage*", crítica**: em certificados de assinatura digital, somente os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment* podem estar ativados; em certificados de sigilo, somente os bits *keyEncipherment* e *dataEncipherment* podem estar ativados;
- **"*Certificate Polices*", não crítica**: deve conter o OID da Política de Certificado correspondente e o endereço *Web* da Declaração de Práticas de Certificação da AC que emite o certificado;
- **"*CRL Distribution Points*", não crítica**: deve conter o endereço *Web* onde se obtém a LCR correspondente;

[1] A RFC 5280 especifica que as extensões de certificados poder ser designadas como crítica ou não-crítica. A extensão crítica se refere às extensões que devem ser rejeitadas quando o sistema de certificação não a conhecer ou não conseguir processar alguma informação da extensão. A extensão não-crítica pode ser ignorada se não for conhecida pelo sistema de certificação, porém deve ser processada se for conhecida.

- ***"Authority Information Access"*, não crítica:** a primeira entrada deve conter o método de acesso *id-ad-caIssuer*, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada pode conter o método de acesso *id-ad-ocsp*, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP. Esta extensão somente é aplicável para certificado de titular final.

A ICP-Brasil ainda define como obrigatória a extensão "***Subject Alternative Name***", **não crítica**, com os seguintes formatos para o certificado de pessoa física (ITI, 2014):

- 3 (três) campos *otherName*, obrigatórios, contendo:
  - **OID = 2.16.76.1.3.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.
  - **OID = 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.
  - **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

- campos *otherName*, não obrigatórios, contendo:
  - **OID = 2.16.76.1.4.n e conteúdo** = de tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente. A AC Raiz, por meio do documento ATRIBUIÇÃO DE OID NA ICP-BRASIL regulamentará a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.

- 1 (um) campo *otherName*, obrigatório, contendo para certificados vinculados à Documento RIC[2], contendo:
    - **OID = 2.16.76.1.3.9 e conteúdo** = nas primeiras 11 (onze) posições, o número de Registro de Identidade Civil.

Em relação aos campos *otherName* definidos como obrigatórios, a ICP-Brasil define as seguintes especificações (ITI, 2014).

a) O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING.

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero”.

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor.

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas.

e) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível.

f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor.

g) Apenas os caracteres de A a Z, de 0 a 9 e os caracteres especiais observados na Tabela 4~~Tabela 4~~~~Tabela 4~~, poderão ser utilizados, não sendo permitidos os

[2] A especificação do campo *otherName* contendo o número RIC foi uma das adaptações realizadas pela ITI no sentido de preparar a ICP-Brasil prevendo a utilização de certificação digital no referido documento.

demais caracteres especiais.

**Tabela 4 – Caracteres especiais admitidos em nomes**

| Caractere | Código NBR9611 (hexadecimal) |
|---|---|
| Branco | 20 |
| ! | 21 |
| “ | 22 |
| # | 23 |
| $ | 24 |
| % | 25 |
| & | 26 |
| ‘ | 27 |
| ( | 28 |
| ) | 29 |
| * | 2A |
| + | 2B |
| , | 2C |
| - | 2D |
| . | 2E |
| / | 2F |
| : | 3A |
| ; | 3B |
| = | 3D |
| ? | 3F |
| @ | 40 |
| \ | 5C |

**Fonte:** DOC-ICP-04 – Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (ITI, 2014).

Conforme já visto, o campo “*Subject”* do certificado digital é aquele que contém o nome do titular que possui o certificado. Para um certificado digital para pessoa física, o nome do titular do certificado, constante do campo “*Subject*”, deverá adotar o “*Distinguished Name*” (DN) do padrão ITU X.500/ISO 9594 (ITI, 2014). A seguir é apresentado um exemplo da atribuição de nome conforme o padrão:

**C** = BR

**O** = ICP-Brasil

**OU** = nome da AC emitente

**CN** = nome do titular do certificado.

Apresenta-se na Figura 4 a composição do campo "*Subject*" para a AC Valid Brasil, ainda que não seja um certificado para pessoa física, para fins de exemplificação.

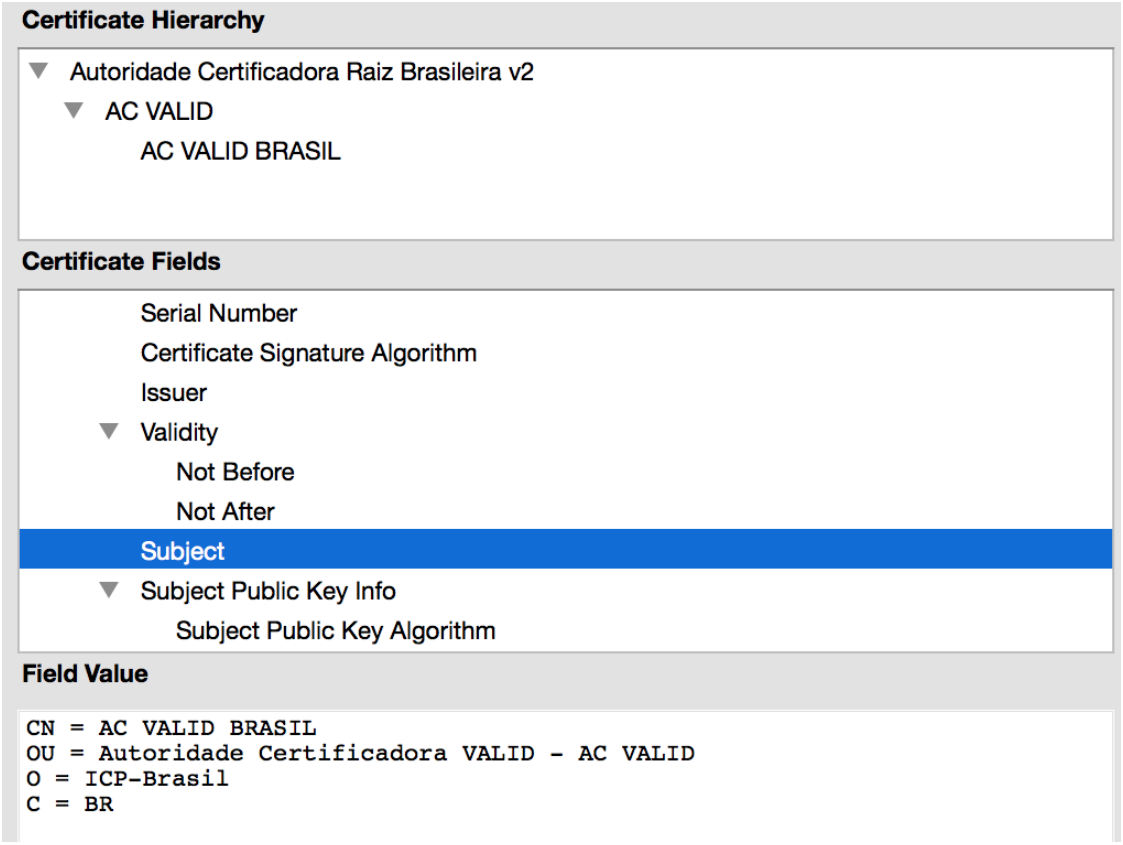


**Figura 4 – Composição do campo *Subject* para a AC VALID BRASIL.**

Vale a pena ressaltar que os nomes constantes nos certificados devem seguir algumas restrições, como não deverão ter sinais de acentuação, tremas ou cedilhas, e, além dos caracteres alfanuméricos, poderão ser utilizados os caracteres especiais apresentados na Tabela 4~~Tabela 4~~~~Tabela 4~~.

### 4.1.2 Ciclo de vida de um certificado digital

O certificado digital possui um ciclo de vida bem definido. De forma geral, pode-se dividir o ciclo de vida de um certificado digital de acordo com as seguintes etapas:

inicialização, utilização e cancelamento. Para fins de ilustração, a Figura 5~~Figura 5~~Figura 5 apresenta um exemplo de ciclo de vida de um certificado digital utilizado para o propósito de assinatura digital.

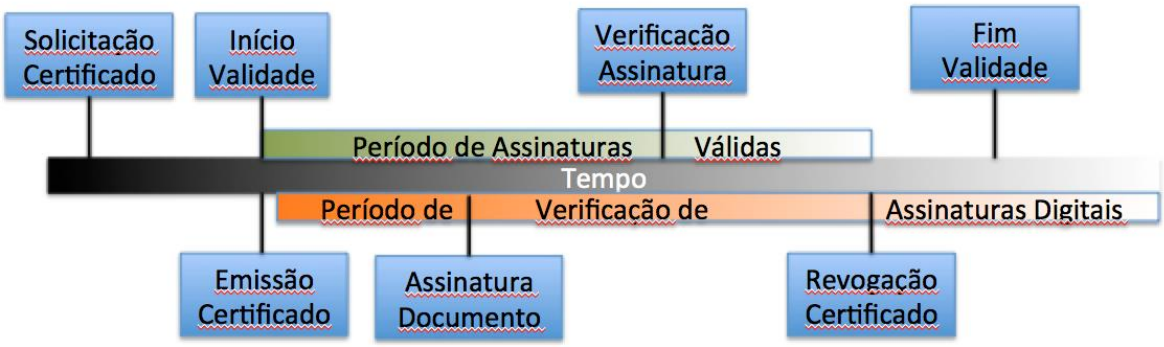


**Figura 5 – Ciclo de vida de um certificado digital para fins de assinatura digital**

### 4.1.2.1 Inicialização

Essa etapa inicia-se com a solicitação do certificado digital. A solicitação consiste no preenchimento de um formulário destinado à AC para que o interessado obtenha o seu certificado digital. Na solicitação é realizado um cadastramento do interessado, o qual fornece os seus dados de cadastro, o que é normalmente recebido por uma Autoridade de Registro (AR) vinculada à AC de interesse. Para o cadastramento, o titular apresenta à AR os documentos e dados necessários para que a AR possa confirmar a identidade do mesmo. Na solicitação, o interessado, também chamado de titular do certificado, deve fornecer a chave pública correspondente ao par de chaves assimétricas para ser adicionado ao certificado. O titular já deve ter executado, em passo anterior, o procedimento de geração do par de chaves.

No âmbito da ICP-Brasil, a geração do par de chaves, via de regra, é de responsabilidade do titular do certificado quando este for uma pessoa física (ITI, 2014). Ao ser gerada, a chave privada da entidade titular deve ser gravada e cifrada por algoritmo simétrico aprovado pela ICP-Brasil, em meio de armazenamento adequado e também definido para cada tipo de certificado da ICP-Brasil.

#### 4.1.2.2 Mídia Armazenadora

O ITI define alguns tipos de mídias armazenadoras para armazenar e proteger o par de chaves correspondentes ao certificado, conforme a Tabela 5~~Tabela 5~~~~Tabela 5~~.

**Tabela 5 – Tipos de mídia armazenadora permitidas na ICP-Brasil**

| Tipo de Mídia | Tipo de certificado | Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos) |
|---|---|---|
| 1 | A1 e S1 | Repositório protegido por senha e/ou identificação biométrica, cifrado por *software* por algoritmo simétrico aprovado em (ITI, 2014). |
| 2 | A2 e S2 | Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica. |
| 3 | A3 e S3 | Cartão Inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou *hardware* homologado junto à ICP-Brasil. |
| 4 | A4, S4, T3, e T4 | *Hardware* criptográfico homologado junto à ICP-Brasil. |

**Fonte:** DOC-ICP-04 – Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (ITI, 2014).

As mídias armazenadoras descritas devem assegurar, por meios técnicos e procedimentos adequados, no mínimo que:

a) a chave privada seja única e seu sigilo seja suficientemente assegurado;
b) a chave privada não possa ser deduzida e deva estar protegida contra falsificações realizadas através de tecnologias atualmente disponíveis;
c) A chave privada possa ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Outra observação a ser feita em relação à mídia armazenadora é que esta não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário (a AC que assinará) antes do processo de assinatura.

Dentre os modelos de mídias armazenadora existentes tem-se o *smartcard* e o *token*. O primeiro, chamado de cartão inteligente, assemelha-se a um cartão de crédito comum, em plástico, PVC ou policarbonato, microprocessador e memória para armazenamento de vários tipos de informação na forma eletrônica. Geralmente contêm

recursos de segurança física comum, cifragem de memória para proteção dos dados armazenados (usualmente com criptografia simétrica), empregam credenciais nas aplicações como senha para acesso de uso da chave privada, memória e uma unidade para cálculos criptográficos, o que possibilita aos *smartcards* poderem armazenar dados e fazer transações de forma rápida e segura, com flexibilidade e conveniência. Isto tem feito com que esses cartões recebam uma variedade de aplicações, tais como os cartões bancários, de identificação pessoal, transporte público, etc.

Há *smartcards* com interface com contato e sem contato, ou as duas interfaces. Um único *chip* armazena o processador e a memória. O chip com contato, quando o cartão for inserido em um leitor, encosta nos conectores elétricos, permitindo tanto a leitura como a escrita de dados. Estes cartões são fabricados de acordo com as Normas ISO/IEC 7816 e ISO/IEC 7810 e não usam bateria porque a energia é fornecida pelo leitor.

Os cartões sem contato possuem um *chip* que se comunica com o leitor através de RFID, com taxas de transmissão de 106 a 848 Kb/s. Tais cartões exigem somente proximidade a um transceptor para o estabelecimento do protocolo de comunicação. Geralmente são utilizados quando a transação deve ser feita rapidamente e com as mãos livres, como em sistemas de trânsito. A fabricação destes cartões é realizada dentro das especificações da norma ISO ISO/IEC 14443 (2001), que define os cartões sem contato da categoria A e categoria B, permitindo comunicação a distâncias de até 10 cm.

#### 4.1.2.3 Algoritmos Criptográficos Simétricos

Conforme já fora mencionado, a chave privada deve ser protegida por algoritmos simétricos, desde quando é transmitida do dispositivo gerador à mídia armazenadora, bem como no armazenamento nesta última. A Tabela 6~~Tabela 6~~~~Tabela 6~~ apresenta aos algoritmos simétricos aprovados pela ICP-Brasil:

**Tabela 6 – Algoritmos Simétricos para proteção da chave privada**

| Algoritmos Simétricos para Guarda de Chave Privada da Entidade Titular e de seu Backup | |
|---|---|
| **Algoritmo e Tamanho de Chave** | 3DES – 112 bits |
| | AES – 128 ou 256 bits |

| Modo de Operação | CBC ou GCM |
|---|---|

**Fonte:** DOC-ICP-01.01 – Padrões e Algoritmos Criptográficos da ICP-Brasil (ITI, 2014).

### 4.1.2.4 Algoritmos Criptográficos Assimétricos

Resta ainda citar, quanto à geração do par de chaves criptográficos, os algoritmos assimétricos aprovados pela ICP-Brasil. Tais algoritmos são apresentados na Tabela 7~~Tabela 7~~~~Tabela 7~~:

**Tabela 7 – Tipos de certificado e os respectivos algoritmos, mídia armazenadora e requisitos temporais**

| Tipo de Certificado | Chave Criptográfica | | | Validade Máxima do certificado (anos) | Período de emissão de LCR (horas) | Tempo limite para revogação (horas) |
|---|---|---|---|---|---|---|
| | Tamanho (bits) | Processo de Geração | Tipo de Mídia Armazenadora | | | |
| A1 e S1 | RSA 1024 (V0 e V1), 2048 (V2) | *Software* | 1 | 1 | 6 | 12 |
| | ECDSA 256 | *Software* | 1 | 1 | 6 | 12 |
| A2 e S2 | RSA 1024 (V0 e V1), 2048 (V2) | *Software* | 2 | 2 | 6 | 12 |
| | ECDSA 256 | *Software* | 2 | 2 | 6 | 12 |
| A3 e S3 | RSA 1024 (V0 e V1), 2048 (V2) | *Hardware* | 3 | 5 | 6 | 12 |
| | ECDSA 256 | *Hardware* | 3 | 5 | 6 | 12 |

| | | | | | | |
|---|---|---|---|---|---|---|
| T3 | RSA 1024 (V0 e V1), 2048 (V2) | *Hardware* | 4 | 5 | 6 | 12 |
| | ECDSA 256 | *Hardware* | 4 | 5 | 6 | 12 |
| A4 e S4 | RSA 2048 (V0 e V1), 4096 (V2) | *Hardware* | 4 | 6 | 6 | 12 |
| | ECDSA 512 | *Hardware* | 4 | 11 | 6 | 12 |
| T4 | RSA 2048 (V0 e V1), 4096 (V2) | *Hardware* | 4 | 6 | 6 | 12 |
| | ECDSA 512 | *Hardware* | 4 | 11 | 6 | 12 |

**Fontes:** DOC-ICP-01.01 – Padrões e Algoritmos Criptográficos da ICP-Brasil (ITI, 2014); DOC-ICP-04 – Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil (ITI, 2014).

#### 4.1.2.5 Solicitação, Criação e publicação do certificado digital

A solicitação de certificado, com os dados cadastrais do titular e a chave pública do par de chaves assimétricas, deve ser validada pela AR. A AR verifica a solicitação e os documentos apresentados pelo titular, obtendo como resultado a aprovação ou não da solicitação. Uma vez que a solicitação seja aprovada, esta é repassada para a AC no formato PKCS#10 (ITI, 2014). O formato PKCS#10 é padronizado pela RFC 2986 (IETF, 2000), a qual trata das mensagens enviadas à AC para solicitação de certificados para uma chave pública.

Recebida a solicitação de certificado, a AC cria o certificado digital. No processo de criação do certificado digital a AC adiciona aos dados fornecidos no PKCS#10 informações da própria AC, tais como o nome da AC signatária, os algoritmos de *hash* e de criptografia utilizados, o número de série do certificado (para identificá-lo de forma única), período de validade do certificado, etc. Posteriormente, todas essas informações, os dados do PKCS#10 e os dados adicionados pela AC, são assinados digitalmente pela AC signatária com a sua chave privada, criando assim a assinatura digital de toda a documentação do certificado digital. Essa assinatura funciona como

uma espécie de selo da AC, dependente do conteúdo assinado, o qual atesta que o certificado digital é verdadeiro. Logo, todos os que confiam na respectiva AC e conhecem a sua chave pública podem verificar a autenticidade e integridade do certificado digital. O processo de geração do certificado digital é representado na Figura 6~~Figura 6Figura 6~~.

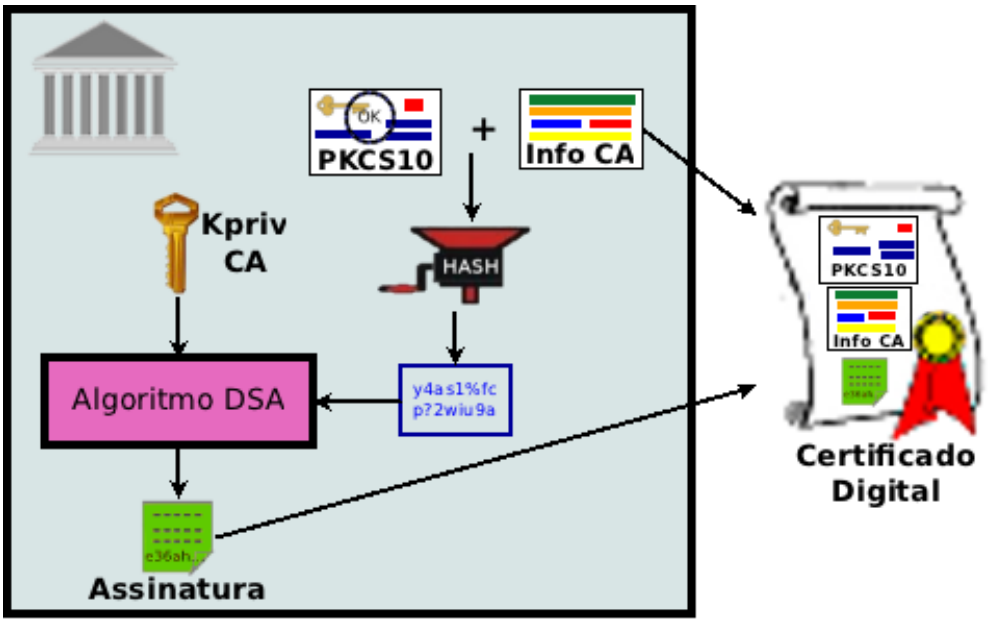


**Figura 6 – Geração de um certificado digital**

Após a criação do certificado digital, este deve ser disponibilizado aos usuários da ICP-Brasil. Uma das formas previstas para disponibilizar o certificado ao titular é utilizando-se o formato PKCS#7 (ITI, 2014). O formato PKCS#7 é padronizado pela RFC 2315 (IETF, 1998), a qual trata da sintaxe de mensagens genéricas que podem ser submetidas a funções criptográficas, tais como assinatura e envelopagem digital. Ou seja, o PKCS#7 é utilizado para disponibilizar o certificado digital ao seu titular de forma segura, com algoritmos relacionados no DOC-ICP-01.01 (ITI, 2014). Ainda é previsto que o certificado possa ser disponibilizado aos usuários por meio de diretório, pela página *Web* da AC ou por outros meios seguros aprovados pelo CG da ICP-Brasil (ITI, 2014). Concluída a disponibilização/publicação, o certificado digital já pode ser utilizado.

#### 4.1.2.6 Utilização

Com a emissão do certificado, isto é, com sua criação e disponibilização, o certificado está pronto para ser utilizado. A utilização do certificado está vinculada à sua finalidade para qual foi criado, seja para assinatura, para sigilo ou autenticação.

É importante ressaltar que um certificado digital tem um tempo de validade, o qual inicia-se a partir do momento de emissão do mesmo. O tempo de validade depende dos parâmetros de segurança utilizados na criação do certificado. Por exemplo, um certificado do tipo A1, com chaves criadas pelo algoritmo RSA, tem requisitos de segurança mais baixos e tem um tempo de vida máximo definido de 1 ano na ICP-Brasil. Já um certificado do tipo A4, o qual exige critérios de segurança mais rígidos, também com chaves criadas pelo algoritmo RSA, tem um tempo de vida máximo de 6 anos na ICP-Brasil.

Um certificado digital somente pode ser utilizado durante o seu tempo de validade, embora os seus efeitos possam ter uma vida maior. Por exemplo, nos certificados destinados à assinatura digital com período de validade de 1 ano, somente dentro desse período o titular pode assinar algum documento. Porém, as assinaturas realizadas dentro do período de validade ainda são consideradas válidas mesmo após a data de expiração do certificado, considerando-se um intervalo curto entre a geração e a conferência da assinatura digital. Ou seja, a assinatura digital é considerada válida da data de criação da assinatura até quando os requisitos de segurança ainda forem considerados válidos, desde que a criação da assinatura seja realizada dentro do período de validade do certificado digital.

No uso do certificado, toda a vez que alguma entidade o recebe, seja um terceiro ou o próprio titular, ela deve realizar a validação do certificado. A validação é essencial para permitir que a entidade possa considerar o certificado apto para uso. Nessa validação é verificado:

- **A assinatura da CA** – verifica-se se a assinatura da CA presente no certificado é verdadeira. Consiste em confirmar se os dados do certificado foram realmente assinados com a chave privada da CA. A verificação é feita aplicando o processo de operação de verificação do algoritmo de assinatura, utilizando-se chave pública da CA.
- **O período de validade do certificado** – é a verificação se o certificado está

válido em relação às suas datas inicial e final de validade. A entidade compara essas datas com o seu relógio, considerando o certificado válido somente se o relógio registrar o tempo entre as duas datas (ver Figura 7~~Figura 7Figura 7~~). É importante observar que o relógio da entidade deve estar configurado corretamente, sendo recomendada a utilização de algum protocolo de sincronismo de relógio, como o NTP.

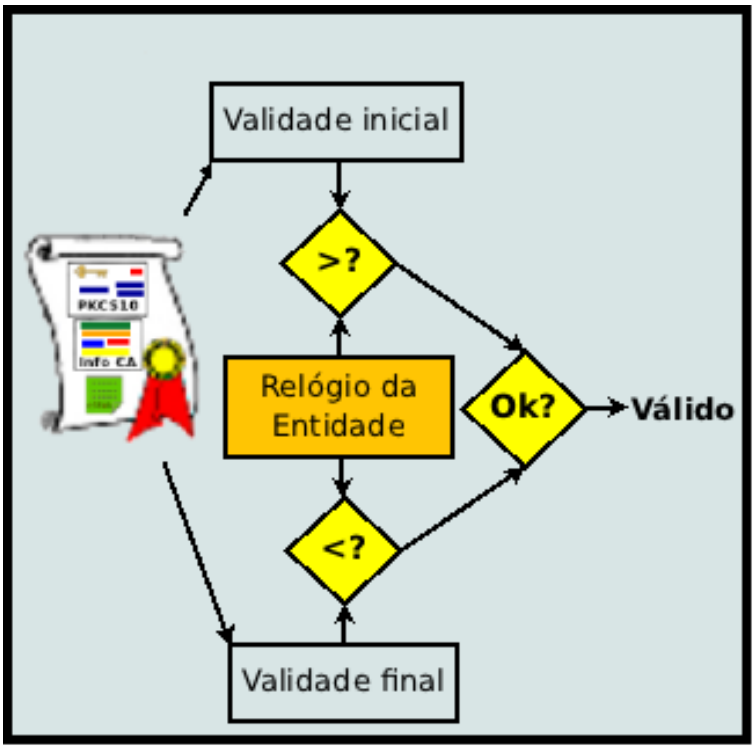


**Figura 7 – Verificação do período de validade do certificado digital**

- **Se o certificado foi revogado** – essa verificação consiste na verificação se o certificado foi invalidado antes do término do período de validade. A justificativa para a revogação é o comprometimento do certificado, por exemplo, pela descoberta da chave privada do titular por outros usuários.

#### 4.1.2.7 Cancelamento

O fim do ciclo de vida de um certificado digital é caracterizado pelo seu cancelamento. O certificado digital pode ser cancelado por dois meios: com o fim do período de validade e com a revogação do certificado.

O cancelamento de um certificado devido ao fim do seu período de validade é realizado de forma automática. Ou seja, expirado o tempo de validade final, as entidades às quais o certificado for apresentado não o reconhecerão como válido, conforme a verificação do período de validade já apresentado na Figura 7~~Figura 7~~Figura 7.

O processo de revogação de um certificado é a forma de invalidá-lo a qualquer instante, antes do seu período de término. A revogação pode ser solicitada pelo titular do certificado ou por decisão motivada da AC. Os motivos que levam podem levar à revogação de um certificado são os seguintes.

a) Quando constatada emissão imprópria ou defeituosa do mesmo.
b) Quando for necessária a alteração de qualquer informação constante no mesmo.
c) No caso de dissolução do titular do certificado.
d) No caso de comprometimento da chave privada da AC ou da chave privada do titular.
e) Fim do propósito do certificado.

Uma vez detectada a necessidade de revogação, deve-se iniciar a solicitação de revogação. Na ICP-Brasil, os responsáveis para a solicitação da revogação podem variar de acordo com a DPC da AC que emitiu o certificado. No entanto, o titular do certificado, a AC emissora e a AC Raiz são entidades comuns que constam nas DPCs das ACs e que podem solicitar tal revogação. Via de regra, a revogação é realizada por meio de formulário próprio ou por meio de formulário eletrônico na *Internet*, devidamente justificada. O solicitante deve ser identificado e todo o processo de revogação e as ações decorrentes registradas e arquivadas.

A conclusão da revogação se dá quando a AC publica sua Lista de Certificados Revogados (LCR), com a inclusão do certificado em questão como inválido. Assim, todas as entidades que tiverem a necessidade de consultar se um certificado é válido podem acessar a LCR da AC, a qual é geralmente publicada em *link* determinado da AC na *Internet*. A autenticidade da LCR deve ser confirmada por meio da verificação da assinatura da AC emissora e do seu período de validade. O tempo de publicação das LCRs depende da política de certificado e da AC. A Tabela 7~~Tabela 7~~Tabela 7 apresenta a periodicidade de emissão de LCR de 6 horas e o tempo limite de revogação de 12 horas, regulamentados na ICP-Brasil (ITI, 2014). O uso de LCRs é o método padrão na

ICP-Brasil para a divulgação dos certificados revogados pelas ACs.

A ICP-Brasil ainda prevê o uso do *Online Certificate Status Protocol* (OCSP), um protocolo do tipo “pedido / resposta” utilizado para a obtenção do status de revogação de um certificado digital X.509. O OCSP é descrito na RFC 6960 (IETF, 2013) e tem a vantagem de permitir a consulta sobre o status de um certificado em tempo real, com menos informação que a LCR, e, consequentemente, menor sobrecarga na rede. Apesar de previsto, o uso do OCSP não é comumente disponibilizado nas ACs da ICP-Brasil.

## 4.2 Assinatura Digital

A assinatura digital é um dos propósitos de uso do certificado digital. A assinatura digital atua como um mecanismo de autenticação que permite ao seu titular anexar um código no documento eletrônico a ser assinado. Esse código é equivalente a uma assinatura convencional e atesta que o titular assinou de fato o documento eletrônico. Assim, a assinatura digital deve ter algumas características básicas (Stallings, 2005) a saber.

- Deve verificar o titular, a data e hora da assinatura.
- Deve autenticar o conteúdo no momento da assinatura.
- Deve ser verificável por terceiros, para resolver disputas.

Baseando-se em tais características, pode-se enumerar os requisitos para a criação de uma assinatura digital (Stallings, 2005)a saber.

a) Precisa ser um padrão de bits que dependa da mensagem que será assinada.
b) Precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação.
c) Deve ser relativamente fácil produzi-la.
d) Deve ser relativamente fácil reconhecê-la e verificá-la.
e) Deve ser computacionalmente inviável falsificá-la.
f) Deve ser prático armazenar uma cópia da assinatura digital.

De forma simplificada, a Figura 8~~Figura 8~~~~Figura 8~~ apresenta o processo adotado para a criação de uma assinatura digital, contemplando as características e requisitos mencionados. A explicação do processo de criação é descrita a seguir (ITI, 2012).

a) O signatário (quem cria a assinatura digital) gera um resumo criptográfico de um

documento eletrônico. Esse resumo criptográfico é criado por meio de funções *hash*, uma espécie de funções criptográficas que resumem o conteúdo do documento eletrônico num determinado número bits aparentemente aleatórios.

b) O signatário cifra o resumo criptográfico com a sua chave privada, associada à chave pública constante do seu certificado digital, gerando a assinatura digital.

c) Associa-se o documento eletrônico e a assinatura digital para futura validação.

O processo de validação da assinatura digital também é esboçado pela Figura 8~~Figura 8~~~~Figura 8~~. De forma simplificada, o processo de validação é descrito a seguir (ITI, 2012):

a) O documento eletrônico e a assinatura digital associada são disponibilizados para o verificador (entidade que valida a assinatura digital) juntamente com o certificado digital do usuário.

b) O verificador calcula novamente o resumo criptográfico do documento eletrônico.

c) O verificador decifra a assinatura digital com a chave pública do signatário, contida no certificado digital, obtendo o resumo criptográfico gerado e cifrado pelo signatário no momento da assinatura.

d) O verificador compara os resumos criptográficos obtidos, o calculado e o decifrado. Se forem iguais, a assinatura digital é considerada válida: mostra que o documento está íntegro e que é possível identificar o signatário por meio do certificado digital. Se forem diferentes, a assinatura digital é considerada inválida.

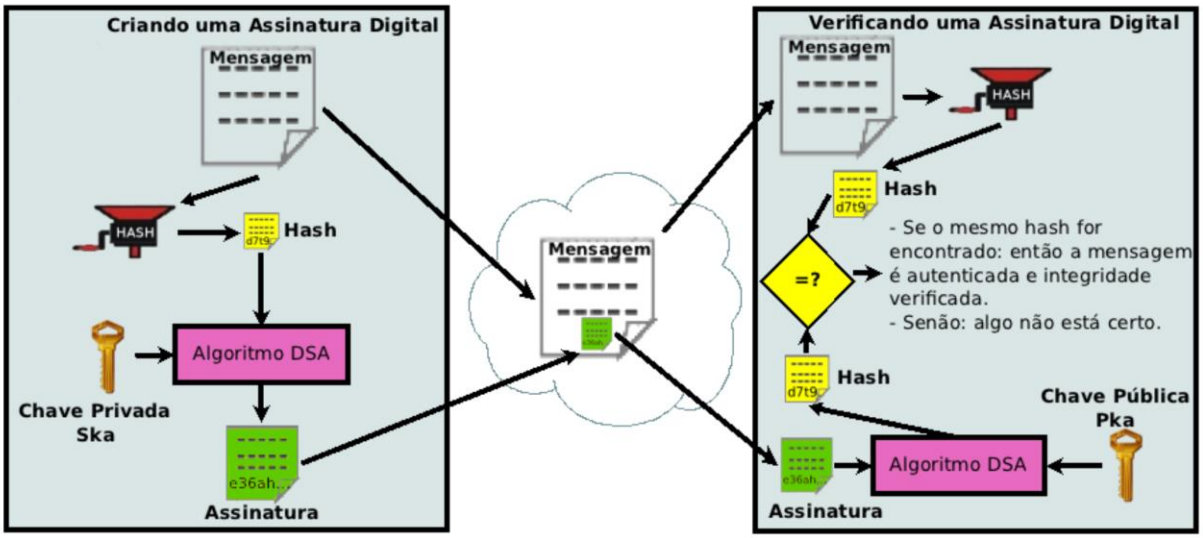


**Figura 8 – Funcionamento da assinatura digital**

É interessante citar que os esquemas de assinatura digital podem ser divididos em dois grupos: esquemas de assinatura digital com apêndice e esquemas de assinatura digital com recuperação de mensagem (Menezes, Oorschot, & Vanstone, 1996)apêndice primeiro requer a mensagem original como entrada para a verificação da assinatura. Já o segundo não requer a mensagem original para a verificação da assinatura, pois ao invés de utilizar uma função de *hash* para criar a assinatura, utiliza-se uma função de redundância donde é capaz de extrair a mensagem original e atestar se a assinatura é válida.

Esquemas de assinatura digital com apêndice utilizam funções de *hash* e são menos propensos a ataques de falsificação. Exemplos de mecanismos de assinatura digital com apêndice são o DSA, ElGamal e Schnorr (Menezes, Oorschot, & Vanstone, 1996). Os esquemas de assinatura digital com recuperação de mensagem têm uso prático para mensagens curtas (Menezes, Oorschot, & Vanstone, 1996). Os esquemas de assinatura de chave pública RSA, Rabin e Nyberg-Rueppel são exemplos de mecanismos de assinatura digital com recuperação de mensagem. Na regulamentação do ITI, percebe-se que a ICP-Brasil utiliza os esquemas de assinatura digital com apêndice, uma vez que há a exigência da mensagem original para a verificação da assinatura digital (ITI, 2012). Os esquemas de assinatura utilizados na ICP-Brasil empregam RSA ou o ECDSA.

### 4.2.1 Assinatura Eletrônica versus Assinatura Digital

É importante diferenciar o conceito de assinatura eletrônica e assinatura digital. Assinatura eletrônica refere-se a um conjunto de dados, no formato eletrônico, que é anexado ou logicamente associado a um outro conjunto de dados, também no formato eletrônico, para conferir-lhe autenticidade ou autoria (ITI, 2012). Ou seja, a assinatura eletrônica pode ser obtida por qualquer mecanismo eletrônico, como mecanismos de *login*/senha, biometria, *Personal Identification Number* (PIN), etc., sem necessariamente utilizar criptografia. A assinatura digital é um dos tipos de assinatura eletrônica, que utiliza um par de chaves criptográficas associado a um certificado digital. A ICP-Brasil trata apenas da assinatura digital em suas normativas.

### 4.2.2 Padrões para assinatura digital

Existem questões relevantes no processo de criação de uma assinatura digital. Uma dessas questões são as informações necessárias para dar valor probante à assinatura digital. Nessa questão de validação o tempo é crítico, pois caso seja necessário validar uma assinatura digital após decorrido um determinado tempo, as informações necessárias para o processo de validação podem não estar disponíveis na AC relacionada, fadando o processo da assinatura digital ao fracasso. Outra questão relevante é quanto à interoperabilidade das assinaturas digitais, o que é vital para que todas as partes envolvidas em uma determinada transação sejam capazes de assinar digitalmente, seguindo os mesmos padrões e formatos, possibilitando a validação da assinatura digital por outras partes. Nesse aspecto foram criados processos e procedimentos com o intuito de guardar as informações necessárias para a validação de uma assinatura digital, bem como definir padrões para garantir a interoperabilidade. Tais processos e procedimentos são conhecidos na literatura por assinaturas digitais avançadas ou *Advanced Eletronic Signatures* (AdES) (Bezerra, 2010), desenvolvidos pelo comitê técnico *Eletronic Signatures and Infrastructures* (ESI), o qual foi criado pelo ETSI.

Entre os trabalhos desenvolvidos pelo comitê ESI destacam-se os padrões *CMS Advanced Eletronic Signature* (CAdES) e o *XML-DSig Advanced Eletronic Signature*

(XAdES). O CAdES e o XAdES são padrões equivalentes adotados na ICP-Brasil.

#### 4.2.2.1 CMS Advanced Eletronic Signature - CAdES

O CAdES se baseia no padrão *Cryptographic Message Syntax* (CMS) (IETF, 2009). O CMS é uma evolução do padrão *Public-Key Cryptography Standards #7* (PKCS#7). O CMS descreve uma estrutura para armazenamento de conteúdos assinados digitalmente, conteúdos cifrados, conteúdos autenticados e conteúdos com resumos criptográficos. De fato, o CMS é o padrão atual mais utilizado nas aplicações de nível mundial, dispondo de ampla documentação e grande variedade de biblioteca de *software* disponível.

Quando se utiliza o padrão CMS para representar o conteúdo digital assinado, a inclusão do conteúdo digital propriamente dito é opcional, permitindo assim a existência de duas representações diferentes:

- estrutura assinada com conteúdo digital anexado (*attached*), na qual o conteúdo digital está incluído na estrutura CMS;
- estrutura assinada com conteúdo digital separado (*dettached*), na qual o conteúdo digital não está incluído na estrutura CMS.

Além dos atributos assinados, os quais fazem parte do resumo criptográfico sobre a qual a assinatura é gerada, o CMS permite adicionar atributos não assinados, bem como gerar assinaturas em paralelo (várias assinaturas digitais feitas por diferentes signatários sobre o conteúdo) e assinaturas em série (assinaturas adicionais que assinam todas as assinaturas anteriores). Porém o CMS não permite assinar partes de um documento, somente o documento como um todo.

O CAdES é uma extensão do CMS criada com a finalidade de prover assinaturas digitais que permitam sua validação por longo prazo. O CAdES é descrito no documento ETSI TR 101 733 (ETSI, 2008). Para validar uma assinatura digital que utiliza o padrão CAdES, a assinatura deve estar de acordo com uma das políticas de assinatura definidas ou aprovadas pela ICP-Brasil (ITI, 2012). É importante ressaltar que a incorporação dos dados de validação às assinaturas digitais leva à criação de diferentes formatos de assinaturas, como será visto adiante.

#### 4.2.2.2 XML-DSig Advanced Eletronic Signature - XAdES

O padrão XAdES é baseado no padrão *XML Digital Signatures* (XML-DSig) (W3C, 2008), padrão de assinaturas digitais representadas em XML, cuja especificação é mantida pelas organizações *World Wide Web Consortium* (W3C) e *Internet Engineering Task Force* (IETF). O padrão XML-DSig pode ser aplicado a qualquer tipo de dado e não somente a dados XML.

O XML-DSig é equivalente ao CMS, porém o XML-DSig apresenta as vantagens da linguagem XML, como a extensibilidade que permite a criação de *tags* XML de modo arbitrário. Tal característica é bastante útil na integração de diversas fontes de informação e apresentação uniforme para tais dados. Além disso, o XML-DSig contempla a assinatura de diversos tipos de conteúdo, como dados codificados em ASCII, dados em código binário ou dados formatados em XML. Outro aspecto interessante do XML-DSig é que o padrão permite gerar uma assinatura digital sobre apenas uma parte de um documento eletrônico, o que não é possível no CMS.

Em relação ao armazenamento do conteúdo digital, o XML-DSig define três representações diferentes (todas suportadas na ICP-Brasil), a saber.

- Estrutura assinada com conteúdo digital separado (*detached*), na qual o conteúdo digital não está incluído na estrutura XML-DSig.
- Estrutura assinada com conteúdo digital anexado (*enveloping*), na qual o conteúdo digital está incluído na estrutura XML-DSig.
- Estrutura assinada incluída no conteúdo digital (*enveloped*), na qual a assinatura digital está incluída no conteúdo digital que está sendo assinado.

Tal como o CAdES, o XAdES trata-se de uma extensão do XML-DSig que tem por finalidade prover assinaturas digitais que permitam sua validação por longo prazo. O XAdES é descrito no documento ETSI TS 101 903 (ETSI, 2004). Da mesma forma como o CAdES, o XAdES possibilita a incorporação de dados adicionais à assinatura, levando a criação de diferentes formatos de assinaturas, padronizadas, incluindo formatos para assinaturas de longo prazo.

### 4.2.3 Formatos de assinatura digital

Conforme já fora mencionado, os padrões CAdES e XAdES padronizam formatos de assinaturas digitais, de acordo com os dados adicionais que são adicionados à assinatura. A seguir são apresentados os formatos de assinatura digital admitidos na ICP-Brasil (ITI, 2012):

a) **Assinatura Digital com Referência Básica (AD-RB)** – é uma assinatura digital de curto prazo, pois não armazena dados fundamentais para sua validação futura e também não tem carimbo de tempo. Sua composição é explicitada na Figura 9~~Figura 9~~Figura 9, na qual a política de assinatura é o identificador da política de assinatura usada para criação e verificação de uma assinatura digital ICP-Brasil. Este tipo de assinatura é mais adequado para autenticação de transações, onde a guarda de informações adicionais não é importante. Esse formato garante a autenticação e a integridade da informação dos atributos assinados. A AD-RB permite múltiplas assinaturas.


**Figura 9 – Assinatura Digital com Referência Básica (Fonte: DOC-ICP-15.01 (ITI, 2012))**

b) **Assinatura Digital com Referência de Tempo (AD-RT)** – possui os mesmos componentes de assinatura da AD-RB, com a adição de um carimbo de assinatura, tal como apresentado na Figura 10~~Figura 10~~Figura 10. O carimbo de tempo deve ser emitido por uma Autoridade de Carimbo de Tempo (ACT) credenciada na ICP-Brasil. Esse formato é adequado para aplicações ou processos de negócios nos quais a assinatura digital necessita de segurança em relação à irretratabilidade de sua criação. O carimbo de tempo serve como evidência de que o certificado do signatário não estava revogado ou expirado no momento da assinatura. Esse formato deve ser utilizado somente quando os dados necessários para validação da assinatura (LCRs ou respostas OCSP) puderem ser obtidos na própria AC. A AD-RT permite múltiplas assinaturas.

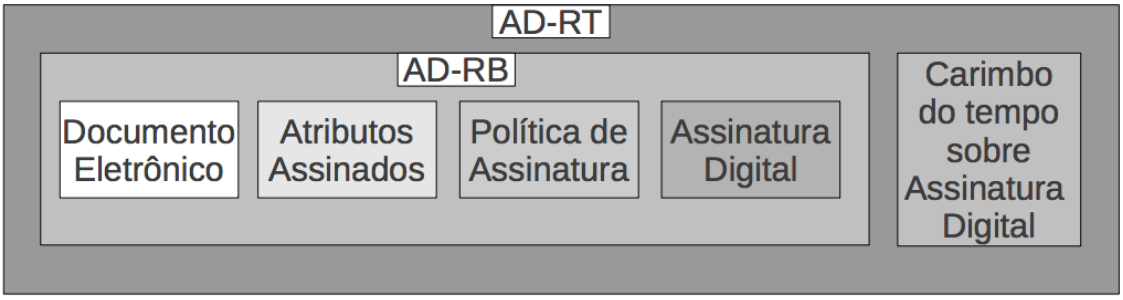


**Figura 10 – Assinatura Digital com Referência de Tempo (Fonte: DOC-ICP-15.01 (ITI, 2012))**

c) **Assinatura Digital com Referências para Validação (AD-RV)** – é formada por uma assinatura AD-RT, acrescentando as referências sobre os certificados que compõem a cadeia de certificação e as referências sobre as informações do estado de revogação do certificado digital do signatário. Também é adicionado outro carimbo de tempo sobre os dados de referência acrescentados, como apresentado na Figura 11~~Figura 11~~~~Figura 11~~. Esse formato de assinatura é utilizado em aplicações que necessitam verificar a assinatura digital a qualquer momento, permitindo a recuperação das informações necessárias a este procedimento. Além de fornecer referência para a garantia de irretratabilidade, permite também a validação da assinatura digital mesmo que ocorra o comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo de tempo sobre as referências tenha sido colocado antes do comprometimento da chave. A AD-RV permite múltiplas assinaturas.

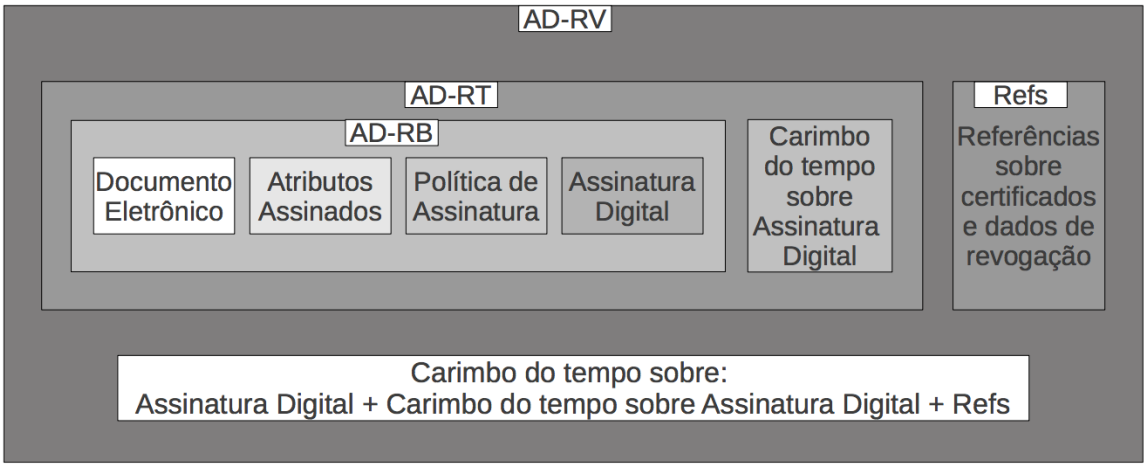


**Figura 11 – Assinatura Digital com Referências para Validação (Fonte: DOC-ICP-15.01 (ITI, 2012))**

d) **Assinatura Digital com Referências Completas (AD-RC)** – é formada por uma assinatura AD-RV com a adição dos valores dos certificados que compõem

a cadeia de certificação e as informações de revogação do certificado digital do signatário. Tal como a assinatura AD-RV, a assinatura AD-RC é indicada para situações nas quais é necessário a verificação completa da validade da assinatura digital a qualquer momento. A diferença entre AD-RV e AD-RC é que a AD-RC não precisa de recuperar informações necessárias para a verificação da assinatura digital, pois os dados estão autocontidos na assinatura. Logo, da mesma forma que a AD-RV, a AD-RC dá garantia de irretratabilidade e permite que se verifique a validade da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário, desde que o carimbo de tempo sobre as referências dos certificados tenha sido colocado antes do comprometimento. A AD-RC permite múltiplas assinaturas.

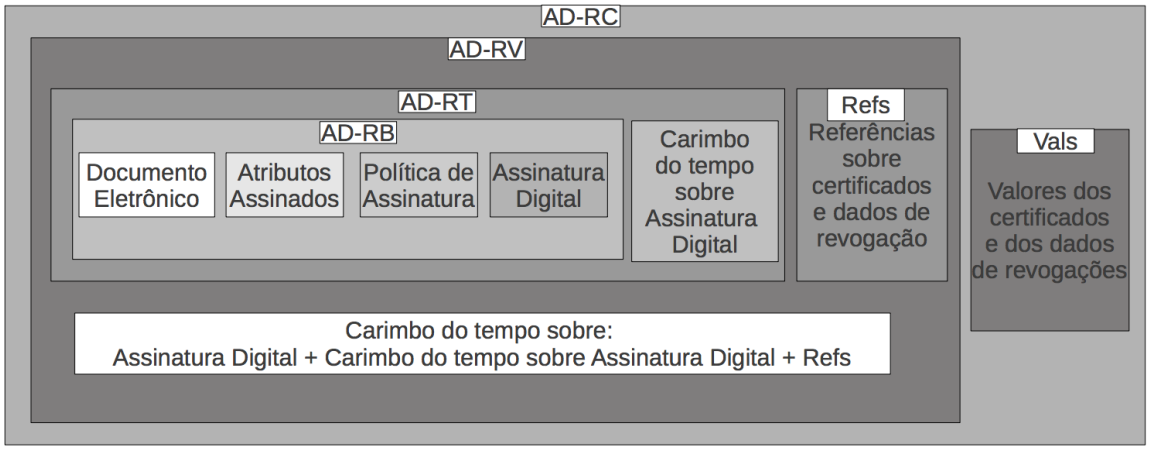


**Figura 12 – Assinatura Digital com Referências Completas (Fonte: DOC-ICP-15.01 (ITI, 2012))**

e) **Assinatura Digital com Referências para Arquivamento (AD-RA)** – é formada por uma assinatura AD-RV e os valores dos certificados que compõem a cadeia de certificação e as informações de revogação do certificado digital do signatário, sobre os quais é emitido um carimbo de tempo de arquivamento. Esse carimbo de tempo de arquivamento deve ser emitido por uma ACT credenciada na ICP-Brasil. A assinatura AD-RA é indicada para aplicações que necessitam realizar o arquivamento do conteúdo digital assinado por longos períodos. Deve-se considerar nesse caso a manutenção criptográfica como medida para fornecer proteção adicional contra a fragilidade dos algoritmos, funções e tamanho de chaves criptográficas ao longo dos anos. Logo, a manutenção criptográfica trata-se de emitir sucessivos carimbos de tempo de arquivamento periodicamente, com algoritmos funções e tamanho de chaves

considerados seguros no momento de sua geração, para garantir a segurança no arquivamento do conteúdo digital. A AD-RA garante a segurança quanto à irretratabilidade e permite a validação da assinatura digital mesmo que ocorra comprometimento da chave privada da AC que emitiu o certificado do signatário. A AD-RA permite múltiplas assinaturas.

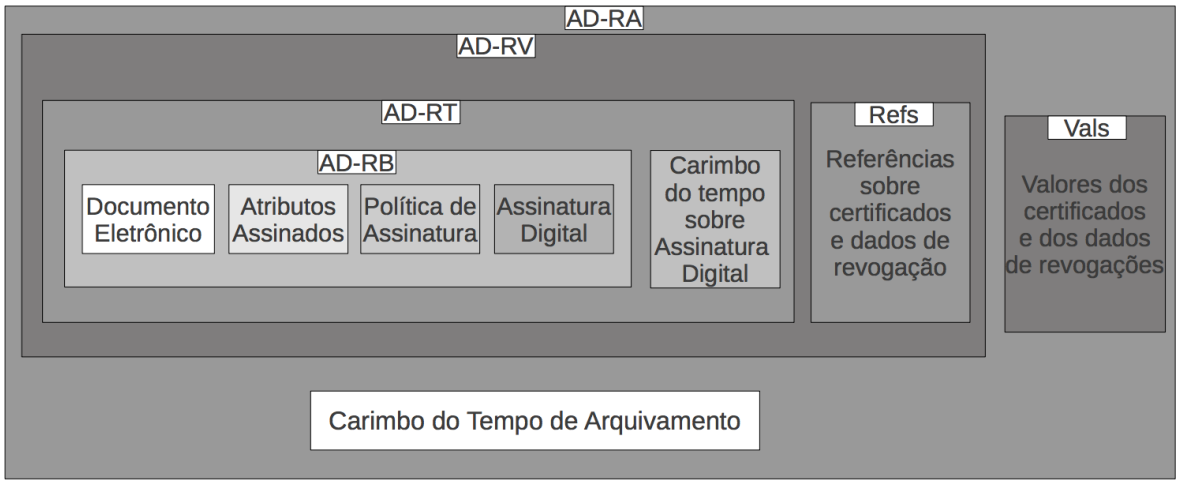


**Figura 13 – Assinatura Digital com Referências para Arquivamento (Fonte: DOC-ICP-15.01 (ITI, 2012))**

### 4.2.4 Perfil de assinatura digital

Os padrões CAdES e XAdES disponibilizam uma diversificada gama de atributos ou propriedades que permitem incorporar às assinaturas digitais informações com os mais diferentes objetivos. Esses atributos ou propriedades são os campos previstos pelos padrões que podem compor a assinatura digital. Uma vez que há grande número desses campos, é possível encontrar assinaturas digitais com atributos ou propriedades diferentes, o que dificulta o trabalho das entidades que tenham que lidar com tais assinaturas. Logo, há a necessidade de definir um subconjunto desses atributos ou propriedades para maximizar a questão da interoperabilidade das assinaturas digitais. Essa seleção de opções é chamada de perfil. Para a ICP-Brasil foi definido um perfil de assinatura para uso geral, para ambos padrões de assinatura, que sintetiza os principais atributos e propriedades a serem utilizados nas assinaturas digitais (ITI, 2012).

As tabelas a seguir apresentam os campos que compõem o perfil de assinatura para o padrão CAdES na ICP-Brasil. No padrão CAdES os campos da assinatura digital são chamados de atributos. Os atributos selecionados para o perfil de assinatura do padrão CAdES estão em conformidade com o documento ETSI TS 101 733 (ETSI, 2008). A Tabela 8~~Tabela 8~~Tabela 8 apresenta os atributos que devem ser assinados. A Tabela 9~~Tabela 9~~Tabela 9 apresenta os atributos que devem não ser assinados.

**Tabela 8 – Atributos assinados para assinaturas no formato CAdES**

| Atributo | Descrição |
|---|---|
| **id-aa-ets-contentTimestamp** | Atribui um carimbo de tempo contendo data e hora ao conteúdo dos dados assinados antes da assinatura |
| **id-aa-ets-signerAttr** | Especifica atributos adicionais do assinante (por exemplo, função, cargo etc.) |
| **id-aa-ets-signerLocation** | Especifica, por meio de uma mnemônica, o endereço do assinante em determinada área geográfica. |
| **id-signingTime** | Atributo de tempo que especifica o tempo em que o signatário afirma ter realizado o processo de assinatura |
| **id-contentType** | Indica o tipo de conteúdo assinado |
| **id-messageDigest** | Especifica uma síntese do *digest* da mensagem assinada. |
| **id-aa-signingCertificate** | Especifica as referências do certificado digital do assinante. |
| **id-aa-ets-sigPolicyId** | Especifica o identificador da política de assinatura. |

**Fontes:** DOC-ICP-15.02 – Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (ITI, 2012); ETSI TS 101 733 – CMS Advanced Eletronic Signatures (CAdES) (ETSI, 2008).

**Tabela 9 – Atributos não assinados para assinaturas no formato CAdES**

| Atributo | Descrição |
|---|---|
| **id-countersignature** | Especifica uma ou mais contra-assinaturas no documento. Usar contra-assinatura é escrever uma segunda assinatura de forma que a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento para a primeira assinatura já presente. |
| **id-aa-signatureTimeStampToken** | Especifica um carimbo de tempo calculado sobre o valor da assinatura para um assinante específico. |
| **id-aa-ets-certificateRefs** | Especifica a referência ao conjunto completo de certificados de AC que deve ser utilizada para validar a assinatura digital com validação completa de dados até (mas não incluindo) o certificado do assinante. |
| **id-aa-ets-revocationRefs** | Especifica a referência para as LCRs ou respostas OCSP que |

| | |
|---|---|
| | devem ser usadas para validar o signatário e os certificados da AC utilizados na validação da assinatura digital. |
| **id-aa-ets-attrCertificateRefs** | Especifica a referência ao conjunto completo de certificados de Autoridade de Atributo (AA) que deve ser utilizada para validar o certificado de atributo. |
| **id-aa-ets-attrRevocationRefs** | Especifica a referência ao conjunto completo de LCRs ou respostas OCSP que devem ser usadas para a validação do certificado de atributo. |
| **id-aa-ets-escTimeStamp** | Especifica a data e hora da assinatura eletrônica completa, com a finalidade de protegê-la de um possível comprometimento da chave da AC. |
| **id-aa-ets-certValues** | Contém os valores dos certificados que são referenciados no atributo CompleteCertificationReferences (id-aa-ets-certificateRefs). |
| **id-aa-ets-revocationValues** | Contém os valores das LCRs e respostas OCSP que são referenciados no atributo CompleteRevocationReferences (id-aa-ets-revocationRefs). |
| **id-aa-ets-archiveTimeStamp** | Especifica a data e hora de vários elementos dos dados assinados. Se os valores de certificados e LCRs não estiverem presentes, eles devem ser adicionados à assinatura eletrônica anteriormente para o cálculo do token de data e hora de arquivamento. |

**Fontes:** DOC-ICP-15.02 – Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (ITI, 2012); ETSI TS 101 733 – CMS Advanced Eletronic Signatures (CAdES) (ETSI, 2008).

Da mesma forma, as tabelas a seguir apresentam os campos que compõem o perfil de assinatura para o padrão XAdES na ICP-Brasil. No padrão XAdES os campos da assinatura digital são chamados de propriedades. As propriedades selecionadas para o perfil de assinatura do padrão XAdES estão em conformidade com o documento ETSI TS 101 903 (ETSI, 2004). A Tabela 8~~Tabela 8~~~~Tabela 8~~ apresenta as propriedades que devem ser assinadas. A Tabela 9~~Tabela 9~~~~Tabela 9~~10 apresenta as propriedades que não devem ser assinadas.

**Tabela 10 - Propriedades assinadas para assinaturas no formato XAdES**

| Propriedade | Descrição |
|---|---|
| **SignatureProductionPlace** | Especifica o local onde o signatário alega ter produzido a assinatura eletrônica. |
| **SignerRole** | Especifica o papel ou função do signatário na criação da assinatura. |

| | |
|---|---|
| **SigningTime** | Especifica a data e hora que o signatário alega ter realizado o processo de assinatura. |
| **AllDataObjectsTimeStamp** | Especifica a data e hora sobre todos os objetos de dados assinados. |
| **IndividualDataObjectsTimeStamp** | Especifica a data e hora sobre objetos de dados assinados selecionados. |
| **DataObjectFormat** | Especifica o formato de um objeto de dados assinado (quando assinaturas eletrônicas não são trocadas num contexto restrito) para permitir sua apresentação ou uso ao verificador (texto, som ou vídeo) exatamente da mesma maneira como pretendido pelo signatário. |
| **SigningCertificate** | Especifica uma referência inequívoca para o certificado do signatário, formada por seu identificador e o valor de *hash* do certificado. |
| **SignaturePolicyIdentifier** | Especifica de forma inequívoca a política de assinatura utilizada para produzir a assinatura eletrônica, o que assegura ao verificador a capacidade de usar a mesma política de assinatura durante o processo de verificação. |

**Fontes:** DOC-ICP-15.02 – Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (ITI, 2012); ETSI TS 101 903 – XML Advanced Eletronic Signatures (XAdES) (ETSI, 2004).

**Tabela 11 - Propriedades não assinadas para assinaturas no formato XAdES**

| Propriedade | Descrição |
|---|---|
| **CounterSignature** | Especifica uma ou mais contra-assinaturas no documento. |
| **SignatureTimeStamp** | Especifica o carimbo de tempo que atesta que a assinatura digital é válida. |
| **CompleteCertificateRefs** | Contém referências para os certificados da AC usados para validar a assinatura. |
| **CompleteRevocationRefs** | Contém referências para todo o conjunto de informações de revogação usadas para a verificação da assinatura eletrônica. |
| **AttributeCertificateRefs** | Contém as referências para todo o conjunto de certificados de Autoridade de Atributo (AA) que devem ser usados para validar um certificado de atributo. |
| **AttributeRevocationRefs** | Contém as referências para todo o conjunto de LCRs e |

| | |
|---|---|
| | respostas OCSP usadas para validar o certificado de atributo presente na assinatura. |
| **SigAndRefsTimeStamp** | Carimbo de tempo que cobre a assinatura digital e as referências para validação de dados. |
| **CertificateValues** | Contém os valores de certificados usados para validar a assinatura. |
| **RevocationValues** | Contém todo o conjunto de informação de revogação usada para a verificação da assinatura eletrônica. |
| **AttrAuthoritiesCertValues** | Contém os certificados de atributo usados para a validação da assinatura. |
| **AttributeRevocationValues** | Contém os dados de revogação usados para a validação do certificado de atributo. |
| **ArchiveTimeStamp** | Carimbo de tempo que cobre a assinatura e outras propriedades requeridas para validação de longo tempo. |

**Fontes:** DOC-ICP-15.02 – Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (ITI, 2012); ETSI TS 101 903 – XML Advanced Eletronic Signatures (XAdES) (ETSI, 2004).

### 4.2.5 Políticas de assinatura digital

Uma política de assinatura consiste num conjunto de regras que formaliza os processos de criação e verificação de uma assinatura digital e define as bases para que a assinatura digital possa ser considerada válida (ITI, 2012). Ou seja, uma política de assinatura tem por objetivo criar um padrão para a criação e verificação da assinatura digital, garantindo a interoperabilidade necessária para o respectivo processo de validação. Logo, quando uma assinatura digital é criada, esta deve estar de acordo com uma política de assinatura, de modo que o verificador adotará a mesma política para efetuar a validação. A vantagem da utilização de políticas de assinatura digital é que torna claro e dá pleno conhecimento às partes envolvidas quanto aos requisitos para geração e verificação das assinaturas, além de formalizar as condições de validade de um documento assinado digitalmente.

No âmbito da ICP-Brasil, a parte que recebe os documentos assinados determina quais políticas de assinaturas podem ser aceitas no seu processo de negócios. O ITI também orienta quanto ao formato e a estrutura usada para a criação de uma política de assinatura, bem como define 10 políticas de assinatura padrão para facilitar o seu uso a usuários finais (ITI, 2012). Tais políticas foram criadas a partir do cruzamento do

perfil de uso geral para assinaturas digitais na ICP-Brasil (ITI, 2012), com os cinco formatos de assinatura digital da ICP-Brasil, derivados dos padrões CAdES e XAdES. Os detalhes das políticas de assinatura padrão criadas pela ITI podem ser observadas no documento DOC-ICP-15.03 - Requisitos das Políticas de Assinatura Digital na ICP-Brasil (ITI, 2012).

É importante ressaltar que, além das 10 políticas definidas pela ITI na ICP-Brasil, podem ser criadas novas Políticas de Assinatura (PA). Uma PA deve ser aprovada pela AC-Raiz da ICP-Brasil, de forma que ao aprovar uma PA, a AC-Raiz publica a PA em seu repositório *Web*, gera e assina digitalmente uma Lista de Políticas de Assinatura Aprovadas (LPA), contendo os dados resumidos sobre a PA. Uma Política de Assinatura passa pelas seguintes etapas de vida, a saber.

- Criação – etapa de definição da PA.
- Aprovação – as PAs aprovadas pela AC-Raiz devem ser submetidas a avaliação prévia do CG da ICP-Brasil.
- Publicação – é a publicação da PA no repositório *Web* da AC-Raiz da ICP-Brasil, sendo também utilizada para a criação da LPA. As LPAs são assinadas e publicadas pela ICP-Brasil, de forma segura, no endereço *Web* *http://www.iti.gov.br/twiki/bin/view/Certificacao/artefatos* , atualizadas a cada 90 dias. As LPAs são assinadas com assinaturas digitais ICP-Brasil, utilizando PKCS#7 para CAdES e XMLdSIG para XAdES, e, codificadas em linguagem de máquina (ASN.1 e XML), trazendo para cada PA aprovada o respectivo nome, breve descrição da política, período de validade, data de revogação (se for o caso), URLs da PA em formato textual e processável por máquina (XML/DER), resumos criptográficos dos arquivos da PA e a assinatura digital.
- Expiração – quando a PA tem o período de validade esgotado.
- Prorrogação de validade – ocorre desde que não tenham sido encontradas fragilidades na PA, as quais não sejam tecnicamente aceitáveis para o novo período de validade. A prorrogação é feita por meio de publicação de uma nova versão da PA, com os dados de data de publicação e período de validade alterados.
- Revogação – realizada a qualquer tempo pela AC Raiz da ICP-Brasil.

## 4.3 Homologação de sistemas e equipamentos de certificação digital

A ICP-Brasil possui normas que definem o processo de homologação de sistemas e equipamentos de certificação digital com o objetivo de garantir a interoperabilidade desse sistemas e equipamentos, bem como a confiabilidade dos recursos de segurança da informação por eles utilizados (ITI, 2012). Os sistemas e equipamentos sujeitos ao processo de homologação são citados a seguir:

- Sistemas de assinatura eletrônica, sistemas de autenticação de assinaturas eletrônicas, sistemas de sigilo de dados, sistemas de carimbo de tempo (*Time-Stamping*) e sistemas de sincronismo de tempo, bem como, sistemas de autoridades certificadoras, sistemas de autoridades de registro, ou quaisquer outros que façam uso daqueles sistemas na forma de subrotinas ou sub-funções.
- Cartões Inteligentes (*Smart Cards*), leitoras de cartões inteligentes, *Tokens* criptográficos, ou quaisquer outras mídias armazenadoras de certificados digitais e suas correspondentes leitoras utilizadas em certificação digital.
- Módulos de Segurança Criptográfica - MSC (*Hardware Security Modules - HSM*), equipamentos de sincronismo de tempo, equipamentos de carimbo de tempo, ou quaisquer outros dispositivos seguros de criação ou verificação de assinaturas eletrônicas utilizados em certificação digital.

O ITI, por meio da AC-Raiz, conduz os processos de homologação de sistemas e equipamentos de certificação no âmbito da ICP-Brasil. O instituto é responsável por emitir normas técnicas e suplementares com os requisitos técnicos e procedimentais a serem observados nos respectivos processos de homologação. Para desempenhar sua atribuição na condução dos processos de homologação de sistemas de certificação digital, pode credenciar instituições para atuarem como seus LEA (ITI, 2012). Da mesma forma, para desempenhar sua atribuição na condução de processos de homologação de equipamentos de certificação digital, o ITI se valerá do processo de avaliação de conformidade no Programa de Avaliação da Conformidade para Equipamentos de Certificação Digital Padrão ICP-Brasil, utilizando-se da infraestrutura do Sistema Brasileiro de Avaliação de Conformidade (SBAC) operacionalizada pelo INMETRO.

De forma sucinta, pode-se enumerar como é dado o processo de homologação (ITI,

2012), saber.

- A parte interessada em pleitear a homologação de um dado sistema ou equipamento de certificação digital no âmbito da ICP-Brasil deve entregar o respectivo Laudo ou Certificado de Conformidade do sistema ou equipamento, acompanhado da devida documentação prevista nas normas. O Laudo ou Certificado de Conformidade é obtido junto ao LEA credenciado ou Organismo de Certificação de Produto (OCP)[3].
- Instruído o processo de homologação, o ITI procederá sua análise e tomará a decisão de deferimento ou não quanto à homologação do sistema ou equipamento correspondente.
- Na hipótese de deferimento, a parte interessada estará autorizada a usar o Selo de Homologação, acompanhado do correspondente número de identificação do sistema ou equipamento homologado.
- O prazo de validade da homologação de sistemas e equipamentos de certificação digital é indeterminado, desde que mantidas as características originais do sistema ou equipamento avaliado. Qualquer alteração, ameaça ou atualização em sistemas ou equipamentos já homologados deve ensejar novo processo de avaliação de conformidade e, consequentemente, a realização de nova homologação.

Existem 3 níveis de segurança de homologação no âmbito da ICP-Brasil, detalhados a seguir (ITI, 2010).

- **NSH 1** – aplicável quando se necessita de confiança na operação correta do sistema ou equipamento, porém sua utilização está prevista para ocorrer em ambiente em que as ameaças à segurança estejam bem controladas e a ocorrência de eventuais problemas de interoperabilidade não é visto como fator importante. No NSH 1 a avaliação é feita com profundidade básica, a partir do depósito de amostras do objeto de homologação e baseada no fornecimento, pela parte interessada, de documentação básica sobre o

[3] Organismo de Certificação de Produto – OCP – é a organização acreditada pelo INMETRO que conduz o processo de Avaliação de Conformidade, no âmbito SBAC, e emite o Certificado de Conformidade de produtos, com base em normas nacionais, regionais e internacionais ou em requisitos técnicos expedidos por agente regulador do setor que se aplica o Programa de Avaliação de Conformidade (PAC).

objeto de homologação. Consiste de testes de funcionalidades, de acordo com as especificações da parte interessada e da avaliação da documentação fornecida. Para este nível de avaliação, não é necessário o depósito de códigos-fonte.

- **NSH 2** – aplicável quando se necessita de confiança na operação correta do sistema ou equipamento e sua utilização está prevista para ocorrer em ambiente em que as ameaças à segurança e a ocorrência de eventuais problemas de interoperabilidade são vistos como relevantes. No NSH 2, a avaliação é feita com profundidade moderada, a partir do depósito de amostras do objeto de homologação e baseada no fornecimento, pela parte interessada, de informações de projeto, resultados de testes já realizados e depósito de partes de códigos-fonte.
- **NSH 3** – aplicável quando se necessita de confiança na operação correta do sistema ou equipamento e sua utilização está prevista para ocorrer em ambiente em que as ameaças à segurança ou problemas de interoperabilidade são vistos como críticos. No NSH 3, a avaliação é feita com profundidade alta, a partir do depósito de amostras do objeto de homologação e baseada no fornecimento, pela parte interessada, de informações mais detalhadas de projeto, resultados de testes já realizados, depósito de partes de códigos-fonte e comprovação da utilização de práticas seguras no seu desenvolvimento e produção.

### 4.3.1 Homologação de cartões criptográficos (*smartcards*)

A homologação de cartões criptográficos (*smartcards*) ICP-Brasil consiste na verificação de conformidade com os requisitos técnicos regulamentados pela ICP-Brasil (ITI, 2014). Entende-se por cartão criptográfico ICP um cartão de circuito integrado (*Integrated Circuit Card* – ICC) com capacidade de geração e armazenamento de chaves criptográficas assimétricas e processamento criptográfico assimétrico e armazenamento de certificados digitais voltados para utilização em uma Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Os requisitos técnicos são aplicados a todos os elementos/componentes (de

*software* e *hardware*) envolvidos diretamente nas operações que envolvem manipulação dos certificados ICP-Brasil contidos no *smartcard*, aplicando-se aos seguintes componentes do módulo criptográfico:

- componentes eletrônicos (*hardware*);
- sistema operacional embarcado (*Card Operating System* – COS);
- funcionalidade PKI;
- biblioteca de *software* disponível para comunicação com o cartão criptográfico ICP-Brasil (*middleware*).

O Manual de Condutas Técnicas 1 da ITI, em seus volumes 1 (ITI, 2014) e 2 (ITI, 2014) contém todo o detalhamento dos processos envolvidos para a homologação dos *smartcards* ICP-Brasil. Em suma, os requisitos de segurança que devem ser atendidos pelos *smartcards* ICP foram elaborados com base nos requisitos de segurança FIPS 140-2 nível 2 (DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL) , 2001), de algoritmos obrigatórios na ICP-Brasil (ITI, 2014), de controle de acesso e de identificação de *hardware*, *software* e *firmware*.

Algumas considerações são realizadas no Manual de Condutas Técnicas 1 Volume 1. Uma consideração importante é a questão da autenticação, na qual se prevê a definição dos papéis de acesso que devem ser suportados no *smartcard* e sua relação com os serviços criptográficos, como apresentado na Tabela 12, bem como serviços disponíveis sem a necessidade de autenticação.

**Tabela 12 – Papéis de acesso e serviços criptográficos**

| Serviço Criptográfico | Usuário | Oficial de Segurança | Não-Autenticado |
|---|---|---|---|
| Gerar chave criptográfica assimétrica | X | | |
| Excluir chave criptográfica assimétrica | X | | |
| Recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como: algoritmo e atributos das chaves criptográficas. | X | | |
| Importar cadeia de certificação para o módulo criptográfico | X | | |
| Importar certificado digital para o módulo | X | | |

| | | | |
|---|---|---|---|
| criptográfico | | | |
| Importar certificado digital de atributo para o módulo criptográfico | X | | |
| Exportar chave criptográfica assimétrica pública do módulo criptográfico | X | | X |
| Exportar certificado digital do módulo criptográfico | X | | X |
| Exportar certificado digital de atributo do módulo criptográfico | X | | X |
| Exportar cadeia de certificação do módulo criptográfico | X | | X |
| Reinicializar o papel de acesso “Usuário” | | X | |
| Desbloquear o papel de acesso “Usuário” | | X | |
| Alterar o PIN corrente do papel de acesso “Usuário” | X | X | |
| Alterar o PUK corrente do papel de acesso “Oficial de Segurança” | | X | |

**Fonte:** Manual de Condutas Técnicas 1 – Volume 1 (ITI, 2014).

O método de autenticação especificado é baseado em PIN (*Personal Identification Number*) e PUK (PIN *Unlock Key*). O PIN é um código alfanumérico, que pode ter caracteres especiais, *case sensitive*, usado como chave para autenticar o usuário no sistema. O PIN é utilizado como mecanismo de identificação e autenticação do papel de acesso *Usuári*o e pode ser substituído por autenticação biométrica.

O PUK também é um código alfanumérico, que pode ter caracteres especiais, *case sensitive*, usado como chave para habilitar o desbloqueio e/ou alteração do PIN. O PUK é considerado como se fosse o PIN do papel Oficial de Segurança.

Em termos de qualidade dos valores PIN e PUK, é requisitado que a probabilidade de que uma única tentativa aleatória de autenticação com senha tenha sucesso inferior a 1 em 1.000.000. Se for empregada autenticação por biometria, a especificação mínima de precisão deve estar em conformidade com o NIST SP 800-76-2:2013 do padrão FIPS 201-2:2013, além de seguir os requisitos de autenticação por métodos biométricos para um cartão criptográfico conforme definido no padrão ISO/IEC 7816-11:2004.

O PIN pode ter o seu valor alterado pelo módulo criptográfico com autenticação do

PIN corrente ou do PUK. Por questões de segurança, o PIN deve ser bloqueado pelo módulo criptográfico após 5 tentativas malsucedidas, sendo desbloqueado apenas com autenticação do PUK. Também é previsto que o módulo criptográfico deve forçar a alteração do PIN padrão no primeiro acesso.

O módulo criptográfico deve ser reinicializado mediante a inserção correta do PUK pela entidade usuária externa, de forma que ao ser reinicializado seja eliminado o valor do PIN e de todas as chaves criptográficas secretas associadas ao papel de acesso Usuário, ficando disponível para reutilização.

O PUK também pode ser alterado por meio da inserção correta do PUK atual. Tal como o PIN, se houver 5 tentativas malsucedidas na inserção do PUK, este deve ser bloqueado pelo módulo criptográfico.

O uso de chaves simétricas e assimétricas privadas só deve ser habilitado se houver autenticação bem-sucedida do papel Usuário. Observa-se que a autenticação requerida pelas normas da ICP-Brasil são basicamente o PIN/PUK e autenticação biométrica, no intuito apenas de identificar e autenticar o usuário externo. Nota-se a ausência de requisitos para a autenticação do provedor de serviço, como o emprego de autenticação passiva ou ativa, empregada em *smartcards* destinados à função de eID (International Civil Aviation Organization, 2006).

As normas estudadas não detalham o protocolo de autenticação do chip. Portanto, a análise de problemas comuns de privacidade em protocolos de autenticação, como o uso de *nonce* semântico, não foi possível.

Outro aspecto relevante na homologação dos cartões criptográficos é quanto ao aspecto da interoperabilidade. Nesse aspecto, os *smartcards* devem seguir as recomendações da família de normas ISO/IEC 7816. Por exemplo, na busca de interoperabilidade entre provedores de serviço, leitoras, módulos criptográficos e aplicações, são definidos um conjunto mínimo de comandos da APDU[4] (*Application Protocol Data Unit*), conforme apresentado na Tabela 13.

[4] Uma APDU (*Application Protocol Data Unit*) contém um comando ou uma resposta trocada com o módulo criptográfico. Uma APDU de comando consiste em duas partes: um cabeçalho de 4 bytes e um corpo de tamanho variável. Uma APDU de resposta também consistem em duas partes: um corpo de tamanho variável e um anexo obrigatório (*trailer*) de 2 bytes [32].

**Tabela 13 – Conjunto mínimo de comandos para módulos criptográficos**

| Comando | Instrução | Parte da ISO/IEC 7816 | Seção |
|---|---|---|---|
| APPEND RECORD | E2 | 4 | 7.3.6 |
| CHANGE REFERENCE DATA | 24 | 4 | 7.5.7 |
| CREATE FILE | E0 | 9 | 6.1 |
| DELETE FILE | E4 | 9 | 6.2 |
| EXTERNAL (/ MUTUAL) AUTHENTICATE | 82 | 4 | 7.5.4 |
| GENERATE ASYMMETRIC KEY PAIR | 46 | 8 | 5.1 |
| GET CHALLENGE | 84 | 4 | 7.5.3 |
| GET DATA | CA | 4 | 7.4.2 |
| GET RESPONSE | C0 | 4 | 7.6.1 |
| MANAGE CHANNEL | 70 | 4 | 7.1.2 |
| MANAGE SECURITY ENVIRONMENT | 22 | 4 | 7.5.11 |
| PERFORM SECURITY OPERATION | 2A | 8 | 5.2 |
| PUT DATA | DA | 4 | 7.4.3 |
| READ BINARY | B0 | 4 | 7.2.3 |
| READ RECORD | B2 | 4 | 7.3.3 |
| RESET RETRY COUNTER | 2C | 4 | 7.5.10 |
| SELECT | A4 | 4 | 7.1.1 |
| UPDATE BINARY | D6 | 4 | 7.2.5 |

| | | | |
|---|---|---|---|
| UPDATE RECORD | DC | 4 | 7.3.5 |
| VERIFY | 20 | 4 | 7.5.6 |

**Fonte:** Manual de Condutas Técnicas 1 – Volume 1 (ITI, 2014).

Os *smartcards* devem ter dimensões compatíveis com as definidas no padrão ISO/IEC 7810 e atender aos requisitos dos padrões ISO/IEC 7816-1:2003 e ISO/IEC 7816-2:2007 (ITI, 2014). Tais *smartcards* sujeitos à homologação podem ser com contato ou sem contato. Os smartcards com contato devem atender aos requisitos de interface elétrica e de protocolos de transmissão definidos no padrão ISO/IEC 7816-3:2006 (ITI, 2014). Já os *smartcards* sem contato devem atender os requisitos da família de padrões ISO/IEC 14443 (ITI, 2014).

A Tabela 14 apresenta os cartões criptográficos homologados pela ICP-Brasil, todos com nível de segurança NSH 1.

**Tabela 14 – Cartões criptográficos (*smartcards*) homologados pela ICP-Brasil**

| Modelo | Fornecedor | Versão do Firmware | Chipset |
|---|---|---|---|
| SCE 4.0 | GIESECKE & DEVRIENT | CID0BJC_ISF-CLX800-005V203 | Infineon SLE66CLX800PE |
| SCE 3.2 72k | GIESECKE & DEVRIENT | CPDHxJC_RSEFI-025CC073V100 | NXP P5CC073V0B |
| SmartCafé Expert 5.0 | GD Burti S/A (GIESECKE) | CPDIxJC_RSCE5.0-CD080_V100 | NXP P5CD080V0C |
| MULTIAPP ID V2.1 | GEMALTO | MultiApp ID V2.1 – Patch V1.3 | NXP P5CC081 |
| IDCORE 30 | GEMALTO | IDCore30 Build 1.16 | INFINEON SLE78CFX3009P |
| TOP DL V2 | GEMALTO | M1005011 | - |
| MULTIAPP ID V2.1 - AET | GEMALTO | MultiApp ID V2.1 – Patch V1.3 | NXP P5CC081 |
| PKI STANDARD S1 | INTELCAV | JCOP 2.4.2 R2 Mask ID 59 PatchID 3 | NXP J2D081 |
| PKI STANDARD S2 | INTELCAV Cartões LTDA | v0204.0355.0702 | ST ST23YR80 |
| YPSID S3-IDEALCITIZ | Morpho Cards do Brasil S/A | v1.6.0 | ST ST23YR80 |
| YPSID S2 | Morpho Cards do Brasil S/A | 02000202-FFFFFFF | INSIDE AT90SC25672RCT-USB |
| BANRISUL CT MÚLTIPLO | Banco do Estado do Rio Grande do Sul | MULTOS 4.2 MC1-36K-61 (R1) | Infineon SLE66CX366PE |

| | | | |
|---|---|---|---|
| ID-ONE Cosmo v7.0.1 | OBERTHUR TECHNOLOGIES | v1.21 | AT90SC28872RC |
| DESINEO ICP D72 FXR1 | GEMALTO | IDCore30 Build 1.16 | INFINEON SLE78CFX3009P |
| SCE 3.2 80k | GIESECKE & DEVRIENT | CPDIXJC_RSEFI-025CD080V100 | NXP P5CD080V0B |
| JCOP 2.4.2 R2 | M.I.MONTREAL | J2D081 | - |
| PKI IDFLEX V1 | Valid S.A | IDPROTECT V6 010B.0352.0005 | AT90SC28872RCU |

**Fonte:** Portal ITI - Processo de Homologação de *Hardware* (ITI, n.d.).

### 4.3.2 Homologação de leitoras de *smartcards*

Os requisitos para a homologação de leitoras de *smartcards* no âmbito da ICP-Brasil são detalhados no Manual de Condutas Técnicas 2, em seus volumes 1 (ITI, 2007) e 2 (ITI, 2007). A leitora de *smartcard*, ou cartão inteligente, consiste num *hardware* instalado no computador que utiliza uma conexão física do tipo serial (RS-232) ou USB, servindo como ponte para interação entre o *smartcard* e uma aplicação.

A homologação das leitoras de *smartcards* se aplicam aos seguintes componentes:

- componentes eletrônicos;
- componentes mecânicos;
- *firmware* e *softwares* embarcados;
- componentes de entrada de dados (quando suportado), por exemplo, PIN pad e dispositivos biométricos;
- interface de comunicação;
- *driver* (*software* de controle) da leitora.

No Manual de Condutas Técnicas 2, Volume 1, há recomendações de segurança, a quais se referem a mecanismos de segurança adicionais que podem estar implementados nas leitoras de *smartcards* com a finalidade de proteger dados críticos de identificação e autenticação da entidade usuária externa pela leitora. Tais mecanismos de segurança adicionais podem ser:

- teclado numérico isolado (PIN pad) para a entrada de dados numéricos que serão enviados ao *smartcard* para fins de identificação e autenticação da entidade usuária externa;

- teclado alfanumérico isolado para a entrada de dados alfanuméricos que serão enviados ao *smartcard* para fins de identificação e autenticação da entidade usuária externa;
- dispositivo biométrico isolado para fins de identificação e autenticação da entidade usuária externa no *smartcard*;
- tela (*display*) isolada para a apresentação de dados críticos de segurança que são gerados pelo *smartcard*.

No aspecto de interoperabilidade, os requisitos que devem ser atendidos pelas leitoras de cartão inteligente devem satisfazer aos padrões ISO/IEC 7816-2 e PC/SC versão 1.0. As propriedades elétricas da leitora e os protocolos de transmissão de dados entre a leitora e o *smartcard* devem atender o padrão ISO/IEC 7816-3.

Em termos de interfaces para entrada e saída de dados (I/O) em um PC, as leitoras devem suportar uma das seguintes interfaces com o seu respectivo *driver*, a saber.

- PS/2 (interface integrada ao teclado).
- RS-232 (interface serial).
- Placa com interface adaptada.
- Interface com porta paralela.
- Interface de PC baseada em cartão externo (exemplo: PCMCIA de *laptops*);
- Interface SCSI.
- Interface USB (é recomendada a implementação do padrão USB CCID Revisão 1.1).

Na Tabela 15 são apresentadas as leitoras de cartões inteligentes homologadas pela ICP-Brasil até o presente momento e um levantamento do respectivo custo no mercado levantado em *sites* da *Internet* em Agosto de 2015.

**Tabela 15 – Leitoras/Gravadoras de *smartcards* homologados pela ICP-Brasil**

| Modelo | Firmware | Fornecedor | Custo | Ref. custo |
|---|---|---|---|---|
| DP 905 | v1.02 / B56 | Vasco Seg. de Dados Brasil LTDA | ? | - |
| ROCKEY 301 | V3.0 | Feitian Technologies Co.,Ltd | ? | - |
| PC USB-TR | GemCore Twin Pro | GEMALTO | R$59,90 | http://goo.gl/6JCQLt |
| Smartnonus | CAS-EMV101U-009 | D.O. BRASIL IND. E COMÉRCIO | R$63,00 | http://goo.gl/7DsgwF |

| | | | | |
|---|---|---|---|---|
| SCR3310 V2.0 RD1-X | v3.04 | CIS Eletrônica Ind. e Comércio | R$54,00 | http://goo.gl/eM4imK |
| PertoSmart - Serial | - | PERTO S.A | R$84,71 | - |
| PertoSmart EMV - USB | - | PERTO S.A | R$84,71 | http://goo.gl/ePS99A |

**Fonte:** Portal ITI - Processo de Homologação de *Hardware* (ITI, n.d.).

### 4.3.3 Homologação de módulos de segurança criptográfica

Módulo de segurança criptográfica (MSC), também conhecida como *Hardware Security Modules* (HSM), corresponde a um servidor ou a placa auxiliar criptográfica fisicamente segura, resistente à violação, que fornece funcionalidades criptográficas com capacidade de geração e armazenamento de chaves criptográficas simétricas e assimétricas voltadas para utilização em uma infraestrutura de chaves públicas (ITI, 2007).

A ITI homologa HSMs com o intuito de garantir a interoperabilidade e operação segura do serviço criptográfico ICP. O escopo dos requisitos técnicos e da avaliação de HSM abrange ao seguinte:

- componentes do módulo criptográfico:
  - componentes eletrônicos;
  - *firmware* e *softwares* embarcados;
  - interface de comunicação;
- mecanismos de segurança física;
- mecanismos de controle de acesso;
- aderência a interfaces de interoperabilidade específicas, como o PKCS#11, CryptoAPI, JCE, OpenSSL ou outra API proprietária.

De forma geral, os requisitos de segurança avaliados em dado HSM são derivados do padrão americano FIPS 140-2 (DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL) , 2001), a qual abrange diferentes áreas de atuação relacionadas ao projeto e implementação de um HSM. Tomando-se as funções criptográficas que devem ser suportadas pelo HSM, é requerido:

- algoritmos simétricos para criptografia de dados: DES, 3-DES e AES (128 bits) nos modos de operação ECB e CBC. Também recomenda-se AES com chaves de 192 e 256 bits.
- algoritmos assimétricos para autenticação de entidades: RSA com tamanho mínimo de chave de 1024 bits. Recomenda-se também DSA com chaves de comprimento maior que 512 bits, para autenticação e assinatura de dados.
- funções *hash*: SHA-1 e SHA-256. Recomenda-se também o suporte às funções SHA-224, SHA-384 e SHA-512.
- de forma opcional, sugere-se que o HSM possa suportar para autenticação e integridade o CBC-MAC com 3-DES ou AES, HMAC, CMAC com 3-DES ou AES e MAC-CCM com 3-DES ou AES.

Os requisitos para a homologação são extensos e detalhados no Manual de Condutas Técnicas 7, em seus volumes 1 (ITI, 2007) e volume 2 (ITI, 2007). A Tabela 16 apresenta os HSMs homologados pela ICP-Brasil.

**Tabela 16 – HSMs homologados pela ICP-Brasil**

| Modelo | Firmware | Algoritmos suportados | Nível de Segurança | Fornecedor |
|---|---|---|---|---|
| ASI-HSM AHX4-NSF2 R2 | v.2.2.2 | RSA 8192, ECDSA BRAINPOOL 256 e 512, | NSH-3 | Kryptus Segurança da Informação Ltda. |
| LUNA SA 5 | v6.10.2 | - | NSH-2 | SAFENET INC |
| LUNA SA 4 | V4.8.7 | DES, 3DES, SHA1, SHA 224, SHA256, SHA384, SHA 512, RSA, AES, DSA, HMAC, | NSH-2 | SAFENET INC |
| nShield Connect 6000 | 2.50.16 | DES, 3DES, SHA-1, SHA-256, SHA-224, SHA-384, SHA-512, RSA, AES, DSA, ECDSA, HMAC | NSH-2 | Thales e-Security Inc |
| nShield Connect 500 | 2.50.16 | DES, 3DES, SHA-1, SHA-256, SHA-224, SHA-384, SHA-512, RSA, AES, DSA, ECDSA, HMAC | NSH-2 | Thales e-Security |

| | | | | |
|---|---|---|---|---|
| HSM Dínamo XP v.2.0.0.0 | 2.0.0.0 | - | NSH-3 | True Access Consulting S.A. |
| HSM Dínamo v.2.0.0.0 | 2.0.0.0 | - | NSH-3 | True Access Consulting S.A. |
| ASI-HSM AHX4 NSF2 R1 | v2.2 | RSA 4096, ECDSA 256 e ECDSA 521 | NSH-3 | RNP |

**Fonte:** Portal ITI - Processo de Homologação de *Hardware* (ITI, n.d.).

## *4.4 Middleware*

*Middleware* é o termo utilizado para designar um código de *software* que atua como um mediador entre dois programas ou *softwares* existentes e independentes (Teleco, n.d.). Há exemplos de *middleware* em sistemas para TV digital, servidores *Web*, servidores de aplicação, etc. Em todos os casos, o *middleware* tem como função trazer a independência dos *softwares* que são mediados, garantindo assim a interoperabilidade dos sistemas.

Para os processos de certificação digital, a *middleware* estabelece mediações entre sistemas operacionais, *softwares* e aplicações. Mais especificadamente, o *middleware* é necessário para mediar a conversão dos comandos da interface de aplicação, o software instalado em um PC, para o *chip* do *smartcard*, o qual usa interface de comandos APDU. A *middleware* é o *software* que atua entre o sistema operacional e o *smartcard*.

Nota-se no âmbito da ICP-Brasil uma certa preocupação relativa ao *middleware*. A qual se deve a vários fatores, entre eles o fato de que os fabricantes passaram a usar comandos otimizados em termos de funções dos *chips*, para evitar o acesso às aplicações por competidores. Adicionalmente, os padrões existentes de comandos não foram suficientes para garantir uma interoperabilidade entre fornecedores de *chip*s e de aplicações, e o legado do investimento em certificação de segurança se tornou um obstáculo a uma convergência de padrão de comandos. Por exemplo, nos cartões emitidos pelo ITI e projeto piloto do RIC em 2012, o acesso a informação da lista de comandos APDU por parte dos desenvolvedores dependia de negociação com o desenvolvedor da *middleware*, uma vez que este se tratava de um *middleware* proprietária. Diante de tal cenário, percebe-se a intenção da ITI em apoiar o desenvolvimento de *middleware* ou emprego de uma *middleware* com código aberto, o

que de fato é mais recomendado.

Em termos de regulamentação, o ITI define algumas regras específicas para a *middleware*. Tais regras são relacionadas no Manual de Condutas Técnicas 1, o qual trata da homologação de *smartcards.* Na ICP-Brasil, o *middleware* deve ser compatível com o *smartcard* com chip utilizando o padrão ISO-7816, o que de certa forma garante a segurança da chave privada que é gerada e armazenada no *chip*, sem nunca usar a memória volátil do sistema, porém não possibilita por completo a interoperabilidade necessária. Abaixo são relacionados alguns requisitos associados ao *middleware* (ITI, 2014).

- O conjunto mínimo de comandos APDU que o *smartcard* deve atender, e, consequentemente o *middleware*, está relacionado na Tabela 13.
- A *middleware* nunca deve manter o código PUK armazenado em cache (armazenamento temporário em memória).
- Sempre que realizar cache, o *middleware* deve manter o valor do PIN de forma protegida (valor do PIN disponível apenas no momento de seu uso) contra observação direta. Uma vez em cache, o valor do PIN deve ser eliminado sempre que a alimentação elétrica do módulo criptográfico for retirada, sempre que a aplicação de usuário associada ou conectada ao módulo for encerrada, e, sempre que o TTL (*Time To Live* – tempo de duração máxima do PIN no cache) for expirado.
- A eliminação do código PIN presente no cache deve ser realizada com sobrescrita de seu valor.
- O *middleware* deve ser capaz de:
    - gerar chave criptográfica assimétrica no módulo criptográfico;
    - excluir chave criptográfica assimétrica;
    - recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como: algoritmo e atributos das chaves criptográficas;
    - importar cadeia de certificação, certificado digital e certificado digital de atributo para o módulo criptográfico;
    - exportar chave criptográfica assimétrica pública, certificado digital, certificado digital de atributo e cadeia de certificação do módulo criptográfico;
    - possibilitar a configuração segura de chaves simétricas, chaves

assimétricas privadas e parâmetros críticos de segurança de tal forma a estarem protegidas contra leitura, modificação, utilização e substituição não autorizada;

- possibilitar a configuração segura de chaves assimétricas públicas de tal forma a estarem protegidas contra modificação e substituição não autorizada;

- propagar automaticamente os certificados digitais contidos em um cartão criptográfico para um repositório de certificados digitais que pode ser lido por aplicações de usuários (ex.: *browsers*, *softwares* de assinatura digital, etc.). De forma complementar, ao propagar automaticamente certificados digitais para um repositório, o middleware deve prover rotinas ou funcionalidades adicionais necessárias para a interação entre aplicação de usuário e cartão criptográfico e que sejam compatíveis com o sistema operacional alvo da avaliação.

Embora haja a existência das regras relativas ao *middleware* na normatização do ITI, o que é homologado no referido documento é o *smartcard* e não o *middleware*. Dessa forma, a normatização abre brecha para que possa existir *middleware* proprietário fechado, sem a possibilidade de interação ou desenvolvimento de aplicações por desenvolvedores. Por exemplo, até pouco tempo o único *middleware* disponível na ICP-Brasil era o Safesign, somente para o sistema operacional Windows e não havia publicidade do manual de comando APDU.

Percebe-se alguns esforços do ITI para o desenvolvimento de *middleware* em código aberto. Em outubro de 2006, o ITI e o Serpro assinaram, na França, o termo de adesão ao Consórcio ObjectWeb, um projeto que reúne 74 entidades dos setores público e privado, fornecedores da área de Tecnologia da Informação, institutos de pesquisa e usuários com a missão de desenvolver ferramentas de middleware em software livre (ITI, 2006). Em 2012 foi firmado um convênio entre o ITI e a USP para o desenvolvimento de *middleware* visando ampliar as possibilidades da utilização de certificados digitais para sistemas operacionais diversos com independência (ITI, 2012). Porém, não há relatos de avanço quanto ao desenvolvimento de *middleware* após a efetivação do convênio mencionado.

## 4.5 Uso de pseudônimos nos certificados digitais

A utilização de pseudônimos é prevista no padrão ITU X.509 e tem o intuito de

reduzir o comprometimento da privacidade do titular, de forma que, ao invés do certificado revelar o nome do titular, seria adotado um nome fictício, um pseudônimo, com o intuito de disfarçar a identidade real do titular e garantir o anonimato. Ainda que as organizações possam associar por meio do uso de pseudônimo os titulares ao seu certificado digital, tais organizações não seriam capazes de determinar as reais identidades dos mesmos.

A RFC 3739, a qual trata de *qualified certificates profile*, estabelece o uso de pseudônimo no campo "*Subject*" do certificado digital (IETF, 2004). Ou seja, ao invés do campo "*Subject*" conter o nome do titular, teria o respectivo pseudônimo. Um ponto de atenção a ser observado é que a extensão "*Subject Alternative Name*", já descrita anteriormente, não é utilizada para o pseudônimo, uma vez que a RFC 5280 define que o uso da referida extensão é para vincular outras identidades ao certificado, como *email*, nome DNS, tal como definido pelo ITI que empregou para associar RG ou mesmo o número RIC.

Uma solução já utilizada em outros países é a adoção de certificados digitais com uso restrito para autenticação. A restrição do uso de tais certificados pode ser feita por meio das extensões "*Key Usage*" e "*Extended Key Usage*". A primeira extensão é composta por uma combinação de bits, os quais definem o propósito do certificado digital (cifragem, assinatura, gerenciamento de chaves, etc.). A segunda extensão também indica um ou mais propósitos para o uso do certificado, adicionalmente aos propósitos básicos indicados pela extensão "*Key Usage*", aparecendo somente em certificados para entidades finais. A extensão "*Extended Key Usage*" agrega maior flexibilidade, motivo pelo qual é adotado em outros países para criar certificados exclusivos para autenticação. Na presença das duas extensões no certificado, ambas devem ser processadas independentemente e o certificado deve somente ser utilizado para o propósito consistente nas duas extensões.

Tomando-se a ideia de criação de certificados com uso restrito, pode-se levantar algumas sugestões interessantes para o RIC. Por exemplo, a adoção de dois certificados com função de autenticação (um com identificação do titular e o outro com pseudônimo) e, outro certificado com função de assinatura com a identificação do titular. O certificado com pseudônimo pode agregar o anonimato com o objetivo de proteger os dados pessoais do titular do certificado e serviria basicamente para autenticar o *token* em serviços remotos de provedores privados, por exemplo.

Observa-se no âmbito da ICP-Brasil que não há uma definição explícita quanto ao uso de pseudônimos. O DOC-ICP-04 (ITI, 2014) que trata das políticas de certificado e estabelece os padrões adotados para os certificados ICP-Brasil não menciona a possibilidade do uso de pseudônimo. Pelo contrário, apenas determina que o nome do titular do certificado deve constar no campo "*Subject*".

Do ponto de vista jurídico, o uso de pseudônimo é analisado sob o ponto de vista do anonimato e da privacidade dos dados. No Brasil o anonimato possui alguma restrição de uso, conforme consta na Constituição Federal, Art. 5°, inciso IV: "*é livre a manifestação do pensamento, sendo vedado o anonimato*" (Brasil, Constituição Federal, 1988). Por outro lado, o Código Civil (Brasil, Lei No 10.406 - Código Civil, 2002) garante em seu Art. 19 que para fins lícitos, como em contratos de provisão de serviços privados, o uso de pseudônimo goza da mesma proteção do nome real da pessoa. Várias regulamentações discorrem sobre a proteção dos dados pessoais, como o Código de Defesa do Consumidor (Brasil, Lei Nº 8.078 - Código de Defesa do Consumidor, 1990) que explicita uma extensa proteção a dados relativos à relações de consumo; as regulamentações da Agência Nacional de Telecomunicações (ANATEL) e do Comitê Gestor da Internet Brasileira (CGI.br) que estabelecem o princípio da neutralidade com um dos seus fundamentos para a privacidade na Internet; a Lei Complementar N° 105/2001 (Brasil, Lei Complementar Nº 105, 2001), que dispõe sobre o sigilo das operações de instituições financeiras; e outras. Recentemente, o Ministério da Justiça lançou uma consulta pública para discutir a proteção de dados pessoais armazenados em centrais dentro e fora do país, abordando a diferenciação conceitual entre os dados pessoais, anônimos e sensíveis e os meios de protegê-los (Câmara dos Deputados, 2015). A consulta pública tem por finalidade gerar um texto preliminar que será tema de um futuro projeto de lei relativo à proteção de dados.

No entanto, mesmo com a existência de várias normas que legislam sobre o anonimato ou a privacidade dos dados, não existe uma definição concreta sobre esse tema, o que é percebido em diversas decisões judiciais diferentes em casos bastante similares. Logo, o uso de pseudônimos nos certificados da ICP-Brasil carece de uma avaliação das autoridades competentes e regulamentação explícita indicando a possibilidade de seu uso e as regras para a sua utilização.

# 5. PROCESSOS DE CERTIFICAÇÃO DIGITAL NO PAÍS E NO MUNDO

A certificação digital possui alto grau de implantação nas transações eletrônicas realizadas pela *Internet*, e vem sendo adotada como padrão de segurança em soluções governamentais e de empresas privadas. No presente capítulo, apresentam-se algumas iniciativas, públicas e privadas, tanto no Brasil, como no mundo, e seus principais benefícios.

## 5.1 Iniciativas do Governo Federal

O Governo Federal tem feito uso da certificação digital em muitas de suas frentes de serviço. No entanto, apesar dos esforços para o uso de certificação digital nos serviços eletrônicos do governo (*ego*), percebe-se que ainda há muito trabalho a ser feito. A Figura 14~~Figura 14~~~~Figura 14~~ ilustra tal situação, na qual vê-se que 75% dos serviços *e-gov* não utilizam certificado digital. Outro fato observado é que a grande maioria dos serviços *e-gov* são ofertados pela Receita Federal. Os outros órgãos, apesar de apresentarem iniciativas interessantes quanto ao uso de certificação digital nos serviços *e-gov*, ainda empregam essa tecnologia de forma muito tímida, o que reforça a ideia de que há muito espaço no governo para a utilização de certificação digital.

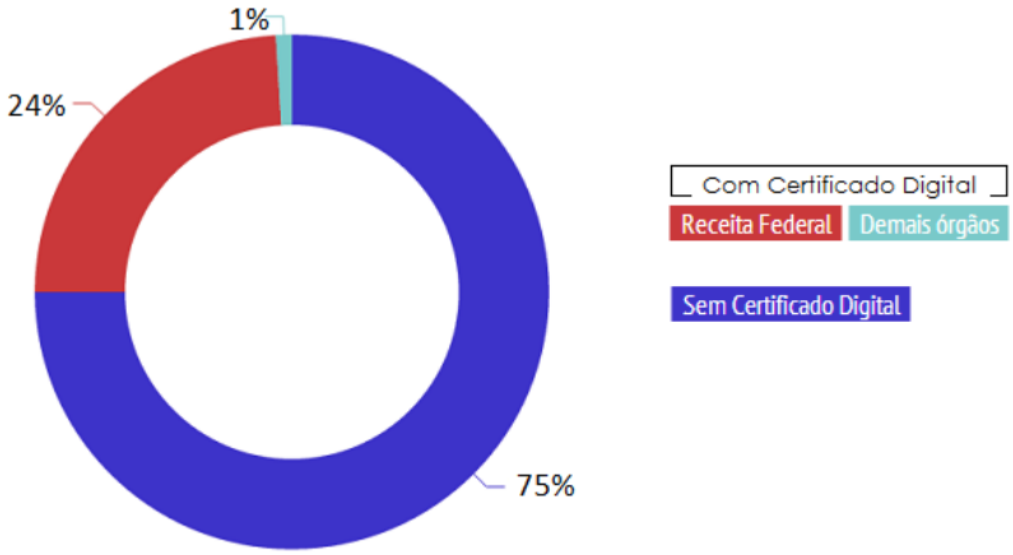


**Figura 14 – Utilização de certificação digital no e-gov (Fonte: (Torres, Deus, & Sousa Júnior, 2015)).**

A seguir são apresentadas algumas experiências de serviços baseadas em certificação digital dentro do contexto nacional, tanto na área privada como na pública. Será observado que embora o certificado digital não seja amplamente utilizado nos dias atuais, há um esforço dentro no cenário nacional de ofertar serviços baseados em certificação digital, sobretudo pela segurança, eficiência e economicidade que tal tecnologia proporciona.

### 5.1.1 Receita Federal do Brasil (RFB)

As iniciativas da Receita Federal do Brasil (RFB) são bastante conhecidas uma vez que afetam muitas empresas, empresários, profissionais liberais e escritórios de contabilidade. A partir dos anos de 2009 e 2010, com a publicação das Instruções Normativas nº 969 (2009), 995, 1036 e 1075 (2010), a RFB passou a exigir de todas as pessoas jurídicas, com exceção das enquadradas no Simples Nacional, o envio das declarações e demonstrativos de tributos federais, e, obrigações acessórias com a aplicação de assinatura digital.

Dentre tais documentos, estão a Declaração de Débitos e Créditos Tributários Federais (DCTF), a Declaração de Informações Econômico-Fiscais das Pessoas Jurídicas (DIPJ), o Demonstrativo de Apuração de Contribuições Sociais (DACON), a

Declaração sobre a Utilização dos Recursos em Moeda Estrangeira Decorrentes do Recebimento de Exportações (Derex), a Declaração sobre a Opção de Tributação de Planos Previdenciários (Dprev), a Declaração de Dedução de Parcela da Contribuição de Intervenção no Domínio Econômico Incidente sobre a Importação e Comercialização de Combustíveis das Contribuições para o PIS/Pasep e Cofins (DCIDE-Combustível), a Declaração Especial de Informações Fiscais relativa à Tributação das Bebidas (DIF Bebidas), dentre outras.

As iniciativas da RFB também alcançam as declarações de IRPF e IRPJ. Usando o certificado digital e-CPF, as pessoas físicas têm acesso ao sistema da RFB para consulta de possíveis entraves, erros de processamentos, correções em suas declarações. Para aqueles que não têm e-CPF, a consulta a estes problemas só pode ser feita presencialmente (ou por procuração) na sede da RFB.

Já o e-CNPJ possibilita às empresas realizar operações no e-CAC (Centro Virtual de Atendimento ao Contribuinte). Utilizando o e-CNPJ, as empresas podem emitir notas fiscais eletrônicas, assinar contratos digitais, acompanhar processos legais, verificar a autenticidade de informações divulgadas na versão *online* do Diário Oficial, consultar e regularizar a situação cadastral e fiscal, emitir certidões, gerar procurações eletrônicas, acompanhar processos fiscais, dentre outras, sem que tenha que se deslocar até uma sede da RFB.

Ao lançar o e-CPF e o e-CNPJ, a RFB possibilitou aos usuários a emissão de certidões negativas e retificação de documentos pessoais e jurídicos. Com esses certificados, cidadãos e empresas podem assinar contratos de financiamentos e abrir conta corrente de forma remota, manter canais de relacionamento com fornecedores, clientes e com o Governo. Os benefícios traduzem-se em termos redução de papel e minimização dos deslocamentos, menor morosidade, redução de burocracia e redução de custos operacionais.

### 5.1.2 PROUNI – Universidade para todos

O Ministério da Educação (MEC) instituiu a certificação digital no PROUNI (programa que concede bolsas de estudo integrais e parciais a estudantes de baixa renda), restringindo o acesso ao SISPROUNI pelas instituições de ensino com a

certificação digital. É por intermédio desse sistema que as universidades conseguem acessar informações como o cadastro dos bolsistas, termos de concessão das bolsas, etc.

Usando o certificado digital, as instituições de ensino, seus coordenadores e representantes podem preencher os termos de cadastro, emitir termos de adesão e termos aditivos, bem como realizar procedimentos de manutenção de bolsas, como atualização, suspensão, transferência e encerramento; aprovação/reprovação de candidatos pré-selecionados, dentre outros.

No caso do PROUNI, o uso de certificado digital garantiu a integridade das informações cadastradas no SISPROUNI, registrando com assinatura digital todos os documentos emitidos. Isto dispensou o envio destes documentos via correio e eliminou a necessidade de reconhecimento de firma dos signatários. Adicionalmente, garantiu maior segurança ao processo de cadastro e concessão de bolsa, agregando mais rapidez e praticidade às operações das instituições de ensino.

No âmbito do PROUNI são utilizados os certificados do tipo A1 e A3 emitidos por alguma AC pertencente à ICP-Brasil, sendo os de pessoa jurídicas usados pelas mantenedoras da instituição de ensino superior, e os de pessoa física aplicados pelos coordenadores do PROUNI/Representantes.

### 5.1.3 Sistema Integrado de Informações Previdenciárias (SIPREVI)

A troca de informações entre o Ministério da Previdência e os entes federativos (estados e municípios) é uma determinação legal. O volume de transações é extremamente elevado, pois estados e municípios contam com mais de dois mil e duzentos regimes de previdência social próprios.

Para aperfeiçoar a gestão e controle financeiro desses regimes, foi criado o Sistema Integrado de Informações Previdenciárias (SIPREVI). Este sistema é um banco de dados em que Estados e Municípios inserem informações cadastrais de seus servidores, possibilitando aos seus gestores disponibilizar o extrato previdenciário aos servidores, conceder benefícios e acessar ao sistema de óbitos da Previdência Social de forma automatizada.

A adoção da certificação digital pelo SIPREVI para receber as prestações de contas

feitas periodicamente pelos entes federativos ao Ministério da Previdência Social, quanto aos benefícios pagos aos servidores aposentados, protegeu o conteúdo dos documentos com sistemas criptográficos e garantiu que apenas os servidores autorizados tivessem acesso aos dados contidos nos processos.

Além disso, o uso do SIPREVI com a certificação digital possibilitou que Estados e Municípios migrassem o controle financeiro de seus regimes de previdência social para o meio eletrônico, eliminando o grande volume de papel até então existente. Como exemplo do acúmulo do papel nas transações, pode-se citar o comprovante de repasse das contribuições, no qual o ente federativo assinava o documento e mandava via correio ou internet para ser analisado pelo Ministério. Isto gerava dúvidas quanto a confirmação, ao certo, de que a pessoa que o enviou tinha autoridade para prestar informações ao Ministério. Com a certificação digital, os representantes legais ficam seguros de que só eles têm a condição de enviar o documento.

### 5.1.4 Conectividade Social – Caixa Econômica Federal

O Conectividade Social é um canal de relação entre a CAIXA e as empresas no que concerne à obrigatoriedade do envio de informações relativas às contribuições do FGTS. Por meio de operações eletrônicas via internet, a CAIXA deu agilidade a uma série de atividades que antes eram efetuadas fisicamente em bancos ou correspondentes bancários. O conectividade social opera por meio de *software* e possibilita às empresas simplificar o envio de remessas e informações relativas aos depósitos mensais para seus funcionários no Fundo de Garantia do Tempo de Serviço (FGTS). Ao mesmo tempo facilita o acesso dos usuários às informações existentes nos bancos de dados da CAIXA.

A partir de 2011, a CAIXA adotou o uso da certificação digital no padrão da ICP-Brasil para o acesso ao conectividade social. O uso do certificado digital A3 facilitou a transmissão dos arquivos gerados pelo programa SEFIP - Sistema de Recolhimento do FGTS e Informações à Previdência Social diretamente via *Internet*, com maior nível de segurança. Além disso, as empresas podem consultar os saldos e as movimentações do FGTS, corrigir possíveis inconsistências nos dados realizar atualizações cadastrais.

Os benefícios do novo sistema podem ser descritos em termos de simplificação do

processo de recolhimento do FGTS, redução de tempo e de gastos operacionais, segurança jurídica na transmissão dos dados, disponibilização de um canal direto de comunicação entre as empresas usuárias e a CAIXA, redução da ocorrência de inconsistências, aumento da proteção da empresa contra irregularidades e facilidade no cumprimento das obrigações da empresa relativas ao FGTS.

### 5.1.5 Programa Juros Zero - FINEP

O programa Juro Zero, instituído pela Financiadora de Estudos e Projetos – FINEP, tem por objetivo estimular a capacidade de inovação das micro e pequenas empresas brasileiras, em termos de processos e negociações de produtos ou serviços. O programa conta com recursos da ordem de R$ 100 milhões, provenientes de uma parceria da FUNEP com o Fundo de Amparo ao Trabalhador (FAT). O empréstimo, para cada empresa, será limitado a R$ 900 mil ou a 1/3 do faturamento do ano anterior. As exigências para a tomada de financiamento estão contidas na Portaria MDIC Nº 176 de 01/10/2002.

Pelo programa, as empresas podem tomar financiamento a longo prazo e com juro real zero, tendo até 100 vezes para pagar. A partir do ano de 2005, a FINEP adotou o uso do certificado digital da ICP-Brasil nas operações do programa. Assim, as negociações passaram a ser feitas por meio digital, incluindo a apresentação de planos de negócios pelas empresas proponentes. Para tanto, foi disponibilizado formulário padronizado e simplificado, cujo acesso e preenchimento é feito por meio da *Internet*. Havendo aprovação dos planos de negócios, as assinaturas dos contratos também são feitas com o uso do certificado digital.

### 5.1.6 Ministério do Trabalho e Emprego

O Ministério do Trabalho e Emprego, a partir de 2014, exige que a transmissão da declaração relativa à Relação Anual de Informações Sociais (RAIS) dos estabelecimentos privados com 11 ou mais vínculos empregatícios, bem como dos órgãos da Administração Pública, seja feita com a aplicação de um certificado digital no padrão ICP-Brasil. Esta exigência atinge também a transmissão da RAIS de exercícios

anteriores (MTE, 2014).

As declarações podem ser transmitidas com o certificado digital de pessoa jurídica, emitido em nome do estabelecimento, ou com certificado digital do responsável pela entrega da declaração, sendo que este pode ser um CPF ou um CNPJ. Para os estabelecimentos que não se enquadrarem nessa obrigatoriedade, bem como a transmissão da RAIS negativa, o uso da certificação digital é facultativo.

O mesmo ocorreu com o Cadastro Geral de Empregados e Desempregados (CAGED) que trata do registro permanente de admissões e dispensa de empregados, sob o regime da Consolidação das Leis do Trabalho (CLT). A partir de 2013, todos os estabelecimentos com 20 ou mais trabalhadores, bem como os órgãos da Administração Pública, foram obrigados a transmitir a declaração CAGED utilizando um certificado digital no padrão da ICP-Brasil.

### 5.1.7 A Nota Fiscal Eletrônica – NF-e

O projeto da NF-e teve sua discussão iniciada em 2004 no I Encontro Nacional dos Administradores Tributários realizado em Salvador. Este evento reuniu titulares das administrações tributárias federal, estaduais, do Distrito Federal e de algumas capitais. O objetivo foi atender a Emenda Constitucional – EC nº 42, inciso XXII, art. 37, uma vez que era preciso buscar soluções conjuntas das três esferas de Governo para a promoção de maior integração administrativa, padronização e melhor qualidade das informações.

O desenvolvimento do sistema de emissão de notas fiscais eletrônicas facilitou as atividades de fiscalização das operações relativas ao Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e Imposto sobre Produtos Industrializados (IPI). Os estabelecimentos passaram a implantar a nota fiscal eletrônica em substituição à emissão do documento fiscal em papel. Para as empresas que utilizam o sistema de NF-e, todos os processos que compreendem a emissão, a validação e a autorização do uso pelas autoridades tributárias são executados obrigatoriamente com a Certificação Digital.

A assinatura digital é parte integrante do processo de emissão de NF-e e garante a

integridade e autoria do arquivo eletrônico. A SEFAZ determina que o certificado digital utilizado para assinatura das notas deve estar dentro do padrão ICP-Brasil. Para emissão de notas fiscais eletrônicas não é permitida a utilização de certificado de procuradores ou contabilistas, mas apenas o da própria empresa.

### 5.1.8 Departamento de Trânsito do Estado de São Paulo - DETRAN/SP

O Departamento de Trânsito do Estado de São Paulo – DETRAN/SP é o maior órgão de trânsito da América Latina com 25 milhões de veículos cadastrados, o que representa 1/3 da frota brasileira. Ao todo são cerca de 21 milhões de condutores que renovam periodicamente suas Carteiras de Habilitação (CNH) e mais os processos para emissão de novas CNHs. Devido a esse elevado contingente, em média, as emissões de CNHs (renovações, provisórias e definitivas), totalizam 350 mil documentos por mês. Além disso, o órgão conta com grande volume demandado de operações para acesso à base de dados de veículos cadastrados.

Visando melhorar a qualidade dos serviços prestados ao cidadão, o DETRAN/SP iniciou em 2009 uma reestruturação de seu sistema. O foco principal foi a redução da burocracia, o investimento em tecnologia, serviços eletrônicos e em infraestrutura, a criação de novos canais de comunicação com o cidadão e o reforço do combate à corrupção.

Nesse contexto, foi criado em 2009 o sistema de gerenciamento eletrônico estruturado em três frentes: sistema *online*, controle biométrico e certificação digital. No que se refere à certificação digital foi criado o e-CNH, destinado a atender 3.400 Centros de Formação de Condutores (CFC), com cerca de 30.000 usuários; 6.255 despachantes, com 18.000 usuários; 2.500 médicos de trânsito e 1.900 psicólogos de trânsito. Todas as necessidades de ordem processual (emissão, cancelamentos, renovação) de CNHs, bem como as emissões de laudos médicos e psicológicos emitidos e assinados pelos profissionais passaram a ser realizados com aplicação do certificado digital do tipo A3.

O novo sistema e-CRV, utilizado pelos despachantes para realização de consultas e emissão de documentos, passou a funcionar como um balcão avançado para facilitar e agilizar os processos submetidos pelos despachantes à apreciação do DETRAN/SP.

Foram disponibilizados vários serviços, tais como: consulta a cadastros de veículos (base do Estado, do Renavan e de outros Estados), emissão de documentos (1º emplacamento, transferências de proprietário e de município/Estado, alteração de dados cadastrais, licenciamento, comunicação de venda, alteração de endereço etc.).

A adoção do certificado digital do tipo A-3, tanto para o e-CNH e e-CRV foi estabelecida como um requisito obrigatório a todos os usuários (pessoas físicas e jurídicas) interessadas em realizar transações/operações dentre as mencionadas. Tal adoção levou o DETRAN/SP a monitorar de forma mais eficiente o acesso às suas bases cadastrais. Essas medidas possibilitaram reduzir custos operacionais com emissão de laudos médicos e psicológicos (papel, tempo, deslocamento etc.), reduzir irregularidades e proporcionar maior eficiência e segurança em suas operações.

### 5.1.9 Associação dos Registradores de Pessoas Naturais do Estado de São Paulo (ARPEN/SP).

A Central de Informações do Registro Civil (CRC) foi instituída em 07 de agosto de 2012 pela Corregedoria Geral de Justiça do Estado de São Paulo. A criação da CRC deu início à implantação do modelo de certidões eletrônicas e certidões negativas, permitindo a transferência de certidões entre os cartórios sediados no Estado de São Paulo.

A CRC integra, obrigatoriamente, todos os Cartórios do Estado de São Paulo, e tem sua base de dados atualizada de forma permanente. Atualmente, já são mais de 32 milhões de registros armazenados e mais de 11.000 certidões emitidas. A consulta a esta base de dados pode ser feita por integrantes dos poderes públicos, assim como pela população e pelos próprios registradores civis, responsáveis pelo constante controle dos registros cancelados e daqueles resguardados por segredo de justiça. Mas o acesso é controlado por seguras ferramentas tecnológicas.

Com as informações centralizadas pela CRC, é possível ao cidadão ir a qualquer cartório e pedir busca por um registro (certidão de nascimento, casamento e óbito), como também solicitar a respectiva certidão. A solicitação da certidão também pode ser feita pelo usuário sem sair de casa, optando por recebê-la em papel pelos Correios, ou em meio digital por *e-mail*. A adoção da certificação digital pela ARPEN/SP possibilitou

a emissão da certidão de nascimento direto dos hospitais, restando aos pais apenas a escolha do cartório.

### 5.1.10 Iniciativas do Poder Judiciário

No Poder Judiciário, o processo eletrônico foi regulamentado pela Lei nº 11.419 de dezembro de 2006. A assinatura digital baseada em certificado digital emitido no âmbito da ICP-Brasil está prevista no artigo 2º, inciso III, alínea “a”. Esta iniciativa levou agilidade no acesso às cortes, simplificou e reduziu custos processuais.

O Tribunal Regional do Trabalho (TRT) da 4ª região disponibilizou o sistema de petição eletrônico (SIPE), por meio do qual os advogados, fazendo uso do certificado digital, fazem as petições eletrônicas de suas peças jurídicas. Destaca-se ainda, a implantação do sistema e-JUS que informatizou todas as sessões de julgamento. Estes sistemas reduziram o uso de papel antes, durante e após os julgamentos.

Tribunais de Justiça de vários Estados (São Paulo, Rio Grande do Sul, Paraná, Rio de Janeiro, dentre outros) também adotaram o uso do certificado digital na tramitação e despacho de processos, obtendo maior agilidade e segurança. Isto, por sua vez, fez com que esses Tribunais eliminassem o uso de papel em várias fases dos processos,

O Superior Tribunal de Justiça (STJ) também está apto a receber por meio eletrônico, petições referentes a processos relativos a habeas-corpus (HC). Em outra esfera, vários Estados têm implantado o serviço de Diário da Justiça On-line, permitindo aos usuários da Justiça verificar a autenticidade e integridade das informações publicadas.

## 5.2 Iniciativas do Setor Privado

A seguir são destacadas algumas iniciativas de uso de certificação digital no setor privado.

### 5.2.1 A certificação digital na Comgás

A Comgás é a maior distribuidora de gás natural canalizado do Brasil, atuando especificamente no Estado de São Paulo. Sua área de concessão atinge aproximadamente 30 milhões de pessoas e 9 milhões de residências, distribuídas em 75 cidades. Atuando nesta área a empresa atende mais de 1 milhão e trezentos mil clientes, vendendo 22% de todo o gás natural vendido no Brasil. Seus clientes são residências, empresas do comércio e prestação de serviços, indústrias, hospitais, usinas termoelétricas, postos de combustível etc.

Objetivando dar maior agilidade e segurança em suas transações comerciais, principalmente nos processos que envolviam assinatura de contratos (novos e renovação) entre a empresa e seus clientes, a Comgás iniciou, em julho de 2012, estudos para a implantação da certificação digital em suas operações de vendas. O tempo gasto para finalizar o trâmite contratual, incluindo as assinaturas e reconhecimento de firmas de todas as partes envolvidas, bem como as respectivas remessas das vias às partes, girava em torno de 15 dias a 20 dias.

Com a implantação da certificação digital, o mesmo trâmite processual teve seu tempo reduzido para 4 horas. Isto gerou para a empresa uma série de benefícios, tais como: agilidade, devido à redução drástica do tempo do trâmite contratual; produtividade, liberando a equipe de suporte para atuar em outras frentes de trabalho; segurança e controle, com a garantia de rastreabilidade e integridade; simplificação, com a desburocratização do processo; qualidade, com a padronização das demandas por assinaturas; mobilidade, na qual a estrutura foi flexibilizada e descentralizada; redução de custos, com uma estimativa de 61%, a qual fez com que o projeto se pagasse em 12 meses; e sustentabilidade, com a eliminação de papel, sistemas de arquivos físicos, menor uso de combustível para remessa/entrega das respectivas, etc.

### 5.2.2 A certificação Digital no Hospital Alemão Osvaldo Cruz

O Hospital Alemão Osvaldo Cruz foi fundado em 1897 em São Paulo e atualmente ocupa uma área de 96 mil metros quadrados de construção. Sua estrutura física é composta por 327 leitos de internação, 34 leitos de UTI, 13 salas para grandes cirúrgicas e 3 salas para pequenas. Atualmente o Hospital conta com 2.158 colaboradores, 5.108 médicos cadastrados e realiza por ano cerca de 18.687

internações, 22.233 procedimentos cirúrgicos, 67.992 consultas, 43.074 exames.

Tradicionalmente, as prescrições sempre foram feitas em papel. Porém, o processo manual gerava diversas inconveniências, como erros de interpretação; risco de perda de informação; aumento da necessidade de espaço físico e informações não estruturadas que causavam dificuldade de acesso aos dados pregressos do paciente, dificuldade de acesso no ambiente hospitalar, dificuldade de acesso para pesquisas e dificuldade na aderência a novos processos clínicos.

Com o objetivo de eliminar tais inconveniências, o Hospital iniciou estudos em 2012 para implantação da certificação digital de todos os profissionais envolvidos no processo de cuidado do paciente. O projeto foi divido em duas fases: a primeira fase, finalizada em março/2014, certificou os enfermeiros, técnicos de enfermagem, fisioterapeutas, nutricionistas e médicos contratados, num total de 900 profissionais. Nessa fase foi adotado o certificado A3. A segunda fase, ainda em implantação, prevê a certificação dos médicos do corpo clínico aberto (cerca de 5.000 profissionais).

O Hospital atingiu muitos benefícios, entre eles: eliminação do papel com amparo legal, melhoria na velocidade do processo, garantia do sigilo, auditoria e integridade dos dados. Além disso, foi obtida a consolidação da informação do paciente de forma estruturada, facilidade de acesso aos dados para os profissionais envolvidos no processo de cuidado do paciente, rastreabilidade da informação (quem, quando e onde acessou), legibilidade da informação e velocidade no processo (atualmente os médicos levam em média 2 minutos para fazer a prescrição).

### 5.2.3 Prontuário Eletrônico do Paciente (PEP)

O Prontuário Eletrônico do Paciente (PEP) é uma ferramenta de tecnologia da Informação e Comunicação em Saúde (TICS) que auxilia o médico nas suas atividades diárias, seja no consultório, centro diagnóstico ou hospital. Trata-se de uma ferramenta de alta qualidade, segura, que possa auxiliá-lo no registro da história clínica e exame físico, bem como na solicitação de exames e prescrição. Outra ferramenta também importante é o Registro Eletrônico de Saúde (RES) que permite o armazenamento e o compartilhamento seguro das informações de um paciente. O PEP/RES tem como marco regulatório a Resolução CFM No 1821/2007 publicada pelo Conselho Federal

de Medicina (CFM).

A informação no PEP tende a ser mais disponível e atualizada, onde e quando o médico precisa; os resultados de exames, laboratoriais ou de imagem, estão também disponíveis para consulta. Todos os dados armazenados têm maior legibilidade, acurácia e exatidão. Com as ferramentas que acompanham o PEP, tais como sistemas de alerta e de apoio à decisão, a possibilidade de erro é reduzida, trazendo assim maior segurança ao paciente. Também é demonstrado por alguns estudos internacionais que a implantação de um PEP traz uma considerável redução de custos para a instituição. Outro aspecto vantajoso é que o PEP é muito mais seguro do que o prontuário em papel e as informações podem ser compartilhadas automaticamente com outros profissionais e instituições que estão cuidando do paciente, possibilitando dessa forma a continuidade da atenção integral à saúde.

Um médico que deseje utilizar o PEP deve providenciar o CRM Digital, o qual corresponde à nova carteira de identificação do médico na forma de *smartcard*, que está substituindo gradualmente a antiga CRM. O CRM Digital é disponibilizado pelos Conselhos Regionais de Medicina (CRM) contendo um *chip* utilizado para o armazenamento do par de chaves e do certificado digital do médico. Os valores para a aquisição do CRM Digital praticado atualmente estão na ordem de R$ 70,00 à R$ 84,00. Uma vez que adquirida a CRM Digital, o médico pode proceder com a obtenção do par de chaves e do certificado digital. O certificado digital adotado pelo CRM Digital é o padrão ICP-Brasil e-CPF A3, de forma que os prontuários assinados digitalmente tem validade jurídica.

## 5.3 PROCESSO DE CERTIFICAÇÃO AO REDOR DO MUNDO

Várias entidades ao redor do mundo, sejam elas privadas ou governamentais, adotam a certificação digital em suas soluções, como forma de fortalecer a segurança e prevenir contra as fragilidades do meio digital, como a clonagem de *sites*, o forjamento de *e-mails*, a adulteração de arquivos, a dificuldade de comprovar fraudes e as dificuldades relativas à autenticidade, integridade, sigilo e irretratabilidade. São inúmeros os casos de uso que poderiam ser exemplificados nos outros países, destacando-se os esforços realizados no uso de certificação digital nos documentos de

identificação eletrônicos (eID). O estudo da aplicação em eIDs é interessante porque mostra que a certificação digital é um instrumento altamente recomendado e utilizado para os fins de autenticação e identificação. Considerando que o RIC pode vir a adotar um modelo de eID, é interessante aprofundamento do estudo sobre como a certificação é utilizada nos eIDs de outros países, sobretudo para conhecer as melhores práticas relativas ao assunto.

De forma geral, percebe-se que o uso autenticação eletrônica nas eIDs de diversos países é algo obrigatório, básico, pois permite a autenticação e identificação do titular de forma segura, bem como permite que o mesmo desfrute de serviços *online*, como serviços *e-gov* e privados. Um aspecto interessante é que a grande maioria dos países que implantaram eID utilizam certificados digitais distintos para a funcionalidade de autenticação e para a assinatura digital, como apresentado na Tabela 17~~Tabela 17~~~~Tabela 17~~. A separação das funcionalidades de autenticação e assinatura é amparada pela diretiva 93/1999/EC do conselho e do Parlamento Europeu. Os certificados qualificados empregados para a assinatura de documentos atendem aos requisitos previstos no Anexo I da diretiva 93/1999/EC, permitindo controle de processo mais rígido e níveis de segurança maiores do que os certificados emitidos com a finalidade única de autenticação. A diferença dos níveis de segurança, sobretudo com menos requisitos para emissão de certificados de autenticação, ajudam a simplificar o processo de emissão.

**Tabela 17 – Certificado de autenticação vs certificado de assinatura**

| País | Certificado de autenticação e de assinatura distintos | Aplicação de assinatura utilizada para autenticação? |
|---|---|---|
| Áustria | Não | Sim |
| Bélgica | Sim | Sim |
| Estônia | Sim | Sim |
| Finlândia | Sim | Sim |
| Dinamarca | Sim | Não |
| Itália | Sim | Sim |
| Portugal | Sim | Sim |
| Espanha | Sim | Sim |
| Suécia | Sim | Sim |

| | | |
|---|---|---|
| Cartão de Cidadania Europeia | Opcional | Opcional |

**Fonte:** *Privacy Features of European eID Card Especifications* (Ingo Naumann, 2009).

A maioria das eIDs europeias emprega *Personal Identification Number* (PIN), uma espécie de senha para acessar as funções de autenticação e de assinatura do eID, mesmo aquelas que utilizam o mecanismo de certificados digitais para autenticação. Via de regra, a função de autenticação é gratuita podendo ou não ser ativada, e o certificado de assinatura é opcional e pago pelo titular. A Tabela 18~~Tabela 18~~~~Tabela 18~~ ilustra o cenário de divisão das funcionalidades de autenticação e assinatura em certificados diferentes, bem como o uso de PINs para acessar as funcionalidades do eID. O estudo confirma a tendência de emissão de certificados distintos, possivelmente emitidos por AC´s distintas, para as funções de assinatura digital e autenticação eletrônica.

**Tabela 18: Emprego de certificação digital em eID´s nacionais.**

| País | AC Raiz | Certificados | Uso de PIN | Ref |
|---|---|---|---|---|
| Áustria | A-TRUST (Privado) | -Aut: *Qualified Certificate*, obrigatório, ECDSA 192 bits (A partir de 2009 256bit)<br><br>-Ass, Aut, Cif: Aditional Certificate, RSA 1536 bit | | (Lehmann, 2013) (Relatório de Melhores Práticas Mundiais) (Study on eID Interoperability for PEGS: Update of Country Profiles, 2009) (Bruegger, 2007) (STORK 2.0 Member State´s eIDs, 2013) |
| Bélgica | Certipost (Publico-Privada) | - Aut: Chave para uso do RRN PIP) RSA 1024bits. Gratuito, pode ser desativado (Fumy & Paeschke, 2011)<br>- Ass: RSA 1024bits. Gratuito, pode ser desativado (Fumy & Paeschke, 2011)<br>- Não possui função de cifragem.<br>- Usa um terceiro certificado básico de autenticação ativa do chip sem PIN. | - Uma PIN (4-6 díg.) para os dois certificados (Fumy & Paeschke, 2011)<br>- PUK para destravar PIN | (Lehmann, 2013) (Ingo Naumann, 2009) (Arora, 2007) (D3.6 Study on ID Documents, 2006) (STORK 2.0 Member State´s eIDs, 2013) |
| Rep. Tcheca | Privados (eIdentity, ICA, PostSignum) | Ass: Qualified Signature não pode ser usado para autenticação. Opcional. Aut: Gratuito | - Chave PIN (4-10 díg.) | (Lehmann, 2013) (EUROSMART, 2013) (STORK 2.0 Member State´s eIDs, 2013) |
| Estônia | AS SK (Bancos/Telecom) | - Aut, Cif, Ass de-mails: Obrigatório e gratuito. RSA-2048 (ECC | - PIN distintas (4-10 dig) | (Lehmann, 2013) (Ingo Naumann, 2009) (Relatório de Melhores Práticas |

| | | | | |
|---|---|---|---|---|
| | Possui Mobile ID | suportado mas não ativado)<br>- Ass. | - PUK para destravar PIN | Mundiais)<br>(STORK 2.0 Member State´s eIDs, 2013) |
| Finlândia | Population Register Center (CA Específico)[1] | - Aut, Cif: Obrigatório e gratuito. RSA-2048<br>- Ass: Opcional. RSA-2048 | - PIN distintas<br>- PUK para destravar PIN | (Lehmann, 2013) (Ingo Naumann, 2009) (Kubicek & Noack, 2010) (Relatório de Melhores Práticas Mundiais) (Stevens, Elliott, Hoikanen, Maghiros, & Lusoli, 2010) |
| Alemanha | | -Aut: Gratuito, pode ser desativado.<br>- Ass: Opcional e pago. ECDSA | | (Lehmann, 2013) (Ingo Naumann, 2009) (Poller, Waldmann, & Vowé, 2012) (STORK 2.0 Member State´s eIDs, 2013) |
| Itália CNS | AC privadas | - Aut: Obrigatório e gratuito.<br>- Ass: Opcional. | | (Lehmann, 2013) (National Strategies and Policies for Digital Identity Management in OECD Countries, 2009) (STORK 2.0 Member State´s eIDs, 2013) |
| Itália CIE | Ministry of the Interior (SSCE) | - Aut: obrigatório, gratuito.<br>- Ass: Opcional | | (Lehmann, 2013) (Ingo Naumann, 2009) (National Strategies and Policies for Digital Identity Management in OECD Countries, 2009) |
| Lituânia | Ministry of the Interior | - Aut.<br>- Ass. | - PIN distintas.<br>- PUK para destravar PIN. | (Lehmann, 2013) (STORK 2.0 Member State´s eIDs, 2013) |
| Espanha | GDP (Polícia-MJ)<br><br>CERES-AC Pública | - Aut. RSA 2048 bits<br><br>- Ass: Opcional. Possui três níveis de assinatura, dependendo da uso de PIN ou biometria. | - PIN distintas.<br><br>- Acesso por PIN ou MOC. | (Lehmann, 2013) (Stevens, Elliott, Hoikanen, Maghiros, & Lusoli, 2010) (Ingo Naumann, 2009) (National Strategies and Policies for Digital Identity Management in OECD Countries, 2009) (STORK 2.0 Member State´s eIDs, 2013) (Aguado, 2014) |
| Portugal | SCEE (Governo-MJ) | - Aut: obrigatório, gratuito. RSA 2048 bits<br><br>- Ass: Opcional (Usam AC´s distintas). | - PIN distintas.<br>- PUK para destravar PIN. | (Lehmann, 2013) (Ingo Naumann, 2009) (Study on eID Interoperability for PEGS: Update of Country Profiles, 2009) (STORK 2.0 Member State´s eIDs, 2013) |

**Notação**: **Aut**: Autenticação; **Ass**: Assinatura; **Cif**: Cifragem

O algoritmo criptográfico assimétrico empregado nos certificados digitais varia de acordo com o país em questão, sendo o RSA o algoritmo de uso mais comum com chaves que variam de 1024 a 2048 bits. Entretanto, existem países que adotam criptossistemas baseados em curvas elípticas como a Áustria, a Alemanha e a Estônia

(nesse último país o ECC é suportado, mas não ativado).

O padrão X.509 é adotado pela maior parte dos países para especificar o formato dos certificados de chave pública, LCR, certificados de atributos e o algoritmo de validação da cadeia de certificado. Para as assinaturas digitais, percebe-se que os países adotam os padrões CMS e o XML-Dsig (XAdES), sendo este último mais comumente utilizado, devido às vantagens mencionadas no presente relatório. Pela diretiva 93/1999/EC adotada pela maioria dos países europeus, uma assinatura eletrônica avançada, gerada através de um certificado qualificado, possui a mesma validade legal que uma assinatura manual.

Apesar das inúmeras vantagens de um país ter o seu documento de identificação baseado em eID, tal como o aperfeiçoamento do serviço de autenticação, melhor segurança, disponibilização de serviços *e-gov* seguros e eficientes, etc, ainda há países onde há uma certa resistência para a implantação de eID nacional. Por exemplo, os EUA ainda hoje não têm um eID para identificação nacional. No entanto, existem grupos nos EUA, como o *Center of Technology and Democracy*, que clamam pela adoção de eID, principalmente para proteger informações pessoais utilizadas em transações *online* e sugerem o estudo do modelo de eID da Estônia dada a alta penetração de uso do eID na população daquele país (Nextgov, 2011).

Para ilustrar algumas características pontuais e funcionalidades, como os padrões utilizados, os tipos de certificados utilizados e outras particularidades, apresenta-se a seguir um resumo do *status* dos eIDs nacionais da Europa.

### 5.3.1 Áustria

Desde 2004 a Áustria possui o seu cartão cidadão destinado para a identificação de sua população, em torno de 9 milhões de habitantes (2012). O eID da Áustria fornece funcionalidades utilizadas em serviços governamentais (*e-gov*), bem como no comércio eletrônico, tendo como base a certificação digital (Lehmann, 2013). Entre as funcionalidades do eID, pode-se citar:

- geração e verificação de assinaturas digitais;
- cifração e decifração de documentos eletrônicos;

- geração e verificação de resumos criptográficos de documentos eletrônicos;
- leitura e escrita de dados em repositório de dados.

O eID austríaco utiliza certificados digitais no padrão X.509, tal como descrito na RFC 5280 (IETF, 2008). A criação e verificação de assinaturas digitais, e, também a cifração e a decifração, suportam tanto o padrão CMS como o padrão XML-Dsig. Os algoritmos utilizados para a assinatura podem ser o RSA, DSA e o ECDSA. São previstos no eID austríaco dois tipos de certificados: o certificado de autenticação, obrigatório, o qual utiliza ECDSA de 256 bits; o certificado de assinatura/autenticação/cifração, opcional, o qual utiliza RSA de 1536 bits.

O eID austríaco é destinado a todos os cidadãos de 16 anos ou acima, o qual é adquirido por uma taxa de 10 Euros (EUROSMART, 2013) e tem tempo de vida de 10 anos.

### 5.3.2 Bélgica

A Bélgica possui o seu eID, o BELPIC (*Belgian Eletronic Personal Identification Card*) desde 2003 empregado na identificação de sua população, em torno de 10 milhões de habitantes (2012). O BELPIC teve como propósito substituir os cartões de identidade anteriores, tornando-se o cartão de identidade oficial da Bélgica, adicionando várias funcionalidades, como a autenticação na *Internet*, criação/verificação de assinaturas eletrônicas e a possibilidade de criar documentos oficiais (Lehmann, 2013).

O BELPIC utiliza certificados digitais no padrão X.509. O eID belga armazena os seguintes certificados: o certificado de autenticação, o qual utiliza RSA de 1024 bits e habilita o uso de serviços eletrônicos de *e-business* e *e-gov*; o certificado de não-repúdio, o qual utiliza RSA de 1024 bits e é destinado para a assinatura eletrônica; o certificado RRN (Rijksregister-Registre National), a qual é associada à chave privada do cartão para estabelecer a autenticação com Registro Nacional a autoridade de registro que gerencia os registros dos cidadãos; e o certificado *Citizen CA*, certificado utilizado para identificar a CA do cidadão, o qual utiliza RSA de 2048 bits, padrão aplicado para a assinatura dos demais certificados. No cartão são armazenadas 3 chaves privadas de 1024 bits, correspondentes às funcionalidades de autenticação,

assinatura e autenticação do cartão com o Registro Nacional. O acesso às chaves privadas armazenadas no cartão de identidade se dá por meio de um *Personal Identification Number* (PIN), comum para ambas as chaves. A criação e verificação de assinaturas digitais suportam o padrão XAdES.

O BELPIC é destinado a todos os cidadãos de 14 anos ou acima, o qual é adquirido por uma taxa de 10 Euros (EUROSMART, 2013). A vida útil do eID atualmente é de 5 anos, mas deve ser estendida para 10 anos com a previsão de uso de chaves de 2048 bits (Cock, 2009).

### 5.3.3 República Tcheca

A República Tcheca possui o seu cartão de identidade nacional tcheco desde 2012 empregado na identificação de sua população, em torno de 11 milhões de habitantes (2012). Em 2012, o número de pessoas que utilizam o eID tcheco era de 1 milhão de habitantes. Entre as funcionalidades previstas no eID tcheco estão a função de autenticação para *e-services* e criação de assinatura digital (Lehmann, 2013).

A função de autenticação é apoiada pelo uso de certificados X.509 seguindo o padrão ICAO EAC (International Civil Aviation Organization, 2006). A função de assinatura digital é opcional, sendo necessária adquirir o certificado para assinatura associado. O eID tcheco utiliza um *smartcard* da Gemalto, o qual permite o uso dos algoritmos criptográficos 3DES (ECB, CBC), RSA até 2048 bits, SHA-1, SHA-2, ECDSA e ECDH até 383 bits. O acesso à chave privada armazenada no cartão de identidade é por meio de PIN.

O eID tcheco é obrigatório para todos os cidadãos de 15 anos ou acima. A vida útil do eID atualmente é de 10 anos (EUROSMART, 2013).

### 5.3.4 Estônia

O EstEID é o cartão de identificação nacional da Estônia, criado em 2003, empregado em toda a população de 1,3 milhões de habitantes em 2012. O EstEID pode ser utilizado para identificação visual, autenticação e assinatura digital (Lehmann, 2013). Uma funcionalidade interessante permitida com o EstEID é o *mobile-ID*, onde

permite-se identificar o cidadão com o uso de *smartphones*.

O EstEID contém dois certificados digitais que seguem o padrão X.509. O primeiro certificado pode ser utilizado para autenticação eletrônica, cifração e assinatura digital de *e-mails*. O segundo certificado pode ser utilizado para criar assinaturas digitais de acordo com o *Estonian Digital Signature Act*. Os certificados não contêm papéis, autorizações ou restrições de uso. Eles podem ser empregados de forma irrestrita em qualquer forma de comunicação, seja entre pessoas comuns, entre organizações ou com o governo. O acesso às chaves privadas armazenadas no cartão de identidade é feito por meio de PINs distintos para cada chave.

Os XAdES é o padrão adotado para as assinaturas digitais, bem como o XMLEnc o padrão para a cifração. O cartão EstEID suporta os algoritmos de *hash* SHA-1, SHA-224 e SHA-256. Para a cifração e assinatura é suportado o algoritmo RSA com 2048 bits. O cartão também suporta ECC, porém não foi ativado nos cartões EstEID.

O EstEID poderia ser obtido em 2009 pelo valor de 150 EEK (antiga moeda da Estônia, o que equivalia a R$ 22,00), tendo vida útil de 10 anos (EUROSMART, 2013).

### 5.3.5 Finlândia

O FINeID é o cartão de identificação nacional da Finlândia, criado em 1999, utilizado por 2,5 milhões de habitantes (total de 5 milhões de habitantes da Finlândia em 2012). O FINeID é um cartão de identificação opcional, o qual tem a intenção de facilitar o acesso a serviços *e-gov* para cidadãos finlandeses e residentes permanentes acima de 18 anos (Lehmann, 2013). Suporta autenticação, cifração e assinatura digital, podendo ser incluído adicionalmente informações de seguro de saúde. A autenticação é empregada nos serviços públicos ou privados que requerem a identificação. A cifração permite proteger documentos ou *e-mails*. A funcionalidade de assinatura possibilita ao cidadão assinar documentos eletrônicos e *e-mails*.

O FINeID armazena duas chaves privadas: uma para autenticação e cifração utilizando RSA de 2048 bits; outra para assinatura, também utilizando RSA de 2048 bits. As chaves privadas são acessadas no cartão de identificação por meio de PINs distintos para cada chave. Os certificados correspondentes às chaves seguem o padrão X.509. O FINeID pode ser obtido pelo valor de 29 euros, tendo vida útil de 10 anos

(EUROSMART, 2013).

### 5.3.6 Alemanha

O cartão de identificação alemão é um cartão de identificação nacional obrigatório para cidadãos acima de 16 anos na Alemanha, criado em 2010, utilizado por 20 milhões de habitantes (total de 80 milhões de habitantes da Alemanha em 2012). Entre suas funcionalidades, o eID alemão suporta autenticação, assinatura e a função de passaporte eletrônico, como destacado a seguir (Lehmann, 2013).

- **Função eID**: permite ao cidadão provar sua identidade na *Internet*. Pode ser utilizado em *logins* e inscrições em sistemas.
- **Função eSign**: permite ao usuário assinar documentos eletrônicos. Embora o cartão esteja preparado para a função eSign, tal funcionalidade é opcional e depende que o usuário adquira o certificado.
- **Função ePass**: permite o uso do eID alemão como um passaporte para viagem na área Schengen (área que compreende todos os países da União Europeia, excetuando a Irlanda e o Reino Unido, e três países que não compõem a UE, a Islândia, Noruega e Suíça).

O eID alemão contém um certificado digital de autenticação, gratuito, que pode ou não ser ativado. O certificado para assinatura é opcional e pago, e permite o uso de ECDSA. A taxa cobrada para a obtenção do eID alemão é de 28,80 euros, tendo vida útil de 10 anos (EUROSMART, 2013).

Além do cartão de identidade, há ainda na Alemanha o *eHealth Card,* um cartão para armazenamento de informações de seguro de saúde. Esse cartão armazena obrigatoriamente os dados básicos (nome, data de aniversário, endereço do segurado e dados administrativos), a prescrição eletrônica e o cartão europeu de seguro de saúde. Adicionalmente, o cartão pode armazenar registros eletrônicos do paciente, dados de emergência, e outros, onde tais informações são acessadas por meio de PIN. O *e-Health Card* também pode ser utilizado para autenticação eletrônica, cifração e assinatura eletrônica. Os certificados associados usam o RSA de 2048 bits com SHA-256. A assinatura também é baseada em RSA de 2048 bits com SHA-256, seguindo o padrão XMLDsig.

### 5.3.7 Itália

A Itália tem dois esquemas de eID, o *Eletronic Identity Card* (CIE – Carta d'Identità Elettronica) e o *National Service Card* (CNS – Carta Nazionale dei Servizi) (Lehmann, 2013). O CNS é o eID emitido pela administração pública italiana. Uma aplicação do CNS é o seu uso pelos governos regionais como um cartão de saúde, combinando a funcionalidade do cartão de seguro de saúde europeu, com as funcionalidades de acesso a serviços *online*, oferecendo serviços de autenticação e de identificação (serviços de assinatura são oferecidos em casos excepcionais). Os cartões CNS são produzidos em massa e enviados aos seus titulares pelo correio. Nessa situação, a função de autenticação é desabilitada. Para ativar tal função, o titular deve participar de um processo de registro no centro regional de saúde, onde é verificado o cartão de identidade e a identidade do titular. Os certificados de autenticação são emitidos usualmente por ACs do setor privado.

O CIE foi planejado para ser emitido aos cidadãos italianos como um passaporte para viagem na área Schengen. Além da funcionalidade de documento de viagem, o CIE também oferece serviços de autenticação e identificação (serviços de assinatura são oferecidos em casos excepcionais). Os certificados de autenticação são emitidos pelo AC do Ministério do Interior.

Em termos de especificação técnica, tanto o CNS quanto o CIE são basicamente idênticos. Ambos suportam algoritmos simétricos TDES e MAC3 e algoritmo assimétrico RSA. O padrão para assinatura digital é o XMLDsig. Quanto ao tempo de validade o cartão CNS tem um tempo de vida de 5 anos, enquanto o CIE pode durar até 10 anos. A taxa para aquisição do CNS é de 20 euros e do CIE de 25 euros (EUROSMART, 2013).

### 5.3.8 Lituânia

O eID da Lituânia, produzido pela Gemalto desde 2009, foi utilizado por 2,49 milhões de habitantes até dezembro de 2012. O novo eID tem como propósito a substituição do cartão de identificação pessoal padrão, introduzido em 2003, que tinha

como principal papel provar a identidade e a nacionalidade do cidadão lituano, sendo obrigatório para cidadãos acima de 16 anos. Uma observação interessante é que para promover uma maior penetração do eID e também para torná-lo mais atrativo, as taxas estaduais foram reduzidas em mais de 60% em 2011 (Lehmann, 2013). No sentido de promoção da utilização do eID, existem terminais especiais nos pontos de emissão de cartão de eID e o desenvolvimento de pontos de acesso à Internet nas zonas rurais, tudo para alcançar o uso mais amplo de *e-services*.

As funcionalidades oferecidas pelo eID lituano são: as funções de autenticação, para o acesso aos serviços *e-gov*; de assinatura, opcional e pago, disponível para pessoas acima de 18 anos; e de passaporte, o qual implementa verificação de identidade com base em dados biométricos (análise de digitais). O eID tem duas aplicações padrão, funcionando como o cartão de cidadania europeia e também como documento de viagem (ICAO 9303). A vida útil do eID é de 10 anos (EUROSMART, 2013).

O eID lituano armazena dois certificados digitais distintos, um para autenticação e outro para assinatura. Os certificados seguem o padrão X.509. As chaves privadas correspondentes são acessadas por PINs distintos. Cada certificado contém um identificador único do proprietário do certificado, o qual é composto por 11 dígitos. O *chip* sem contato do eID lituano fornece autenticação passiva, gerenciada por uma certificação do terminal. Assim, quando o eID é utilizado a aplicação de serviço valida a *string* do identificador único, valida o certificado e realiza a autenticação.

### 5.3.9 Espanha

A Espanha é um estado descentralizado composto por dezessete comunidades (regiões) autônomas e duas cidades autônomas. Tal situação acarreta às iniciativas de *e-gov* central e regional diferirem em termos do nível, velocidade de desenvolvimento e extensão das aplicações de *e-gov*. No entanto, há um grande esforço para o uso do cartão DNIe (DNI – Documento Nacional de Identidad). O DNIe é obrigatório para pessoas acima de 14 anos. As iniciativas *e-gov* regionais que utilizam sistemas de autenticação eletrônico são conduzidas e coordenadas pelas suas administrações regionais (Lehmann, 2013). Entre os serviços *online* oferecidos pelo DNIe, pode-se citar

os serviços de benefício de seguro nacional, de registro de carro, de procura de trabalho, de imposto de renda, os relacionados à saúde, etc.

O DNIe fornece as funções de autenticação para provar a identidade do titular e assinatura de documentos com valor legal equiparado à assinatura manuscrita. Essas funções são associadas aos dois certificados e aos pares de chaves correspondentes armazenados no cartão DNIe. O DNIe é obtido nas Estações de Polícia Nacional e a Direção Geral da Polícia (Ministério do Interior) exerce o papel de AC. O tempo de validade do documento DNIe é de 10 anos e sua aquisição tem uma taxa de 10,40 euros (EUROSMART, 2013).

O cartão DNIe contém o número DNI, que também é utilizado em outros documentos, como o passaporte e a carteira de habilitação. O certificado do DNIe também contém o número DNI. Os certificados do DNIe seguem o padrão X.509v3. Utiliza-se o RSA de 2048 bits no certificado de autenticação. O certificado de assinatura é opcional, possuindo três níveis de assinatura, dependendo do uso de PIN ou biometria.

### 5.3.10 Portugal

Portugal implantou desde 2007 o Cartão de Cidadão, um cartão de identidade obrigatório e emitido para qualquer pessoa para registro da população acima de 6 anos. O Cartão de Cidadão surgiu para substituir os cartões anteriores, listados a seguir: o cartão de identidade nacional, o cartão de imposto, o cartão de seguridade social, o cartão de eleitor e o cartão de assistência médica. A solução portuguesa de eID é fornecida pela Gemalto e também pela Zete Burtica (Lehmann, 2013).

A motivação da criação do Cartão de Cidadão foi a simplificação do procedimento de identificação, colocando vários documentos nacionais de identificação juntos em um único documento, seguindo os requisitos da UE. Além disso, o Cartão de Cidadão suporta interações eletrônicas seguras entre as entidades e os cidadãos estatais e privadas, ou seja, a sua multifuncionalidade permite que cada cidadão a se identificar eletronicamente e ter uma assinatura eletrônica legalmente válida à sua disposição, contribuindo, assim, para a implantação de serviços públicos / privados orientados ao cliente.

O eID português contém dois certificados: um para autenticação (obrigatório) e outro para assinatura (opcional). Ambos os certificados têm validade de 5 anos. A assinatura utiliza o algoritmo RSA de 2048 bits e SHA-1. Existem três PINs distintos para o acesso às funcionalidades do eID: para autenticação, para assinatura eletrônica e para o acesso de informação de endereço contido no eID. A PKI que controla os certificados do eID português estão sob a responsabilidade do Ministério da Justiça. A tempo de vida do eID é de 10 anos (EUROSMART, 2013).

# 6. Aspectos práticos para o uso de certificação digital no RIC

Nesse capítulo serão abordados aspectos práticos para a utilização de certificação digital no RIC, tais como a necessidade de uso da ICP-Brasil, as possíveis ACs parceiras que já fazem parte da ICP-Brasil e a alternativa de montagem de uma AC própria para o RIC. Também é realizada uma análise dos algoritmos criptográficos empregados nos certificados digitais e uma avaliação do custo dos certificados para uso nos documentos RIC.

## 6.1 Necessidade de uso da ICP-Brasil para o RIC

A Medida Provisória N° 2.200-2 (Brasil, Medida Provisória N 2.200-2, 2001), a qual institui a ICP-Brasil e define as competências gerais da AC Raiz, prevê no § 1° do artigo 10 que os documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil são presumidos verdadeiros em relação aos signatários. Os documentos em forma eletrônica que utilizam o processo de certificação da ICP-Brasil são considerados documentos públicos (Guelfi, 2007), uma vez que são oriundos de Pessoa Jurídica de Direito Público. Tais características, a presunção de serem verdadeiros em relação aos signatários e terem fé pública, são interessantes para o RIC e, de certa forma, justificam o uso da infraestrutura da ICP-Brasil.

Por outro lado, é previsto também na Medida Provisória N° 2.200-2 (Brasil, Medida Provisória N 2.200-2, 2001), em seu artigo 10 § 2°, a possibilidade de outros meios de

comprovação da autoria e integridade de documentos em forma eletrônica fora da ICP-Brasil, sob a condição de que tais meios sejam admitidos pelas partes como válido ou sejam aceitos pela pessoa a quem for oposto o documento. Percebe-se assim que não há impedimento para que o uso de certificação digital no RIC seja implementado com uma infraestrutura fora da ICP-Brasil. Contudo, tal opção deve ter o amparo da admissão das partes para considerar os certificados e os documentos eletrônicos assinados como válidos.

Assim, baseando-se na Medida Provisória n° 2.200-2, pode-se entender que não seria necessário para o RIC utilizar a ICP-Brasil. No entanto, o Decreto n° 3.996 (Brasil, DECRETO Nº 3.996, 2001) sinaliza que a questão não é tão simples, pela definição de que as entidades da Administração Pública Federal somente poderão prestar ou contratar serviços de certificação digital mediante autorização prévia do Comitê Executivo do Governo Eletrônico. O mesmo decreto ainda cita que os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal devem ser providos no âmbito da ICP-Brasil.

Nota-se algumas poucas iniciativas de PKI no âmbito da administração pública federal. Pode-se citar entre elas a PKI para o Exército Brasileiro (Vieira, 2008) e também a ICPEdu (PKI para Ensino e Pesquisa utilizada por universidades federais e estaduais) (RNP, n.d.). Observa-se, no entanto, que tais PKIs possuem uso restrito internamente às instituições, e são implantadas aos moldes da ICP-Brasil, visando garantir a compatibilidade com os padrões. Cabe ainda mencionar que há uma tendência de tais iniciativas a serem incorporadas à ICP-Brasil, como o caso da PKI do Exército, a qual deve se transformar na ICP-Defesa, já em processo de implantação (ITI, 2013).

Diante o exposto, depreende-se que é necessário um debate junto ao ITI e do Comitê da ICP-Brasil sobre a interpretação da obrigatoriedade de uso da ICP-Brasil para serviços de certificação digital no RIC. O emprego de uma PKI própria para uso exclusivo de autenticação eletrônica pode ser uma alternativa para garantir a legalidade. A possibilidade do RIC funcionar fora da ICP-Brasil deve ser avaliada mediante a autorização do Comitê Executivo do Governo Eletrônico, além de levar em conta outros aspectos a fim de verificar as vantagens e desvantagens da ICP-Brasil. Entre os aspectos a serem estudados, pode-se elencar o custo de implantação de uma AC, seja dentro da ICP-Brasil ou fora, e as possíveis ACs Públicas que poderiam fazer

parceria para a emissão de documentos RIC. Tais aspectos serão cobertos a seguir.

## 6.2 Construção de uma AC na ICP-Brasil

Nesse tópico será considerado a construção de uma AC de 1° nível na ICP-Brasil subordinada à AC-Raiz. Essa AC de 1° nível seria capaz de emitir os certificados para os documentos RIC. Para implementar uma AC na ICP-Brasil, a AC candidata deve se submeter ao processo de credenciamento junto à ICP-Brasil. As regras para credenciamento estão descritas no documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil – DOC-ICP-03 (ITI, 2014).

Os critérios gerais para o credenciamento de entidades na ICP-Brasil são apresentados a seguir.

a) Ser órgão ou entidade de direito público ou pessoa jurídica de direito privado – uma AC nunca poderá ser entendida como uma pessoa física.
b) Estar quite com todas as obrigações tributárias e os encargos sociais instituídos por lei.
c) Atender aos requisitos relativos à qualificação econômico-financeira estabelecidos, conforme a atividade a ser desenvolvida – tais requisitos correspondem a uma lista de documentos exigidos que comprovem a saúde financeira da entidade candidata. Entre os principais documentos exigidos pode-se destacar: balanço patrimonial do último exercício financeiro ou demonstrativo financeiro, certidão negativa de falência ou concordata e, em alguns casos, documentos que comprovam patrimônio líquido igual ou superior a R$ 2.500.000,00 e fiança bancária no valor de seu capital social integralizado.
d) Atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica – nesse critério a AC candidata deve apresentar documentos técnicos como, DPC da AC, Políticas de Certificado (PC), Políticas de Segurança e documento explicitando se pretende ou não emitir certificados às autoridades certificadoras inferiores ao seu nível.

A seguir são apresentados os critérios específicos para o credenciamento de uma AC na ICP-Brasil.

a) Apresentar, no mínimo, uma entidade operacionalmente vinculada, candidata

ao credenciamento para desenvolver as atividades de AR, ou solicitar o seu próprio credenciamento como AR.

b) Apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS.

c) Ter sede administrativa localizada no território nacional.

d) Ter instalações operacionais e recursos de segurança física e lógica, inclusive sala-cofre, compatíveis com a atividade de certificação, localizadas no território nacional, ou contratar PSS que as possua.

Havendo o cumprimento de todos os critérios para credenciamento, a AC candidata encaminha à AC-Raiz a solicitação de credenciamento apresentando uma série de documentos, como o formulário Solicitação de Credenciamento de AC, documentos probantes do cumprimento dos critérios requeridos para credenciamento, documento Solicitação de Credenciamento de AR, etc. A solicitação de credenciamento dever ser protocolada no Protocolo-Geral da AC-Raiz e recebida, em até 30 dias, por intermédio de despacho fundamentado.

Dando continuidade ao processo de credenciamento da AC, após a publicação do despacho de recebimento da solicitação pela AC-Raiz, inicia-se o processo de auditoria pré-operacional, com a submissão de formulário de Requerimento de Auditoria pela AC candidata no prazo máximo de 30 dias, no qual declara estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil e estar pronto para ser auditado no prazo de 15 dias.

Finalizadas as tarefas de auditoria e fiscalização, será apresentado o relatório de auditoria final à AC-Raiz, a qual deve manifestar, no prazo máximo de 30 dias, sobre o deferimento ou indeferimento da solicitação de credenciamento da AC candidata, cabendo recurso administrativo desta junto ao CG da ICP-Brasil. O ato de deferimento do credenciamento se limita às PCs indicadas na solicitação. Pode haver deferimento total ou parcial do credenciamento, no qual o deferimento parcial se refere àquele que não contempla todas as PCs propostas pela AC candidata. Em caso de deferimento, o ato de credenciamento da AC condicionará a emissão do certificado pela AC-Raiz ao pagamento de tarifa estabelecida nas Diretrizes da Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil (ITI, 2008) e também à apresentação, no prazo máximo de 10 dias após o deferimento do credenciado, de apólice de contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e

de registro, com cobertura suficiente e compatível com o risco dessas atividades. O credenciamento consome-se com a emissão do certificado da AC. Após o deferimento do credenciamento, a AC-Raiz deve emitir no prazo máximo de 10 dias o certificado da AC credenciada, a qual terá um prazo de 60 dias para entrar em operação.

Em termos de custo de implantação de uma AC de 1º nível, a tarifa de emissão de certificado pela AC Raiz é definida com o valor de R$ 500.000,00. Além disso, há também o custo do serviço prestado na auditoria pré-operacional no valor de R$ 50.000,00. Porém, a Administração Direta da União é dispensada do pagamento das tarifas de emissão de certificado e auditoria pré-operacional pela AC-Raiz da ICP-Brasil (ITI, 2008), de forma que o custo se restringe à aquisição de equipamentos e serviços necessários para implantar uma AC e à apólice de seguro mencionada.

Observa-se que o custo para implantação de uma AC própria para o RIC é equivalente em ambos cenários, tanto se a AC estivesse na ICP-Brasil como se estivesse fora, tendo em vista a dispensa de pagamento das tarifas para a Administração Direta da União. Logo, a questão do uso da ICP-Brasil para criação de uma AC própria para o RIC deve ser permeada pelas vantagens já mencionadas dos certificados emitidos no âmbito da ICP-Brasil, bem como as implicações técnicas quanto à adequação dos padrões exigidos pelo ITI. Uma estimativa dos custos envolvidos para a implantação da infraestrutura de uma AC pode ser obtida em projetos como o ICPEdu, a infraestrutura de Chaves Públicas para Ensino e Pesquisa, lançada em 2007, pela iniciativa de algumas instituições de ensino e pela RNP (Rede Nacional de Ensino e Pesquisa), ou pela implantação recente da AC-MRE.

## 6.3 Possíveis parceiras - ACs Públicas

Como já fora mencionado, a ICP-Brasil é composta por entidades públicas e privadas. Nesse contexto, é natural associar as entidades públicas da ICP-Brasil como prováveis parceiras para a implantação do projeto RIC, no que diz respeito ao uso de certificação digital. Baseando-se nesse pressuposto, é apresentada uma lista das ACs públicas de 1° nível que poderiam atuar como futuras parceiras do RIC. Limitou-se os estudos para as ACs de 1° nível no intuito de simplificar a busca dos possíveis parceiros, haja visto o grande número de entidades que atuam no 2° nível.

### 6.3.1 AC Serviço Federal de Processamento de Dados (AC-SERPRO)

A AC-SERPRO foi a primeira Autoridade Certificadora de 1° nível credenciada pela ICP-Brasil. Atualmente o SERPRO está entre as quatro únicas empresas que possuem infraestrutura necessária para a prestação de serviços de certificação digital. Além de manter infraestrutura de sua própria AC, o SERPRO hospeda também as ACs da Presidência da República, Receita Federal, Justiça Federal, Casa da Moeda e Proderj (SERPRO, 2011), e, recentemente, do Ministério de Relações Exteriores. Cabe ressaltar a Instrução Normativa nº 4 MP/SLTI para a concentração de serviços em uma única infraestrutura, com o objetivo de reduzir os custos, e o Decreto 8135 sobre o uso de bases públicas para aplicações críticas da segurança da informação. Pelas diretrizes supracitadas, a eventual implantação de uma AC RIC deveria ser feita dentro da infraestrutura de segurança de dados existente (e.g. Serpro), a exemplo do que foi adotado em diversos órgãos públicos.

A AC-SERPRO emite certificados para ACs de nível imediatamente subsequente ao seu. Assim, os titulares de seus certificados são entidades pessoas jurídicas, credenciadas pela AC-Raiz para integrar a ICP-Brasil e autorizadas pela AR da AC-SERPRO a receberem certificados digitais emitidos pela AC-SERPRO (AC-SERPRO, 2012). A

Tabela 19

~~Tabela 19~~

~~Tabela 19~~ apresenta algumas características relativas ao padrão de segurança adotado para a geração do par de chaves criptográficas na AC-SERPRO.

**Tabela 19 – Características gerais da AC-SERPRO**

| Característica | Descrição |
|---|---|
| **Titulares de Certificado** | AC de nível imediatamente ao seu. |
| **Aplicabilidade dos certificados** | Utilização exclusiva para a assinatura de certificados digitais e LCRs emitidos pelas ACs de nível imediatamente subsequentes ao da AC-SERPRO. |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-4096 bits para a AC-SERPRO V3 e RSA-2048 bits para as AC-SERPRO V1 e V2. |

| | |
|---|---|
| **Prestador de Serviço** | Não utiliza. |

**Fonte:** Portal AC-SERPRO (AC-SERPRO, 2012).

A AC-SERPRO abriga duas ACs do próprio SERPRO de 2° nível: a AC-SERPRO-ACF e a AC-PRODERJ. A Tabela 20~~Tabela 20~~~~Tabela 20~~ apresenta as características básicas dos certificados e chaves de tais ACs.

**Tabela 20– Características gerais da AC-SERPRO-ACF e AC-PRODERJ**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | AC-SERPRO-ACF: certificados A1, A3, SPB A1, S1, S3 e T3. |
| | AC-PRODERJ: certificados A3. |
| **Titulares de Certificado** | SERPRO A1, A3, S1 e S3: pessoas físicas ou jurídicas. |
| | SERPRO SPB A1: instituições do Sistema Brasileiro de Pagamentos. |
| | SERPRO T3: pessoas jurídicas responsáveis por Autoridades de Carimbo de Tempo. |
| | PRODERJ A3: pessoas físicas. |
| **Aplicabilidade dos certificados** | A1 e A3: assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal para as aplicações de confirmação de Identidade na *Web*, correio eletrônico, transações *online*, Redes privadas virtuais (VPN), transações eletrônicas e criação de chave de sessão e assinatura de documentos eletrônicos com verificação de integridade de suas informações. |
| | S1 e S3: apenas para aplicações de sigilo como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo. |
| | T3: em aplicações mantidas por Autoridades de Carimbo de Tempo para assinaturas de carimbos de tempo. |
| **Algoritmo/Tamanho das chaves criptográficas** | A1 e A3: RSA-1024 bits (cadeia de certificados V1) e RSA-2048 bits (cadeia de certificados V2) |
| | S1, S3 e T3: RSA-2048 bits. |

**Fonte:** Portal AC-SERPRO (AC-SERPRO, 2012).

### 6.3.2 AC Caixa Econômica Federal (AC-CAIXA)

A Caixa Econômica Federal (CEF) é a única instituição financeira, até o presente momento, credenciada como Autoridade Certificadora ICP-Brasil. A AC-CAIXA é sua AC de 1° nível, a qual tem por objetivo assinar os certificados digitais de nível imediatamente subsequente ao seu. A AC-CAIXA não utiliza prestador de serviço de suporte em suas operações, contando com infraestrutura própria. A Tabela 21~~Tabela 21~~~~Tabela 21~~ apresenta um resumo das principais características relativas ao padrão de segurança adotado para a geração do par de chaves criptográficas na AC-CAIXA.

**Tabela 21 – Características gerais da AC-CAIXA**

| Característica | Descrição |
|---|---|
| **Titulares de Certificado** | AC de nível imediatamente ao seu. |
| **Aplicabilidade dos certificados** | Identificação das ACs de nível imediatamente subsequente ao seu e a divulgação das suas chaves públicas de forma segura. |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-2048 bits para a cadeia de certificação V1 e RSA-4096 bits para a cadeia de certificação V2. |
| **Prestador de Serviço** | Não utiliza. |

**Fonte:** Portal AC-CAIXA (CEF, 2014).

A CEF tem trabalhado para que a certificação digital integre serviços que resultem em melhoras para seus funcionários, clientes e titulares das contas de Fundo de Garantia por Tempo de Serviço (FGTS). Para tal propósito a CEF possui ACs de 2° nível: a AC-CAIXA-PF, a AC-CAIXA-PJ e a AC-CAIXA-SPB, destinadas para criação de certificados digitais para Pessoas Físicas (PF), Pessoas Jurídicas (PJ) e Pessoas Jurídicas do Sistema de Pagamentos Brasileiro (SPB). De forma sucinta, a Tabela 22~~Tabela 22~~~~Tabela 22~~ mostra as características de segurança das chaves dessas ACs.

**Tabela 22 – Características gerais da AC-CAIXA-PF, AC-CAIXA-PJ e AC-CAIXA-SPB**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | AC-CAIXA-PF: certificados A1 e A3 |
| | AC-CAIXA-PJ: certificados A1, A3, T3 e T4 |
| | AC-CAIXA-SPB: certificados A1 |
| **Titulares de Certificado** | AC-CAIXA-PF: Pessoas Físicas |

| | |
|---|---|
| | AC-CAIXA-PJ: Pessoas Jurídicas |
| | AC-CAIXA-SPB: Pessoas Jurídicas do Sistema de Pagamentos Brasileiro |
| **Aplicabilidade dos certificados** | A1 e A3: Destinam-se à utilização em aplicações como confirmação de identidade, correio eletrônico, transações *on-line*, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação de integridade de suas informações. |
| | T3 e T4: destinam-se à utilização em aplicações do tipo Servidor de Carimbo de Tempo para a confirmação de identidade e assinatura de carimbos de tempo. |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-1024 bits (cadeia de certificados V1) e RSA-2048 bits (cadeia de certificados V2) |

**Fonte:** Portal AC-CAIXA (CEF, 2014).

### 6.3.3 AC Imprensa Oficial do Estado de São Paulo (AC-Imprensa-Oficial)

A Imprensa Oficial do Estado de São Paulo tem por objetivo principal organizar e divulgar, por meio do Diário Oficial, as leis e os atos das três esferas do governo do Estado de São Paulo – Executivo, Legislativo e Judiciário (Imprensa Oficial SP, 2015). Ao longo de sua história, a Imprensa Oficial passou por muitas transformações, sendo a mais recente a de assumir a responsabilidade de se tornar uma Autoridade Certificadora, alinhando o compromisso de aprofundar a modernização, introduzir novos processos de gestão, elevar os investimentos em tecnologia de informação e consolidar as parcerias com a sociedade civil.

A AC-Imprensa Oficial oferece produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, incluindo todas as esferas da administração pública, direta ou indireta, nos âmbitos federal, estadual e municipal. A Tabela 23~~Tabela 23~~~~Tabela 23~~ apresenta algumas características da AC-Imprensa-Oficial de 1° nível.

**Tabela 23 – Características gerais da AC-Imprensa-Oficial**

| Característica | Descrição |
|---|---|
| **Titulares de Certificado** | AC de nível imediatamente ao seu. |

| | |
|---|---|
| **Aplicabilidade dos certificados** | Utilização exclusiva para a assinatura de certificados digitais e LCRs emitidos pelas ACs de nível imediatamente subsequentes ao da AC Imprensa Oficial. |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-4096 bits (mínimo). |
| **Prestador de Serviços de Suporte** | Digitalsign Certificadora Digital Ltda |

**Fonte:** Portal AC-Imprensa-Oficial (Imprensa Oficial SP, 2015).

A AC-Imprensa-Oficial de 1° nível, também conhecida como a AC Principal da Imprensa Oficial abriga a AC-Imprensa-Oficial de 2° nível. A Tabela 24~~Tabela 24~~~~Tabela 24~~ apresenta algumas características da AC-Imprensa-Oficial de 2° nível.

**Tabela 24 – Características gerais da AC-Imprensa-Oficial de 2° nível**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A1, A3, A4, T3, T4, S1, S3 e S4 |
| **Titulares de Certificado** | Pessoas Físicas ou Jurídicas de direito público ou privado, nacionais ou internacionais. |
| **Aplicabilidade dos certificados** | A1, A3 e A4: uso em aplicações como assinatura digital em correio eletrônico; assinatura de código de *software*; acesso a aplicações da Receita Federal ou de qualquer órgão da Administração Pública Direta ou Indireta que aceitem o certificado; *software* de assinatura elaborado em parceria com outros órgãos, entidades ou empresas; confirmação de identidade na *Web*; transações eletrônicas e transações on-line; redes privadas virtuais (VPN); cifração de chaves de sessão. |
| | T3 e T4: uso em aplicações como confirmação de identidade e assinatura digital de documentos eletrônicos com verificação da integridade e de suas informações. |
| | S1, S3 e S4: uso em aplicações tais como cifra de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo. |
| **Algoritmo/Tamanho das chaves criptográficas** | A1, A3, T3, S1 e S3: RSA-2048 bits. |
| | A4, T4 e S4: RSA-4096 bits. |

**Fonte:** Portal AC-Imprensa-Oficial (Imprensa Oficial SP, 2015).

### 6.3.4 Autoridade Certificadora da Justiça (AC-JUS)

A AC-JUS alavancou a implantação da Certificação Digital no Judiciário fomentando o desenvolvimento de aplicações para comunicação e troca de documentos eletrônicos, agora com validade legal, viabilizando dessa forma o advento do Processo Judicial Eletrônico, viabilizando dentre outros, o Processo Judicial Eletrônico (PJ-e). A AC-JUS por ser AC de 1º nível não emite certificados para usuários finais, isto é, apenas emite certificados para as suas Autoridades Certificadoras subordinadas. Estas sim emitem os certificados para os usuários finais, que podem ser Magistrados e servidores, equipamentos e aplicações dos poderes judiciário, executivo ou legislativos federal ou estadual. Atualmente compõe a cadeia da AC-JUS: Certisign-JUS, SERASA-JUS, VALID-JUS, SOLUTI-JUS, SERPRO-JUS e CAIXA-JUS. A Tabela 23~~Tabela 23~~~~Tabela 23~~ apresenta algumas características da AC-JUS de 1° nível.

**Tabela 25 – Características gerais da AC-JUS**

| Característica | Descrição |
|---|---|
| **Titulares de Certificado** | AC de nível imediatamente ao seu. |
| **Aplicabilidade dos certificados** | Utilização exclusiva para a assinatura de certificados digitais e LCRs emitidos pelas ACs de nível imediatamente subsequentes ao da AC-JUS. |
| **Algoritmo/Tamanho das chaves criptográficas associadas a certificados emitidos pela AC CAIXA** | RSA-2048 bits para certificados emitidos até 31/12/2011 e RSA-4096 bits para certificados emitidos a partir de janeiro de 2012. |
| **Prestador de Serviços de Suporte** | SERPRO |

**Fonte:** Portal AC-JUS (AC-JUS, 2014).

A AC-JUS criou a marca **Cert-JUS** para identificar os certificados emitidos na sua cadeia de certificação. Na cadeia de certificação AC-JUS foram definidos quatro perfis de certificado, a saber.

- **Cert-JUS Institucional** - certificado Pessoa Física do tipo A3 ou A4 destinado a magistrados e servidores do judiciário, para assinatura de documentos oficiais e *e-mail*, *login* na rede e acesso a aplicações.

- **Cert-JUS Poder Público** - certificado Pessoa Física do tipo A3 ou A4 destinado a autoridades e servidores público em geral, dos Poderes Executivo, Legislativo, Ministério Público, Tribunais de Contas etc, para assinatura de documentos oficiais e *e-mail*, *login* na rede e acesso a aplicações.
- **Cert-JUS Equipamento Servidor** - certificado Pesssoa Jurídica, do tipo A1, para utilização em servidores de aplicação internos ou disponíveis na *Internet*. Já é utilizado em vários servidores do Judiciário para autenticar aplicações e portais, bem como para estabelecer conexões *Web* seguras.
- **Cert-JUS Código Seguro**- certificado pessoa Jurídica, tipo A1 ou A3, utilizado para assinatura do código das aplicações *online* disponíveis ao público. Assim será possível ao usuário dos portais e aplicações da Justiça verificar a autenticidade de *applets* e outros códigos que seja necessário instalar para acesso às aplicações.

Uma observação a ser feita é que os certificados Cert-JUS só serão emitidos após autorização de autoridade competente do órgão. Para fins de ilustração, apresenta-se na Tabela 26~~Tabela 26~~Tabela 26 as características gerais da AC de 2° nível SERPRO-JUS:

**Tabela 26 – Características gerais da AC-SERPRO-JUS**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A1, A3 |
| **Titulares de Certificado** | Órgãos da administração pública direta e indireta. Órgãos não pertencentes ao Poder Judiciário, mediante cadastramento aprovado pela AC-JUS. |
| **Aplicabilidade dos certificados** | A1: conforme Cert-JUS Equipamento Servidor e Cert-JUS Código Seguro. |
| | A3: conforme Cert-JUS Institucional, Cert-JUS Poder Público e Cert-JUS Código Seguro |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-1024 bits (ACSERPRO-JUS V1 e V3) e RSA-2048 bits (ACSERPRO-JUS V4). |

**Fonte:** Portal AC-JUS (AC-JUS, 2014).

### 6.3.5 AC da Presidência da República (AC-PR)

Credenciada a emitir Certificados Digitais totalmente aderentes às normas, padrões estabelecidos pelo Comitê Gestor da ICP-Brasil, a Autoridade Certificadora da Presidência da República – AC-PR foi criada em abril de 2002, por uma iniciativa da Casa Civil, no âmbito do governo eletrônico (*e-Gov*). A AC-PR emite certificados para autoridades e servidores da Presidência da República e da Vice-Presidência da República e para autoridades e servidores do Poder Executivo Federal que necessitam utilizar certificado digital para autenticação em aplicativos geridos pela PR.

**Tabela 27 – Características gerais da AC-PR**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A1 e A3 |
| **Titulares de Certificado** | a) Servidores que integram a estrutura da Presidência da República ou Vice-Presidência da República, que necessitam de certificados digitais para o exercício de suas funções; □<br>b) Agentes públicos, indicados pelos Gestores dos Órgãos Essenciais da PR, que necessitam de certificados digitais para utilização em serviços geridos por esses órgãos.<br>c) Autoridades que não pertencem ao Poder Executivo Federal, autorizadas pela Secretaria Geral a receberem certificados digitais. |
| **Aplicabilidade dos certificados** | A1: utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações. |
| | A3: Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal.□Podem ser usados nas seguintes aplicações;<br>□ Confirmação de Identidade na *Web*; □<br>□ Correio eletrônico; □<br>□ Transações *online*; □<br>□ Redes privadas virtuais (VPN); □<br>□ Transações eletrônicas; □<br>□ Criação de chave de sessão e assinatura de documentos □eletrônicos com verificação da integridade de suas □informações.<br>□ Assinatura de códigos □ |

| | |
|---|---|
| **Algoritmo/Tamanho das chaves criptográficas** | RSA 1024 (V0 e V1) e 2048 (V2) |
| **Prestador de Serviços de Suporte** | SERPRO |

**Fonte:** Portal AC-PR (AC-PR, 2011).

### 6.3.6 AC Secretaria da Receita Federal do Brasil (AC-RFB)

A AC-RFB disponibiliza serviços com o objetivo de simplificar ao máximo a vida dos contribuintes, facilitando o cumprimento espontâneo das obrigações tributárias para os que possuem certificados digitais ICP-Brasil. A AC-RFB, por ser AC de 1º nível, não emite certificados para usuários finais, isto é, apenas emite certificados para as suas Autoridades Certificadoras subordinadas. A Tabela 28~~Tabela 28~~~~Tabela 28~~ apresenta algumas características da AC-RFB de 1° nível.

**Tabela 28 – Características gerais da AC-RFB**

| Característica | Descrição |
|---|---|
| **Titulares de Certificado** | AC de nível imediatamente ao seu. |
| **Aplicabilidade dos certificados** | Utilização exclusiva para a assinatura de certificados digitais e LCRs emitidos pelas ACs de nível imediatamente subsequentes ao da AC-RFB. |
| **Algoritmo/Tamanho das chaves criptográficas associadas a certificados emitidos pela AC CAIXA** | RSA-4096 bits para certificados emitidos pela AC-RFB a partir da sua versão 3 (AC-RFBv3) e RSA-2048 bits para certificados AC-RFBv1 e AC-RFBv2. |
| **Prestador de Serviços de Suporte** | SERPRO |

**Fonte:** Portal AC-RFB (AC-RFB, 2013).

Atualmente a AC-RFB abriga 17 ACs de 2° nível credenciadas, relacionadas a seguir: AC-CERTISIGN-RFB, AC-IMESP-RFB, AC-PRODEMGE-RFB, AC-SERASA-RFB, AC-SERPRO-RFB, AC-SINCOR-RFB, AC-FENACON-CERTISIGN-RFB, AC-NOTARIAL-RFB, AC-BR-RFB, AC-INSTITUTO-FENACON-RFB, AC-PRODEST-RFB, AC-VALID-RFB, AC-DIGITALSIGN-RFB, AC-BOA-VISTA-RFB, AC-SINCOR-RIO-RFB, AC-SAFEWEB-RFB e AC-CNDL-RFB. As ACs de 2° nível da AC-RFB devem seguir aos padrões de certificados estabelecidos no documento “Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil” (AC-RFB, 2013), o qual prevê os

seguintes padrões.

- **e-CPF**: certificado digital destinado a todas as pessoas físicas que possuem registro no Cadastro de Pessoa Física da Receita Federal do Brasil (CPF). Os certificados e-CPF são utilizados para assinatura digital e autenticação do seu titular em sistemas e aplicações. O algoritmo utilizado para a geração das chaves dos certificados e-CPF é o RSA. São quatro os tipos de certificados admitidos: A1, A2, A3 e A4.
- **e-CNPJ**: certificado digital destinado a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ). Os certificados e-CNPJ são utilizados para assinatura digital e autenticação do seu titular em sistemas e aplicações. O algoritmo utilizado para a geração das chaves dos certificados e-CNPJ é o RSA. São quatro os tipos de certificados admitidos: A1, A2, A3 e A4.
- **e-Servidor**: certificado digital destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ). Os certificados e-Servidor são utilizados para a identificação de equipamentos servidores *Web.* O algoritmo utilizado para a geração das chaves dos certificados e-Servidor é o RSA. São quatro os tipos de certificados admitidos: A1, A2, A3 e A4.
- **e-Aplicação**: certificado digital destinado a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ). Os certificados e-Aplicação são utilizados exclusivamente para autenticação de aplicações. O algoritmo utilizado para a geração das chaves dos certificados e-Aplicação é o RSA. São quatro os tipos de certificados admitidos: A1, A2, A3 e A4.
- **e-Código**: certificado digital destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ). Os certificados e-Código são utilizados exclusivamente para assinatura de código de *software*. O algoritmo utilizado para a geração das chaves dos certificados e-Código é o RSA. São quatro os tipos de certificados admitidos: A1, A2, A3 e A4.

Para fins de ilustração, apresenta-se na Tabela 29~~Tabela 29~~Tabela 29 as

características gerais da AC de 2° nível AC-SERPRO-RFB:

**Tabela 29 – Características gerais da AC-SERPRO-RFB**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A1, A3 |
| **Titulares de Certificado** | Pessoas físicas ou jurídicas. |
| **Aplicabilidade dos certificados** | Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal.□Podem ser usados nas seguintes aplicações;<br>□ Confirmação de Identidade na *Web*; □<br>□ Correio eletrônico; □<br>□ Transações *online*; □<br>□ Redes privadas virtuais (VPN); □<br>□ Transações eletrônicas; □<br>□ Criação de chave de sessão e assinatura de documentos □eletrônicos com verificação da integridade de suas □informações. |
| **Algoritmo/Tamanho das chaves criptográficas** | RSA-1024 bits (ACSERPRO-RFB V1 e 2) e RSA-2048 bits (ACSERPRO-RFB V3 e V4). |

**Fonte:** Portal AC-RFB (AC-RFB, 2013).

### 6.3.7 AC Casa da Moeda do Brasil (AC-CMB)

A Casa da Moeda do Brasil está entre as mais antigas instituições públicas brasileiras, e busca por meio da AC-CMB consolidar a modernização de sua estrutura produtiva e administrativa, bem como se habilitar para atender ao mercado de segurança na era virtual. Tal como a AC-PR, a AC-CMB é uma AC de 1° nível que fornece certificados a usuários finais. A Tabela 30~~Tabela 30~~~~Tabela 30~~ apresenta as características gerais da AC-CMB.

**Tabela 30 – Características gerais da AC-CMB**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A1, A3 e A4 |
| **Titulares de Certificado** | A1: os órgãos e entidades que integram a estrutura da |

| | |
|---|---|
| | Casa da Moeda do Brasil, cuja área de atuação abrange a responsabilidade pela aplicação ou equipamento para os quais serão emitidos certificados. |
| | A3: pessoas físicas ou jurídicas autorizadas pelas AR vinculadas a receber certificados digitais emitidos pela AC-CMB, para sua própria utilização. |
| | A4: Pessoas Físicas e Jurídicas de órgãos e entidades que integram a estrutura da Casa da Moeda do Brasil ou por ela autorizados. |
| **Aplicabilidade dos certificados** | Utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações. |
| **Algoritmo/Tamanho das chaves criptográficas associadas a certificados emitidos pela AC PR** | RSA-2048 bits e RSA-4096 bits |
| **Prestador de Serviços de Suporte** | SERPRO |

**Fonte:** Portal AC-CMB (AC-CMB, 2011).

Um aspecto interessante relativo a AC-CMB é a criação de certificados digitais para as carteiras de identificação profissional e passaportes, que são produzidas pela Casa da Moeda (ITI, 2015). Desde 2010, os passaportes veem sendo emitidos pela Polícia Federal (PF) e pela Casa da Moeda (CMB) com o uso de certificação digital, o que auxilia na segurança e no combate contra a falsificação do documento. O passaporte emitido pela PF e CMB passou a atender a todos os quesitos estipulados pela Organização Internacional de Aviação Civil (*International Civil Aviation Organization* - ICAO), uma entidade internacional que estabelece regras para o transporte de passageiros por todo o mundo (ITI, 2015).

### 6.3.8 AC Ministério das Relações Exteriores (AC-MRE)

Criada recentemente, a AC-MRE é a 14ª AC de 1° nível credenciada à ICP-Brasil, tendo por objetivo a emissão do certificado digital que assina os componentes eletrônicos do novo passaporte brasileiro, aderente ao *Public Key Directory* – PKD da Organização da Aviação Civil Internacional (ICAO), agência especializada das Nações Unidas. De fato, a AC-MRE emite certificados digitais para pessoas jurídicas autorizadas, as quais são responsáveis por assinar e gerar certificados eletrônicos para

os passaportes do Governo Brasileiro. Uma novidade adicionada na ICP-Brasil com a criação da AC-MRE é que se trata da primeira AC que utiliza o sistema de criptografia de curvas elípticas (ECC). A Tabela 31~~Tabela 31~~~~Tabela 31~~ apresenta as características gerais da AC-MRE.

**Tabela 31 – Características gerais da AC-MRE**

| Característica | Descrição |
|---|---|
| **Tipos de certificados** | A4 |
| **Titulares de Certificado** | Pessoas jurídicas autorizadas pela AR responsável a receber um certificado digital, emitido pela AC-MRE, para utilização em assinatura eletrônica de passaportes do Governo Brasileiro. |
| **Aplicabilidade dos certificados** | Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal.□Podem ser usados nas seguintes aplicações;<br>□ Assinatura de documentos oficiais do tipo passaporte. |
| **Algoritmo/Tamanho das chaves criptográficas associadas a certificados emitidos pela AC PR** | ECDSA-512 bits |
| **Prestador de Serviços de Suporte** | SERPRO |

**Fonte:** Portal AC-MRE (AC-MRE, 2015).

## 6.4 Análise das adequações da ICP-Brasil para conformidade com as normas ICAO e com a legislação RIC

A ICAO (*International Civil Aviation Organization*), entidade internacional que estabelece regras para o transporte de passageiros por todo o mundo, apresenta normas com requisitos quanto à confecção de passaportes e é uma referência em termos de padronização de tais documentos. Com o esforço do governo em modernizar o passaporte brasileiro e torná-lo aceitável internacionalmente, foi necessário verificar os requisitos necessários para adequá-lo às normas ICAO. Tais requisitos incidem também nos processos de certificação digital da ICP-Brasil, bem como no RIC.

### 6.4.1 Adequações à legislação referente ao RIC

Em virtude da perspectiva anterior de emprego de *applet* de certificação digital conforme o padrão ICP-Brasil no projeto piloto do documento RIC, em 2012, algumas adequações da ICP-Brasil ao RIC já foram feitas.

A resolução nº 84 de 17/11/2010 altera os DOC-ICP-04 e DOC-ICP-05, adequando o procedimento de emissão do certificado no documento RIC. É criado um campo *otherName* obrigatório para certificados vinculados a documento RIC, com OID=2.16.76.1.3.9 e com conteúdo das 11 primeiras posições equivalente ao número RIC. Ademais, descreve a necessidade de verificação biométrica no processo de solicitação do certificado no Órgão de Identificação.

### 6.4.2 Adequações ao padrão ICAO

A ICAO instituiu repositório próprio e específico denominado PKD (*Public Key Directory*) para a distribuição das cadeias de certificação utilizadas nas emissões de passaportes eletrônicos por todos os países membros. Inicialmente, o Brasil era um dos poucos países que possuía passaporte eletrônico, mas não participava do programa PKD, devido à não conformidade encontrada entre a PKD/ICAO e a ICP-Brasil. No entanto, foram realizados trabalhos pelo ITI, tendo em vista ao interesse de adesão ao referido diretório da ICAO, no sentido de adequar as normas da ICP-Brasil para entrarem em conformidade com as normas ICAO. Considerando que os certificados ICAO, usados no passaporte eletrônico brasileiro, são gerados usando a ICP-Brasil, e considerando algumas especificidades previstas nas normas ICAO, como o número de níveis da cadeia de certificação, a validade dos certificados embarcados nos passaportes e as limitações previstas nas normas ICAO para o emprego da ICP, diversas adaptações foram realizadas nas normas ICP-Brasil, conforme descrito a seguir.

#### 6.4.2.1 Número de níveis da cadeia de certificação ICAO

Segundo a norma ICAO Doc 9303, parte 3, vol2 (ICAO, 2008), a autoridade superior de cada país dentro da cadeia de certificação dos passaportes é denominada CSCA (*Country Signing Certificate Authority*). No âmbito da aplicação ICAO, a chave privada

do CSCA ($Kpriv_{CSCA}$) é usada para assinar certificado do *Document Signer* ($C_{DS}$), e por sua vez a chave privada do *Document Signer* ($Kpriv_{DS}$) é usada para assinar o *Document Security Objects* ($S_{OD}$), gravados no passaporte. Conforme o item 5.5.1 da referida norma, o certificado da CSCA deve ser auto-assinado e emitido pelo próprio CSCA. Na implementação inicial da cadeia ICAO no Brasil a Casa da Moeda do Brasil era assinada pela Raiz ICP- Brasil. Este problema foi resolvido através da Resolução nº 101 de 09/10/2013, que determinou a geração de certificados auto-assinados para a cadeia ICAO dentro do Brasil.

Inicialmente a função CSCA foi atribuída pela AC-CMB, entidade confeccionadora do passaporte brasileiro (ITI, 2015). Porém, com a criação da AC-MRE, cuja finalidade será a geração de certificados dos passaportes, é esperado que esta seja a nova CSCA no Brasil.

#### 6.4.2.2 Validade do certificado do passaporte e tamanho da chave

Segundo o documento da ICAO 9303, parte 1, volume 2 (ICAO, 2006), (item 9.3) o prazo de validade do certificado do emissor de passaporte deve ser igual à soma de 2 períodos:

- o tempo que esse certificado será usado para emitir passaportes;
- a maior validade de um passaporte emitido por esse emissor.

Para emitir passaporte com validade de 5 ano durante 1 ano, um emissor precisa de um certificado com 6 anos de prazo de validade. Ou seja, um emissor não pode emitir um documento com prazo de validade maior do que o seu próprio certificado.

Para que fosse compatibilizada a estrutura da ICP-Brasil com as normativas ICAO dever-se-ia aumentar o prazo de validade do certificado $C_{DS}$, de modo a atender ao requisito de que este certificado esteja válido durante todo o prazo de validade de todos os documentos assinados por ele. Na época o passaporte possuía validade de 5 anos, e considerando o prazo de uso de um ano para cada $C_{DS}$, foi adotada uma validade de 6 anos para o $C_{DS}$. A resolução nº 87 do ITI, dentre outras alterações, aumentou a validade dos certificados A4 para 6 anos.

Ademais, a adequação da ICP-Brasil para emissão de certificados com validade de 10 anos, compatível com a validado de 10 anos do novo passaporte, foi realizada

através da Resolução Nº 99 de 09/10/2013, que altera a tabela de períodos de certificados do DOC-ICP-04 para:

**Tabela 32 – Período de validade dos certificados ICP-Brasil**

| Tipo de Certificado | Validade (anos) | Chave |
|---|---|---|
| A1 e S1 | 1 | RSA 1024(V0 e V1) ou 2048 (V2), ECDSA 256 |
| A2 e S2 | 2 | RSA 1024(V0 e V1) ou 2048 (V2), ECDSA 256 |
| A3, S3 e T3 | 5 | RSA 1024(V0 e V1) ou 2048 (V2),ECDSA 256 |
| A4, S4 e T4 | 11 (para cadeias de Curvas Elípticas) | ECDSA 512 |
| | 6 (para as demais cadeias) | RSA 2048(V0 e V1),4096 (V2) |

### 6.4.2.3 Uso específico da cadeia de certificação

A Resolução ITI nº 101 de 09/10/2013 restringe o uso dos certificados correspondentes ao DS (*Document Signer*) da ICAO para assinatura digital documentos de viagem eletrônicos.

Entretanto, o item 5.5.1 do documento 9303, parte 3, volume 2, da ICAO determina para a aplicação ICAO que:

1) a chave privada do *Country Signing* CA ($Kpriv_{CSCA}$) seja usada para assinar certificado do *Document Signer* ($C_{DS}$);
2) a chave privada do *Document Signer* ($Kpriv_{DS}$) seja usada para assinar os *Document Security Objects* ($S_{OD}$).

Por uma interpretação literal da norma, entende-se que a mesma define a função das chaves dentro da cadeia ICAO, e que, portanto, para que a verificação dos certificados seja possível, apenas essas chaves podem ser usadas para gerar a assinatura do $S_{OD}$. Não há no texto nenhum termo restritivo de uso, como a palavra “somente”. Portanto, considerando que a autenticação passiva é obrigatória na aplicação ICAO, na hipótese do RIC possuir esta aplicação, a Resolução nº 101 do ITI, ao criar indevidamente uma restrição do uso da chave, obriga o uso de no mínimo duas cadeias de certificação distintas, para a autenticação passiva dos dados ICAO e da aplicação eID com os dados RIC.

Sugere-se, portanto, a proposição de uma revisão e flexibilização da norma

Resolução ITI nº 101 de 09/10/2013, para que se permita o uso da cadeia de certificação ICAO para a geração de certificados e a assinatura de dados de outras aplicações.

## 6.5 Análise de algoritmos criptográficos assimétricos

Pela Tabela 7~~Tabela 7~~~~Tabela 7~~ percebe-se a possibilidade de utilizar dois tipos de algoritmos assimétricos no âmbito da ICP-Brasil, o algoritmo RSA e o algoritmo ECDSA. Ambos algoritmos são considerados seguros, embora o critério empregado para garantir a segurança de cada um deles seja diferente.

O algoritmo RSA foi criado por Rivest, Shamir e Adleman em 1977, sendo ainda o algoritmo mais empregado nas assinaturas digitais de *e-commerce* (Subramaniam, Chaudhry, & Ahmad, 2012) (Bos, et al., 2013). A força do algoritmo é baseada na dificuldade de fatorar números, onde dado dois números primos *p* e *q*, a dificuldade de conseguir fatorar *n* (*n=pq*), sendo o conhecimento de *p* ou *q* proibitivo (Subramaniam, Chaudhry, & Ahmad, 2012). Logo, para que o RSA seja seguro deve-se empregar números grandes, o que resulta em tamanho de chaves também grandes. Para se ter uma ideia do tamanho das chaves, em aplicações *e-commerce*, o tamanho mínimo de chave RSA deve ser de 1024 bits para que se tenha segurança (Subramaniam, Chaudhry, & Ahmad, 2012). A manipulação de números grandes torna o algoritmo RSA muito lento, chegando a ser 100 vezes mais lento que o algoritmo simétrico DES (Subramaniam, Chaudhry, & Ahmad, 2012). A velocidade de processamento é a desvantagem do algoritmo RSA para a implementação em *hardware* ou *software*.

O algoritmo de criptografia de curva elíptica (*Elliptic Curve Cryptography* - ECC) foi descoberto em 1985 por Victor Miller e Neil Koblitz como um mecanismo alternativo para implementar a criptografia de chave pública (Subramaniam, Chaudhry, & Ahmad, 2012). A segurança do ECC é baseada no problema de encontrar logaritmos discretos sobre um grupo finito (Subramaniam, Chaudhry, & Ahmad, 2012). Embora não seja o algoritmo mais utilizado em *e-commerce*, nota-se um gradual crescimento de seu uso, devido ao menor tamanho de chave (Bos, et al., 2013).

O algoritmo de assinatura digital em curvas elípticas (*Elliptic Curve Digital Signature Algorithm* – ECDSA) é uma variação do algoritmo de assinatura digital (*Digital Signature*

*Algorithm* – DSA) que opera em grupos de curvas elípticas (Johnson, Menezes, & Vanstone, 2001). Foi proposto por Scott Vanstone em 1992. Foi aceito em 1999 como padrão ANSI (ANSI X9.62) e em 2000 como padrão IEEE (IEEE 1363-2000) e padrão NIST (FIPS 186-2) (Subramaniam, Chaudhry, & Ahmad, 2012). Em suma, o ECDSA emprega operações sobre curvas elípticas ao invés de utilizar as exponenciações utilizadas no padrão de assinatura digital (*Digital Signature Standard* – DSS) (Johnson, Menezes, & Vanstone, 2001).

Outra implicação do uso de curvas elípticas é que as partes envolvidas na comunicação segura devem compartilhar os parâmetros de domínio de curva elíptica em que as chaves foram geradas, ou seja, tais parâmetros são definidos previamente e tornados públicos a fim de que seja possível saber em qual domínio de curva elíptica estão operando. Foram propostos, definidos e recomendados alguns padrões de curvas elípticas para o uso na criptografia, divulgando-se os respectivos parâmetros das curvas. Como exemplo, podem ser citadas as curvas propostas pelo NIST (nistp192, nistp224, nistp256, nistp384 e nistp521) (U.S. Department of Commerce/National Institute of Standards and Technology, 2013) e pela Certicom (secp192r1, secp224r1, secp256r1, secp384r1 e secp521r1) (Certicom Research, 2000). A ICP-Brasil adota as curvas elípticas definidas no padrão *brainpool*, padrão definido pelo grupo europeu ECC *Brainpool*, o qual define as curvas brainpoolP160r1 (160 bits), brainpoolP192r1 (192 bits), brainpoolP224r1 (224 bits), brainpoolP256r1 (256 bits), brainpoolP320r1 (320 bits), brainpoolP384r1 (384 bits), brainpoolP512r1 (512 bits) e suas variantes *twisted,* brainpoolP160t1 (160 bits), brainpoolP192t1 (192 bits), brainpoolP224t1 (224 bits), brainpoolP256t1 (256 bits), brainpoolP320t1 (320 bits), brainpoolP384t1 (384 bits), brainpoolP512t1 (512 bits) (ECC Brainpool, 2005). As curvas *twisted* oferecem o mesmo nível de segurança que as curvas correspondentes e tem a vantagem de potencialmente permitir uma aritmética mais eficiente devido ao parâmetro de curva elíptica *A=-3*, conforme menção na RFC 6954 (IETF, 2013). Porém, as curvas *twisted* carecem de cuidado especial na implementação, pois são mais difíceis de proteger contra *side-channel attacks*. Ressalta-se que a proteção contra-ataques de *side-channel* depende também do *chip* e do OS utilizados. Se o chip possuir recursos de proteção, com *wait states* aleatórios, gerados por True RNG, o risco de usar a ECC *twisted* é menor.

A Tabela 33~~Tabela 33~~~~Tabela 33~~ apresenta um quadro resumindo os problemas

matemáticos e o melhor método conhecido para solucioná-los atualmente os criptossistemas de chave pública.

**Tabela 33 – Problema matemático dos algoritmos de criptografia assimétrica**

| Sistema de chave pública | Problema Matemático | Melhor método conhecido para resolver o problema matemático | Tempo de execução |
|---|---|---|---|
| Fatoração de inteiros | Dado um número *n*, encontrar os fatores primos | Algoritmo *General Number Sieve* | Sub-exponencial |
| Logaritmo discreto | Dado um número primo *n*, e números *g* e *h*, encontrar *x* tal que *h=gx* mod *n* | Algoritmo *General Number Sieve* | Sub-exponencial |
| Logaritmo discreto de curva elíptica | Dada uma curva elíptica *E* e pontos *P* e *Q* em *E*, encontrar *x* tal que *Q=xP* | Algoritmo Pollard-rho | Totalmente exponencial |

**Fonte:** *ECDSA for Reliable E-commerce Aplications* (Subramaniam, Chaudhry, & Ahmad, 2012).

Para fins comparativos, a Tabela 34~~Tabela 34~~~~Tabela 34~~ apresenta a equivalência da força de segurança entre os algoritmos RSA, ECC e de chaves simétricas. Tomando-se especificamente os algoritmos RSA e ECC, nota-se que para um mesmo nível de segurança as chaves ECC são muito menores que as chaves RSA. Por exemplo, utilizando o ECC-*Brainpool* com uma chave de 512 bits o padrão de segurança é equivalente ao uso de RSA com uma chave de 15360 bits (Gupta, Gupta, & Chang, 2002). O menor tamanho das chaves ECC é uma das principais vantagens do uso desse algoritmo, pois uma chave menor leva a uma redução da memória necessária para armazenamento da chave pública no certificado digital. Tal vantagem se sobressai em dispositivos com memória limitada, como *smartcards*. Logo, pode-se associar rapidamente o uso de ECC no RIC, uma vez que as informações a serem gravadas no cartão RIC devem ser sucintas respeitando e economizando o pouco espaço disponível para guardar dados.

**Tabela 34 – Equivalência de segurança entre os algoritmos RSA, ECC e de chave simétrica**

| Tamanho de chave | Algoritmo de | Modulo curva | Módulo RSA | Tempo de |
|---|---|---|---|---|

| simétrica | | *Hash* | elíptica (bits) | (bits) | vida |
|---|---|---|---|---|---|
| 80 | 3DES (2 Key) | SHA-1 | 160 | 1024 | 2010 |
| 112 | 3DES (2 Key) | SHA-224 | 224 | 2048 | 2030 |
| 128 | AES-128 | SHA-256 | 256 | 3072 | 2031+ |
| 192 | AES-192 | SHA-384 | 384 | 7680 | 2031+ |
| 256 | AES-256 | SHA-512 | 512 | 15360 | 2031+ |

**Fonte:** *ECDSA for Reliable E-commerce Aplications* (Subramaniam, Chaudhry, & Ahmad, 2012).

As três tabelas a seguir mostram um comparativo entre os algoritmos RSA e ECC quanto ao desempenho de processamento. A

Tabela 35

~~Tabela 35~~

~~Tabela 35~~ apresenta o comparativo de desempenho relativo ao processo de geração das chaves, na qual vê-se que para chaves pequenas o desempenho dos algoritmos é equivalente. No entanto, com o crescimento das chaves, o tempo de processamento de geração das chaves ECC cresce linearmente enquanto o tempo de processamento de geração das chaves RSA cresce exponencialmente. Isso se deve ao fato de que o algoritmo ECC não precisa gastar recursos computacionais para gerar números primos e assim pode criar o par de chaves privada/pública em velocidade superior ao algoritmo RSA.

**Tabela 35 – Comparação de desempenho na geração de chaves**

| Tamanho da Chave (bits) | | Tempo (s) | |
|---|---|---|---|
| **ECC** | **RSA** | **ECC** | **RSA** |
| 163 | 1024 | 0,08 | 0,16 |
| 233 | 2240 | 0,18 | 7,47 |
| 283 | 3072 | 0,27 | 9,80 |
| 409 | 7680 | 0,64 | 133,90 |
| 571 | 15360 | 1,44 | 679,06 |

**Fonte:** Performance Comparison of Elliptical Curve and RSA Digital Signatures (Jansma & Brandon, 2004).

A Tabela 36~~Tabela 36~~~~Tabela 36~~ apresenta o comparativo de desempenho no

processo de geração da assinatura digital. Observa-se nesse quesito o algoritmo RSA é melhor que o ECC para chaves pequenas, porém o quadro se inverte quando os tamanhos das chaves equivalentes crescem.

**Tabela 36 – Comparação de desempenho na geração de assinatura**

| Tamanho da Chave (bits) | | Tempo (s) | |
|---|---|---|---|
| **ECC** | **RSA** | **ECC** | **RSA** |
| 163 | 1024 | 0,15 | 0,01 |
| 233 | 2240 | 0,34 | 0,15 |
| 283 | 3072 | 0,59 | 0,21 |
| 409 | 7680 | 1,18 | 1,53 |
| 571 | 15360 | 3,07 | 9,20 |

**Fonte:** Performance Comparison of Elliptical Curve and RSA Digital Signatures (Jansma & Brandon, 2004).

A Tabela 37~~Tabela 37~~~~Tabela 37~~ apresenta o comparativo de desempenho no processo de verificação da assinatura digital. Nota-se que o processo de verificação do algoritmo RSA tem melhor desempenho em todos os tamanhos de chave equivalentes quando comparado com o ECC. Praticamente o tempo para a verificação de uma mensagem assinada com RSA é desprezível para os tamanhos de chave usados. Já o tempo de verificação no algoritmo ECC aumenta de forma linear de acordo com o tamanho da chave.

**Tabela 37 – Comparação de desempenho na verificação de assinatura**

| Tamanho da Chave (bits) | | Tempo (s) | |
|---|---|---|---|
| **ECC** | **RSA** | **ECC** | **RSA** |
| 163 | 1024 | 0,23 | 0,01 |
| 233 | 2240 | 0,51 | 0,01 |
| 283 | 3072 | 0,86 | 0,01 |
| 409 | 7680 | 1,80 | 0,01 |
| 571 | 15360 | 4,53 | 0,03 |

**Fonte:** Performance Comparison of Elliptical Curve and RSA Digital Signatures (Jansma & Brandon, 2004; Subramaniam, Chaudhry, & Ahmad, 2012).

Em suma, tem-se que o algoritmo ECC apresenta tamanho de chaves equivalentes

menores que o RSA, bem como tem melhor desempenho na geração da chave e também na geração da assinatura. O algoritmo RSA só é superior ao ECC no processamento de verificação da assinatura, porém o tempo de verificação de assinatura ECC, mesmo sendo maior, é aceitável. A Tabela 38~~Tabela 38~~~~Tabela 38~~ simplifica os resultados de análise baseando-se em cinco fatores, na qual pode-se concluir que o uso de ECC é recomendável para aplicações de *e-commerce*, dispositivos eletrônicos móveis, *smartcards*, e quaisquer outra aplicação que tenha limitação de recursos (memória e processamento).

**Tabela 38 – Resultado de análise entre ECC e RSA**

| Propriedades | ECC | RSA |
|---|---|---|
| Maior Segurança | Não afeta o desempenho da aplicação | Afeta o desempenho da aplicação |
| Desempenho | Elevado | Lento |
| Tamanho de chave | Menor | Maior |
| Custo Computacional | Baixo | Alto |
| Geração de chave | Muito rápido | Muito lento |

**Fonte:** *Performance comparison of public-key* (Wiener).

Uma observação a ser feita sobre os algoritmos baseados em ECC é quanto ao tamanho da chave pública. O nome da curva faz referência ao tamanho da chave privada. Por exemplo, a curva brainpoolP256r1 possui uma chave privada de 256 bits. No entanto, o tamanho da chave pública correspondente é diferente e depende se for representada na forma compactada ou descompactada (American National Standards Institute, 1998). Na prática, a chave pública na forma descompactada contém dois pontos da curva elíptica, ambos de mesmo tamanho do campo finito subjacente. Logo, para uma curva elíptica de 256 bits, a chave pública na forma descompactada consiste em dois valores de 256 bits, totalizando 512 bits. Por sua vez, na chave pública na forma compactada um dos pontos da curva elíptica é suprimido e armazenado no outro ponto, de modo que possa ser derivado, ficando o tamanho final com o adicionamento de somente 1 byte. Assim, para uma curva elíptica de 256 bits, a chave pública na forma compactada totaliza 264 bits.

Outro comentário relevante é quanto ao tamanho da assinatura digital com o algoritmo ECDSA. De forma simplificada, na geração da assinatura digital obtêm-se

como resultado dois parâmetros de tamanho igual ao tamanho da chave privada do algoritmo. Assim, o tamanho final da assinatura digital ECDSA seria o dobro da chave privada, com alguns bytes codificados em ASN.1.

A adoção do algoritmo ECDSA (baseado em ECC) é altamente recomendável para o RIC, em virtude dos fatores já mencionados. Pensando-se estritamente no documento RIC, o tamanho menor da chave ECC economiza espaço para o armazenamento da chave pública no certificado digital, economia desejada mesmo que o RIC implementado em cartões *smartcard* com *chip* ou sem *chip* utilizando autenticação passiva (o documento contém a assinatura digital do emissor impressa no cartão para fins de autenticação). Outro aspecto a ser ressaltado é que como o nível de segurança com uma chave ECC é alto, o tempo de validade do certificado pode ser maior. Tal aspecto é visto na regulamentação da ITI, a qual considera que um certificado digital com chave ECDSA de 512 bits tem validade de 11 anos (ITI, 2014). Ou seja, a definição do algoritmo a ser utilizado também impacta na questão temporal de validade do certificado digital empregado no documento RIC. Uma proposta factível para o RIC seria a utilização de um certificado digital A3 com algoritmo ECDSA de 256 bits, o qual permite o tempo máximo de validade do certificado de 5 anos (ITI, 2014). Tal proposta tenta balancear o custo-benefício do tempo de validade do certificado *versus* tamanho da chave, uma vez que o tempo de 5 anos é razoável para a troca dos certificados nos documentos e o tamanho da chave não seria grande. Embora recomenda-se o uso de ECDSA para o RIC, baseando-se uma proposta apoiada na questão custo-benefício do tempo de validade do certificado *versus* tamanho da chave, há a necessidade de um estudo mais aprofundado para a avaliação do tamanho de chave ECDSA e o respectivo tempo de validade dos certificados, levando-se em conta também a adequação de certificados ICP-Brasil aos requisitos ICAO[5].

## 6.6 Avaliação do custo de utilização dos certificados digitais

[5] A ICAO estabeleceu normas internacionais para os passaportes eletrônicos, definindo critérios de segurança a serem obrigatoriamente implementados nos documentos oficiais de viagem dos países membros. Tais critérios de segurança são aplicáveis ao RIC.

Outro aspecto prático a ser avaliado é a questão do custo de utilização de certificados digitais nos documentos RIC. Nesse quesito serão desconsiderados os custos intrínsecos à implantação e manutenção de uma AC, focando-se especificadamente nos custos para emissão de um documento de identificação com a utilização de certificados digitais.

Conforme já fora visto, atualmente a ICP-Brasil oferece basicamente dois tipos de certificados: os certificados de sigilo (S1, S2, S3 e S4) e os certificados de assinatura (A1, A2, A3 e A4). Os certificados de assinatura naturalmente são os indicados para a aplicação no RIC, partindo-se do pressuposto que não se pretende o sigilo das informações num documento RIC, mas sim a garantia de sua autenticidade e integridade, visando a identificação unívoca de seu dono.

Atualmente o mercado nacional os oferece certificado digital para usuários finais sob duas formas de mídia armazenadora: *smartcard* e *token*. No presente estudo será considerado somente os certificados digitais cujo par de chaves seja mantido em *smartcard*, uma vez que este se assemelha a um documento de identidade. Para fins de avaliação do custo de um certificado praticado no mercado, foi realizada uma pesquisa quanto ao custo de um certificado de assinatura A3, cujo tempo de validade é de 3 anos. A pesquisa foi realizada em junho de 2015, por meio de acesso aos portais das organizações que representam as ACs ofertantes de tais certificados. Os valores encontrados correspondem ao valor do certificado de assinatura A3 somado ao valor do cartão com *chip*. Tomou-se o cuidado, para se ter o mesmo referencial, verificando o valor dos certificados denominados como e-CPF para pessoa física. O resultado do levantamento de custo desses certificados é apresentado na Tabela 39~~Tabela 39~~~~Tabela 39~~.

**Tabela 39 – Pesquisa de custo de um certificado digital A3 e-CPF com 3 anos de validade**

| Organização | Certificado | Usuário | Preço [R$] | Validade | Mídia |
|---|---|---|---|---|---|
| Serasa | A3 | Pessoa Física | 275,00 | 3 anos | Cartão |
| Certisign | A3 | Pessoa Física | 270,00 | 3 anos | Cartão |
| Valid | A3 | Pessoa Física | 268,00 | 3 anos | Cartão |
| Imprensa Oficial | A3 | Pessoa Física | 185,00 | 3 anos | Cartão |
| Boa Vista | A3 | Pessoa Física | 268,00 | 3 anos | Cartão |
| AC Caixa | A3 | Pessoa Física | 220,00 | 3 anos | Cartão |
| DigitalSign | A3 | Pessoa Física | 260,00 | 3anos | Cartão |

**Fontes:** Portal Serasa (SERASA, n.d.), Portal Certisign (CERTISIGN, n.d.) e Portal Valid (2014) (SERASA, n.d.), Portal Impresa Oficial (IMPRENSA OFICIAL, n.d.), Portal Boa Vista (BOA VISTA, n.d.), Portal Caixa (CAIXA, n.d.), Portal DigitalSign (DIGITALSIGN, n.d.).

Da análise da Tabela 39~~Tabela 39~~~~Tabela 39~~ observa-se que um certificado A3 e-CPF com 3 anos de validade tem um custo médio em torno de R$ 238,00 para uma Pessoa Física. O valor mínimo encontrado para o certificado A3 é de R$ 185,00. Tomando-se o valor mínimo encontrado para os certificados A3 e-CPF, o custo de R$ 185,00 para um certificado digital é impraticável para o RIC, sobretudo quando é avaliado o custo total para a confecção de documentos RIC para a população brasileira, o que representaria um valor em torno de 37 bilhões de reais[6]. Deve ser ressaltado que o valor de 37 bilhões é o gasto estimado a cada 3 anos, pois os certificados A3 devem ser renovados nesse período de tempo.

Para tentar desassociar o custo do certificado digital e o do cartão com *chip*, ainda com o foco no mercado nacional, procurou-se observar o projeto encabeçado pelo Conselho Federal de Medicina (CFM), o qual publicou em 2011 uma resolução instituindo a carteira digital de médico (CRM Digital) que utiliza certificação digital (CFM, n.d.). O CRM Digital é uma identidade médica confeccionado em cartão rígido de policarbonato e contém um *chip* para armazenar o par de chaves e o certificado digital correspondente, os quais são utilizados para assinar eletronicamente o prontuário eletrônico de paciente (PEP) (CFM, n.d.). O médico que optar pelo CRM Digital deve adquirir o cartão de policarbonato com *chip*, inicialmente sem certificado digital, o qual é obtido posteriormente por meio de aquisição de certificados e-CPF junto a uma AC do mercado nacional. Em termos de custo, os valores cobrados pelos Conselhos Regionais de Medicina para a confecção da nova identidade, ou seja, somente do cartão com o *chip* sem certificado digital, variam em torno de R$ 70,00 a R$ 84,00 (CREMEGO, n.d.) (CREMESP, n.d.). As organizações Valid e Caixa Econômica ofertam em seus produtos certificados digitais para pessoas que já tem um *smartcard* ou *token*, como é o caso da CRM Digital, praticando, respectivamente, os valores de R$ 214,00 e R$ 250,00. Conclui-se assim, pelos valores apresentados no CRM Digital, que o custo unitário de um documento RIC com certificado digital para assinatura observado no cenário nacional é impraticável, sendo o custo ainda maior que os valores observados

[6] Considerou-se uma população de 200 milhões de habitantes, segundo o último censo do IBGE de 2010.

na aquisição do e-CPF, uma vez que o custo unitário mínimo do CRM Digital com o certificado digital, desconsiderando possíveis acordos ou convênios para diminuição de custos, seria de R$ 284,00.

Por outro lado, pesquisas recentes mostraram que o custo de cartões de policarbonato com *chip* tem caído nos últimos anos, possivelmente pela ampla concorrência entre fornecedores de policarbonato com a entrada de empresas chinesas no mercado e também pela saturação do mercado de *chips* para *smartcard*. Por exemplo, o novo cartão de identidade do Uruguai confeccionado em policarbonato e com dois *chips* foi contratado da empresa Gemalto pelo valor de U$ 2,81 (Gemalto, 2015) (R$ 8,43, considerando o dólar a R$ 3,00). É interessante observar que a mesma empresa foi contratada para fornecer um cartão em policarbonato sem *chip* ao custo de U$ 0,57 (R$ 1,71 com o dólar a R$ 3,00). Isso demonstra que o custo da inserção de *chips* e das tecnologias é bem superior ao custo do cartão em si. Outro exemplo recente é o caso de Bangladesh, o qual contratou em 2015 um cartão em policarbonato com *chip* com contato por um valor ainda menor, de aproximadamente U$1,00 (Project, Bangladesh Election Commission IDEA, 2014) (R$ 3,00 com o dólar a R$ 3,00). Tais exemplos mostram que o valor do cartão em policarbonato pode ser bastante reduzido quando comparado aos valores observados no CRM Digital.

Mesmo com a redução possível do custo do cartão em policarbonato percebe-se que a adoção de um certificado digital para cada usuário, tomando-se como base os certificados e-CPF, ainda é inviável devido aos valores praticados atualmente. Pode-se pensar como solução para a redução de gastos a implantação de uma AC específica para o RIC, a qual forneceria certificados digitais, com as mesmas funcionalidades do e-CPF, de forma gratuita ou a baixo custo. Porém, a adoção de tal solução também é remota, haja visto que afetaria todo um segmento de mercado que vem crescendo nos últimos anos e ainda luta para se consolidar.

De fato, analisando as funcionalidades do certificado digital destinado à assinatura digital no âmbito da ICP-Brasil, nota-se que estes possuem uma dupla função: a de assinar documentos e também a de autenticação. Uma possível solução que permitiria reduzir os custos relacionados ao uso do certificado digital, seria a separação dessas funcionalidades, criando-se assim certificados digitais destinados para a assinatura digital e certificados destinados somente à autenticação. Nesse sentido, os certificados digitais relacionados à autenticação poderiam ser emitidos a baixo custo ou mesmo de

forma gratuita para documentos RIC, reduzindo o custo do documento ao valor de confecção do cartão. Salienta-se que com a separação das funcionalidades, não haveria o comprometimento do segmento de mercado de certificação digital já instalado no país, uma vez que a funcionalidade de assinatura poderia ser adquirida segundo os moldes atuais, de forma opcional, possibilitando que o titular possa pagar por um certificado para assinatura, se este o desejar.

Em termos técnicos a separação de funcionalidades do certificado digital é possível e também é previsto nas especificações. O padrão X.509 prevê, conforme especificado na RFC 5280 (IETF, 2008), a indicação de um ou mais propósitos para os quais o certificado digital será utilizado. Esses propósitos são definidos através dos parâmetros de extensão *Key Usage* e *Extended Key Usage* da seguinte forma: se não houver a extensão o certificado tem uso genérico; se for especificada a extensão a chave somente pode ser usada para o propósito indicado. Os usos definidos na norma incluem autenticação do servidor e autenticação do cliente.

Tal separação já foi sugerida na tese “Uma Proposta para a Regulamentação da Certificação Digital no Brasil” (Bertol, 2009), onde percebe-se que além da redução do custo já mencionada anteriormente, a separação de funcionalidades ajuda a mitigar o risco de segurança dos titulares. Para exemplificar os riscos envolvidos quando um certificado acumula as funcionalidades de autenticação e assinatura, pode-se pensar que um titular pode inadvertidamente assinar um documento pensando se tratar de um processo de autenticação, ou, no impacto em caso de perda ou comprometimento certificado. Outra situação de risco é observada nos casos de comprometimento da chave privada ou perda do cartão, pois a mesma chave privada utilizada para autenticação pode ser usada para assinar documentos de cunho legal e financeiro. Logo, a captura ou comprometimento de chave privada por terceiros dos certificados para autenticação não implicaria em graves prejuízos ao titular, sobretudo os de ordem financeira.

É importante ressaltar também que o uso de certificados digitais para autenticação é praticado em documentos de identificação de vários países com a possibilidade do titular adquirir, opcionalmente, o certificado para assinatura. Tal prática é observada em vários países, por exemplo, na Alemanha, Áustria, Bélgica, República Checa, Finlândia, Irlanda, Itália, Portugal (Lehmann, 2013) (EUROSMART, 2013), etc.

Observa-se, no entanto, que a adoção de certificados digitais com funcionalidades

distintas na ICP-Brasil carece de alterações nas normas atuais. Pelo documento DOC-ICP-04 da ITI, é previsto somente os certificados de assinatura digital e de sigilo, ambos especificados pelo campo *Key Usage* do certificado (ITI, 2014). O campo *Extended Key Usage*, o qual poderia estender os propósitos de uso do certificado, só é utilizado na ICP-Brasil para identificar os certificados de carimbo de tempo, não devendo ser empregado para qualquer outro tipo de certificado. Contudo, a redução de custos com emissão de certificados destinados à autenticação justificaria a revisão da normatização vigente da ITI, uma vez que o custo unitário de um cartão com *chip* com certificado de autenticação cairia para cerca de R$ 3,00 (considerando somente o valor do cartão em Bangladesh, com certificado gratuito) e, consequentemente, em torno de R$ 600 milhões para a população brasileira. É interessante citar que o custo de implantação da referida solução, com certificado digital de autenticação gratuito e cartão com *chip*, não é tão alto quando comparado aos custos da solução com certificado digital com assinatura, apresentando como gasto principal o valor do cartão com *chip*. Além disso, pensando-se nos custos de manutenção de um sistema de identificação ao longo dos anos, a referida solução pode ter uma otimização de tais custos mesmo quando os certificados de autenticação gratuitos expirarem o respectivo período de validade, uma vez que os cartões com *chip* podem ser reutilizados, bastando a substituição do certificado digital de autenticação armazenado no *chip*.

Uma outra possibilidade ainda seria o uso de cartão sem *chip* empregando como método de segurança a autenticação passiva. A autenticação passiva permite verificar a integridade e a autoria de emissão do cartão através da assinatura digital dos dados pelo emissor, como se fosse uma espécie de selo que atesta a autenticidade das informações constantes no documento de identificação. De forma mais concreta, na autenticação passiva os donos do cartão de identificação não têm o seu certificado digital próprio; são os emissores do cartão quem possuem o certificado digital e assinam os dados dos respectivos donos de cartão, criando assim uma assinatura digital, a qual geralmente é adicionada ao cartão sob a forma de código de barras bidimensional. Nesse cenário elimina-se a necessidade do uso de um certificado para cada usuário, diminuindo os custos do uso de certificação no documento de identificação. A autenticação dos dados é garantida pela assinatura digital do emissor impressa no cartão de identificação, ressaltando-se que a autenticação passiva por si só não previne clonagem e falsificação do documento, devido à possibilidade de

replicação da assinatura eletrônica (Fumy & Paeschke, 2011). Ademais, a aplicação de autenticação eletrônica não seria suportada pelo cartão, e outras alternativas deveriam ser propostas como tecnologias MobileID e aplicações eID em cartões bancários EMV. O detalhamento do funcionamento da autenticação passiva pode ser verificado nas normas ICAO (ICAO 9303) (International Civil Aviation Organization, 2006).

Voltando à questão do custo na solução de cartão sem *chip* com o emprego da autenticação passiva, elimina-se praticamente o custo do certificado digital para cada usuário, levando o valor de um documento de identificação ser equivalente ao custo do cartão de policarbonato sem *chip*. Utilizando-se o valor já mencionado de R$ 1,71 para a confecção de uma unidade de cartão sem *chip* pela Gemalto, o custo de implantação para a população brasileira ficaria em torno de R$ 342 milhões. Dois pontos críticos devem ser observados em relação ao ciclo de vida destes cartões: o primeiro, em caso de comprometimento da chave privada do emissor, todos os documentos emitidos com o uso da referida chave devem ser cancelados, já que não há como garantir sua autenticidade; o segundo, uma vez que o documento ou assinatura digital correspondente expire sua validade é necessário confeccionar um novo cartão. Portanto, o emprego de poucos certificados de emissores, com maior controle e com uso de HSM, seria recomendado para reduzir o risco de comprometimento e consequente revogação. A Tabela 40~~Tabela 40~~~~Tabela 40~~ apresenta um resumo com os custos e valores discutidos. Percebe-se claramente que a utilização dos certificados digitais para assinatura digital existentes hoje, segundo os moldes da ICP-Brasil, eleva consideravelmente os gastos para a emissão de um documento de identificação, tornando-se impraticável para o RIC. Tal percepção justifica a criação de certificado digital para fins exclusivos de autenticação, alocados de forma gratuita para os documentos de identificação, a exemplo do que é praticado em outros países (EUROSMART, 2013). A vantagem do menor custo de um documento de identificação confeccionado com cartão sem *chip* tem um grande apelo para momentos de restrição orçamentária e além disso provê um bom grau de segurança da identificação, sendo portanto o modelo mais recomendado atualmente para o RIC. No entanto, os cartões com *chip* apresentam uma tendência de queda de custo, além de permitir um grau de segurança maior por meio da autenticação ativa (International Civil Aviation Organization, 2006), o que pode mudar o modelo sugerido num futuro próximo.

**Tabela 40 – Custo estimado de documento de identificação com certificação digital**

| Descrição | Custo unitário | | | Custo total |
|---|---|---|---|---|
| | Cartão e Certificado | Cartão | Certificado | |
| Cartão com *chip* e certificado digital e-CPF (valor mínimo) | R$ 185,00 | - | - | R$ 37 bilhões |
| Cartão com *chip* e certificado digital e-CPF (valor médio) | R$ 238,71 | - | - | R$ 47,7 bilhões |
| Cartão com *chip* (CRM Digital) e certificado digital de assinatura | - | R$ 70,00 | R$ 214,00 | R$ 56,8 bilhões |
| Cartão com *chip* (Uruguai) e certificado digital de assinatura | - | R$ 8,71 | R$ 214,00 | R$ 44,5 bilhões |
| Cartão com *chip* (Bangladesh) e certificado digital de assinatura | - | R$ 3,00 | R$ 214,00 | R$ 43,4 bilhões |
| Cartão com *chip* (Uruguai) e certificado digital de autenticação gratuito | - | R$ 8,71 | - | R$ 1,7 bilhões |
| Cartão com *chip* (Bangladesh) e certificado digital de autenticação gratuito | - | R$ 3,00 | - | R$ 600 milhões |
| Cartão sem *chip* (Uruguai) com autenticação passiva | - | R$ 1,71 | - | R$ 342 milhões |

# 7. CONCLUSÃO

O presente relatório apresentou o diagnóstico atual da certificação digital. Ela foi contextualizada no cenário brasileiro, onde desde 2001 há um amparo legal por meio da Medida Provisória (MP) 2.200-2 para alavancar o seu uso, criando-se a ICP-Brasil, esta sustentada com normativas advindas da ITI. A principal vantagem de se utilizar a ICP-Brasil é o fato de que, por força da medida provisória, os documentos eletrônicos produzidos com os certificados digitais ICP-Brasil são presumidos verdadeiros e são considerados documentos públicos. Porém, o uso da ICP-Brasil implica em aceitar e seguir as normas estabelecidas pela ITI, o que pode representar um obstáculo, dependendo da aplicação a ser dada ao certificado digital.

A estrutura hierárquica é uma das principais características da ICP-Brasil, apresentando no topo da hierarquia como entidade principal a AC-Raiz (controlada pela ITI), e, abaixo dela as ACs de 1° Nível, as ACs de 2° Nível, as ARs correspondentes e demais entidades que dão suporte à PKI nacional. A adoção da estrutura hierárquica permite ao governo, por meio da ITI, um maior controle de toda a cadeia de regulamentação, garantindo assim que a certificação digital funcione adequadamente.

O estudo das normas da ITI mostra que as especificações adotadas para a certificação adotadas para a certificação digital estão coerentes com os padrões internacionais e tem proporcionado um certo grau de avanço da certificação digital no país. Por exemplo, os certificados digitais da ICP-Brasil seguem o padrão X.509v3, padrão amplamente adotado por vários outros países para especificar o formato dos certificados de chave pública, LCR, certificados de atributos e o algoritmo de validação da cadeia de certificado. Pode-se afirmar o mesmo para a definição dos algoritmos de criptografia adotados; os padrões, formatos, perfis e políticas de assinatura digital; à mídia de armazenamento para o par de chaves e certificados, etc.

Algumas recomendações baseadas no estudo realizado pelo presente relatório podem ser mencionadas para a implantação do RIC. É importante ressaltar que tais recomendações não são mandatórias e, em alguns casos preliminares, devendo ser realizados estudos e testes aprofundados para amadurecê-las. A seguir são apresentadas as recomendações e considerações relativas à certificação digital aplicadas ao RIC:

1) **Mídia de armazenamento** – o número RIC visa, além da identificação dos cidadãos, a emissão de identidade. Nesse sentido, a utilização de cartões rígidos no formato ID-1, seja em policarbonato PET ou Teslin, compatível ao mesmo tempo com a especificação ICAO para documentos de viagem e com o padrão de mídia *smartcard* da ICP-Brasil, é interessante. A questão do emprego de cartão com ou sem *chip* deve ser analisada pela ótica do custo e também da funcionalidade. Em termos de custo, o cartão sem *chip* é mais vantajoso, podendo custar até um quinto do custo do cartão com chip, como no caso da eID e da identidade Uruguaia. Em termos de funcionalidade, ambos os cartões possibilitam a autenticação dos dados segura – mesmo o cartão sem *chip* permite uma autenticação segura, por meio do emprego da autenticação passiva. Porém, o uso de cartão de *chip* agrega maior segurança, além de permitir mais funcionalidades, como o uso de certificados para autenticação eletrônica ou assinatura digital. Nesse cenário, uma medida possível seria adotar inicialmente cartões sem *chip* para o RIC, visando o menor custo e segurança aceitável na autenticação, com uma previsão futura de migração gradual para o cartão com *chip*, custeada pelo cidadão ou pelos estados, já que estes apresentam uma tendência de barateamento de custos. No caso do uso de uma eID, considerando que o ITI apenas homologa chips com contato, deve-se avaliar também o custo benefício da emissão de uma eID com *chip* com contato ou dual interface, levando-se em conta também a durabilidade, ou, se possível, propor uma revisão da norma pelo ITI.
2) **Algoritmo de criptografia simétrica** – entre os dois algoritmos permitidos pela ICP-Brasil, o 3-DES e o AES, o AES é o mais recomendado, tanto por ser o algoritmo mais recente, como por ser mais eficiente e rápido (o 3-DES executa o algoritmo DES 3 vezes). Recomenda-se também o modo de operação GCM, devido à melhor eficiência e desempenho, além de proporcionar confidencialidade e integridade dos dados (o CBC só proporciona a confidencialidade dos dados).
3) **Algoritmo de criptografia assimétrica** – em relação aos algoritmos criptográficos de criptografia assimétrica recomendados para o uso no RIC, a escolha mais adequada é o ECDSA para a criptografia de chaves públicas. O ECDSA, devido ao uso das curvas elípticas, e, consequentemente, pelo menor tamanho de chave, traz vantagens significativas para dispositivos com pouco espaço de armazenamento, conforme já mencionado no relatório. Para a verificação de assinatura, o uso do

RSA apresenta uma menor complexidade, quando comparada ao ECDSA, portanto, caso sejam especificados protocolos de autenticação do terminal ou do provedor de serviços com base em certificados verificáveis pelo cartão (CVC), o uso de RSA é recomendado. Dessa forma, o emprego de duas raízes, ECDSA e RSA pode ser interessante.

4) **Tipo de certificado digital** – especificadamente para o RIC recomenda-se a utilização de par de chaves pública e privada gratuito apenas para fins de autenticação eletrônica. Esta recomendação se apoia na constatação de que o emprego de certificados digitais para assinatura digital é impraticável pelo seu alto custo. O certificado de autenticação, apesar de ser tecnicamente factível no padrão X.509v3 e também ser adotado por vários países em seus eIDs, ainda não é previsto no âmbito da ICP-Brasil. Logo, caso defina-se pela utilização da ICP-Brasil, deve-se num primeiro momento alterar as normas da ITI para a inclusão do certificado de autenticação. Cabe ressaltar ainda que é necessário um estudo mais detalhado, em outro relatório, sobre o uso de protocolos de autenticação eletrônica, alternativos ao padrão X.509, com recursos de privacidade. Como recomendação, sugere-se também, caso haja compatibilidade de interface e de requisitos do *chip* adotado, a inclusão de certificados digitais para assinatura digital, os quais seriam adquiridos opcionalmente pelos usuários RIC. Para fins de segurança, as funcionalidades de autenticação eletrônica e assinatura digital devem ser acessadas por PINs distintos. Quanto à forma de utilização de tais certificados, pode-se adotar a utilização segundo os moldes observados na Estônia: uso irrestrito do protocolo de autenticação–os certificados podem ser empregados de forma irrestrita em qualquer forma de comunicação, seja entre pessoas comuns, entre organizações ou com o governo. De fato, baseando-se no modelo da Estônia, o certificado de autenticação pode ser utilizado também para cifração (sigilo, com o uso de XMLEnc) e assinatura de *e-mail*. Tais características de uso têm o propósito de auxiliar a popularização da certificação digital. Outra abordagem seria o uso de certificados distintos para a autenticação eletrônica, um para setor público com maior segurança, e outro para o setor privado com maior privacidade. Neste sentido, o uso de pseudônimos, ainda não previsto pelas normas ICP-Brasil, é interessante. Por fim, é interessante ressaltar a possibilidade do uso de AC´s distintas para os certificados de

autenticação eletrônica e de assinatura digital, como observados nos esquemas de alguns países.

5) **Tempo de validade do certificado digital** – por se tratar de um documento pessoal, pelo aspecto da durabilidade do cartão e também da necessidade de atualização de dados biográficos (como a foto impressa) ou biométricos, é interessante a sua renovação periódica. Por economia, é óbvio que o tempo de validade do certificado digital, bem como do próprio documento RIC deve ser maximizado. Sob essa perspectiva da segurança dos algoritmos, considerando também o uso do algoritmo ECDSA já recomendado, o tempo máximo de validade de um certificado digital previsto na ICP-Brasil é de 11 anos, com o uso de chave ECDSA de 512 bits. Entretanto, um estudo deve ser realizado para atestar se a chave de 512 bits é a melhor alternativa, com base na capacidade de armazenamento e de processamento do modelo do cartão RIC a ser adotado. Cabe ressaltar que, caso seja adotado um modelo de eID, a renovação dos certificados com validade inferior à da identidade pode ser possível, caso o projeto do *chip* permita uma personalização pós-emissão.
6) **Função de *Hash*** – a função de *hash* deve seguir o padrão adotado quanto ao tamanho da chave. Assim, se a chave privada tiver 512 bits, a função de *hash* recomendada é a SHA-512; se a chave tiver 256 bits, a função de *hash* deve ser a SHA-256. Tal correspondência é necessária para que se mantenha a coerência quanto à equivalência de segurança entre o algoritmo de criptografia assimétrica e à função de *hash*.
7) **Padrão de assinatura digital** – recomenda-se a adoção do padrão XAdES, pelas vantagens da utilização da linguagem XML. O XAdES tem maior flexibilidade e permite assinar partes de um documento eletrônico.
8) **Formato de assinatura digital** – levando-se em conta que é desejável ter no documento RIC todas as informações necessárias para validar a assinatura digital do documento, a recomendação natural é o formato AD-RC, o qual carrega juntamente com a assinatura digital toda a cadeia de certificação necessária para a sua validação. No entanto, um estudo deve ser realizado para verificar a questão do espaço disponível no cartão RIC. Testes podem evidenciar que o formato mais adequado possa ser o AD-RV (guarda somente as referências para acessar a

cadeia de certificação), ou mesmo o AD-RT (tem somente um carimbo de tempo e supõe que as informações para validação podem ser obtidas na AC).

9) **Uso de pseudônimo** – pressupondo a recomendação da separação de funcionalidades com certificados para fins de autenticação e de assinatura, sugere-se a adoção de dois certificados com função de autenticação (um com identificação do titular e o outro com pseudônimo) e, outro certificado com função de assinatura com a identificação do titular. O certificado com pseudônimo pode agregar o anonimato com o objetivo de proteger os dados pessoais do titular do certificado e serviria basicamente para autenticar o *token* em serviços remotos de provedores privados. Porém, uma vez que se admita a utilização de certificados digitais da ICP-Brasil no RIC, será necessário rever as normas da ITI para contemplar o uso de pseudônimos no âmbito da ICP-Brasil.

10) **Uso da ICP-Brasil** – conforme visto, é recomendado que os certificados empregados no RIC sejam criados dentro do âmbito da ICP-Brasil, haja vista que a legislação atual define que as entidades da Administração Pública Federal somente podem exercer serviços de certificação mediante a autorização do Comitê Executivo do Governo Eletrônico e ainda determina que tais entidades devem prover esses serviços no âmbito da ICP-Brasil. Adicionalmente, é vantajoso para o RIC que os documentos eletrônicos produzidos pelos seus certificados sejam presumidos verdadeiros e considerados documentos públicos. Outro fator que reforça a recomendação pelo uso da ICP-Brasil para o RIC é o fato de que o custo para construir uma AC fora ou dentro da ICP-Brasil é equivalente, tendo em vista a dispensa de pagamento das tarifas para a Administração Direta da União. Há, no entanto, um ponto de ressalva para o uso da ICP-Brasil no que tange às adequações de suas normas para contemplar algumas recomendações já sugeridas, como a criação de certificados para autenticação e o uso de pseudônimo ou o eventual emprego de *chip* com interface sem contato.

11) **Uso de AC própria ou parceria com ACs existentes** – não é possível determinar se é mais vantajoso o RIC criar uma AC própria ou fazer uma parceria com uma AC existente da ICP-Brasil, devido à ausência de análise dos custos envolvidos para a criação de uma AC. Uma estimativa poderia ser feita com base na experiência de implantação de uma infraestrutura própria pela ICPEdu ou pelo emprego de uma infraestrutura existente como no caso da AC-MRE que usa a infraestrutura do

SERPRO, porém não foi possível obter dados até o presente momento com os responsáveis pela sua implantação. De qualquer forma, verificou-se que a AC-MRE seria a AC candidata mais recomendada para concretizar parceria na emissão de certificados digitais para o RIC, devido ao fato de ser a única AC no âmbito da ICP-Brasil que utiliza certificados com o algoritmo de criptografia assimétrica ECDSA.

12) **Adequações da ICP-Brasil com as normas ICAO** – o ITI vem trabalhando nos últimos anos, adequando as normas da ICP-Brasil no sentindo de compatibilizar com as normas ICAO, sobretudo diante da perspectiva de que os passaportes eletrônicos brasileiros estejam em conformidade com a PDK/ICAO. Entre as adequações já realizadas, pode-se citar quanto ao número de níveis da cadeia de certificação, onde foi admitido, em caráter excepcional na ICP-Brasil, para a emissão de passaportes eletrônicos que o certificado da CSCA (anteriormente a AC-CMB e hoje a AC-MRE) deve ser auto-assinado e emitido pelo próprio CSCA; ajuste no tempo de validade do certificado digital ICP-Brasil para contemplar o tempo em que o certificado digital do emissor será utilizado para a emissão de passaportes e a maior validade de um passaporte emitido por esse emissor. No entanto, ainda existem pontos nas normas ICP-Brasil a serem revistos, como o caso da restrição quanto ao uso dos certificados correspondentes ao DS (*Document Signer*) da ICAO para assinatura digital de documentos de viagem eletrônicos, ponto em que se sugere a proposição de revisão e flexibilização da norma para que se permita o uso da cadeia de certificação ICAO para a geração de certificados e a assinatura de dados de outras aplicações.

13) **Autenticação eletrônica dos *smartcards*** – observa-se pelas normas de homologação da ICP-Brasil que o fator de autenticação empregado nos *chips* de *smartcard* é o PIN/PUK, com uma previsão de autenticação biométrica. Porém a ênfase dada às normas é quanto ao fator, e não foram encontradas especificações do protocolo adotado pela ICP-Brasil. Recomenda-se para o RIC a análise de recursos de privacidade dos protocolos de autenticação, com detalhamento do protocolo usado na ICP-Brasil e o estudo de protocolos de autenticação ativa empregados em eIDs de outros países.

Em geral, observando os exemplos de utilização de certificação digital no Brasil e no mundo, pode-se afirmar que a certificação digital proporciona benefícios em termos de racionalidade, agilidade, economia de tempo e de recursos materiais, humanos e

financeiros obtidos pelas organizações e usuários referidos nas iniciativas analisadas. Os benefícios citados nesta análise, além das análises de custo, podem subsidiar a escolha do modelo de identidade, bem como opção de aplicação da certificação digital no RIC.

# REFERÊNCIAS

AC-CMB. (2011). Acesso em 10 de 04 de 2015, disponível em https://goo.gl/8CFfae.

AC-JUS. (2014). Acesso em 07 de 04 de 2015, disponível em http://goo.gl/OvY2xJ

AC-MRE. (2015). Acesso em 28 de 06 de 2015, disponível em https://goo.gl/ykifgk

AC-PR. (2011). Acesso em 07 de 04 de 2015, disponível em https://goo.gl/osRzsI

AC-RFB. (2013). Acesso em 10 de 04 de 2015, disponível em http://goo.gl/4w7yUf

AC-SERPRO. (30 de 10 de 2012). Acesso em 27 de 03 de 2015, disponível em Documentos AC-SERPRO: https://goo.gl/Fpkhk8

Aguado, J. L. (2014). DNI 3.0 Seguridd Informatica y Communicaciones. *Regional Smeinar on MRTDs and Traveller Identification Management.* Madrid.

American National Standards Institute. (1998). *X9.62.*

Arora, S. (2007). *Review and Analysis od Current and Future European e-ID Card Schemes.* Eoyall Holloway University od London.

Bertol, V. R. (2009). *Uma Proposta para Regulamentação da Certificação Digital no Brasil*. (ENE/FT/UnB, Produtor, & Universidade de Brasília) Acesso em 2014 de Março de 18, disponível em http://goo.gl/GqW0m9

Bezerra, E. L. (15 de 03 de 2010). *Assinaturas Digitais Avançadas em PDF - PAdES*. Acesso em 01 de 06 de 2015, disponível em https://goo.gl/tVB4zm

BOA VISTA. (s.d.). *Portal Boa Vista*. Acesso em 28 de 06 de 2015, disponível em http://goo.gl/tb6Bz9

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2013). Elliptic Curve Cryptography in Practice. *Cryptology ePrint Archive*.

Brasil. (1988). *Constituição Federal*. Acesso em 08 de 05 de 2015, disponível em http://goo.gl/27TzJP

Brasil. (1990). *Lei Nº 8.078 - Código de Defesa do Consumidor*. Acesso em 08 de 05 de 2015, disponível em http://goo.gl/k0Va1p

Brasil. (31 de 10 de 2001). *DECRETO Nº 3.996*. Acesso em 31 de 07 de 2015, disponível em http://goo.gl/SdRnez

Brasil. (2001). *Lei Complementar Nº 105*. Acesso em 08 de 05 de 2015, disponível em http://goo.gl/BqOp3c

Brasil. (24 de 08 de 2001). *Medida Provisória N 2.200-2*. (C. C. República, Produtor)

Acesso em 15 de 04 de 2015, disponível em http://goo.gl/8zChLO

Brasil. (2002). *Lei No 10.406 - Código Civil*. Acesso em 08 de 05 de 2015, disponível em http://goo.gl/BgYdP6

BRASIL. (2008). *Decreto nº 6.605 de 14 de outubro de 2008*. (C. C. República, Produtor) Acesso em 2014 de Abril de 14, disponível em http://goo.gl/IlAeqO

Bruegger, B. P. (2007). *Discussion Paper: An Inexpensive Privacy Protection Strategy for eID Cards.* IDABC Interoperability for PEGS.

CAIXA. (s.d.). *Portal Caixa*. Acesso em 28 de 06 de 2015, disponível em http://goo.gl/Jd7SZ1

Câmara dos Deputados. (28 de 01 de 2015). *Consulta pública será base para projeto de lei sobre proteção de dados pessoais*. Acesso em 30 de 07 de 2015, disponível em http://goo.gl/o778ZV

CEF. (2014). *Identidade Digital, Certificado Digital da Caixa*. Acesso em 31 de 03 de 2015, disponível em CAIXA Econômica Federal: http://goo.gl/HAnXlr

Certicom Research. (2000). *Standards for efficient cryptography 2: Recommended elliptic curve domain parameters. Standard SEC2.* Certicom.

CERTISIGN. (s.d.). *Portal Certisign*. Acesso em 28 de 06 de 2015, disponível em https://goo.gl/AWHDoK

CFM. (s.d.). *CRM Digital*. Acesso em 29 de 06 de 2015, disponível em http://goo.gl/k62eyB

Cock, D. D. (2009). *Evolutions of Belgian eID cards*. Acesso em 01 de 07 de 2015, disponível em https://goo.gl/UAf7mk

CREMEGO. (s.d.). *Portal do Conselho Regional de Medicina de Goiás*. Acesso em 29 de 06 de 2015, disponível em http://goo.gl/UzLD9f

CREMESP. (s.d.). *Portal do Conselho Regional de Medicina de São Paulo*. Acesso em 29 de 06 de 2015, disponível em http://goo.gl/Y6NgzS

(2006). *D3.6 Study on ID Documents.* Future of Identity in the Information Society.

DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL) . (2001). *Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules - FIPS PUB 140-2.* Washington.

DIGITALSIGN. (s.d.). *Portal DigitalSign*. Acesso em 28 de 06 de 2015, disponível em https://goo.gl/BLbN7u

ECC Brainpool. (2005). *ECC Brainpool Standard Curves and Curve Generation v. 1.0 .* ECC Brainpool.

ETSI. (04 de 2004). *TS 101 903 V1.2.2 (2004-04); XML Advanced Electronic Signatures (XAdES)*. Acesso em 16 de 04 de 2015, disponível em http://goo.gl/oMrY53

ETSI. (25 de 07 de 2008). *TS 101 733 - V1.7.4 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*. Acesso em 16 de 04 de 2015, disponível em https://goo.gl/LsXJBE

EUROSMART. (2013). Landscape of eID in Europe in 2013. *Eurosmart White Paper*.

Fumy, W., & Paeschke, M. (2011). *Handbook of eID Security Concepts, Practical experiences an Technologies.* Publicis.

Gemalto. (2015). *Nuevo Documento de Identidad.*

Guelfi, A. R. (2007). *Análise De Elementos Jurídico-Tecnológicos Que Compõem A Assinatura Digital Certificada Digitalmente Pela Infra-Estrutura de Chaves Públicas do Brasil - ICP-Brasil.* São Paulo: Universidade de São Paulo.

Gupta, V., Gupta, S., & Chang, S. (2002). Performance Analisys of Elliptic Curve Cryptography for SSL. *WiSe'02-ACM Workshop on Wireless Security.* portal.acm.org.

ICAO. (2006). *Doc 9303 Part 1 Volume 2.*

ICAO. (2008). *Doc 9303 part 3 volume 2.* Acesso em 01 de 08 de 2015, disponível em http://goo.gl/QzVa1p

IETF. (1998). *RFC 2315*. Acesso em 18 de 05 de 2015, disponível em http://goo.gl/uSkckj

IETF. (11 de 2000). *RFC 2986*. Acesso em 15 de 05 de 2015, disponível em https://goo.gl/LKRssI

IETF. (03 de 2004). *RFC 3739*. Acesso em 30 de 07 de 2015, disponível em https://goo.gl/wUDpCD

IETF. (05 de 2008). *RFC 5280*. Acesso em 20 de 06 de 2015, disponível em https://goo.gl/eCj5yA

IETF. (09 de 2009). *RFC 5652*. (Vigil Security, LLC) Acesso em 08 de 06 de 2015, disponível em https://goo.gl/VHEHxI

IETF. (07 de 2013). *RFC 6954*. Acesso em 28 de 06 de 2015, disponível em https://goo.gl/xTHVnE

IETF. (06 de 2013). *RFC 6960*. Acesso em 01 de 06 de 2015, disponível em

https://goo.gl/a7wDaT

IMPRENSA OFICIAL. (s.d.). *Portal Imprensa Oficial*. Acesso em 28 de 06 de 2015, disponível em https://goo.gl/M1IxoJ

Imprensa Oficial SP. (2015). Acesso em 07 de 04 de 2015, disponível em http://goo.gl/JVxca1

Ingo Naumann, G. H. (2009). *Privacy Features of European eID Card Specifications.* European Network and Information Security Agency (ENISA).

International Civil Aviation Organization. (2006). *Machine Readable Travel Documents - Part 1- Machine Readable Passports. Volume 2 - Specifications for Electronically Enabled Passports with Biometric Identification Capability.*

ITI. (01 de 11 de 2006). *a importância de participar do Objectweb* . Acesso em 08 de 08 de 2015, disponível em http://goo.gl/WMw8JG

ITI. (26 de 11 de 2007). *Manual de Condutas Técnicas - Volume 2*. Acesso em 08 de 08 de 2015, disponível em http://goo.gl/1zkRwo

ITI. (22 de 11 de 2007). *Manual de Condutas Técnicas 2 - Volume 1*. Acesso em 04 de 08 de 2015, disponível em http://goo.gl/mYRQ1g

ITI. (22 de 11 de 2007). *Manual de Condutas Técnicas 2 - Volume 2*. Acesso em 04 de 08 de 2015, disponível em http://goo.gl/CZyMTN

ITI. (23 de 11 de 2007). *Manual de Condutas Técnicas 7 - Volume 1*. Acesso em 08 de 08 de 2015, disponível em http://goo.gl/5UpXMs

ITI. (01 de 12 de 2008). *DOC-ICP-06*. Acesso em 15 de 04 de 2015, disponível em http://goo.gl/AUTfe2

ITI. (01 de 10 de 2010). *DOC-ICP-10.02*. Acesso em 03 de 08 de 2015, disponível em http://goo.gl/AukrqC

ITI. (09 de 12 de 2010). *Estrutura Normativa da ICP-Brasil*. Acesso em 27 de 04 de 2015, disponível em http://goo.gl/v5La2G

ITI. (27 de 09 de 2012). *DOC-ICP-10*. Acesso em 01 de 08 de 2015, disponível em http://goo.gl/2AFIio

ITI. (05 de 07 de 2012). *DOC-ICP-15*. Acesso em 16 de 04 de 2015, disponível em http://goo.gl/fBtDAH

ITI. (05 de 07 de 2012). *DOC-ICP-15.01*. Acesso em 16 de 04 de 2015, disponível em http://goo.gl/ceXLcZ

ITI. (05 de 07 de 2012). *DOC-ICP-15.02*. Acesso em 16 de 04 de 2015, disponível em

http://goo.gl/NT7Quh

ITI. (19 de 09 de 2012). *DOC-ICP-15.03*. Acesso em 16 de 04 de 2015, disponível em http://goo.gl/2XhgiV

ITI. (08 de 08 de 2012). *ITI e USP: desenvolvimento de Middleware para certificado digital da ICP-Brasil*. Acesso em 08 de 08 de 2015, disponível em http://goo.gl/97osWI

ITI. (09 de 10 de 2013). *Criação da AC-Defesa*. Acesso em 31 de 07 de 2015, disponível em http://goo.gl/DP1EHd

ITI. (10 de 07 de 2014). *DOC-ICP-01.01*. Acesso em 27 de 03 de 2015, disponível em ITI: http://goo.gl/ngRLMx

ITI. (29 de 04 de 2014). *DOC-ICP-03*. Acesso em 15 de 04 de 2015, disponível em http://goo.gl/eOA0fC

ITI. (29 de 04 de 2014). *DOC-ICP-04*. Acesso em 31 de 03 de 2015, disponível em ITI: http://goo.gl/QcHyxm

ITI. (17 de 12 de 2014). *Manual de Condutas Técnicas 1 - Volume 1*. Acesso em 03 de 08 de 2015, disponível em http://goo.gl/vv7MPV

ITI. (17 de 12 de 2014). *Manual de Condutas Técnicas 1 - Volume 2*. Acesso em 03 de 08 de 2015, disponível em http://goo.gl/yrt67M

ITI. (2015). *Portal do ITI*. Acesso em 05 de 03 de 2015, disponível em www.iti.gov.br

ITI. (s.d.). *Documentos Principais*. Acesso em 27 de 04 de 2015, disponível em http://goo.gl/BjQnVj

ITI. (s.d.). *O que é Certificado Digital?* Acesso em 28 de 04 de 2015, disponível em http://goo.gl/FEAc5B

ITI. (s.d.). *Processo de Homologação de Hardware*. Acesso em 03 de 08 de 2015, disponível em http://goo.gl/0xOJmu

Jansma, N., & Brandon, A. (2004). Performance Comparison of Elliptic Curve and RSA Digital Signatures. *nicj. net/files*.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security, 1*(1), 36-63.

Kubicek, H., & Noack, T. (2010). *Different countries-different paths extended comparison of the introduction od eIDs in eight European countries.* Springer.

Lehmann, A. (2013). *Survey and Analysis of Existing eID and Credential Systems.* Future Id Project.

Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* CRC Press.

(2009). *National Strategies and Policies for Digital Identity Management in OECD Countries.* OECD Publishing.

Nextgov. (2011). *GROUP URGES U.S. TO ADOPT ELECTRONIC ID CARDS FOR CITIZENS*. Acesso em 01 de 07 de 2015, disponível em http://goo.gl/SBWwdH

Poller, A., Waldmann, U., & Vowé, S. (Feb de 2012). Electronic Identity Cards for User Authentication- Promise and Practice. *Security & Privacy, IEEE*, pp. 46-54.

Project, Bangladesh Election Commission IDEA. (2014). *Notification Award.*

Rankal, W., & Effing, W. (2003). *Smart Card Handbook* (3rd Edition ed.). John Wileys & Sons, Ltd.

(s.d.). *Relatório de Melhores Práticas Mundiais.* Portugal: UMIC/UCMAC.

RNP. (s.d.). *ICPEdu*. Acesso em 09 de 07 de 2015, disponível em http://goo.gl/UB2qnF

SERASA. (s.d.). *Portal SERASA*. Acesso em 28 de 06 de 2015, disponível em https://goo.gl/aZV4j0

SERPRO. (2011). *Certificação Digital — Serpro*. Acesso em 27 de 03 de 2015, disponível em Serpro: https://goo.gl/lR88PQ

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices* (Fourth Edition ed.). Prentice Hall.

Stevens, T., Elliott, J., Hoikanen, A., Maghiros, I., & Lusoli, W. (2010). *The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies.* JRC Scientific and technical Reports, IPTS, Comissão Européia.

(2013). *STORK 2.0 Member State´s eIDs.* STORK 2.0.

(2009). *Study on eID Interoperability for PEGS: Update of Country Profiles.* IADBC European Comission.

Subramaniam, A., Chaudhry, J., & Ahmad, M. (2012). A Study on Elliptic Curve Digital Signature Algorithm (ECDSA) for Reliable E-Commerce Applications. *Smart Computer Review, 2*(1), 71-78.

Teleco. (s.d.). *Padrões de Middleware para TV Digital*. Acesso em 08 de 08 de 2015, disponível em http://goo.gl/ZM1ak1

Torres, J. A., Deus, F. E., & Sousa Júnior, R. T. (2015). Diagnóstico do governo eletrônico brasileiro – uma análise com base no modelo de gerenciamento de identidades e no novo guia de serviços.

U.S. Department of Commerce/National Institute of Standards and Technology. (2013). *Digital Signature Standard (DSS). FIPS-186-4*. Fonte: http://goo.gl/7MchcL

Vieira, J. E. (15 de 12 de 2008). *Proposta de uma Solução de Certificação Digital para o Exército Brasileiro*. (Universidade de Brasília) Acesso em 13 de 04 de 2015, disponível em http://goo.gl/yZ6jWL

W3C. (06 de 2008). Acesso em 07 de 06 de 2015, disponível em XML Signature Syntax and Processing: http://goo.gl/kGpkgy

Wiener, M. J. (s.d.). Performance comparison of public-key. *4*.

**Universidade de Brasília – UnB**

**Centro de Apoio ao Desenvolvimento Tecnológico – CDT**

**Laboratório de Tecnologias da Tomada de Decisão – LATITUDE**

www.unb.br – www.cdt.unb.br – www.latitude.eng.br