


Cartilha Sobre Certificação Digital

Versão 1.0



CERTIFICAÇÃO DE ENTIDADES BENEFICENTES
DE ASSISTÊNCIA SOCIAL NA ÁREA DE EDUCAÇÃO

 Ministério da Educação

Geral | Detalhes

Este certificado foi atestado para os seguintes usos:

Autoridade Certificadora do SS.

Emitido para

Common Name (CN)	Autoridade Certificadora Raiz Brasileira
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	Instituto Nacional de Tecnologia da Informação - ITI
Número de série	04

Emitido por

Common Name (CN)	Autoridade Certificadora Raiz Brasileira
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	Instituto Nacional de Tecnologia da Informação - ITI

Validade

Exatidão em	11/30/2001
-------------	------------

Ministério da Educação

Secretaria Executiva

Secretaria de Educação Básica - SEB

Diretoria de Tecnologia da Informação -DTI

Secretaria de Educação Superior - SESu

Instituto Nacional de Estudos e Pesquisa Educacionais Anísio Teixeira - INEP

Ministério da Saúde

Ministério do Desenvolvimento Social e Combate à Fome

Manual elaborado pela Diretoria de Tecnologia da Informação/SE

Introdução / Objetivo

Introdução	4
Objetivo	4

ICP-Brasil

ICP-Brasil	5
------------------	---

Passos

Passos	6
--------------	---

Introdução

O que é Certificação Digital?

A tecnologia que oferece sigilo, agilidade e validade jurídica em transações eletrônicas.

Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.

No cerne da certificação digital está o certificado digital, um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de Informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos.

A certificação digital tem trazido inúmeros benefícios para os cidadãos e para as instituições que a adotam. Com a certificação digital é possível utilizar a Internet como meio de comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos. A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos.

Objetivo

O objetivo dessa cartilha é apresentar ao usuário o certificado digital, um documento eletrônico assinado digitalmente que cumpre a função de associar uma pessoa ou entidade a uma chave pública.

Essa associação é feita através de suas informações públicas contidas num certificado que são colocados em repositórios públicos. Um Certificado Digital normalmente apresenta as seguintes informações:

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

Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet. Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor do banco. E o cliente, ao solicitar um serviço, como por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Por que confiar em um certificado digital?

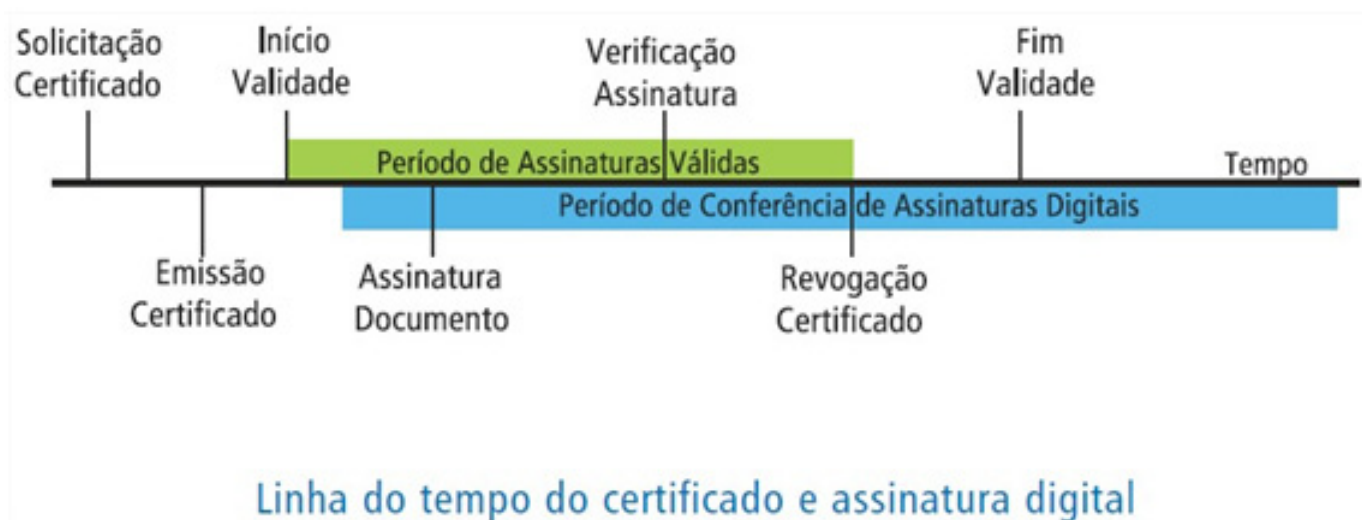
Entre os campos obrigatórios do certificado digital encontra-se a identificação e a assinatura da entidade que o emitiu, os quais permitem verificar a autenticidade e a integridade do certificado. A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. O usuário de um certificado digital precisa confiar na AC.

A escolha de confiar em uma AC é similar ao que ocorre em transações convencionais, que não se utilizam o meio eletrônico. Por exemplo, uma empresa que vende parcelado aceita determinados documentos para identificar o comprador antes de efetuar a transação. Estes documentos normalmente são emitidos pela Secretaria de Segurança de Pública e pela Secretaria da Receita Federal, como o RG e o CPF. Existe, aí, uma relação de confiança já estabelecida com esses órgãos. Da mesma forma, os usuários podem escolher uma AC à qual desejam confiar a emissão de seus certificados digitais.

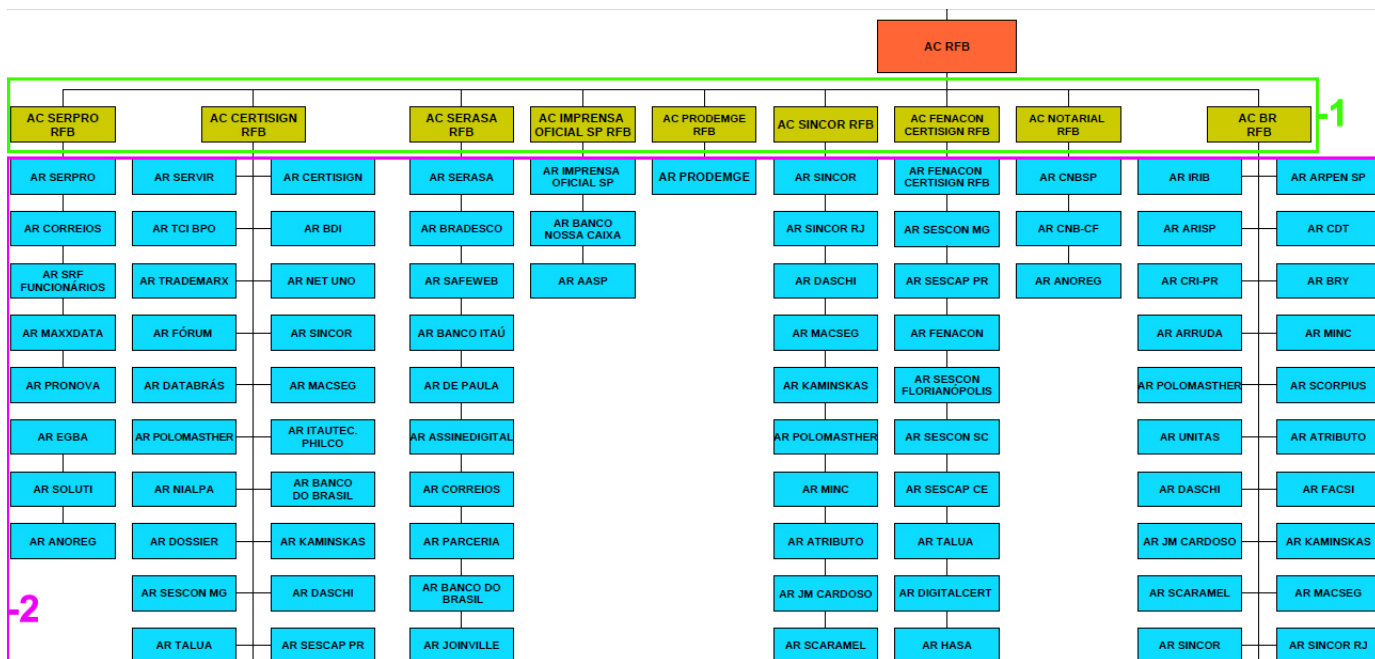
Para a emissão dos certificados, as ACs possuem deveres e obrigações que são descritos em um documento chamado de Declaração de Práticas de Certificação – DPC. A DPC deve ser pública, para permitir que as pessoas possam saber como foi emitido o certificado digital. Entre as atividades de uma AC, a mais importante é verificar a identidade da pessoa ou da entidade antes da emissão do certificado digital. O certificado digital emitido deve conter informações confiáveis que permitam a verificação da identidade do seu titular.

Por estes motivos, quanto melhor definidos e mais abrangentes os procedimentos adotados por uma AC, maior sua confiabilidade. No Brasil, o Comitê Gestor da ICP-Brasil é o órgão governamental que especifica os procedimentos que devem ser adotados pelas ACs. Uma AC que se submete às resoluções do Comitê Gestor pode ser credenciada e com isso fazer parte da ICP-Brasil. O cumprimento dos procedimentos é auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. A não concordância com as regras acarreta em aplicações de penalidades, que podem ser inclusive o descredenciamento. As ACs credenciadas são incorporadas à estrutura hierárquica da ICP-Brasil e representam a garantia de atendimento dos critérios estabelecidos em prol da segurança de suas chaves privadas.

Como funciona o processo de um certificado digital?



1º Passo: O usuário deve procurar uma autoridade certificadora - AC (1) a sua escolha ou de registro - AR (2).



2º Passo: Solicitar na própria página da internet da AC escolhida a emissão de certificado digital de pessoa física (ex: e-CPF) e/ou jurídica (ex: e-CNPJ).

Os tipos mais comercializados são: A1 (validade de um ano – armazenado no computador) e A3 (validade de até três anos – armazenado em cartão ou token)

criptográfico).

A AC também deve informar sobre aplicações, custos, formas de pagamento, equipamentos, documentos necessários e demais exigências;

3º Passo: Para a emissão de um certificado digital é necessário que o solicitante vá pessoalmente a uma Autoridade de Registro (AR) da Autoridade Certificadora escolhida para validar os dados preenchidos na solicitação.

Esse processo é chamado de validação presencial e será agendado diretamente com a AR que instruirá o solicitante sobre os documentos necessários.

Atenção: *Os documentos necessários para compra de um certificado e-CPF são:*

- Foto 3x4 colorida (recente);
- Cédula de Identidade;
- Cadastro de Pessoa Física - CPF;
- Comprovante de Endereço recente, emitido há no máximo 90 dias;
- Título de eleitor (Opcional);
- PIS-PASEP (Opcional);

OBS: A solicitação desses documentos podem variar de AC para AC.

Atenção: *Os documentos necessários para compra de um certificado e-CNPJ são:*

- Registro comercial, no caso de empresa individual;
- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado no órgão competente, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- Prova de inscrição do Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Toda a documentação necessária para e-CPF.

Importante: Caso no estatuto, contrato social ou documento equivalente de sua empresa, conste que o representante legal da empresa cadastrado na Receita Federal não possa assinar isoladamente, será necessário que as pessoas citadas neste documento como representantes legais compareçam para validação presencial de posse de seus documentos.

Os hardwares criptográficos utilizados para certificado A3 são:

SMART CARD: É um tipo de cartão plástico (semelhante a um cartão de crédito) com um ou mais microchips embutidos, capaz de armazenar e processar dados. Um smart card pode ser programado para desempenhar inúmeras funções, inclusive pode ter capacidade de gerar Chaves Públicas e Privadas e de armazenar Certificados Digitais. Pode ser utilizado tanto para controle de acesso lógico como para controle de acesso físico.

TOKEN: Hardware para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o smart card a grande diferença é que ele possui conexão com o computador via USB e o Smart Card necessita de uma leitora.

Quem escolher o certificado tipo A3 poderá receber na própria AR o cartão ou token com o certificado digital.

4º Passo: Emissão do certificado. A AC e/ou AR notificará o cliente sobre os procedimentos para baixar o certificado.

5º Passo: Instalar os driver's do hardware criptográfico e cadeia de certificação. Para isso entre em contato com a AC escolhida.


6º Passo: Período de utilização do certificado.

Atenção: Se durante esse período acontecer algum problema com o certificado, o mesmo deve ser revogado (cancelado).

7º Passo: Quando o seu certificado digital estiver perto do vencimento, este poderá ser renovado eletronicamente, uma única vez, sem a necessidade de uma nova validação presencial.



CERTIFICAÇÃO DE ENTIDADES BENEFICENTES
DE ASSISTÊNCIA SOCIAL NA ÁREA DE EDUCAÇÃO

 Ministério da Educação