



Ministério da Fazenda

Serviço Federal de Processamento de Dados (SERPRO)

APRESENTAÇÃO

CERTIFICAÇÃO DIGITAL

Palestrante: Lusimar Moraes

Soluções para um
Brasil de Todos



Ministério
da Fazenda



www.serpro.gov.br

Certificação Digital



"On the Internet, nobody knows you're a dog."

“Na Internet ninguém sabe quem você é.”

(The New York Times)

O QUE É CERTIFICAÇÃO DIGITAL?

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.

Para viabilizar essa prática, em todo o seu potencial, é necessário adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas.



O QUE É CERTIFICAÇÃO DIGITAL?

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 disponibilização de diversos serviços com maior agilidade, facilidade de acesso e substancial redução de custos.



O QUE É CERTIFICAÇÃO DIGITAL?

A Certificação Digital fornece recursos básicos de segurança que são necessários para que as transações eletrônicas na Internet possam ser feitas com conforto, confiança e de maneira segura.

Como garantir quem são as partes envolvidas?

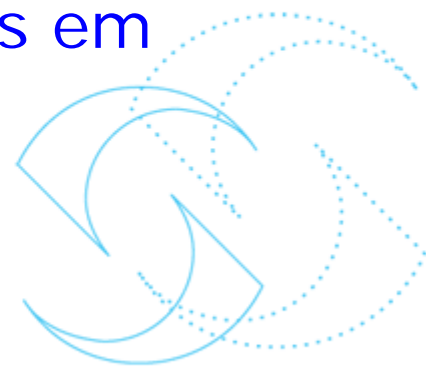
Hoje, a Certificação Digital é considerada a ferramenta de segurança mais eficaz, não só para garantir a identificação da origem e do destino, como também a integridade das mensagens na Internet



O QUE É CERTIFICAÇÃO DIGITAL?

Pode-se destacar quatro aspectos fundamentais dentre os requisitos que formam os níveis de segurança recomendados para as transações eletrônicas:

1) Confidencialidade – Certamente nenhum de nós gostaria que correspondências de negócios fossem lidas, ou que seja visto o valor de compras ou saldo bancário, sem o nosso consentimento. Privacidade, sigilo e discrição são aspectos fundamentais em qualquer tipo de negócio.



O QUE É CERTIFICAÇÃO DIGITAL?

2) Autenticidade - Queremos saber qual a real origem das informações que recebemos.

Que é do autor a quem se atribui, que é verdadeiro, legítimo.

3) Integridade - Mais do que ter certeza da origem das informações, queremos confiar que nenhuma delas foi alterada no caminho que percorreram. Não gostaríamos de descobrir mais tarde que um valor ou número crucial não era bem aquele que recebemos.



O QUE É CERTIFICAÇÃO DIGITAL?

4) Irretratabilidade ou Não repúdio - Igualmente não queremos que alguém que nos faça uma encomenda, nos diga depois que não foi o autor do pedido, sem que consigamos provar quem fez a operação.

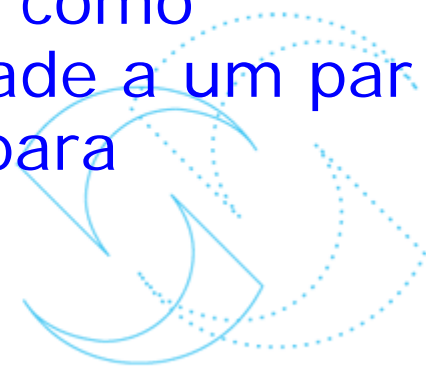


O QUE É CERTIFICAÇÃO DIGITAL?

Certificação Digital é o equivalente eletrônico de carteiras de identidade, passaportes e cartões de associados.

Você pode apresentar uma Identificação Digital eletronicamente para provar sua identidade ou seu direito a acessar informações ou serviços on-line.

Identificações Digitais, também conhecidas como Certificados Digitais, vinculam uma identidade a um par de chaves eletrônicas que pode ser usado para criptografar e assinar informações digitais.



O QUE É CERTIFICAÇÃO DIGITAL?

Certificação Digital é a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.



QUEM EMITE UM CERTIFICADO DIGITAL?

Um Certificado Digital ou Identificação Digital, é emitida por uma **Autoridade de Certificação (AC)** e é assinada com a Chave Privada desta AC.

Uma Identificação Digital normalmente contém:

- A Chave Pública do proprietário
- O nome do proprietário
- A data de vencimento da Chave Pública
- Nome do emissor (a AC que emitiu a Identificação Digital)
- O número de série da Identificação Digital
- A assinatura digital do emissor



O QUE É UMA AUTORIDADE CERTIFICADORA?

Autoridade Certificadora AC - são entidades credenciadas pela **Autoridade Certificadora Raiz – AC-Raiz** a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular.



O QUE É UMA AUTORIDADE CERTIFICADORA RAIZ?

Autoridade Certificadora Raiz – AC-Raiz: É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais.



O QUE É ICP-BRASIL?

A Infra-Estrutura de Chaves Públicas Brasileira - ICP-BRASIL é um conjunto de técnicas, práticas e procedimentos a ser implementado pelas organizações governamentais e privadas brasileiras, com o objetivo de estabelecer os fundamentos, técnicas e metodologias de um sistema de Certificação Digital baseado em Chaves Públicas.

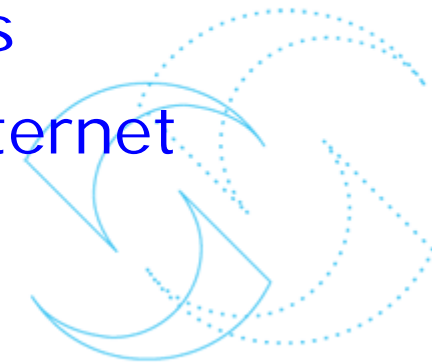
O Instituto Nacional de Tecnologia da Informação (ITI), autarquia pública federal, vinculada a Casa Civil da Presidência da República é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.



O QUE É ICP-BRASIL?

A Certificação Digital foi instituída no Brasil com a criação da **Infra-estrutura de Chaves Públicas Brasileira – ICP-BRASIL**, através da MP 2.200-2 visando garantir:

- ✓ Autenticidade e a validade de documentos em forma eletrônica, de aplicações
- ✓ Autenticidade a aplicações de suporte e de aplicações habilitadas que utilizem certificados digitais
- ✓ Realização de transações eletrônicas na Internet



O QUE É ICP-BRASIL?

A ICP-BRASIL é composta por:

- ✓ Autoridade Gestora de Políticas
- ✓ Cadeia de Autoridades Certificadoras – AC
- ✓ Autoridade de Registros – AR



O QUE É UMA ASSINATURA DIGITAL?

As assinaturas digitais são utilizadas para identificar autores ou co-assinantes de dados eletrônicos, e assim:

- ✓ Autenticar a identidade de quem assinou os dados - desse modo, você saberá quem participou na transação e terá a certeza que não foi falsificado por ninguém.
- ✓ Proteger a integridade dos dados - dessa maneira, você terá certeza que a mensagem que leu não foi alterada, tanto acidentalmente como intencionalmente.



O QUE É UMA ASSINATURA DIGITAL?

- ✓ Permite a você provar futuramente quem participou em uma transação (uma capacidade chamada de não-repúdio) - assim, ninguém poderá negar que assinou ou recebeu os dados.



O QUE É UMA ASSINATURA DIGITAL?

DOCUMENTO EM PAPEL X DOCUMENTO ELETRÔNICO

A semelhança da assinatura digital e da assinatura manuscrita restringe-se ao princípio de atribuição de autoria a um documento.

Na assinatura manuscrita, segue-se um padrão de semelhança e características pessoais e biométricas de cada indivíduo. Ela é feita sobre algo tangível, o papel.

A veracidade da assinatura é feita por comparação visual a uma assinatura verdadeira.



O QUE É UMA ASSINATURA DIGITAL?

DOCUMENTO EM PAPEL X DOCUMENTO ELETRÔNICO

No documento eletrônico não existe um modo simples de relacionar o documento com a assinatura. Ambos são apenas representação eletrônica de dados, que necessitam de um computador para a sua visualização e conferência.

Na assinatura digital, a assinatura gerada é diferente para cada documento, pois está relacionada ao resumo do documento.



O QUE É UMA ASSINATURA DIGITAL?



Validade Jurídica

Apesar das diferenças, a técnica de assinatura digital é uma forma eficaz de garantir autoria de documentos eletrônicos.



O QUE É UMA ASSINATURA DIGITAL?



Validade Jurídica

Em agosto de 2001 a MP 2.200-2, art. 10 § 1º, garantiu validade jurídica de documentos eletrônicos e a utilização de certificação digital para atribuir autenticidade e integridade aos documentos.

Este fato tornou a assinatura digital um instrumento válido juridicamente.



O QUE SÃO CHAVES PÚBLICAS E PRIVADAS?

A criptografia de chave pública é utilizada para assegurar a privacidade da informação, porém fornece outra função vital na troca segura da informação eletrônica: **a autenticação**.

Autenticação, nesse contexto, se refere ao processo que o receptor de uma mensagem eletrônica realizará para verificar a integridade da mensagem e também a identidade do remetente.



O QUE SÃO CHAVES PÚBLICAS E PRIVADAS?

Em um sistema de criptografia de chave pública, duas chaves são necessárias para que duas partes troquem informação de forma segura: uma chave **pública** e uma chave **privada**.

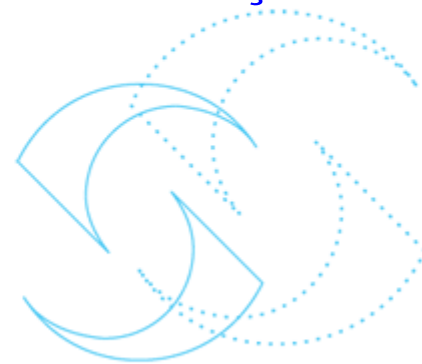
Se uma dessas chaves for utilizada para criptografar uma mensagem, então somente a outra chave do par poderá ser usada para decifrá-la.



O QUE SÃO CHAVES PÚBLICAS E PRIVADAS?

Embora o par de chaves **pública** e **privada** seja relacionado matematicamente, computacionalmente é impossível derivar uma chave da outra, assim, a chave privada está protegida contra duplicação e falsificação até mesmo quando alguém souber a sua chave pública.

Consequentemente, é seguro distribuir abertamente a sua chave pública para que todos possam utilizá-la, porém é essencial que sua chave privada permaneça em segredo.

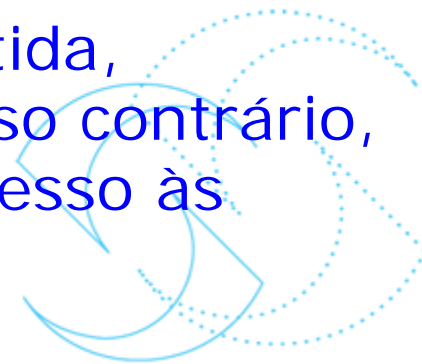


O QUE SÃO CHAVES PÚBLICAS E PRIVADAS?

Se alguém quiser lhe mandar uma mensagem criptografada, esta pessoa criptará a mensagem com a sua chave pública, e somente você, possuidor da chave privada correspondente, poderá decifrá-la.

A grande vantagem deste sistema é permitir que qualquer um possa enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la.

A **confidencialidade** da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso a chave privada terá acesso às mensagens.



TIPOS DE CERTIFICADOS

Foi estabelecido inicialmente pela ICP-BRASIL, oito tipos de certificados, sendo que quatro deles são específicos para Assinatura Digital, e os outros quatro de Sigilo.

Os certificados para Assinaturas são A1 A2 A3 e A4

Os de Sigilo são S1 S2 S3 e S4.

Os tipos A1 e S1 estão associados ao requisito de menor segurança e A4 e S4 aos requisito de segurança mais rigorosa.



COMO ARMAZENAR UM CERTIFICADO DIGITAL?

Existem vários meios de armazenamento de um certificado digital:

- ✓ Utilização de Browser: aplicativo instalado na estação de trabalho do usuário que permite a recuperação e envio de dados pela Internet (ex.: Internet Explorer, Mozilla, Netscape, etc.).



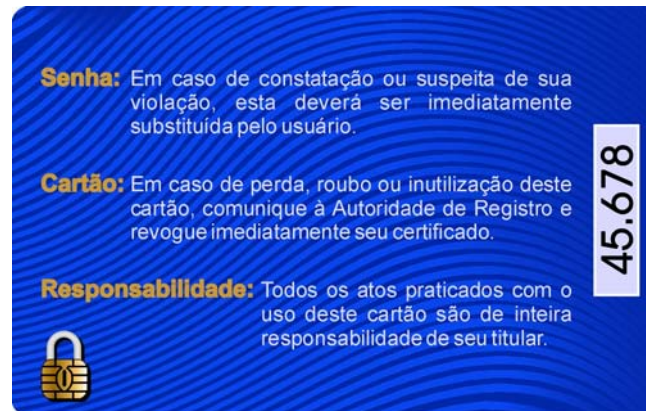
COMO ARMAZENAR UM CERTIFICADO DIGITAL?

- ✓ Utilização de E-Token: dispositivo a ser utilizado na porta USB (Universal Serial Bus), similar a um Pen Drive. Este dispositivo normalmente contém um microprocessador que permite a autenticação de informações.



COMO ARMAZENAR UM CERTIFICADO DIGITAL?

- ✓ Utilização de Smart Card: dispositivo similar a um cartão de crédito, possuindo um ou mais circuitos integrados que executam as funções de microprocessador, memória e I/O.



A Autoridade Certificadora SERPRO- ACSERPRO- é uma entidade, credenciada pela AC-RAIZ que emite certificados digitais para outras entidades (organizações ou indivíduos), de acordo com a Política de Certificação e Declaração de Práticas de Certificação, possibilitando a eles provar sua identidade eletrônica.



AUTORIDADE CERTIFICADORA

Assim, a sua principal função é, emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados (LCR), identificar e registrar todas as ações executadas, conforme as normas, praticas e regras estabelecidas pelo Comite Gestor da ICP-BRASIL.



A Autoridade de Registro: é a entidade credenciada pela AC-RAIZ imediatamente superior, responsável pela verificação documental de todas as solicitações de emissão ou de revogação de certificados.

Este processo é realizado somente por pessoas credenciadas por órgão competente.

Essas pessoas são responsáveis pela aprovação, rejeição ou revogação dos certificados e pelo armazenamento destes documentos.



O Autoridade de Registro - AR vinculada a ACSERPRO terá a responsabilidade de tratar solicitações de certificados, autenticando a identidade ou outras credenciais do candidato, aprovando ou rejeitando então sua solicitação.



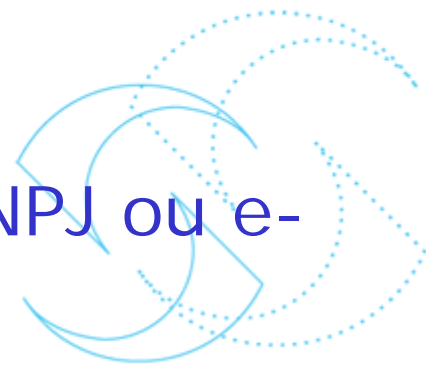
PASSO A PASSO PARA A CERTIFICAÇÃO DIGITAL



SOLICITAÇÃO DE CERTIFICADO

São 3 as etapas que devem ser seguidas para obtenção do Certificado Digital e-CPF, e-CNPJ ou e-Equipamento

- a) Preenchimento da solicitação do Certificado
- b) Comparecimento a uma Autoridade de Registro - AR
- c) Instalação do certificado e-CPF, e-CNPJ ou e-Equipamento



SOLICITAÇÃO DE CERTIFICADO

ETAPA 1 -

Preenchimento da Solicitação do Certificado



SOLICITAÇÃO DE CERTIFICADO

1º Passo: Acessar a Internet

2º Passo: Acesse a página:

<https://ccd.serpro.gov.br/serproacf>

3º Passo: Escolha do Tipo de Certificado (A1 ou A3);
(e-CPF, e-CNPJ)

4º Passo: Clique em Solicitar Certificado

5º Passo: Preencher os dados solicitados e click em enviar



SOLICITAÇÃO DE CERTIFICADO

6º Passo: Aparecerá uma tela com os dados digitados para conferência e confirmação

7º Passo: Aparecerá duas telas com os dados digitados para conferência.

Tela A: Anote o “**número de referência para a solicitação**”, a ser utilizado no preenchimento do TERMO DE TITULARIDADE



SOLICITAÇÃO DE CERTIFICADO

Tela B: TERMO DE TITULARIDADE
parcialmente preenchido.

Preencha as informações conforme
solicitado e depois clique em “Gerar
versão para impressão”.



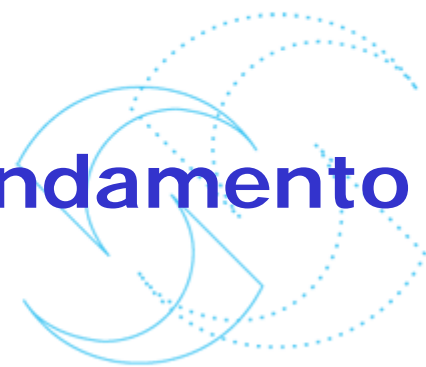
8º Passo: Após aparecer a versão para impressão, imprima-o em 3 vias.



ETAPA 2

Comparecimento à Autoridade de Registro – AR

- ✓ Ligar na Central de Atendimento
**SERPRO – CAS, telefone:
08007282323 para solicitar o
agendamento**
- ✓ Aguardar contato para o agendamento



SOLICITAÇÃO DE CERTIFICADO

Comparecer junto à Autoridade Certificadora munido dos seguintes documentos:

- ✓ Cédula de Identidade (duas cópias autenticadas ou apresentar original)
- ✓ Cadastro de Pessoa Física – CPF (duas cópias autenticadas ou apresentar original)
- ✓ Título de Eleitor (duas cópias autenticadas ou apresentar original)
- ✓ PIS/PASEP (duas cópias)
- ✓ Comprovante de Residência (duas cópias)
- ✓ Termo de Titularidade (três cópias)
- ✓ 2 fotos 3 x 4 recente



Etapa 3

Instalação do certificado



SOLICITAÇÃO DE CERTIFICADO

1º Passo: Quando devidamente aprovado pelo AR, acessar a Internet, da mesma estação de trabalho da qual foi solicitado o certificado e o mesmo endereço de solicitação do certificado

2º Passo) Clique em “Baixar Certificado” e siga as instruções



SOLICITAÇÃO DE CERTIFICADO

IMPORTANTE:

Após concluir o processo de instalação do Certificado Digital entrar na opção *Cadeia de Certificados* -
> *Certificados*

Baixar e instalar as três Cadeias de Certificados: ICP-Brasil; Autoridade Certificadora da Receita e Autoridade Certificadora SERPRO-SRF

