

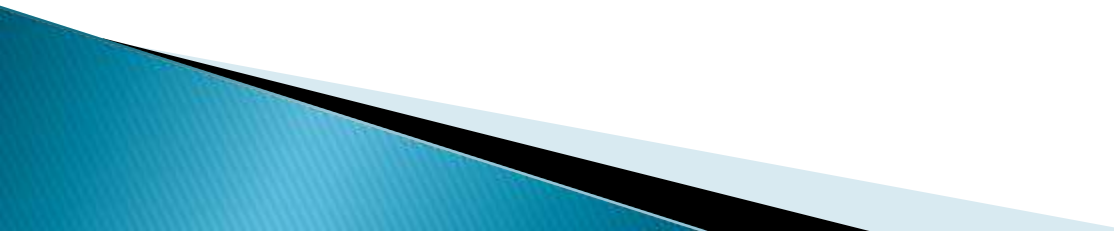
# Assinatura e Certificado Digital



Carlos Henrique M. da Silva  
[carloshenrique.85@globocom.com](mailto:carloshenrique.85@globocom.com)

# Assinatura Digital OU Assinatura Eletrônica?

O termo assinatura eletrônica, por vezes confundido, tem um significado diferente: refere-se a qualquer mecanismo, não necessariamente criptográfico, para identificar o remetente de uma mensagem eletrônica. A legislação pode validar tais assinaturas eletrônicas como endereços Telex e cabo, bem como a transmissão por fax de assinaturas manuscritas em papel.



# Assinatura Digital

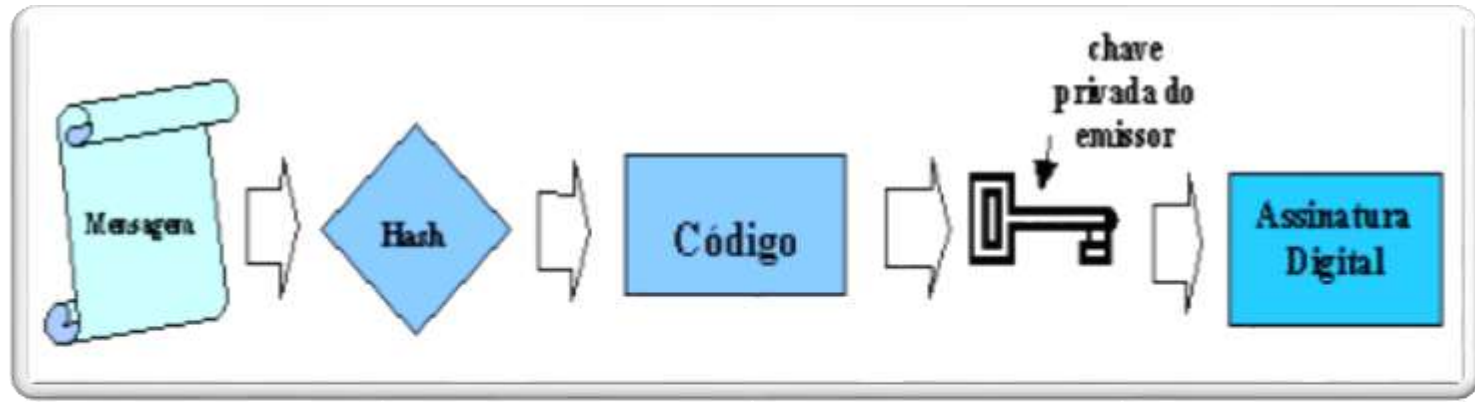
A assinatura digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos. É um conjunto de operações criptográficas aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital.



# Assinatura Digital

A assinatura digital permite comprovar:

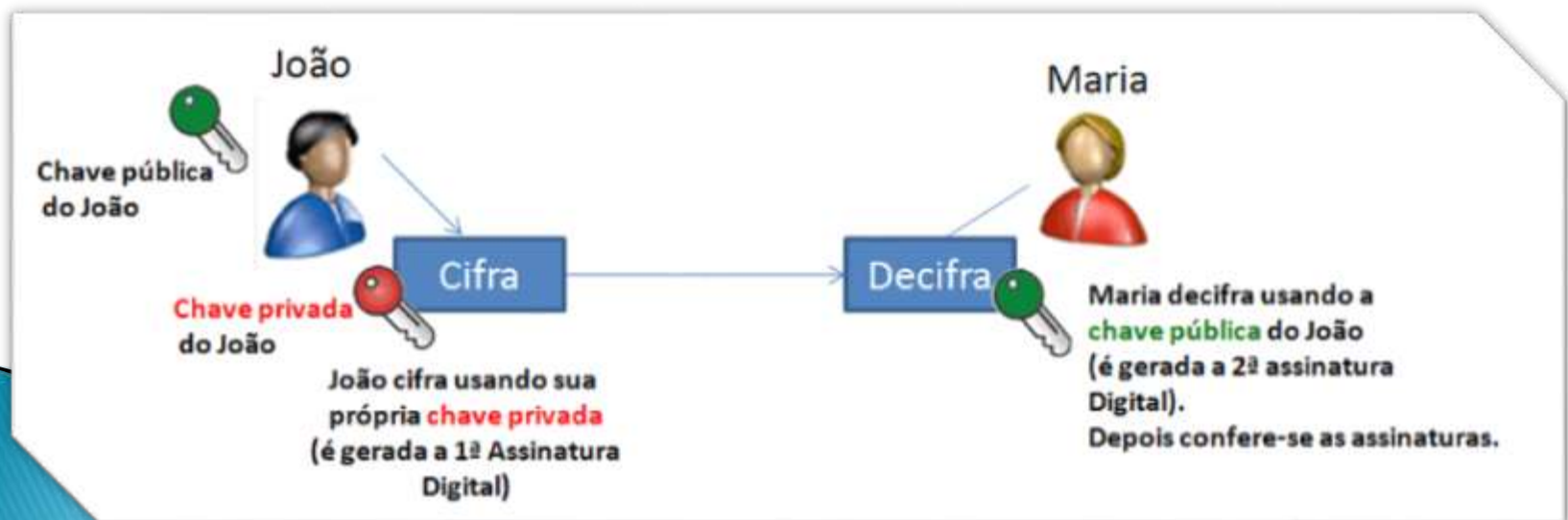
- Que a mensagem ou arquivo não foi alterado e
- Que foi assinado pela entidade ou pessoa que possui a chave criptográfica (chave privada) utilizada na assinatura.



# Assinatura Digital

A tecnologia de assinatura digital é baseada num par de chaves criptográficas:

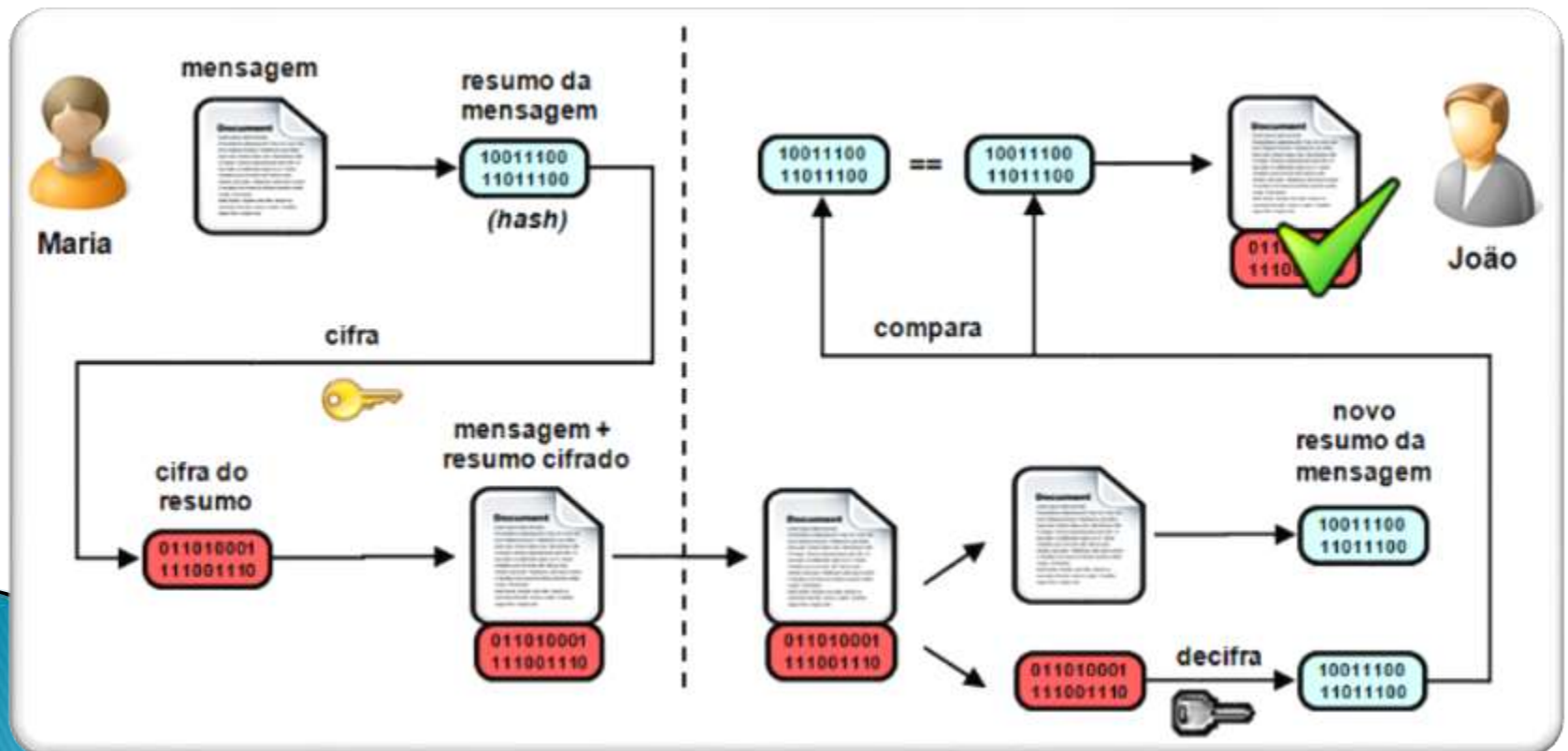
- A chave pública, distribuída livremente dentro do certificado, para permitir a validação das assinaturas.
- A chave privada, é guardada pelo seu proprietário também chamado titular do certificado, é a que se utiliza para assinar os documentos.





# Assinatura Digital

Para assinar digitalmente um arquivo, aplica-se inicialmente uma função matemática a esse arquivo, obtendo-se um resumo criptográfico (hash) desse arquivo.



# Assinatura Digital

## Como elas são feitas?

Para conseguir uma assinatura digital, qualquer pessoa ou empresa deve ir até uma entidade autorizada pelo Instituto Nacional de Tecnologia da Informação (ITI) — chamadas de Autoridades Certificadoras (AC) — e requisitar uma chave privada.



# Certificação Digital

Outro trunfo da assinatura digital é que, com o crescente número de pessoas e empresas usando esse artifício, foi necessário organizar e padronizar essas operações. A ICP-Brasil faz isso por meio da **certificação digital** e das assinaturas das AC (Autoridade Certificadora).





# Certificação Digital

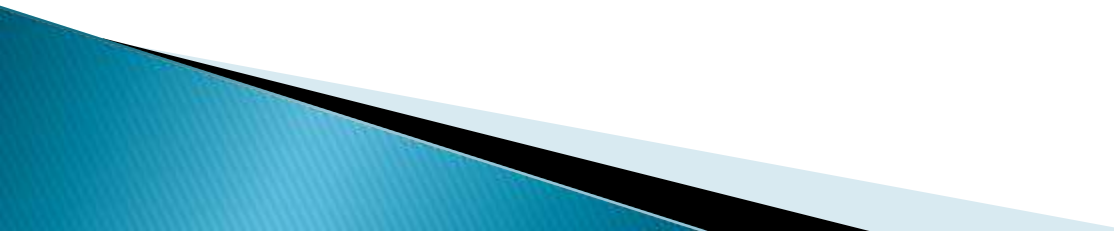
A ICP-Brasil fiscaliza e audita o processo de emissão de certificados digitais das autoridades certificadoras integrantes a fim de garantir total confiabilidade do processo de certificação. Desta forma dá respaldo à presunção legal de integridade, autenticidade e não-repúdio dos arquivos assinados digitalmente.



# Autoridades Certificadoras

## AC – Raiz

A Autoridade Certificadora Raiz da ICP–Brasil (AC–Raiz) é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP–Brasil. Portanto, compete à AC–Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das ACs de nível imediatamente subsequente ao seu.



# Autoridades Certificadoras

## AC – Autoridade Certificadora

Uma AC é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.

Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC).

[EXEMPLO de Listas de uma AC](#)

# Certificação Digital

Os certificados contêm os dados de seu titular, como nome, número do registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros, conforme especificado na Política de Segurança de cada Autoridade Certificadora.

QUANTIDADE DE CERTIFICADOS  
EMITIDOS EM 2012/2013



# Tipos de Certificado

- **Assinatura (A1, A2, A3, A4)**

- Utilizados na confirmação de identidade na Web, em e-mail, em VPN e em documentos eletrônicos com verificação da integridade de suas informações.

- **Sigilo (S1, S2, S3, S4)**

- Utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.



# Tipos de Certificado

Tipo de certificado	Chave criptográfica			Validade máxima (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smart card ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smart card ou token, com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smart card ou token, com capacidade de geração de chave	3

# Certificação Digital

O Brasil possui **3,5 MILHÕES** de certificados digitais **ATIVOS** e vem emitindo cerca de **200 MIL A CADA MÊS** conforme dados apresentados pelo Instituto Nacional de Tecnologia da Informação (ITI), no 11º Certforum, em Brasília, nesta quinta-feira, 12/9. Nesse universo do sistema de identificação digital reconhecido pelo país, com base no modelo de chaves públicas ICP Brasil, menos de um terço são usadas por pessoas físicas – há **1,1 MILHÃO** de brasileiros com pelo menos um certificado digital.



# Certificação Digital

Mas ainda que seja uma ferramenta ainda **'corporativa'**, a imensa maioria dos 3,5 milhões, **80%** deles, é de **certificados portáteis** – chamados **A3**, são aqueles que podem ser inseridos em **pen drives** ou **tokens**. Os demais, cerca de **660 MIL**, são os tipo **A1**, que ficam instalados em discos rígidos.



# Certificação Digital

## ASPECTOS LEGAIS



Conforme a Medida provisória 2.200-2, a lei brasileira determina que qualquer documento digital tem validade legal se for certificado pela ICP-Brasil. A medida provisória também prevê a utilização de certificados emitidos por outras infra-estruturas de chaves públicas, desde que as partes que assinam reconheçam previamente a validade destes.



# Certificação Digital

E, na prática, como tudo isso é usado?

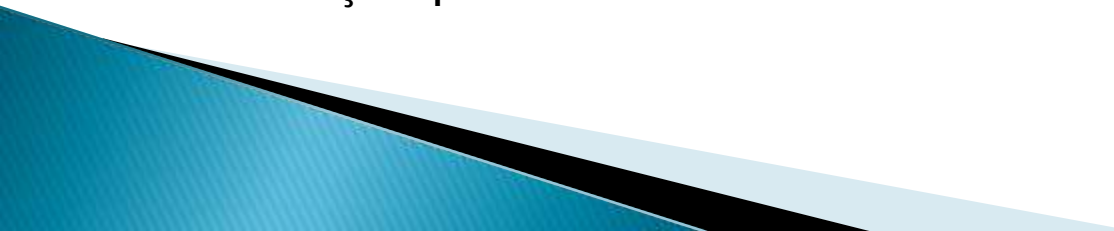
Você pode não perceber, mas o seu navegador confere os certificados dos sites acessados o tempo todo. Cada browser identifica problemas de uma maneira diferente — no caso do Chrome, os cadeados verdes são usados para certificados reconhecidos, amarelos para mostrar problemas e vermelhos para os não identificados.

Ícone	O que significa
	<b>O site não está usando SSL.</b> A maioria dos sites não precisa usar SSL porque não lida com informações confidenciais. Evite digitar informações confidenciais, como nomes de usuários e senhas, na página.
 https://	<b>O Google Chrome estabeleceu uma conexão segura com o site.</b> Caso você seja solicitado a fazer login no site ou inserir informações confidenciais na página, procure esse ícone e certifique-se de que o URL possui o domínio correto.  Se o site utilizar um certificado EV-SSL (Extended Validation SSL), o nome da organização também aparecerá em verde ao lado do ícone.
 https://	<b>O site usa SSL, mas o Google Chrome detectou conteúdo não seguro na página.</b> Tenha cuidado caso você esteja digitando informações confidenciais nessa página. Conteúdo não seguro pode oferecer uma brecha para que alguém modifique a aparência da página.
 https://	<b>O site usa SSL, mas o Google Chrome detectou conteúdo não seguro de alto risco na página ou problemas com o certificado do site.</b> Não digite informações confidenciais nessa página. Um certificado inválido ou outros problemas sérios com https podem indicar que alguém está tentando adulterar sua conexão com o site.



# Certificação Digital

## COMO OBTER

- 1 – Escolher uma Autoridade Certificadora (AC) da ICP-Brasil;
  - 2 – Solicitar no próprio portal da internet da AC escolhida a emissão de certificado digital de pessoa física ou jurídica.
  - 3 – 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.
  - 4 – A AC e/ou AR notificará o cliente sobre os procedimentos para baixar o certificado e deverá prestar todo o suporte técnico quando solicitada pelo usuário;
  - 5 – Quando o certificado digital estiver perto do vencimento, este poderá ser renovado eletronicamente, uma única vez, sem a necessidade de uma nova validação presencial.
- 

# Certificação Digital

VALORES\$



Certificação Digital

# Portal de Assinaturas



# Outros Tipos de Certificados Digitais



# OBRIGADO!

**Carlos Henrique M. da Silva**  
**[carloshenrique.85@globo.com](mailto:carloshenrique.85@globo.com)**

- } Formado em Análise de Sistemas
- } Pós-Graduado em Auditoria em T.I.
- } Gerente de TI da CLIOC – Coleção de *Leishmania* do Instituto Oswaldo Cruz – Fiocruz
- } Certificado em Gestão de Segurança da Informação e Gerenciamento de T.I. pela Academia Latino-Americana (Microsoft TechNet / Módulo Security)

