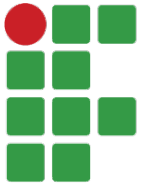
Segurança Computacional

Certificação Digital

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau

Certificação Digital

Certificação Digital

- **Certificação Digital** é uma tecnologia de identificação de entidades no meio computacional.
- Possui mecanismos que garantem
  - Autenticidade
  - Confidencialidade
  - Integridade
  - Não-repúdio

Certificação Digital

- Vantagens:
  - Desburocratização (até certo ponto)
  - Eliminação de papel
  - Segurança

Certificação Digital

Figura: Certificado Digital.

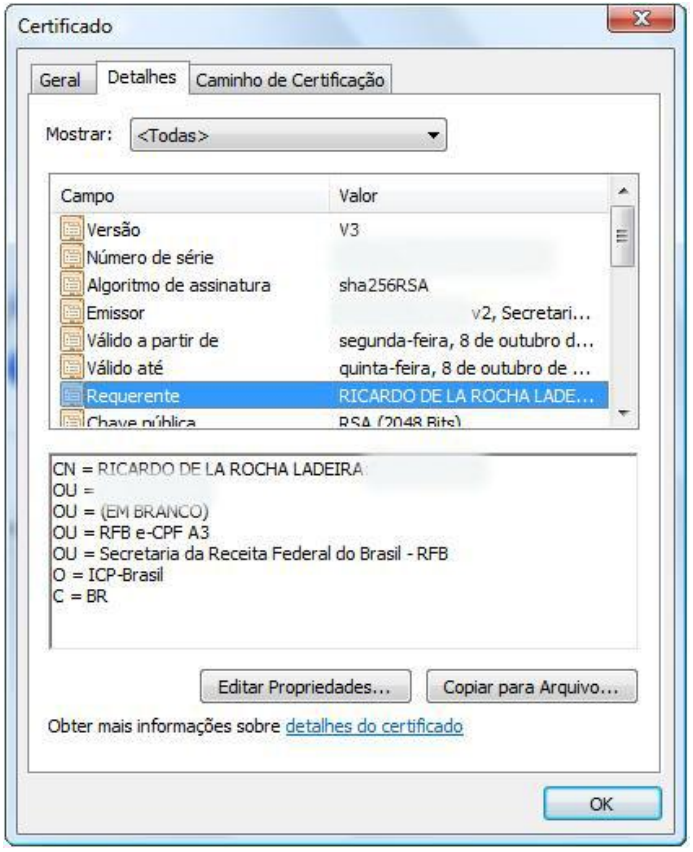
Fonte: elaborado pelo autor.

Certificado Digital

- **Certificado Digital** é um documento eletrônico que permite a identificação de uma entidade no contexto computacional.
  - Possui nome, número serial, nome do emissor, data de emissão, data de revogação etc.
  - Acompanha uma chave pública (a privada é mantido em sigilo).
- Uma entidade pode ser uma pessoa, uma empresa, um servidor...

Certificação Digital

Figura: Certificado Digital.



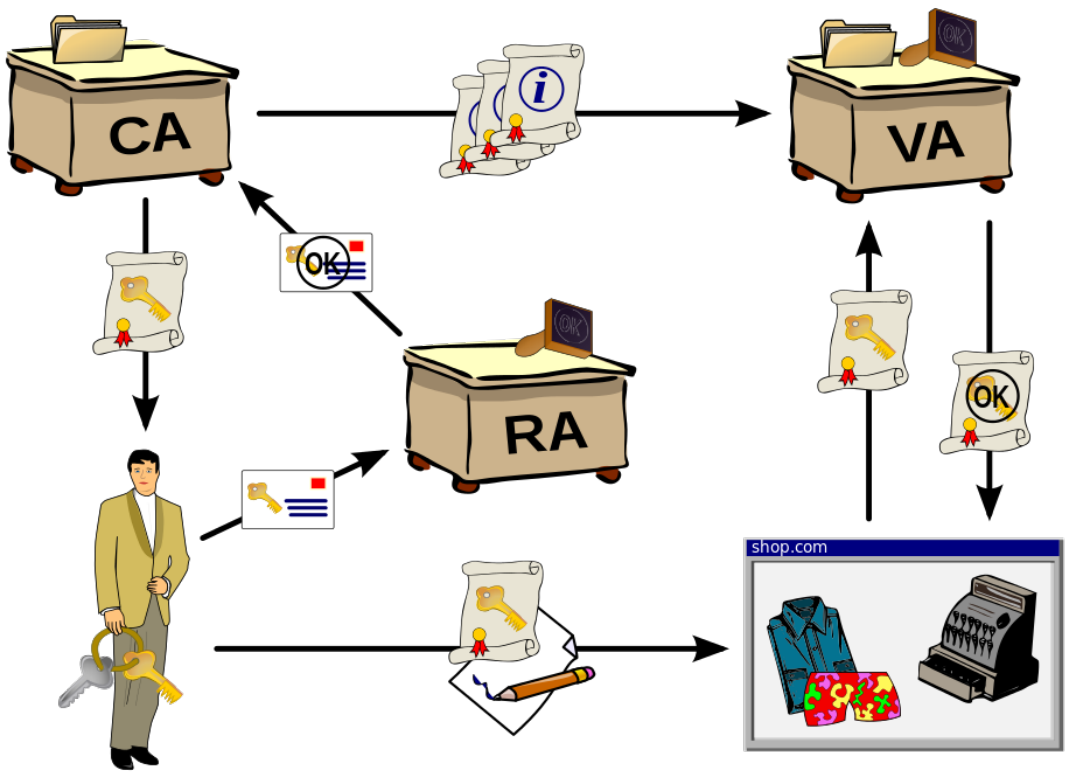
Fonte: elaborado pelo autor.

Certificado Digital

- O Certificado Digital é emitido dentro de uma **Infraestrutura de Chave Pública** – ICP, ou *Public Key Infrastructure* – PKI.
- "A Infraestrutura de Chaves Públicas brasileira (ICP-Brasil) é um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública" (IOERJ, s. d.).
  - Asseguram validade jurídica às transações.

Certificação Digital

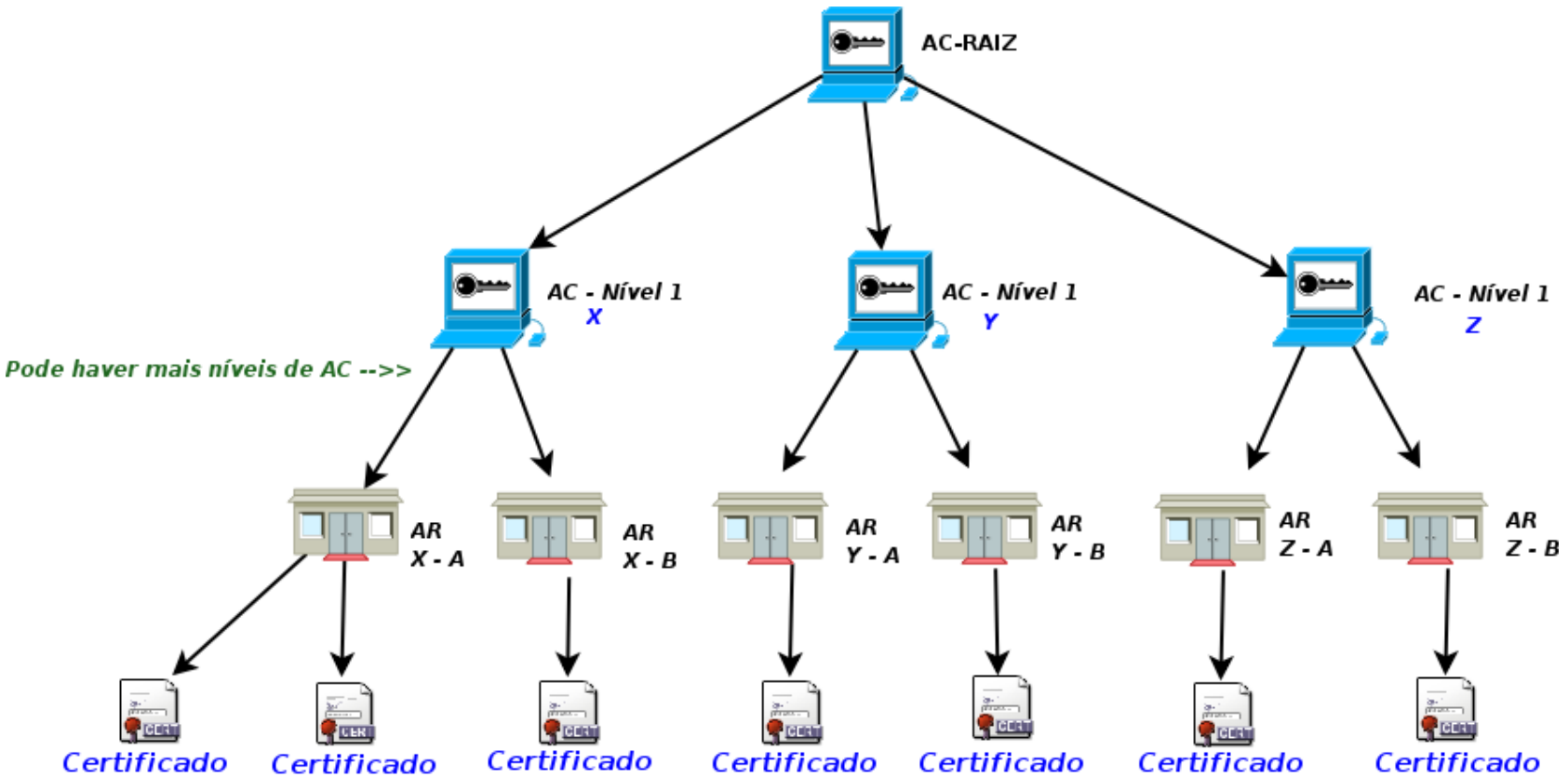
Figura: Infraestrutura de Chaves Públicas.



Fonte: Wikipédia, 2016.

Certificação Digital

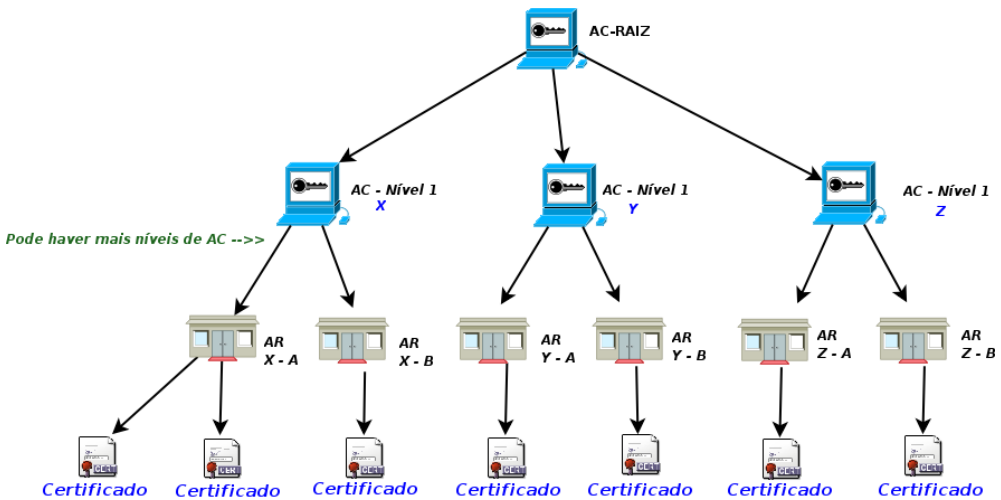
Figura: Hierarquia de uma PKI.



Fonte: DevMedia, 2016.

Certificação Digital

Figura: Hierarquia de uma PKI.



Fonte: DevMedia, 2016.

- Havendo ACs de nível 1 e 2, as ACs de nível 1 podem emitir certificados para pessoas (PF e PJ), dispositivos e ACs de níveis inferiores. ACs de nível 2 não podem emitir certificados para outras ACs, exceto se houver outros níveis abaixo dela (3, 4...).

Certificado Digital

- Certificados de Assinatura Digital
- Certificados de Sigilo
- Certificados de (Carimbo de) Tempo
- $\rightarrow$ **Certificados de Atributo**

Certificado Digital

- Pode ser instalado e armazenado diretamente em um dispositivo de armazenamento, tal como um HD (exemplos: certificados A1 e S1).

- Pode ser instalado em uma mídia criptográfica, tal como um cartão inteligente ou um token (exemplos: certificados A3 e S4).

- Pode ser armazenado na nuvem em um *Hardware Security Module* – HSM[1] em caso de certificado A3, sendo utilizado por smartphone e outros dispositivos. Um exemplo disso é o NeoID.

[1] Hardware que fornece funções criptográficas para a geração e armazenamento de chaves criptográficas simétricas e assimétricas. São dispositivos resistentes à adulteração e protegem processos criptográficos.

Certificação Digital

Figura: Mídias Criptográficas.

Fonte: digiblu, s.d.

Certificação Digital

Figura: Carteira Profissional.

Fonte: CRC-BA, 2007.

Certificado Digital

Assinatura Digital

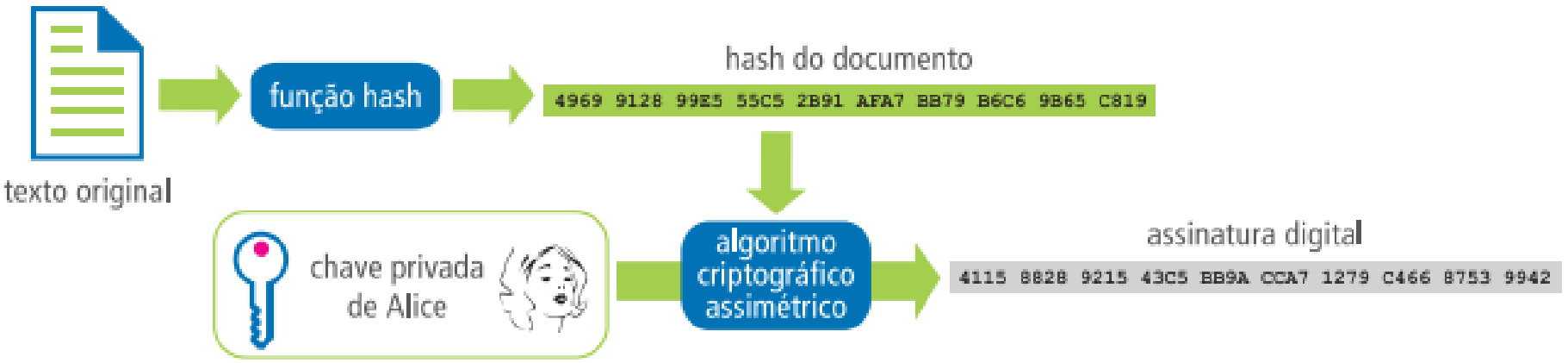
- "O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamada de assinatura digital" (ITI, 2005).

- Assinatura digital **não é sinônimo** de assinatura eletrônica. Assinatura eletrônica é um termo genérico que identifica uma entidade no meio digital, o que envolve senhas, digitação de um nome no fim de um e-mail, assinatura de próprio punho escaneada etc. Essas assinaturas não têm valor jurídico, sendo necessário laudo pericial para comprovar a origem da transação ou do seu remetente. A assinatura digital possui valor jurídico quando estiver nos padrões legais.

Certificação Digital

Assinatura Digital

Figura: Assinatura digital utilizando algoritmos de chave pública.



Fonte: ITI, 2005.

Certificado Digital

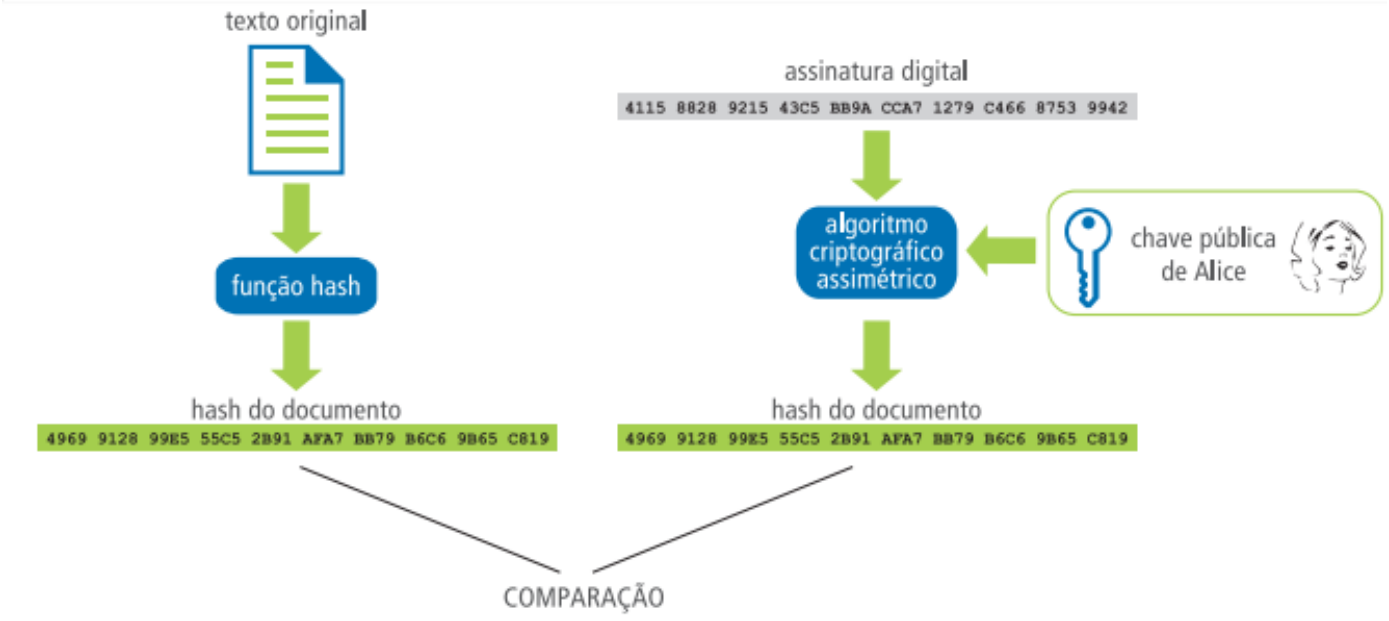
Assinatura Digital

- Como isso garante integridade?
- Como isso garante não-repúdio?
- Por que fazer isso no resumo e não diretamente no arquivo?

Certificação Digital

Assinatura Digital

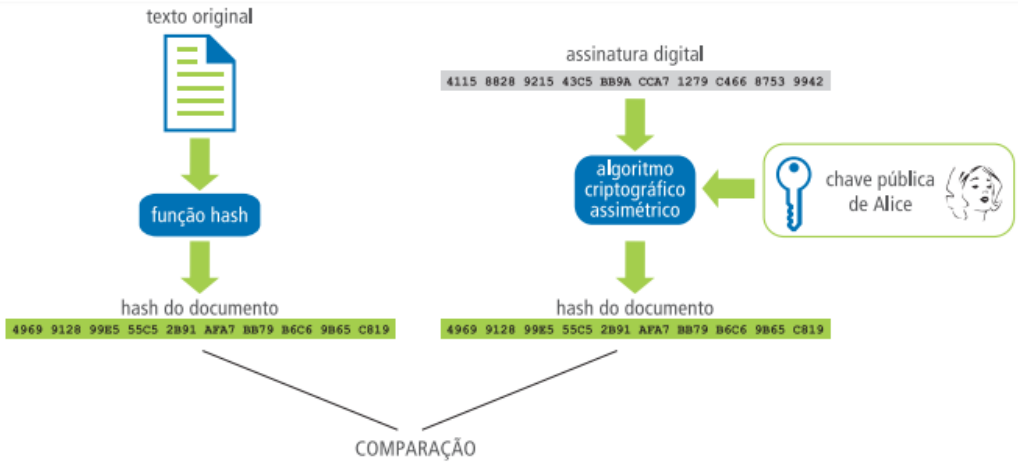
Figura: Conferência de Assinatura Digital.



Fonte: ITI, 2005.

Certificação Digital

Assinatura Digital



- Na ICP-Brasil (e em outras PKIs), o processo técnico de validação de assinaturas possui alguns passos antes, tais como:

1. Validar a cadeia de certificados.
2. Verificar a validade do certificado do assinante.
3. Verificar se o certificado não foi revogado.
4. Validar a aderência ao formato de assinaturas aceito pela ICP-Brasil.

Certificação Digital

Assinatura Digital

- Na ICP-Brasil, o processo técnico de validação de assinaturas pode ser feito no endereço `https://verificador.iti.br/`.

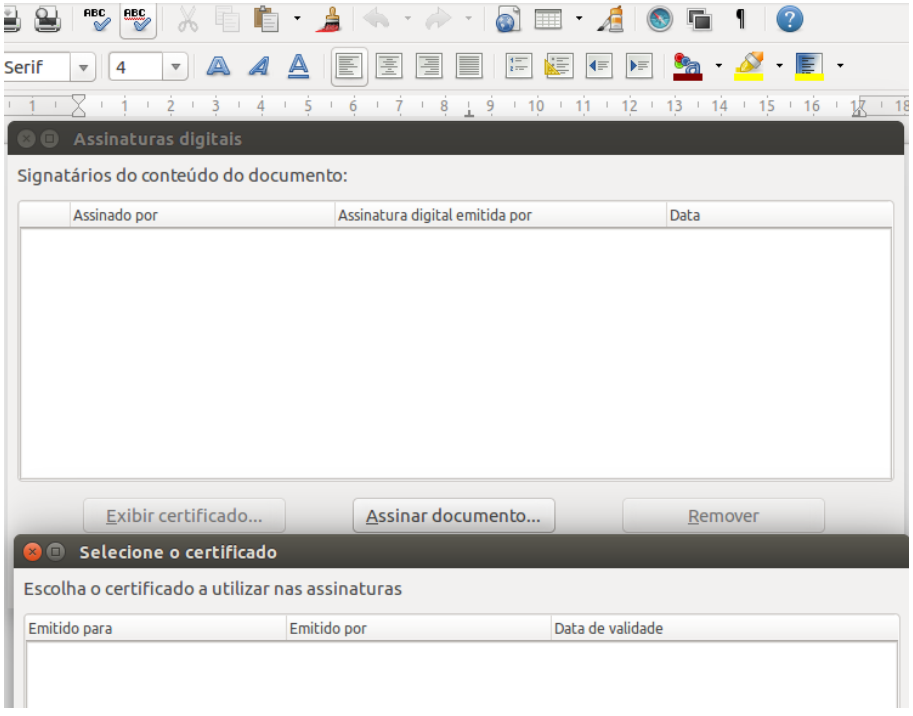
- É possível testar com algum arquivo assinado conhecido (exemplo: documento-assinado-verificador-iti.pdf), como na imagem:

Figura: Validação de assinatura com o verificador do ITI.

Certificação Digital

Assinatura Digital

Figura: Funcionalidade de Assinatura Digital no LibreOffice Writer.

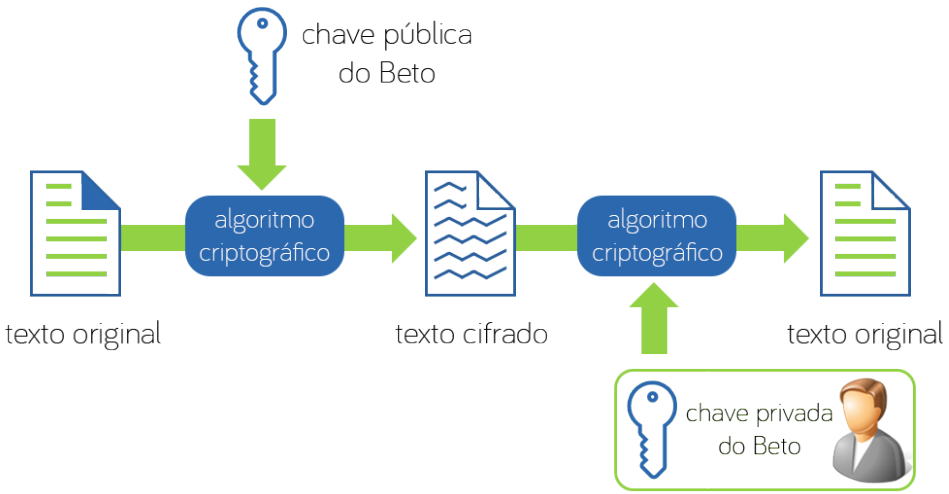


Fonte: elaborado pelo autor.

Certificação Digital

Sigilo

Figura: Sigilo utilizando criptografia assimétrica.



Fonte: ITI, 2005.

- O certificado de sigilo criptografa dados deixando-os acessíveis apenas a certificados digitais autorizados. Assim, o conteúdo fica inacessível a entidades não autorizadas.

Certificação Digital

Carimbo de Tempo

- Certificados de Carimbo de Tempo são emitidos apenas para equipamentos de Autoridade Certificadora de Tempo (ACT). São responsáveis por gerar os Carimbos do Tempo que são adquiridos pelo usuário final.

- Os carimbos do tempo funcionam como um protocolo, atestam a data em que um documento foi recebido, criado ou assinado. São muito utilizados em processos licitatórios e jurídicos.

- Na ICP-Brasil costumam ser chamados de "T".

- Mais informações:
  `https://loja.serpro.gov.br/carimbodetempo`

Certificado Digital

OpenSSL

- OpenSSL: biblioteca que implementa SSL/TLS.
- Permite gerar certificados digitais SSL.
- Quando instalado em um servidor web, por exemplo, pode ativar o protocolo HTTPS e permitir conexões seguras entre cliente e servidor.

Certificado Digital

OpenSSL

- Criação de uma chave privada com OpenSSL:

- `openssl genrsa -des3 4096 > seunome.key`
  `#genrsa`: gera uma chave privada RSA.
  `#des3`: algoritmo utilizado para criptografar a chave privada.
  `#4096`: tamanho da chave.
  `#seunome.key`: nome do arquivo.

- Crie uma senha.

- Este arquivo deve ser mantido em sigilo.

Certificado Digital

OpenSSL

- Criação da respectiva chave pública:
- `openssl req -new -key seunome.key > seunome.csr`
  Necessário informar a senha.
  Pede sigla do país, estado, cidade, organização, departamento, nome, e-mail, chave de recuperação e nome opcional para a organização.
- Este arquivo pode ser distribuído livremente.

Certificado Digital

OpenSSL

- Criação do certificado:

- `openssl x509 -req -days 730 -in ricardo.csr -signkey seunome.key -out seunome.crt`
- Associa o certificado ao par de chaves gerado.
- Define a validade para 2 anos.
- Novamente exige senha.

Certificado Digital

OpenSSL

- Criação de um arquivo para assinatura:
- `echo "Meu documento, vamos assinar!">> abc.txt`
- `openssl dgst -sha256 -sign seunome.key -out abc.txt.sha256 abc.txt`
- Exige novamente a senha.
- `abc.txt` tem o conteúdo.
- `abc.txt.sha256` tem o hash assinado do arquivo `abc.txt`.

Certificado Digital

OpenSSL

- Verifica se a a assinatura do arquivo procede:
- `openssl dgst -sha256 -verify <(openssl x509 -in seunome.crt -pubkey -noout) -signature abc.txt.sha256 abc.txt`
- `Verified OK!`

- Altere o arquivo e salve-o. Digite novamente:
- `openssl dgst -sha256 -verify <(openssl x509 -in seunome.crt pubkey -noout) -signature abc.txt.sha256 abc.txt`
- `Verification Failure`

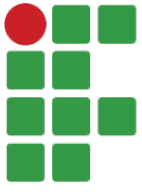
Referências

- ITI. 2005. O que é certificação digital? Cartilha. Disponível em: <https://esaj.tjms.jus.br/WebHelp/documentos/iticertificacao_digital.pdf>. Acesso em: 11 jul. 2021.
- IOERJ. O que é a ICP - Brasil. Disponível em: <https://www.ioerj.com.br/portal/modules/smartfaq/faq.php?faqid=60>. Acesso em: 2 ago. 2024.
- WIKIPÉDIA. Public key infrastructure. Disponível em: <https://en.wikipedia.org/wiki/Public_key_infrastructure>. Acesso em: 14 set. 2016.

Segurança Computacional

Certificação Digital

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau