Infraestrutura de Chaves Públicas do Brasil – ICP Brasil

✓ Autoridade Certificadora do Tempo (ACT)

• A ACT tem a responsabilidade geral pelo fornecimento do **Carimbo do Tempo**, conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período.

Fonte: https://www.iti.gov.br/icp-brasil/entes-da-icp-brasil

Principais Tipos de Certificados Digitais

(Pessoas físicas e jurídicas)

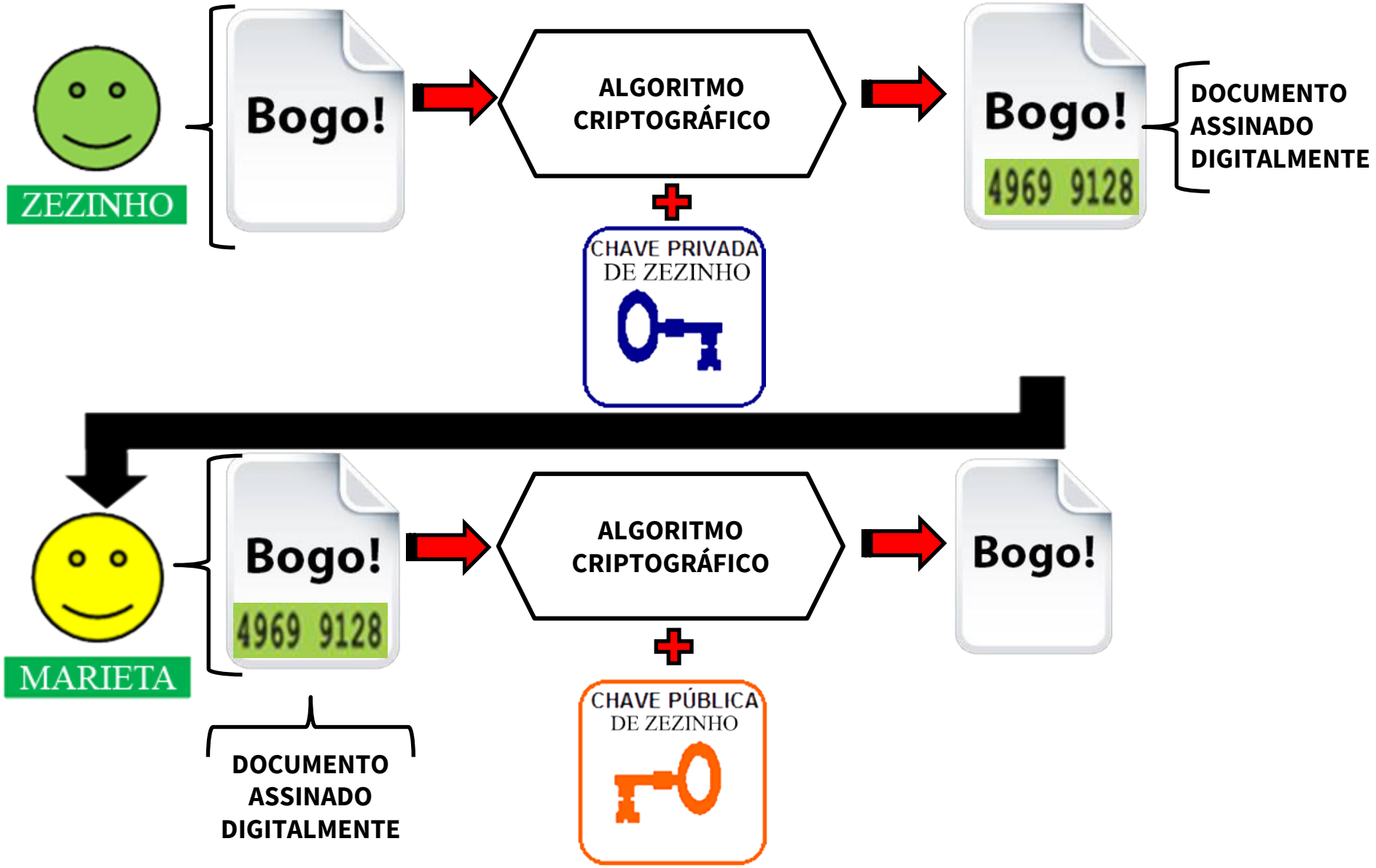
Certificado A1

Validade de 1 ano

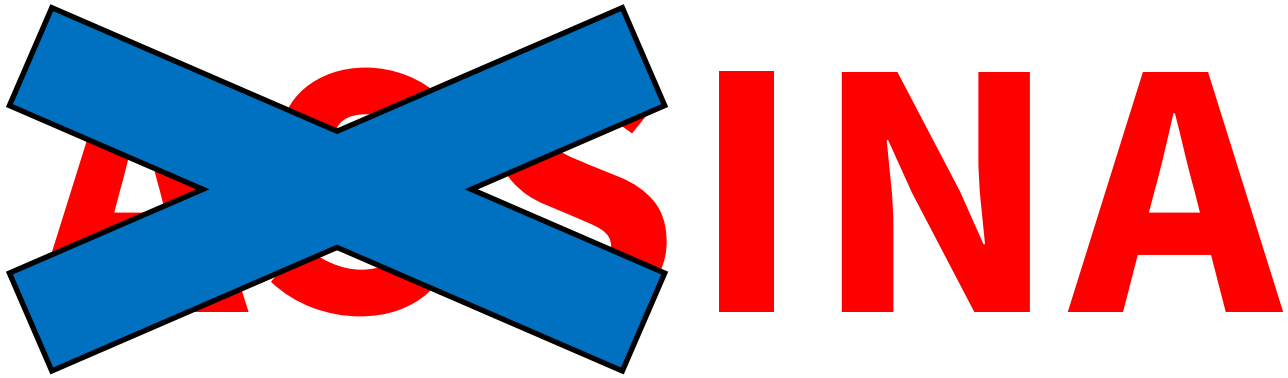
Certificado A3

Validade de 1 a 3 anos

Assinatura Digital


ZEZINHO
Bogo!
ALGORITMO CRIPTOGRÁFICO
Bogo!
4969 9128
DOCUMENTO ASSINADO DIGITALMENTE
CHAVE PRIVADA DE ZEZINHO
MARIETA
Bogo!
4969 9128
ALGORITMO CRIPTOGRÁFICO
Bogo!
DOCUMENTO ASSINADO DIGITALMENTE
CHAVE PÚBLICA DE ZEZINHO

Algoritmo Hash (MD5 – SHA1 – SHA2)


ASINA

CRIPTOGRAFIA ASSIMÉTRICA

CRIPTOGRAFAR

REMETENTE

DESTINATÁRIO

ASSINATURA DIGITAL

REMETENTE

DESTINATÁRIO

Ass.: Tio Bogo!

Principais algoritmos Criptográficos

- **SIMÉTRICOS**

  - ✓ **RC4, RC5, RC6**
  - ✓ **DES, 3DES**
  - ✓ **IDEA**
  - ✓ **AES**
  - ✓ **BLOWNFISH**
  - ✓ **TWOFISH**
  - ✓ **CAST**

Principais algoritmos Criptográficos

- **ASSIMÉTRICOS**
  - ✓ **RSA**
  - ✓ **RABIN**
  - ✓ **ELGAMAL**
  - ✓ **DSA**
  - ✓ **DIFFIE-HELLMAN**
  - ✓ **ECC**

Assinatura Digital

Da Classificação das Assinaturas Eletrônicas

Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

I - assinatura eletrônica **simples**:

a) a que permite identificar o seu signatário;

b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

Fonte: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm

Assinatura Digital

Da Classificação das Assinaturas Eletrônicas

Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

II - assinatura eletrônica **avançada**: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:

a) está associada ao signatário de maneira unívoca;

b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;

c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;

Fonte: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm

Assinatura Digital

Da Classificação das Assinaturas Eletrônicas

Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

III - assinatura eletrônica **qualificada**: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

Fonte: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm

Terminologia

Art. 3º Para os fins desta Lei, considera-se:

I - **autenticação**: o processo eletrônico que permite a identificação eletrônica de uma pessoa natural ou jurídica;

II - **assinatura eletrônica**: os dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos nesta Lei;

III - **certificado digital**: atestado eletrônico que associa os dados de validação da assinatura eletrônica a uma pessoa natural ou jurídica;

IV - **certificado digital ICP-Brasil**: certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na forma da legislação vigente.

Fonte: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm

8) Q3152320 Ano: 2024 Banca: FGV Prova: Prefeitura de Caraguatatuba

O sistema de criptografia simétrica tem como característica o uso de algoritmos e o compartilhamento de uma única chave secreta compartilhada entre o remetente e o destinatário. Assinale a opção que indica um algoritmo de criptografia simétrica.

A) AES.

B) DSS.

C) ECC.

D) PKI.

E) RSA.

9) Q3135262 Ano: 2024 Banca: CEBRASPE Prova: CAU - Analista de Infraestrutura de Tecnologia da Informação

Um certificado digital do tipo A1 armazena a chave no próprio equipamento do usuário; no tipo A3, a chave é armazenada em dispositivos físicos portáteis, como tokens e cartões.

CERTO

10) Q3134334 Ano: 2024 Banca: CEBRASPE Prova: CAU - Assistente de Tecnologia da Informação - 2024

Para ser considerado íntegro, determinado conjunto de dados não pode ser alterado sem a devida autorização.

CERTO

11) Q3152572 Ano: 2024 Banca: Instituto VerbenaProva: Câmara de Anápolis

O uso de assinaturas digitais fornece comprovação da identidade de um usuário, site ou entidade. Utiliza tecnologia de criptografia para garantir autenticidade e integridade. Os três tipos de assinatura atualmente utilizados são:

A) simples, avançada e qualificada.

B) simples, extrajudicial e PJ.

C) avançada, PF e qualificada.

D) simples, qualificada e PJ.

12) Q3135306 Ano: 2024 Banca: CEBRASPE Prova: CAU - Analista de Infraestrutura de Tecnologia da Informação - 2024

Os sistemas criptográficos simétricos também são chamados de sistema de segredo compartilhado, seja entre duas ou mais partes, visto que o segredo compartilhado pode ser utilizado para manter uma informação confidencial entre as partes na comunicação.

CERTO

13) Q3134332 Ano: 2024 Banca: CEBRASPE Prova: CAU - Assistente de Tecnologia da Informação

A assinatura digital de determinado documento digital permite a verificação da integridade dos dados desse documento.

CERTO

14) Q3116483 Ano: 2024 Banca: FGV Prova: Analista de Gestão - Área Tecnologia da Informação

Um importante procedimento de segurança da informação, que é a garantia da integridade e autenticidade dos documentos trocados pela Internet, pode ser obtido com o uso de certificados digitais. Avalie as seguintes afirmativas sobre o uso de certificados digitais:

I. Certificados digitais podem ser usados para gerar assinaturas digitais em documentos.

II. Certificados digitais aumentam o desempenho e a velocidade de transferência de informações na Internet.

III. Um certificado digital, uma vez emitido, não pode ser revogado antes do fim de sua validade.

Está correto o que se afirma em

A) I, apenas.

B) II, apenas.

C) I e III, apenas.

D) II e III, apenas.

E) I, II e III.

15) Q2687171 Ano: 2023 Banca: CEFETMINAS Prova: Prefeitura de Contagem - Analista Fazendário

A respeito da segurança da informação em redes de computadores, julgue as afirmações a seguir como verdadeiras (V) ou falsas (F).

( ) O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública.

( ) A “Lista de Assinaturas Revogadas” (LAR), contendo assinaturas digitais não confiáveis, é emitida periodicamente pelas Autoridades Certificadoras (ACs).

( ) A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isso.

A sequência correta é

A) V, F, F.

B) V, F, V.

C) F, F, V.

D) F, V, F.

E) F, V, V.

16) Q3224786 Ano: 2024 Banca: Instituto Verbena Prova: TJ AC - Analista Judiciário - Área Analista de Suporte

A criptografia de chave pública, também conhecida como criptografia assimétrica, é um pilar fundamental da segurança digital, permitindo a comunicação segura entre partes em um ambiente em que a interceptação de dados por terceiros não autorizados é uma preocupação constante. Neste sistema de criptografia de chave pública, como é garantida a confidencialidade na comunicação entre duas partes?

A) Utilizando uma única chave compartilhada para criptografia e descriptografia dos dados.

B) Utilizando a chave pública para criptografar os dados, que só podem ser descriptografados pela correspondente chave privada do destinatário.

C) Empregando a mesma chave privada tanto para criptografar quanto para descriptografar a mensagem, garantindo que apenas o remetente e o destinatário tenham acesso.

D) Codificando a mensagem com a chave privada do remetente, de modo que qualquer parte com a chave pública correspondente possa descriptografar.