SEGURANÇA DA INFORMAÇÃO V

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.

Exemplo: imaginemos uma situação em que há um horário determinado para o envio de um documento assinado eletronicamente.Conforme mencionado anteriormente, todos os elementos se entrelaçam e se combinam, não se isolam. O documento é enviado dentro do horário estipulado, mas a outra parte questiona a validade do envio.

A autoridade certificadora do tempo atua como um juiz entre as partes envolvidas em uma divergência. Supondo que o documento foi enviado às 14 horas, no horário oficial, e a outra parte alega que o envio ocorreu após esse horário, o carimbo do tempo registra o momento exato em que o documento foi gerado. O envio pode depender de diversas circunstâncias, mas o horário será validado. É importante lembrar que há validade jurídica neste processo. Dependendo do questionamento, o carimbo do tempo pode ser utilizado como prova. Embora a certificação do tempo não seja sempre exigida, é relevante estar ciente de sua existência.

Principais tipos de certificados digitais (pessoas físicas e jurídicas)

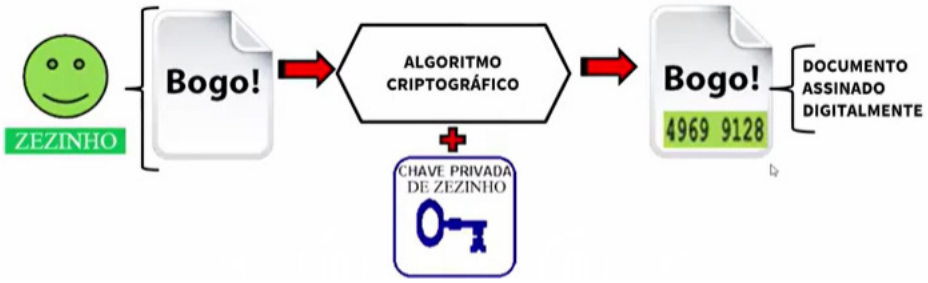
O certificado digital A1 é um arquivo eletrônico que, após a compra, é enviado por e-mail. Deve-se instalar este arquivo no computador ou nos computadores que necessitam do certificado digital. Sua validade é de um ano, sendo necessário renovar o certificado anualmente.

O certificado digital A3, por sua vez, é um dispositivo físico, como um pendrive ou um cartão que armazena o certificado digital, sendo utilizado em leitores específicos. A validade deste dispositivo varia de um a três anos, havendo uma modalidade na nuvem com validade de até cinco anos.

Assinatura digital

A assinatura digital é um método de validar documentos de forma eletrônica. Similar à assinatura manuscrita, que é validada em um cartório, a assinatura digital comprova a identidade do signatário. A analogia com a assinatura manuscrita serve para entender que ambas têm o propósito de autenticar a autoria de um documento, como um cheque ou contrato.

A assinatura digital comprova a autenticidade do documento, assegurando que foi o signatário quem realmente assinou. O certificado digital, utilizado nesse processo, é essencial para esta comprovação. O processo de assinatura digital utiliza criptografia assimétrica, que envolve o uso de duas chaves para garantir a autenticidade e segurança desde o início.



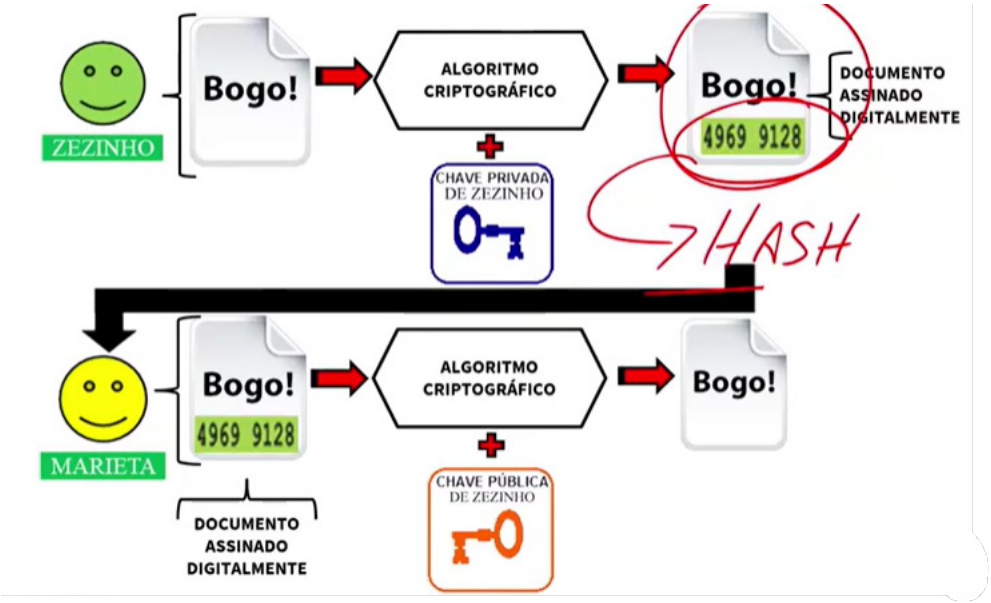
O processo de assinatura digital envolve a aplicação de um algoritmo criptográfico e a utilização da chave privada do signatário.

Exemplo: o indivíduo, Zezinho, assina digitalmente um texto utilizando sua chave privada. Para garantir o sigilo, anteriormente utilizava-se a chave pública do destinatário, pois as chaves de uma mesma pessoa são uma combinação única e perfeita. Assim, a chave privada de uma pessoa não se encaixa com a chave pública de outra.

Quando Zezinho usa sua chave privada para assinar o documento, a verificação será feita com sua chave pública. Na criptografia assimétrica, ao contrário da criptografia simétrica que utiliza uma única chave privada, a chave pública é amplamente divulgada, eliminando problemas de distribuição.

5m

Para a assinatura digital, aplica-se a chave privada ao documento, gerando um documento assinado digitalmente. Esse processo envolve o uso de um algoritmo hash, que cria um resumo da mensagem. Essa abordagem não criptografa o documento para sigilo, mas sim para autenticação e integridade.



Ainda no exemplo, perceba que Marieta recebe o documento que contém esse hash, que será verificado gerando-o novamente para validar a integridade do documento. Esse processo garante a autenticidade e o não repúdio, pilares fundamentais.

Marieta recebeu o documento assinado e usará o algoritmo criptográfico, aplicando a chave pública de Zezinho. Quando uma chave de uma pessoa é utilizada, a outra chave dessa mesma pessoa deve ser usada no contexto.

Por exemplo, se a chave pública de Maria é utilizada, a chave privada dela será necessária. Se a chave privada de Zezinho foi usada para assinar digitalmente o documento, a chave pública dele será usada para verificar.

Assim, evita-se confusão com as chaves. O documento terá sua autenticidade, não repúdio e integridade comprovados.

Algoritmo Hash (MD5 – SHA1 – SHA2)

O algoritmo hash, como MD5, SHA-1 e SHA-2, é utilizado para gerar um resumo único a partir de uma mensagem. Esses algoritmos são mencionados ocasionalmente em provas, embora não com muita frequência.

O algoritmo hash gera um resumo único para cada mensagem, o que significa que se a mesma mensagem for processada várias vezes, o resultado será sempre o mesmo. Por outro lado, qualquer alteração na mensagem, como um espaço ou vírgula, resultará em um resumo diferente, pois o texto se torna outro.

Mesmo pequenas alterações, como a modificação ou supressão de uma vírgula, mudam o hash. É importante entender que o hash gerado deve ser idêntico sempre que a mensagem original é processada sem alterações. Qualquer mudança na mensagem, mesmo que mínima, alterará o hash, indicando que a mensagem não é mais a mesma.

Quando o texto é processado pelo algoritmo hash, ele gera um resumo, por exemplo, "4969". Esse resumo é mais complexo do que parece.

Exemplo:

Marieta, ao receber o mesmo texto, também o processa pelo mesmo algoritmo hash. Se os hashes gerados forem idênticos, isso confirma que o texto não foi alterado. A garantia de integridade vem do fato de que o hash original foi criptografado com a chave privada de Zezinho, o que impede alterações não autorizadas.

10m

Marieta verifica que o documento foi enviado por Zezinho, confirmando sua autenticidade e integridade. A principal finalidade do algoritmo hash é assegurar que o documento não foi alterado.

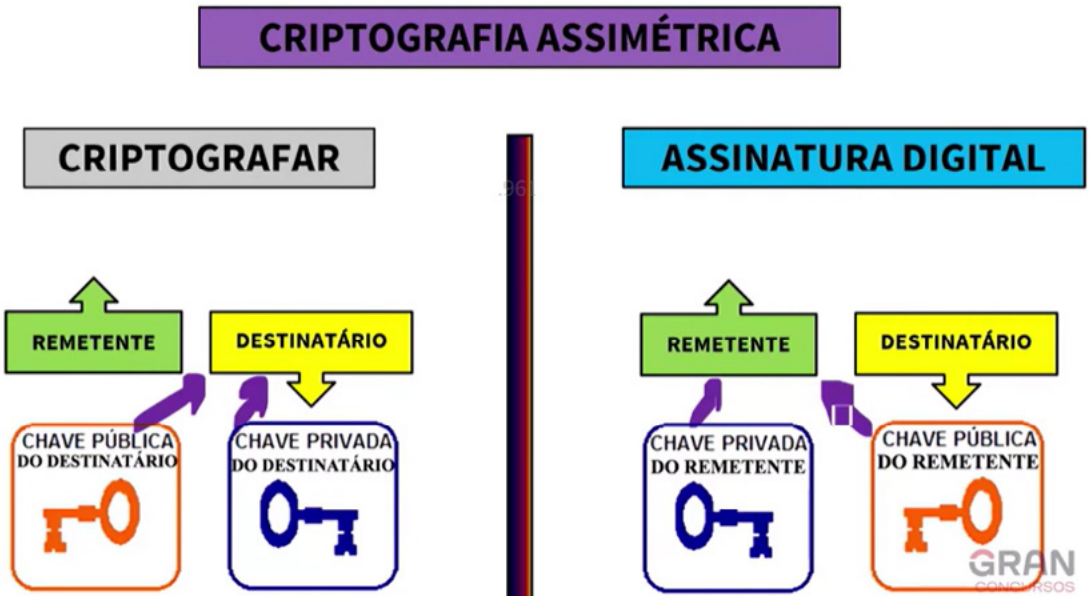
Em suma, ao assinar um documento digitalmente, garante-se sua integridade, não repúdio e autenticidade. A integridade assegura que o documento não foi modificado, o não repúdio impede que o autor negue a autoria, e a autenticidade confirma que o remetente é realmente quem diz ser.

Assinar digitalmente não garante a confidencialidade do documento, pois ele pode ser aberto com a chave pública do destinatário, que é amplamente disponível. No entanto, há um método chamado encapsulamento duplo para proteger a confidencialidade. Neste método, a mensagem é primeiro assinada digitalmente com a chave privada do remetente, e depois criptografada com a chave pública do destinatário. Isso garante que apenas o destinatário, usando sua chave privada, possa acessar o conteúdo.

Embora raro em provas, esse segundo encapsulamento assegura a confidencialidade do documento, similar ao depósito de dinheiro em uma conta bancária, onde apenas o titular da conta pode sacar os fundos.

Criptografia assimétrica

Segue um resumo para clarificação. A criptografia simétrica é usada em dois contextos distintos. Veja-os:



Primeiro, para criptografar a mensagem, garantindo sigilo e confidencialidade. Nesse caso, o remetente usa a chave pública do destinatário e o destinatário usa sua chave privada. Assim, ambas as chaves utilizadas pertencem ao destinatário.

Segundo, para assinatura digital, assegurando integridade, não repúdio e autenticidade da mensagem. Aqui, o remetente usa sua chave privada para assinar, e o destinatário usa a chave pública do remetente para verificar. Portanto, ambas as chaves usadas pertencem ao remetente.

15m

Principais algoritmos criptográficos

a. Simétricos

Os principais para a sua prova são:

- RC4, RC5, RC6;
- DES, 3DES;
- IDEA;
- AES;
- BLOWNFISH;
- TWOFISH;
- CAST.

b. Assimétricos

Os principais para a sua prova são:

- RSA;
- RABIN;
- ELGAMAL;
- DAS;
- 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;
> 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;
> II – assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória n. 2.200-2, de 24 de agosto de 2001.

20m

Esses tópicos não são muito frequentes, mas questões sobre essa lei estão começando a surgir. Portanto, é necessário incluir artigos da lei para que você esteja preparado para a prova. Embora o foco principal seja informática e segurança da informação, esses temas começam a se entrelaçar. Assim, artigos da lei serão citados em questões de informática, tornando-se inevitável.

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

DIRETO DO CONCURSO

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.

O AES (Advanced Encryption Standard) é um algoritmo de criptografia simétrica amplamente utilizado. Ele utiliza uma única chave secreta compartilhada entre o remetente e o destinatário para cifrar e decifrar os dados. Portanto, o AES se encaixa nas características mencionadas para um algoritmo de criptografia simétrica.

---

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.

De fato, um certificado digital A1 guarda a chave diretamente no dispositivo do usuário, enquanto no certificado digital A3, a chave é guardada em dispositivos físicos portáteis, como tokens e cartões.

---

10. (Q3134334/ANO: 2024/BANCA: CEBRASPE/PROVA: CAU-ASSISTENTE DE TECNOLOGIA DA INFORMAÇÃO) Para ser considerado íntegro, determinado conjunto de dados não pode ser alterado sem a devida autorização.

Quando uma pessoa devidamente autorizada realiza uma autorização, a integridade não é comprometida, pois a integridade é afetada apenas quando uma pessoa não autorizada faz modificações. Dessa forma, o item em questão está totalmente correto.

---

11. (Q3152572/ANO: 2024/BANCA: INSTITUTO VERBENA/PROVA: 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.

Os três tipos de assinatura atualmente utilizados são simples, avançada e qualificada.

---

12. (Q3135306/ANO: 2024/BANCA: CEBRASPE/PROVA: CAU-ANALISTA DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO) 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.

Na criptografia simétrica, o segredo é compartilhado entre as partes envolvidas. A confidencialidade depende da confiança entre essas partes, já que se uma delas compartilhar a chave com pessoas não autorizadas, a confidencialidade é comprometida. Portanto, o item está correto.

---

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.

A assinatura digital garante três pilares da segurança da informação: autenticidade, integridade e não repúdio.

25m

---

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.

II – 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.16
b. II, apenas.
c. I e III, apenas.
d. II e III, apenas.
e. I, II e III.

I – Eles são utilizados justamente para essa finalidade.

II – Quando se aplica segurança, seja na verificação da mensagem ou na segurança da informação em geral, quanto maior o nível de segurança, menor será a velocidade. Portanto, é inevitável que haja uma perda de desempenho. Por exemplo, gerar um hash e assinar o

hash é muito mais rápido do que criptografar a mensagem inteira. O processo criptográfico é demorado, especialmente se a segurança for reforçada com chaves mais robustas.
III – Lembre-se de que existem vários critérios para a sua revogação.

---

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 elà 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.

I – Esse é o princípio do certificado digital.
II – O que ele emite é a Lista de Certificados Revogados (LCR).
III – Se o documento foi assinado com a chave privada, apenas o proprietário tem conhecimento dela. Se não houver menção à exceção, é necessário considerar a regra. Apenas o proprietário conhece a chave privada.

---

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.

30m

O ponto crucial nesta questão é a confidencialidade da comunicação, que pode ser assegurada através da criptografia assimétrica.
Nesse caso, utilizando a chave pública para criptografar os dados, os quais somente podem ser descriptografados pela chave privada correspondente.

GABARITO

8. a
9. C
10. C
11. a
12. C
13. C
14. a
15. b
16. b