CST0210-Arte de garantir a integridade: Parte 2 - Assinaturas digitais

Data do Post	@August 26, 2022 9:00 AM
Status	Not started
Palavras-chave	Arte de garantir a integridade
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☐

Post- Linkedin

Como a transformação digital, hoje em dia já é possível, e cada vez mais comum vermos pessoas a assinar documentos digitalmente. Assinatura digital é uma técnica que utiliza diferentes recursos de criptografia para conferir maior segurança e integridade na emissão de documentos electrónicos.

Nesse artigo, apresento alguns aspectos técnicos sobre assinaturas digitais e como elas são usadas em todo mundo da computação. Leia o artigo na íntegra

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/

#cybersecurity #technology #linux #programming #hacking #digitalsignature #protection

Introdução

As assinaturas manuscritas e selos estampados comprovam a autoria do conteúdo de um documento. As assinaturas digitais fornecem a mesma funcionalidade que as assinaturas manuscritas.

Documentos digitais desprotegidos são muito fáceis de mudar por qualquer pessoa. Uma assinatura digital pode determinar se alguém edita um documento após ter sido assinado pelo utilizador. Uma assinatura digital é um método matemático usado para verificar a autenticidade e integridade de uma mensagem, documento digital ou software.

Assinaturas e a Lei

As assinaturas digitais têm propriedades específicas que permitem a autenticação da entidade e a integridade dos dados, conforme se mostra na figura.

- As assinaturas digitais são uma alternativa ao HMAC.
- **Autêntica**: Não é falsificável e fornece a prova de que signatário, e nenhum outro, foi quem assinou o documento;
- **Inalterável**: após um documento estar associado, não pode ser alterado;
- **Não-reutilizável**: A assinatura faz parte do documento e não pode ser movida para um documento diferente;
- **Não pode ser repudiada**: São consideradas coisas físicas. O signatário não pode afirmar que não assinaram.

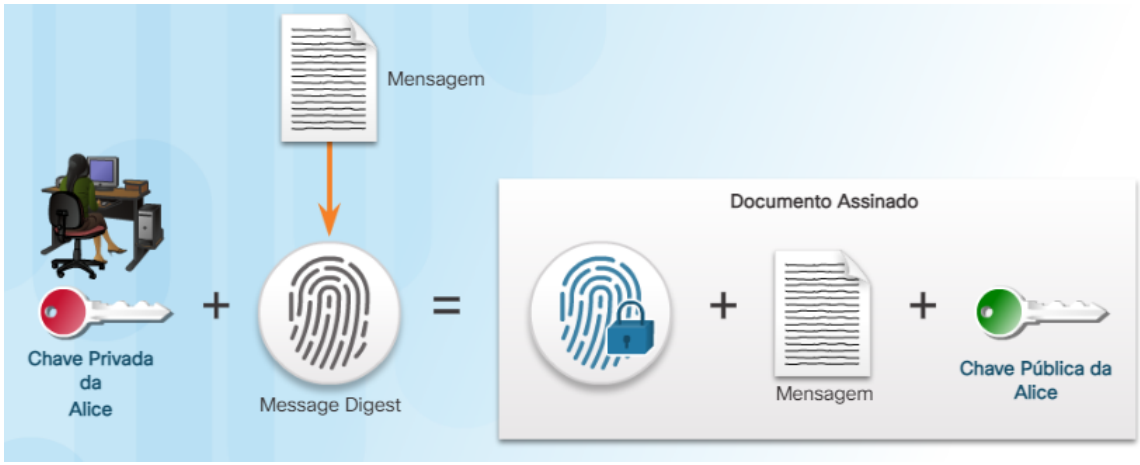
Visto que uma assinatura digital é única para o indivíduo que a cria, esse indivíduo não pode negar mais tarde que forneceu a assinatura.

Como funciona tecnologia de assinatura digital.

A criptografia assimétrica é a base para as assinaturas digitais. Um algoritmo de chave pública como o RSA gera duas chaves: uma privada e outra pública. As chaves estão matematicamente relacionadas.

A Alice quer enviar ao Bob um e-mail que contém informações importantes para a implantação de um novo produto. A Alice quer ter certeza de que Bob sabe que a mensagem veio dela, e que a mensagem não foi modificada desde que foi enviada.

A Alice cria a mensagem com um resumo da mensagem. A seguir, ela cifra o resumo com sua chave privada, como se mostra na Figura 1. A Alice empacota a mensagem, o resumo cifrado da mensagem, e a sua chave pública, para criar o documento assinado. Alice envia este conjunto de informação para Bob como ilustrado na Figura 2.



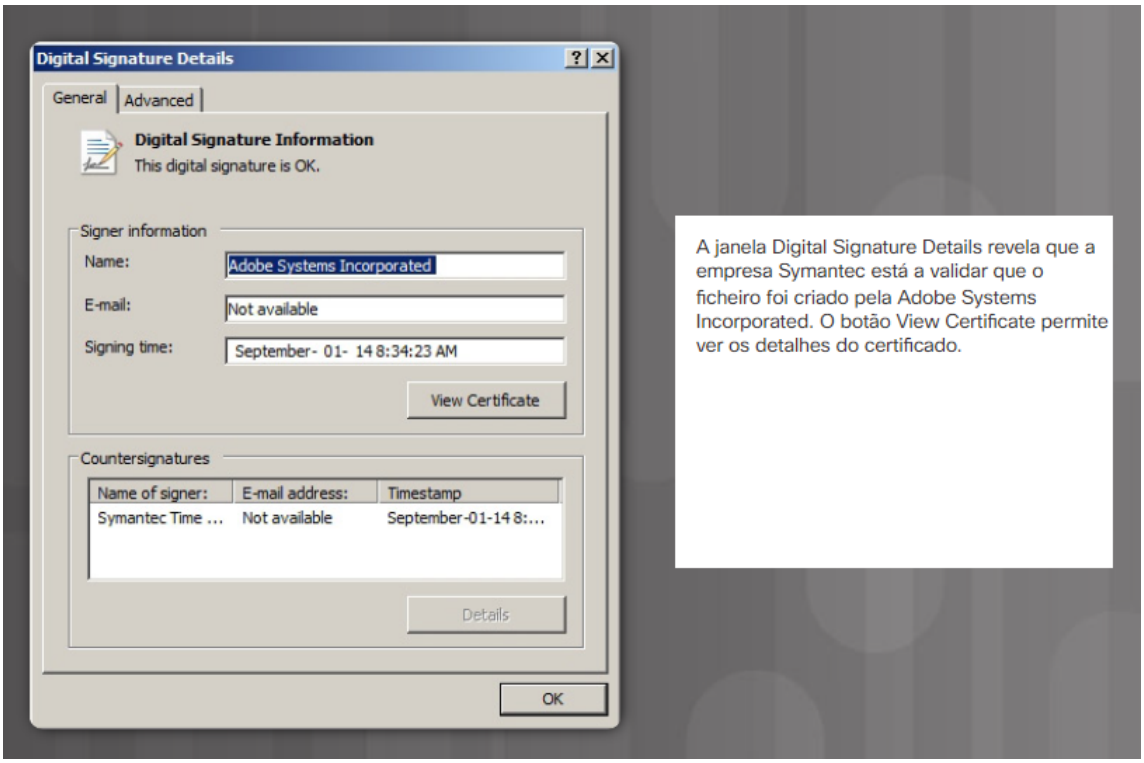
O Bob recebe a mensagem e lê-a. Para se certificar de que a mensagem veio de Alice, o Bob cria um resumo da mensagem. Pega no resumo cifrado da mensagem da Alice recebida e decifra-o usando a chave pública da Alice. O Bob compara o resumo da mensagem da Alice recebido com o que gerou. Se ambos corresponderem, o Bob fica a saber que ninguém alterou a mensagem original da Alice, como ilustrado na Figura 3.

Uso de assinaturas digitais

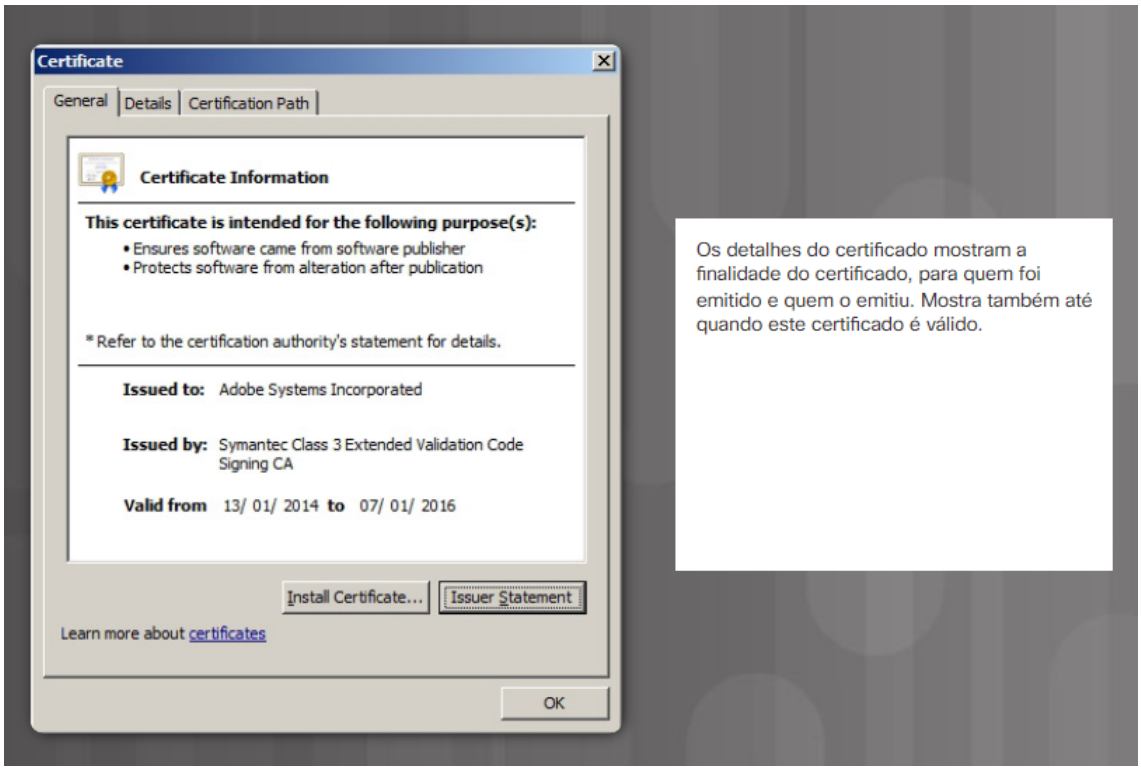
Assinar um hash em vez de todo o documento fornece eficiência, compatibilidade e integridade. As organizações podem querer substituir documentos em papel e assinaturas de tinta por uma solução que garanta que o documento electrónico cumpra com todos os requisitos legais.

As duas situações seguintes fornecem exemplos de uso de assinaturas digitais:

- Assinatura de código - Usado para verificar a integridade dos ficheiros executáveis transferidos de um website de um fabricante. A assinatura de código também usa certificados digitais assinados para autenticar e verificar a identidade do site (Figura 1).



- Certificados Digitais - Usados para verificar a identidade de uma organização ou indivíduo para autenticar um site de fornecedor e estabelecer uma ligação cifrada para trocar dados confidenciais (Figura 2)



Comparação de algoritmos de assinatura digital

Os três algoritmos comuns de assinatura digital são: Digital Signature Algorithm (DSA), Rivest-ShamirAdleman (RSA), e Elliptic Curve Digital Signature Algorithm (ECDSA). Todos os três geram e verificam assinaturas digitais. Estes algoritmos dependem da criptografia assimétrica e de técnicas de chave pública. As assinaturas digitais exigem duas operações:

1. Geração de chaves
2. Verificação de chave

Ambas as operações precisam de chaves de cifra e de decifra. O DSA usa factorização de grandes números. Os governos usam o DSA para assinar para criar assinaturas digitais. O DSA não se estende para lá da assinatura da própria mensagem.

O RSA é, actualmente, o algoritmo de criptografia de chave pública mais comum. O RSA foi criado em 1977 e recebeu o nome dos seus criadores: Ron Rivest, Adi Shamir e Leonard Adleman. O RSA depende da criptografia assimétrica. O RSA abrange a assinatura da mensagem e a cifra do seu conteúdo.

O DSA é mais rápida do que o RSA como serviço de assinatura para um documento digital. O RSA é mais adequado para as aplicações que exijam a assinatura e verificação de documentos electrónicos, e a cifragem de mensagens.

Como na maioria das áreas de criptografia, o algoritmo RSA é baseado em dois princípios matemáticos: o módulo e a factorização de números primos. Clique aqui para saber mais sobre como o RSA utiliza o módulo e a factorização de números primos.

O ECDSA é o mais recente algoritmo de assinatura digital e substitui gradualmente o RSA. A vantagem deste novo algoritmo é que ele pode usar tamanhos de chave muito menores para a mesma segurança e requer menos esforço de computação que o RSA.

Conclusão

Em muitos países, as assinaturas digitais têm o mesmo valor legal de um documento assinado manualmente. As assinaturas electrónicas são vinculativas para contratos, negociações ou qualquer outro documento que exija uma assinatura manuscrita. Uma trilha de auditoria permite o rastreio do histórico do documento electrónico para fins regulamentares e de defesa legal. Uma assinatura digital ajuda a estabelecer autenticidade, integridade e não-repúdio.

Repudiar significa negar. Não-repúdio é uma maneira de garantir que o remetente de uma mensagem ou documento não possa negar ter enviado a mensagem ou documento e que o destinatário não pode negar ter recebido a mensagem ou documento. Uma assinatura digital garante que o remetente assinou electronicamente a mensagem ou documento.

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.

Guarde para rever noutro momento.

Compartilha o conteúdo com os amigos e não só

Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/

#cybersecurity #technology #linux #programming #hacking #digitalsignature #protection