SEGURANÇA DA INFORMAÇÃO

Certificados e Assinaturas Digitais

ROTEIRO

- Revisão dos objetivos da criptografia
- Assinatura digital
- Infraestruturas de chaves públicas
- Certificados digitais

Revisão – Objetivos da criptografia

	Privacidade	**Integridade da Mensagem/ Autenticação**
Chaves Simétricas	Criprografia Simétrica	Código de Autenticação de Mensagens (MAC)
Chaves Assimétricas	Criptografia Assimétrica (Chaves Públicas) encryption)	Assinatura Digital

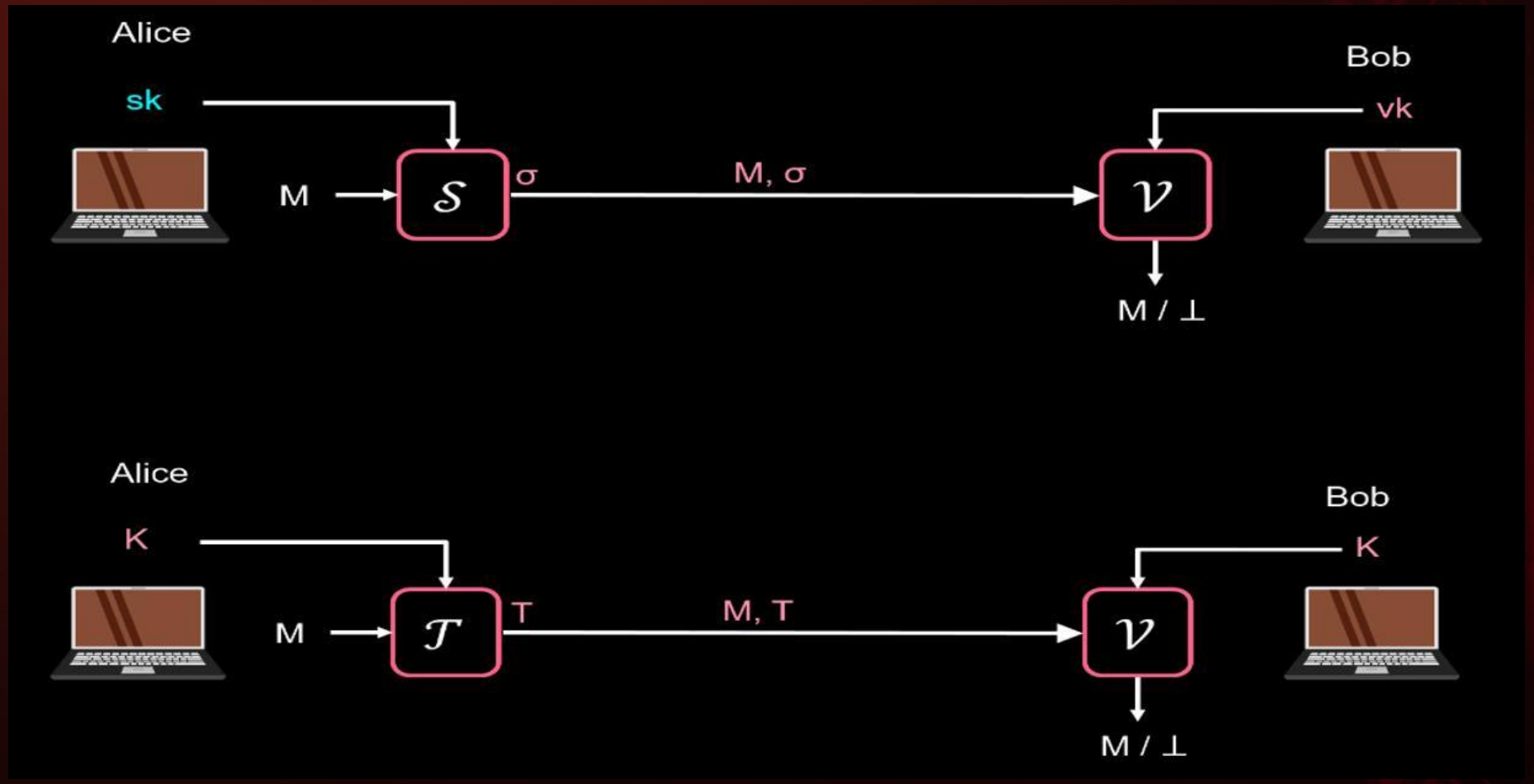
Troca de chaves

Revisão – Objetivos da criptografia

INTEGRIDADE DOS DADOS:
um interceptador não pode ser capaz de modificar a mensagem enviada

AUTENTICIDADE DOS DADOS:
mensagem foi realmente originada pelo remetente

ASSINATURA DIGITAL x MAC



Fonte: 5

ASSINATURA DIGITAL x MAC

A assinatura digital pode ser verificada por qualquer um

O MAC somente pode ser verificado pelas partes que compartilham a mesma chave

APLICAÇÕES DA ASSINATURA DIGITAL

Assinar eletronicamente documentos

Certificados SSL/TLS

Instalação de software e desenvolvimento de códigos

Autenticar o emissor do e-mail

Bitcoin

INFRAESTRUTURA DE CHAVES PÚBLICAS

- Há muitos usuários conhecidos com o mesmo nome
  - Por exemplo, temos muitos usuários que se chamam Alice e também que se chamam Bob
  - Como sabemos que uma chave pertence a essa Alice em particular e a esse Bob em particular?

- *Precisamos vincular chaves públicas a essas entidades*

- *Na Internet: vincular chaves públicas a nomes de domínio*

INFRAESTRUTURA DE CHAVES PÚBLICAS

- Como vincular chaves públicas de maneira confiável na Internet?
  - Já que o interceptador/atacante poderia ter criado as chaves

- Solução
  - Certificados digitais

INFRAESTRUTURA DE CHAVES PÚBLICAS

CERTIFICADOS DIGITAIS

Uma forma de vincular uma chave pública a uma entidade

Um certificado consiste em:

Um monte de informações que identificam a entidade

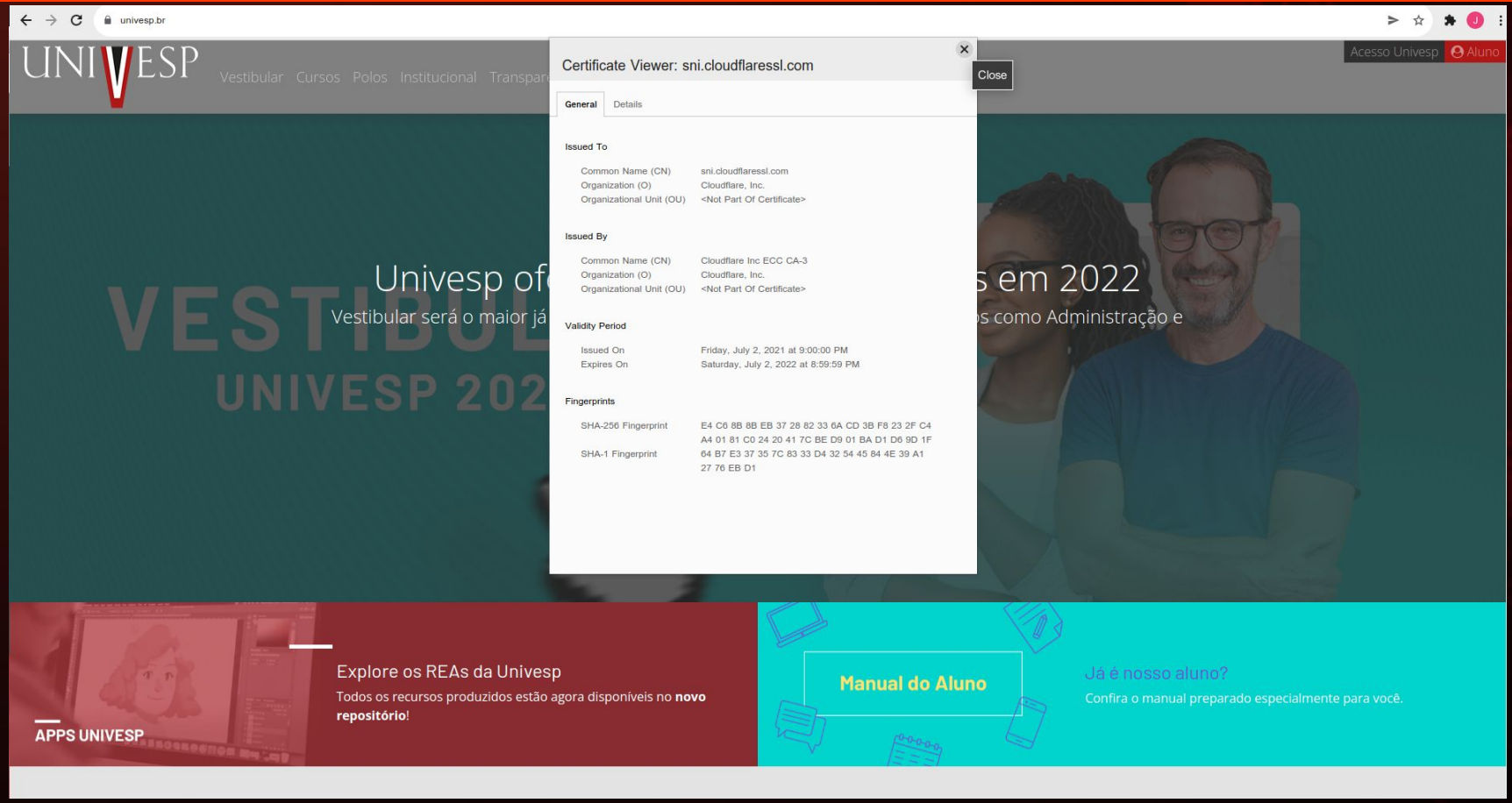
- Nome
- Endereço
- Ocupação
- URL
- Endereço de e-mail
- Número de telefone

A uma chave pública da entidade

Uma assinatura digital em todos os itens acima por uma autoridade de certificação (CA)

INFRAESTRUTURA DE CHAVES PÚBLICAS

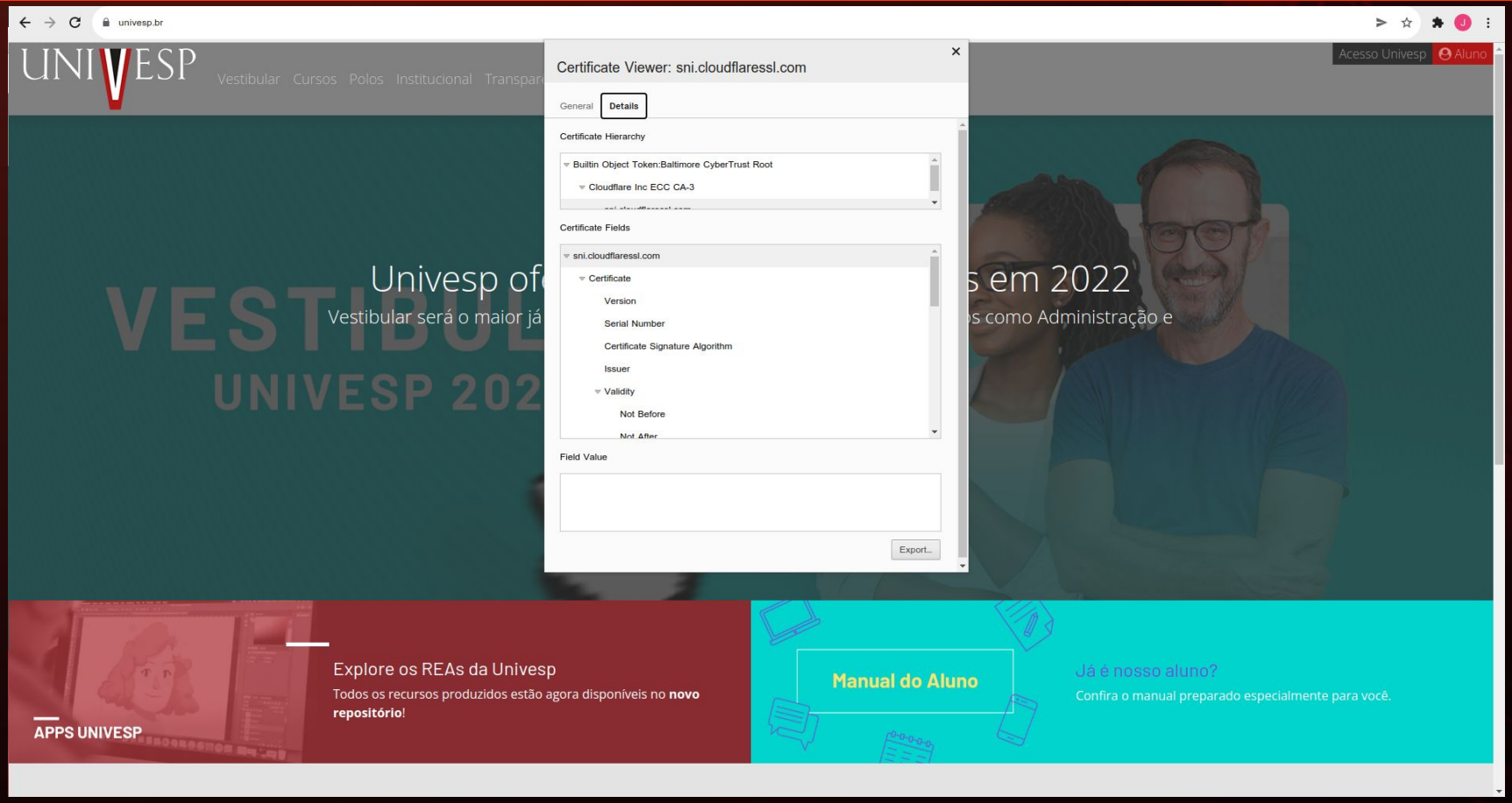
CERTIFICADOS DIGITAIS



Fonte: 6

INFRAESTRUTURA DE CHAVES PÚBLICAS

CERTIFICADOS DIGITAIS



Fonte: 6

INFRAESTRUTURA DE CHAVES PÚBLICAS

AUTORIDADE CERTIFICADORA

CA: um emissor de certificados digitais

- Atua como um terceiro confiável, certificando (ou seja, assinando) as chaves públicas de outras entidades
- Verifica a identidade de um proprietário de chave pública reivindicado
- *É a base de uma infraestrutura de chave pública (PKI)*

INFRAESTRUTURA DE CHAVES PÚBLICAS

AUTORIDADE CERTIFICADORA RAIZ *(ROOT CAS)*

CAs raiz: CAs que assinam as chaves públicas de outras Cas

- Apenas algumas CAs raiz precisam ser confiáveis pelos usuários finais
- CAs raiz podem distribuir a assinatura + carga de verificação para CAs menores

CAs raiz para a Internet: algumas grandes corporações multinacionais

INFRAESTRUTURA DE CHAVES PÚBLICAS

A ICP - BRASIL

Fiscaliza e audita o processo de emissão de certificados digitais das autoridades certificadoras a fim de garantir a confiabilidade no processo de certificação

Presunção legal de: integridade, autenticidade e não-repúdio do que é assinado digitalmente

https://www.gov.br/iti/pt-br/assuntos/icp-brasil

INFRAESTRUTURA DE CHAVES PÚBLICAS

TIPOS DE CERTIFICADOS DIGITAIS

Tipo A - certificado de assinatura digital (A1, A3, A4)

É o mais utilizado e pode ser aplicado para conferir autenticidade a qualquer tipo de documento e arquivo virtual.

Seu principal objetivo é identificar o assinante, confirmar a integridade do documento e atestar a autenticidade da operação realizada.

INFRAESTRUTURA DE CHAVES PÚBLICAS

TIPOS DE CERTIFICADOS DIGITAIS

Tipo S - certificado de sigilo/confidencialidade (S1, S3, S4)

Busca trazer sigilo para uma determinada transação, já que, por meio de sua utilização, é possível criptografar os dados de um documento, que, a partir desse momento, somente poderá ser acessado através de um certificado autorizado, evitando o vazamento de informações.

INFRAESTRUTURA DE CHAVES PÚBLICAS

TIPOS DE CERTIFICADOS DIGITAIS

TIPO T - certificado de tempo (T3)

Conhecido como carimbo de tempo, uma vez que seu objetivo é atestar quando um documento digital foi emitido, tornando evidente a data e a hora que determinada informação digital passou a existir

Utiliza uma terceira parte certificadora para atestar o exato instante em que o documento foi emitido, evitando fraudes

Pode ser utilizado em conjunto com os demais certificados para garantir ainda mais segurança às transações.

INFRAESTRUTURA DE CHAVES PÚBLICAS

OUTROS TIPOS DE CERTIFICADOS DIGITAIS

e-CPF:

O CPF, principal documento de identificação de pessoa física, também tem uma versão digital para garantir a autenticidade das transações eletrônicas realizadas por pessoas físicas

e-CNPJ:

A versão digital da principal identificação de pessoa jurídica no Brasil garante a autenticidade e a integridade de transações de empresas no meio eletrônico

NF-e:

arquivo que garante a autoria e a validade jurídica das emissões de notas fiscais pela empresa aos órgãos responsáveis.

REFERÊNCIAS

1. https://www.gov.br/iti/pt-br/assuntos/icp-brasil
2. https://www.senior.com.br/blog/conheca-os-tipos-de-certificados-digitais-e-suas-vantagens
3. https://dllautomacao.com.br/2018/11/23/tipos-de-certificados-digitais/
4. https://univesp.br/
5. https://www.uio.no/studier/emner/matnat/its/TEK4500/h20/lectures/
6. https://www.geeksforgeeks.org/digital-signatures-certificates/