Blockchain, Criptomoedas & Tecnologias Descentralizadas

Certificação Digital:

Identidades & Carimbo de tempo

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

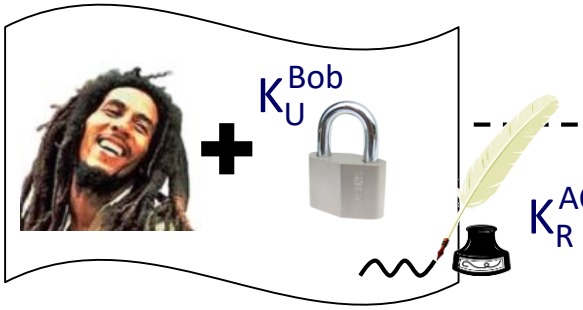
Objetivos

- Visão geral sobre Certificação digital
  - Certificados de Identidades
  - Certificados de Carimbo de tempo

Distribuição de chaves públicas

Certificados Digitais

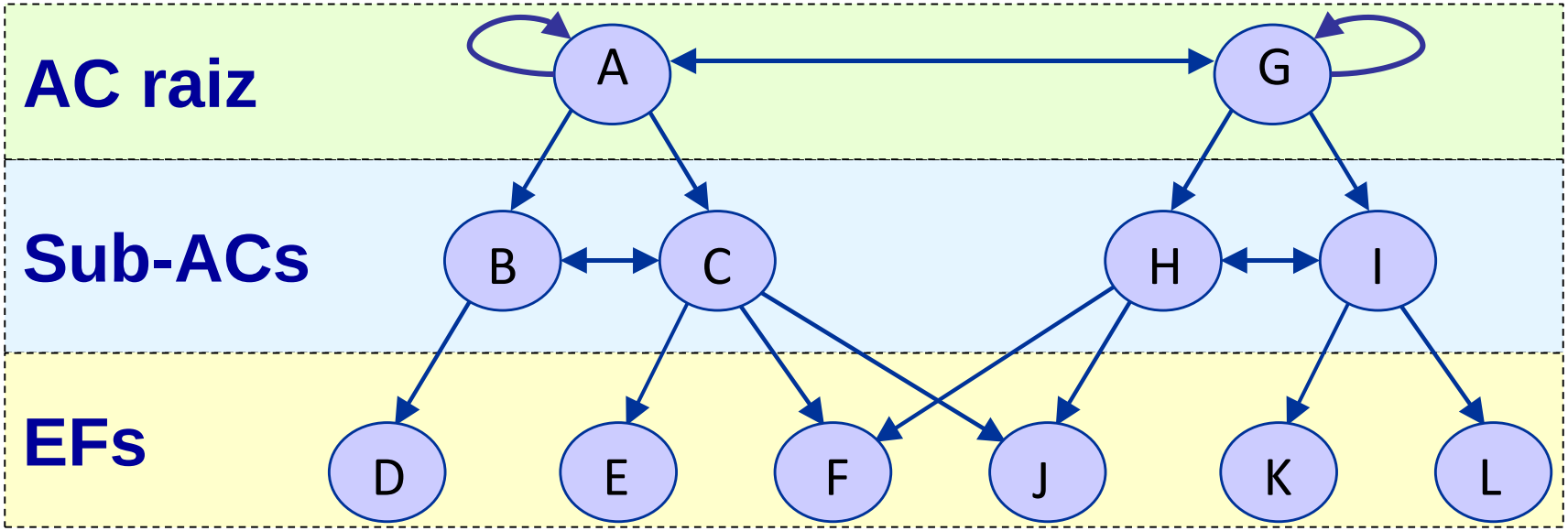
- Associam uma chave pública ao seu dono.
  - Atestado dizendo qual é a chave pública de Bob
- Modelo PKI: certificado contém **chave pública** de Bob assinada por uma Autoridade Certificadora (AC)
  - **Premissa**: chave pública da AC é amplamente conhecida.
  - Na prática, **certificados das ACs são pré-instalados** em sistemas computacionais, como navegadores Web.
    - Também podem ser instalados por usuário



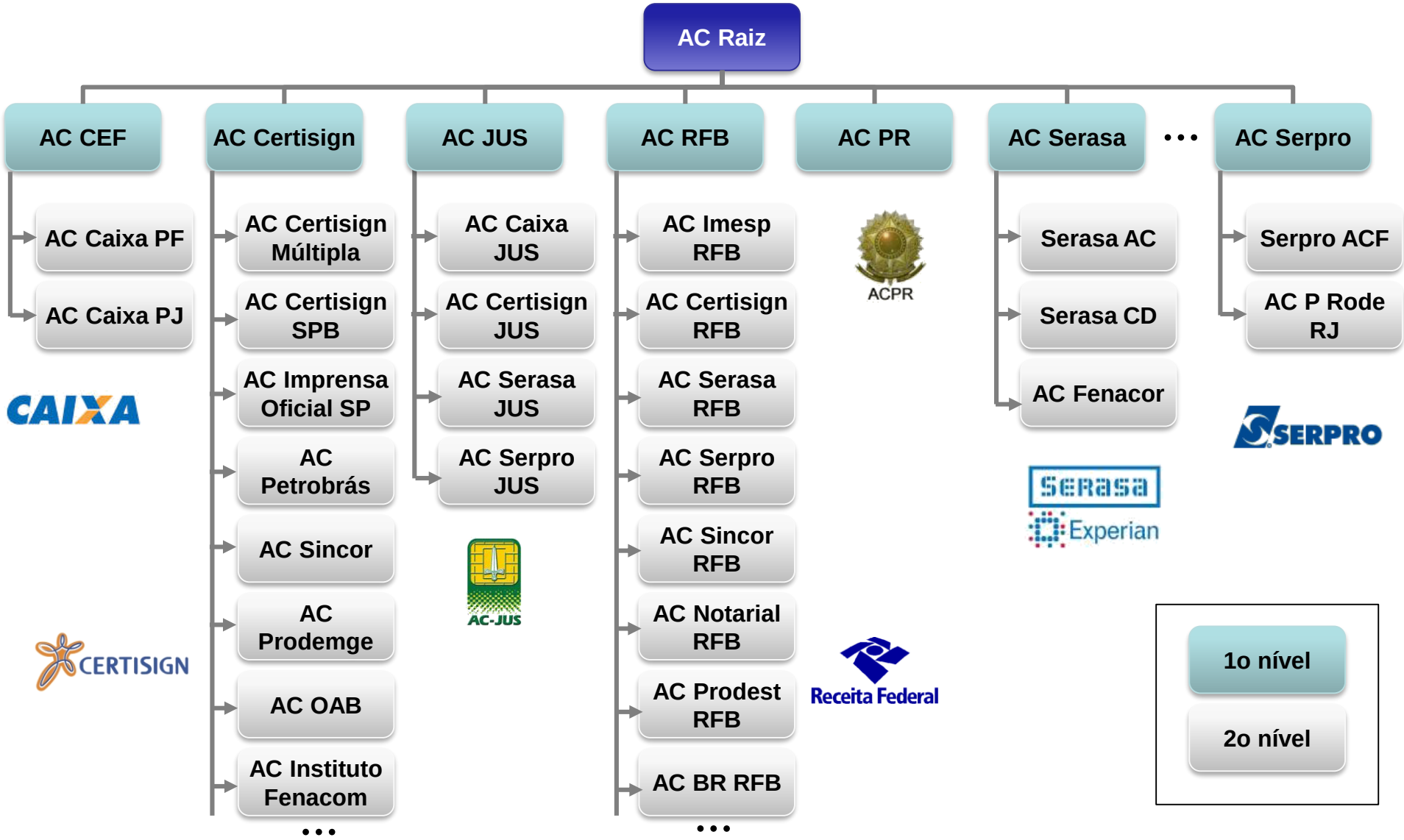
Alice usa K_U^{AC} para verificar a atenticidade do certificado

Certificados Digitais: ICP

- Modelo ICP (Infraestrutura de Chaves Públicas), ou PKI (*Public Key Infrastructure*): **cadeias de certificação**
  - Usa chave no certificado da **AC raiz** (auto-assinado) para assinar outras chaves na cadeia, até entidades finais (EFs)
  - **Proteção** das chaves mais críticas (mais próximas da raiz)
  - ACs dedicadas a **vários fins**



Exemplo: ICP-Brasil



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

Certificados ICP-Brasil: tipos

- Tipos principais:

  - **A: assinatura digital**
    - Assinatura de documentos; confirmação de identidade (SSL).
    - Key usage: *digitalSignature*, *keyEncipherment*, *nonRepudiation*

  - **S: sigilo**
    - Cifração de documentos, bancos de dados, mensagens.
    - Key usage: *keyEncipherment* e *dataEncipherment*

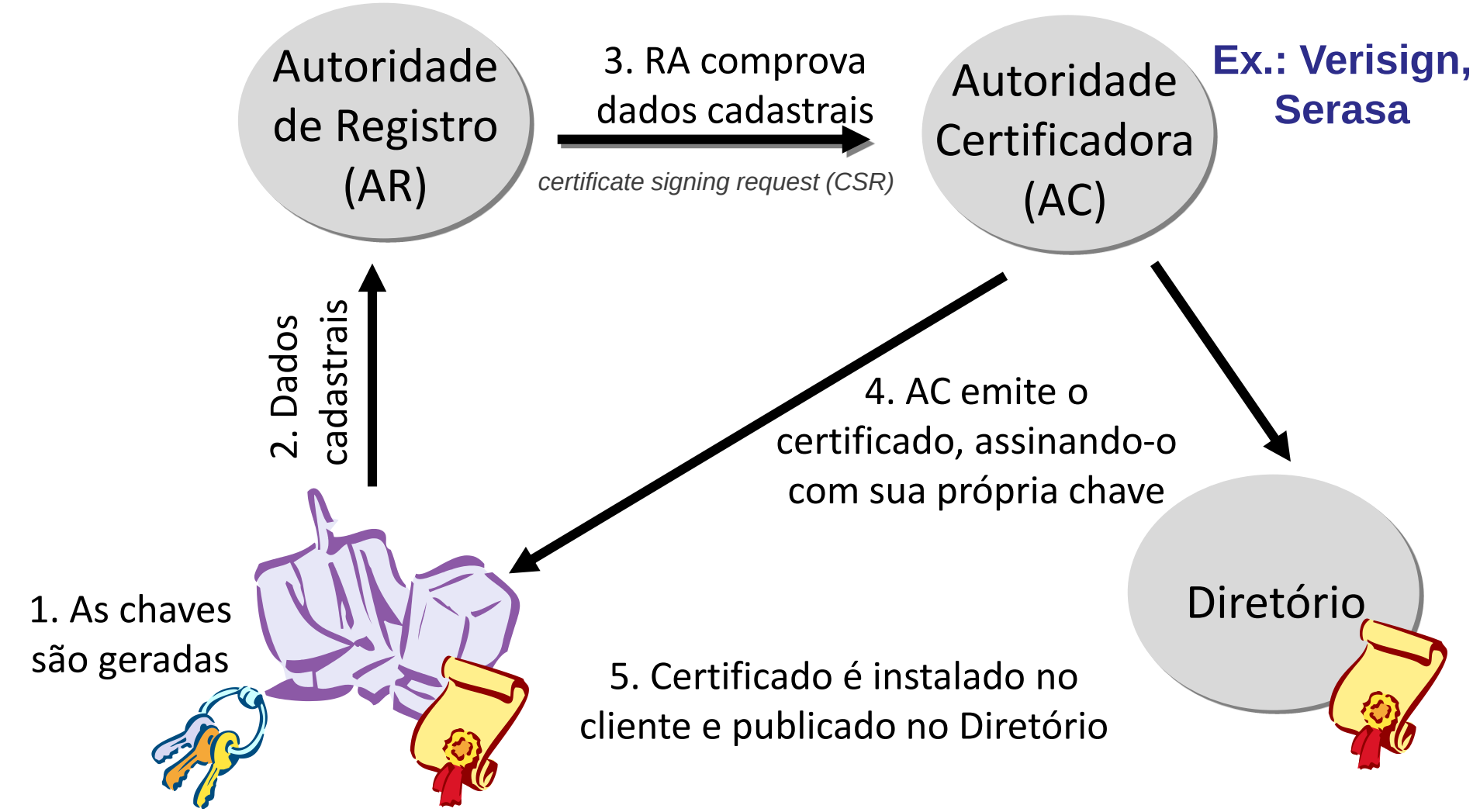
  - **T: Carimbo de tempo**
    - Garante temporalidade da informação assinada
    - Usado por Autoridade de Carimbo de Tempo (ACT)
    - (Ext.) key usage: *digitalSignature*, *nonRepudiation*, *timeStamping*
  - **Outros (uso específico)**
    - A CF-e-SAT: assinatura de Cupom Fiscal Eletrônico
    - OM-BR: equipamentos de medição

Certificados ICP-Brasil: tipos

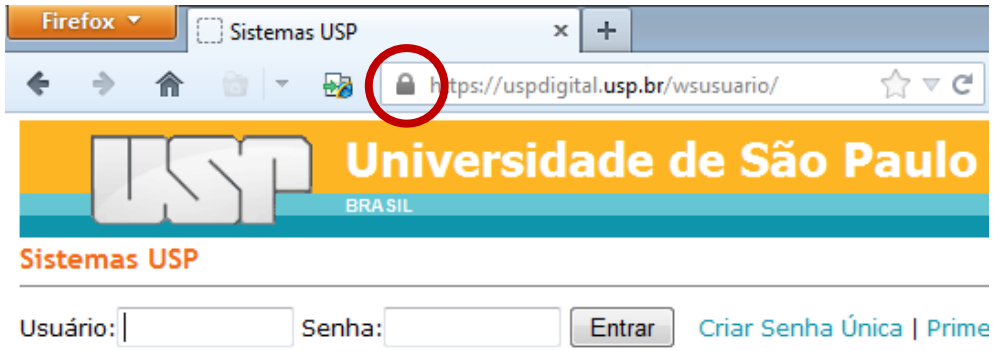
- Níveis: define requisitos mínimos
  - **A1/S1**: geração por software; armazenamento em **dispositivos tradicionais** (e.g., disco/pendrive) e protegido por senha/biometria. Validade: até 1 ano
  - **A2/S2**: geração por software e armazenamento em **smart card ou token sem capacidade de geração** de chave e protegido por senha/biometria. Validade: até 2 anos
  - **A3/S3/T3**: geração e armazenamento em **hardware criptográfico** (smart card ou token USB com capacidade de geração de chaves). Validade: até 5 anos
  - **A4/S4/T4**: geração e armazenamento em **hardware criptográfico** (smart card ou token USB com capacidade de geração de chaves). Validade: até 6 anos (11 se algoritmo de curvas elípticas). **Chaves maiores**: maior nível de segurança

Fonte: https://www.iti.gov.br/legislacao/documentos-principais (DOC-ICP-04 – V.7.1)

Processo de certificação



Usando certificados (web)



Autoridade Certificadora

[3.1. Consulta OCSP: revogação]

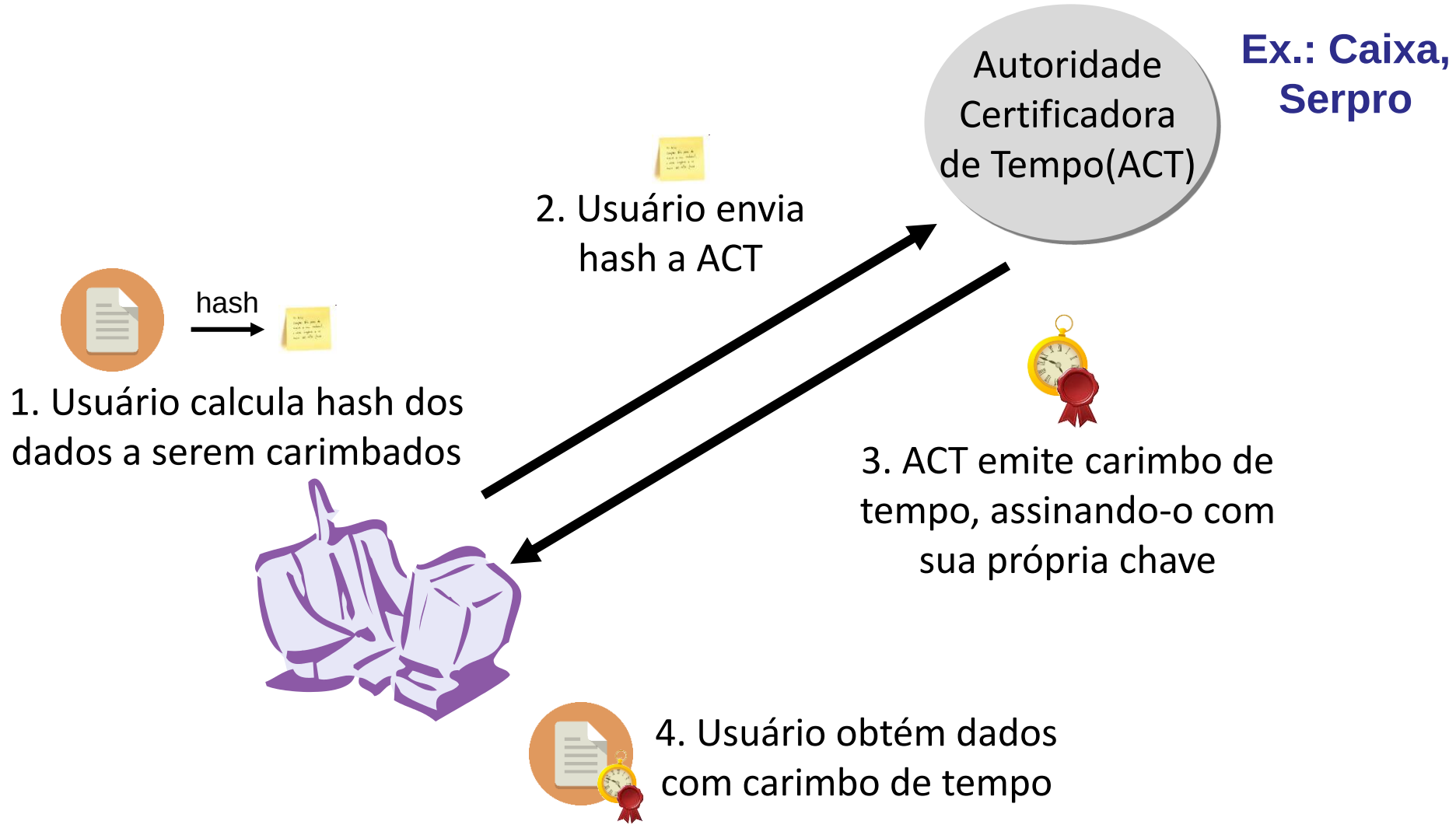
3. Verifica validade do certificado (chave pública da AC)

1. Requisita Certificado

2. Fornece certificado assinado por AC

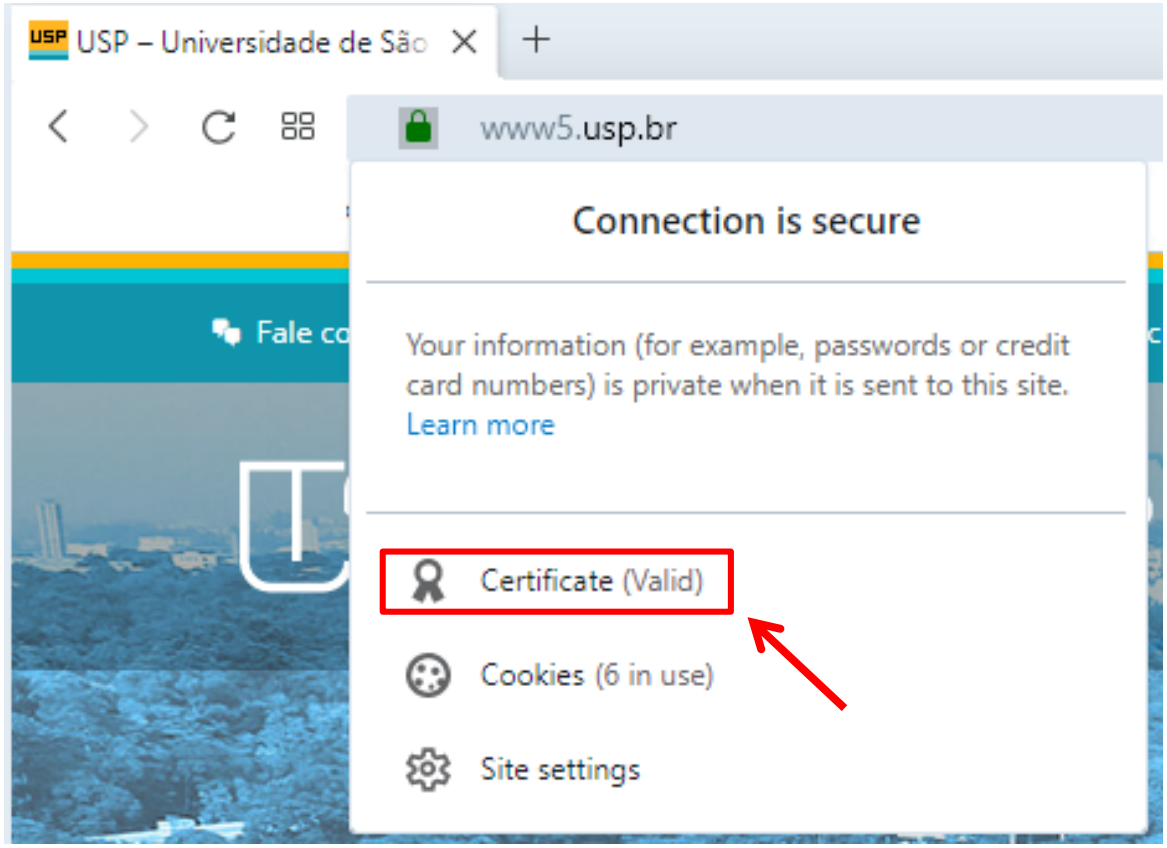
4. Usa chave pública: “fecha cadeado” no navegador

Processo de Carimbo de Tempo



https://www.gov.br/iti/pt-br/assuntos/icp-brasil/autoridades-de-carimbo-do-tempo

Exemplo: Certificado USP (X.509)



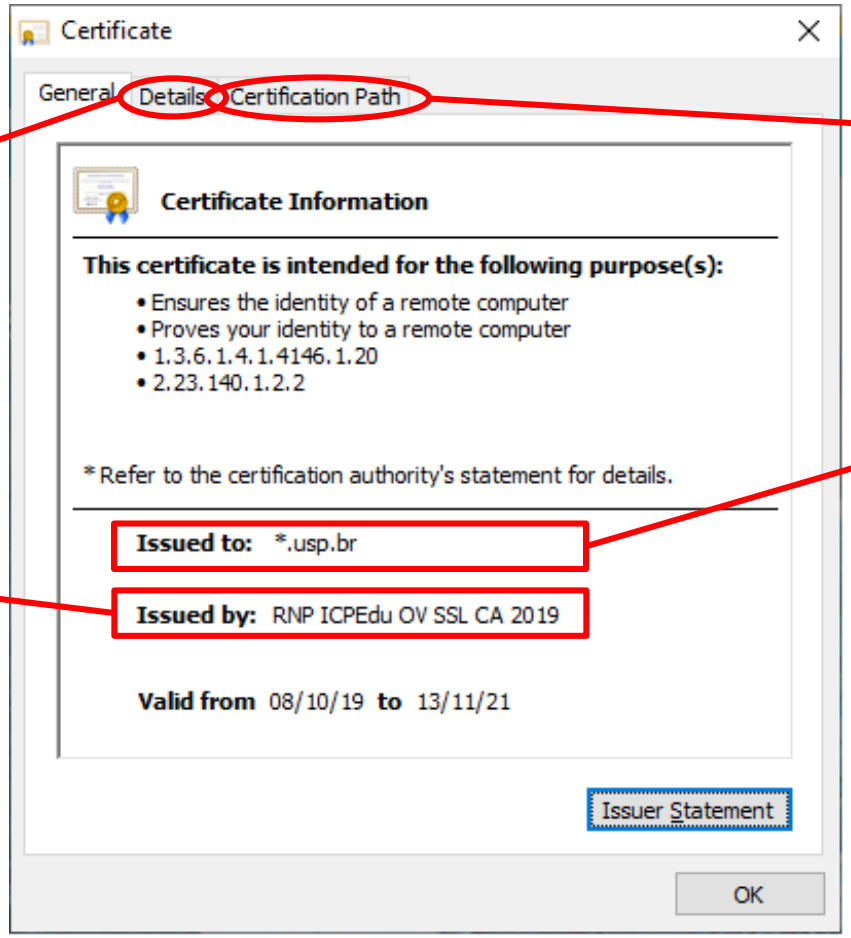
Exemplo: Certificado USP (X.509)

Para detalhes adicionais

Para ver cadeia de certificados

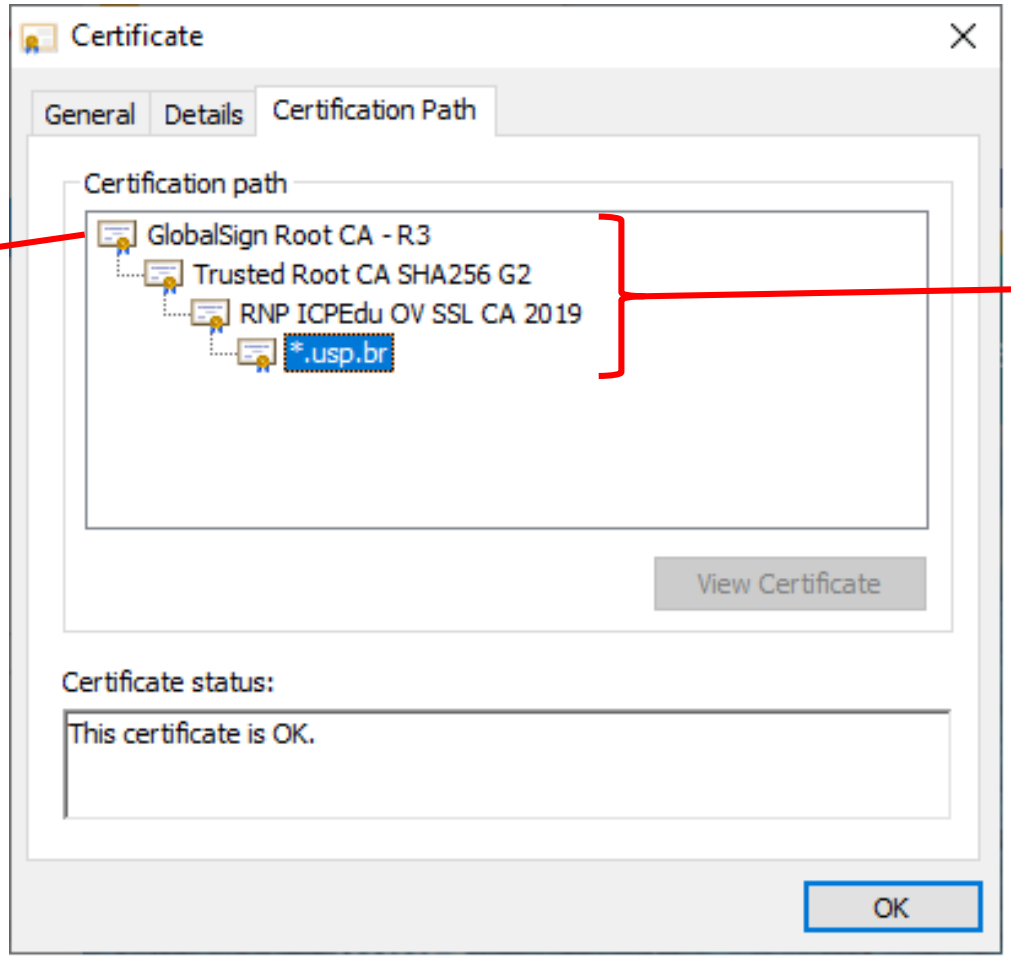
Domínio ao qual corresponde o certificado

AC



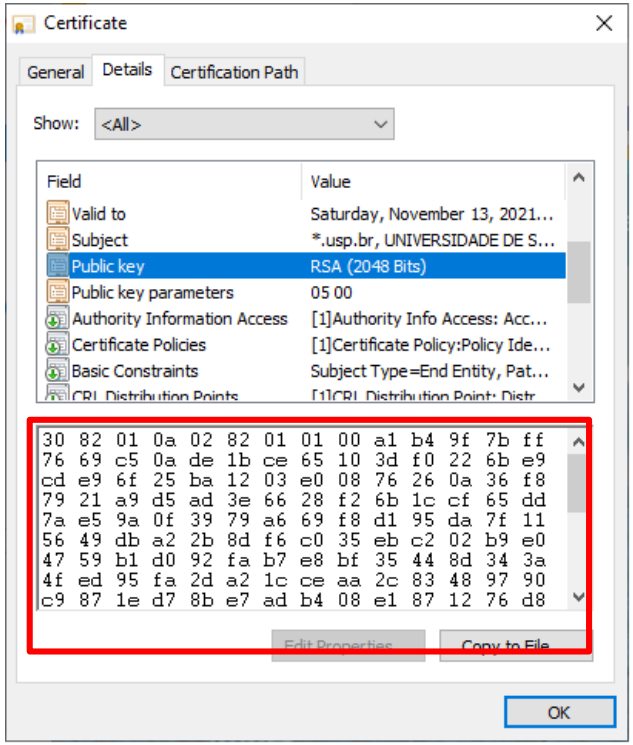
Exemplo: Certificado USP (X.509)

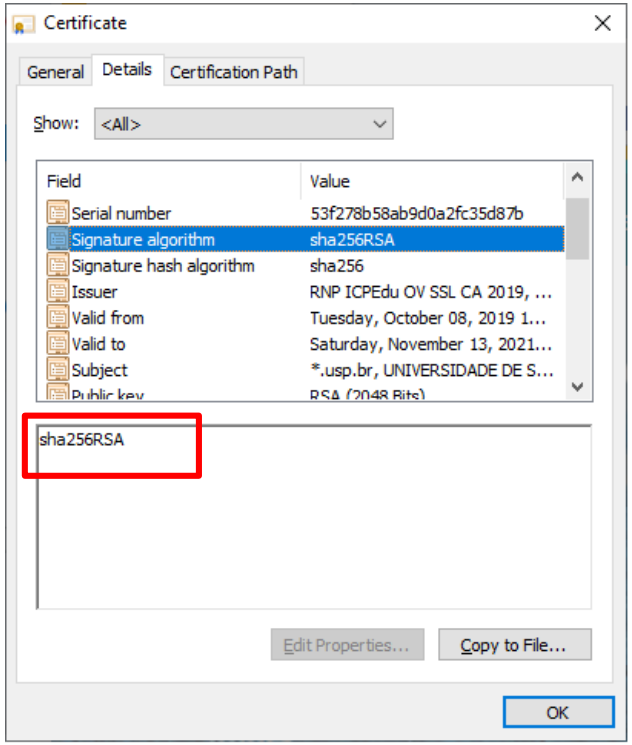
AC raiz

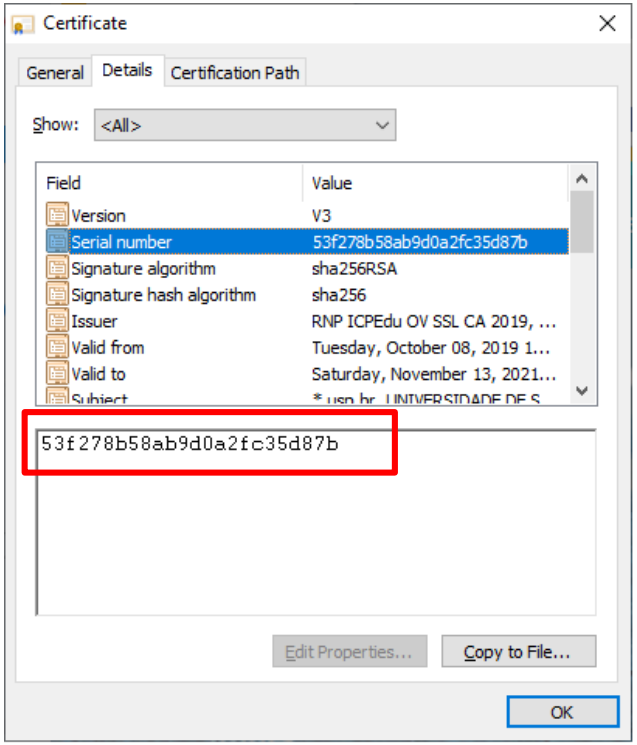


Cadeia de certificados

Exemplo: Certificado USP (X.509)







Chave pública (RSA 2048 bits)

Algoritmo de assinatura: RSA+SHA-256

Número serial (útil para revogação)

Distribuição de chaves públicas

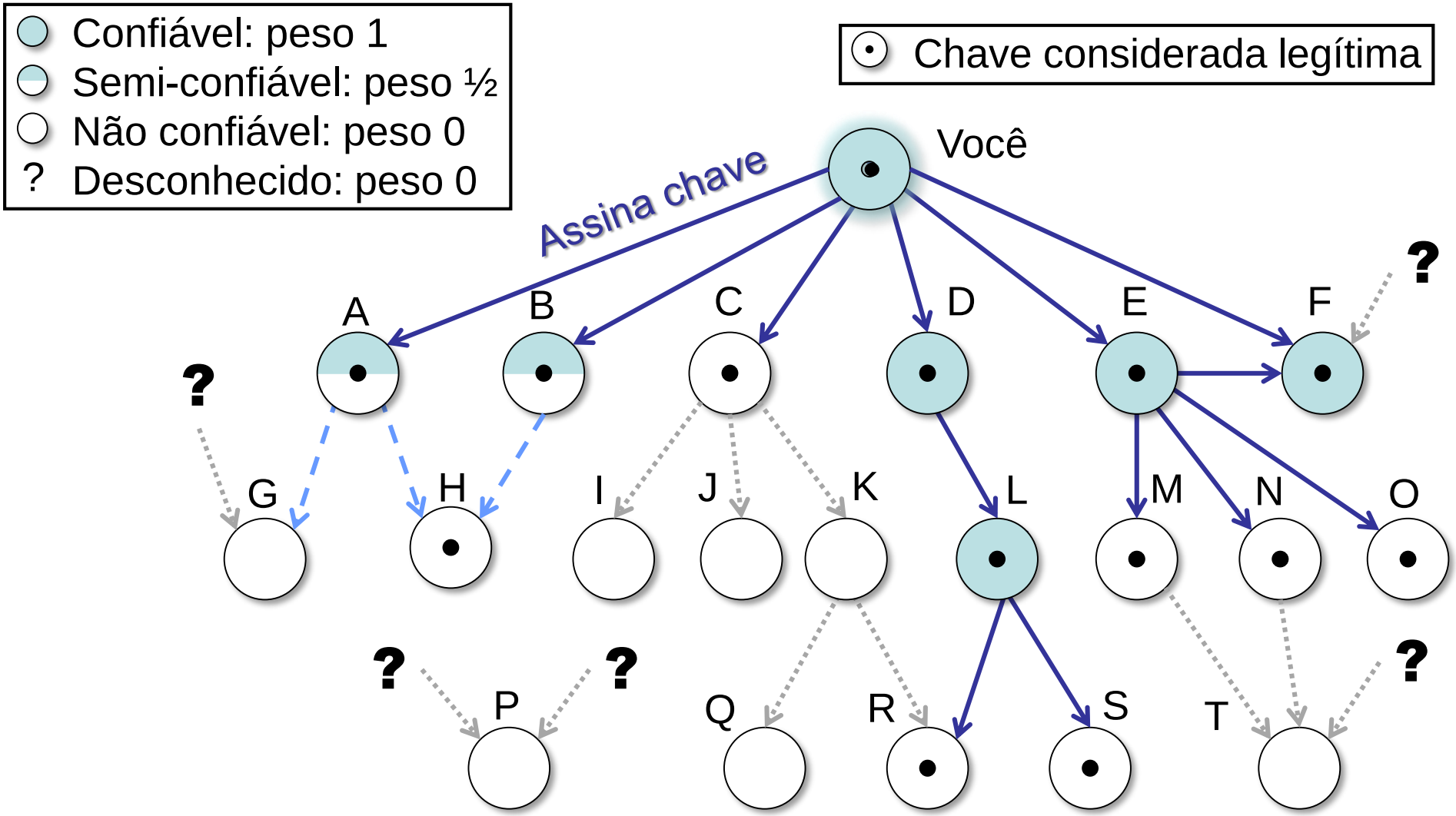
- Distribuição de certificados
  - Por e-mail (S/MIME), páginas web, etc.
  - Durante o estabelecimento de conexão das aplicações (ex.: HTTPS)
- Confiança nas chaves públicas

  - Certificados com chaves públicas assinadas por **entidade de confiança**
  - Confiança de que os certificados não foram alterados no caminho até o receptor (ex.: **certificados auto-assinados**)
  - "**Web of trust**": se A confia em B e B confia em C, então A pode confiar em C (ex.: PGP)

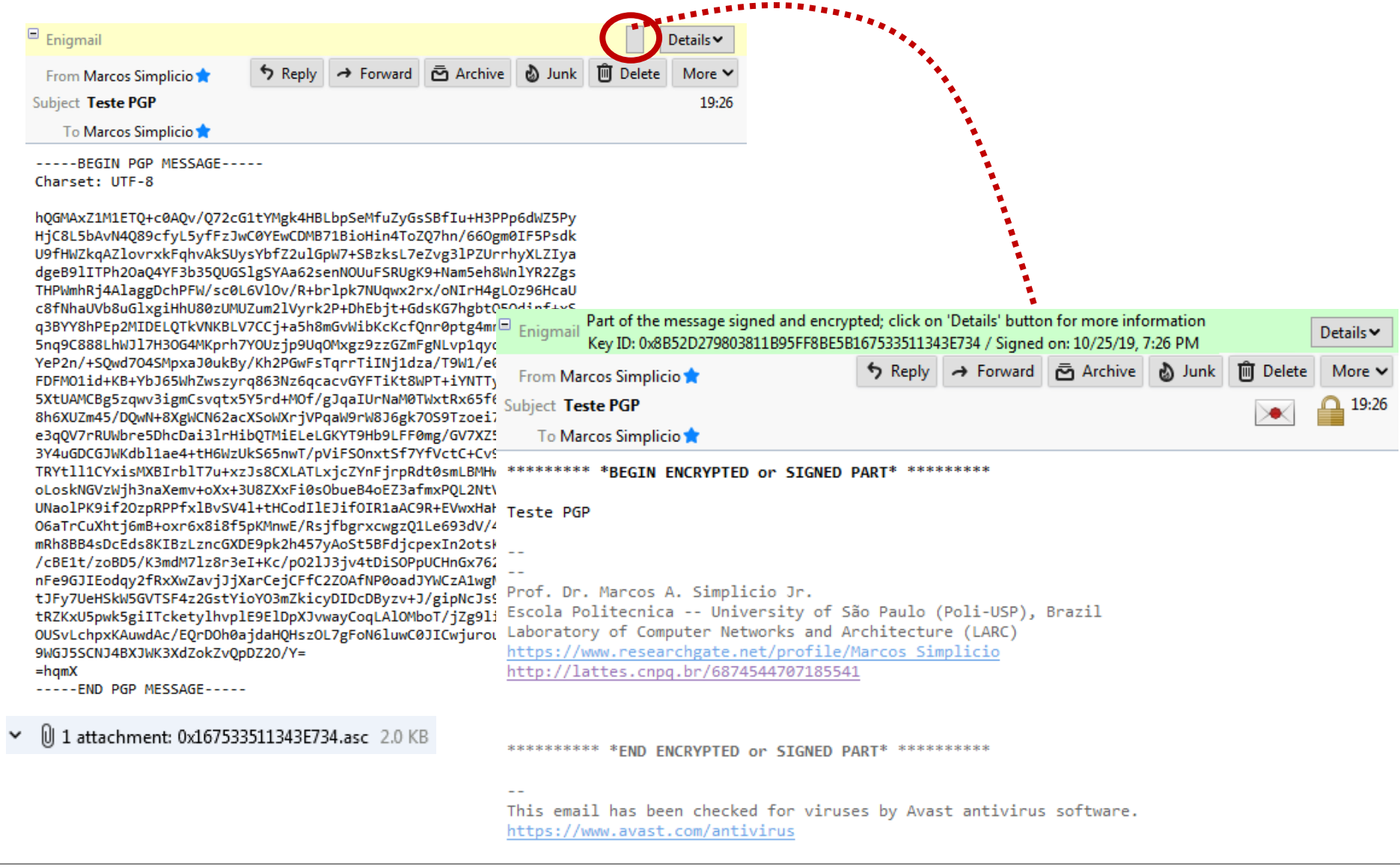
Pretty Good Privacy (PGP)

- Objetivo: prover um mecanismo de cifração forte e de uso fácil para todos
  - Foco: e-mails (cifração e assinatura)
  - Lançado por Phil Zimmermann em 1991
  - Versões abertas: OpenPGP e GNUPG
- Usa conceito de “molho de chaves”: elevada **descentralização** (Web of Trust)
  - Usuários usam **certificados auto-assinados**
  - Usuários podem **assinar certificados uns dos outros** e definir **níveis de confiança**

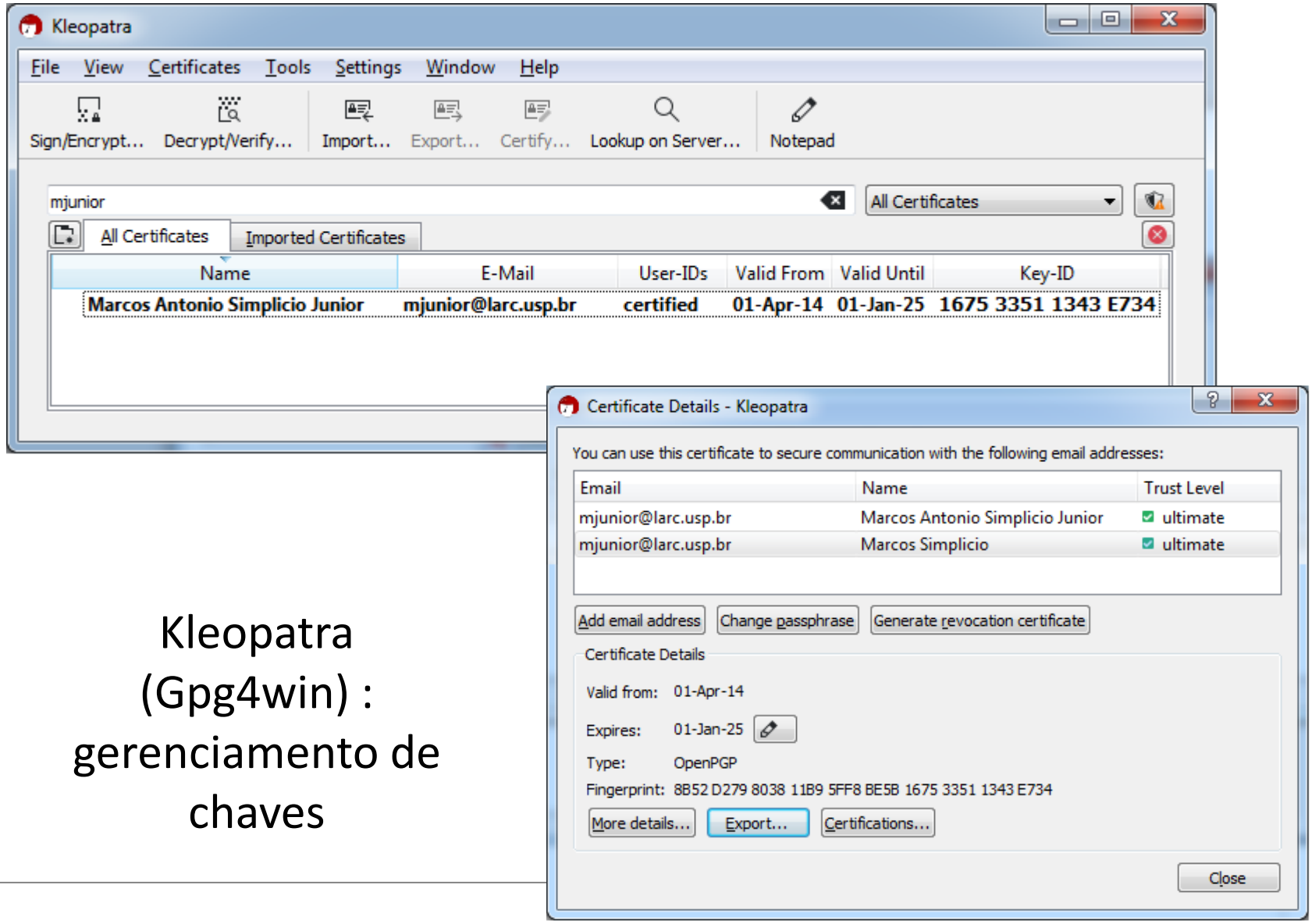
Web of Trust (PGP)



Exemplo: PGP no Thunderbird



Exemplo: PGP no Thunderbird



Kleopatra (Gpg4win) : gerenciamento de chaves

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Certificação Digital:

Identidades & Carimbo de tempo

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Apoio financeiro: d24n.org <https://d24n.org>
ripple impact | university blockchain research initiative

Referências

- W. Stallings, L. Brown “Computer Security Principles and Practice – 2nd/3rd/4th edition”. Prentice-Hall, ISBN: 0-13-277506-9. 2011/2015/2018.
  - Em português: W. Stallings, L. Brown. “Segurança de Computadores - Princípios e Práticas” (2ª Ed), Elsevier, 2014
- W. Stallings: “Cryptography and Network Security” (6th/7th Ed.), Prentice-Hall 2013/2016.
  - Em português: W. Stallings: “Criptografia e Segurança de Redes” (6ª Ed.), Pearson-Prentice-Hall (2014).
- S. Wykes. Criptografia Essencial: A Jornada do Criptógrafo, 1a ed. Elsevier, 2016.
- A. Narayanan, J. Bonneau, E. Felten. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction". Princeton University Press, 2016. ISBN: 0691171696. Available: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1
- C. Adams, P. Cain, D. Pinkas, R. Zuccherato. RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP). Internet Engineering Task Force, August 2001. URL: https://datatracker.ietf.org/doc/html/rfc3161