



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

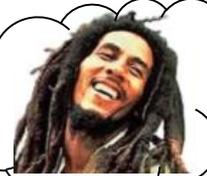
Distribuição de chaves públicas



Aqui é o Bob.
Anote minha
chave pública...

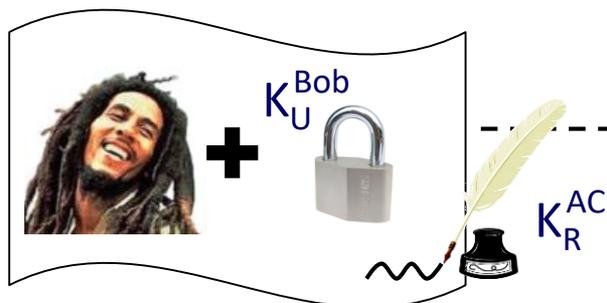


Oi Bob. Pode falar,
estou anotando...



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

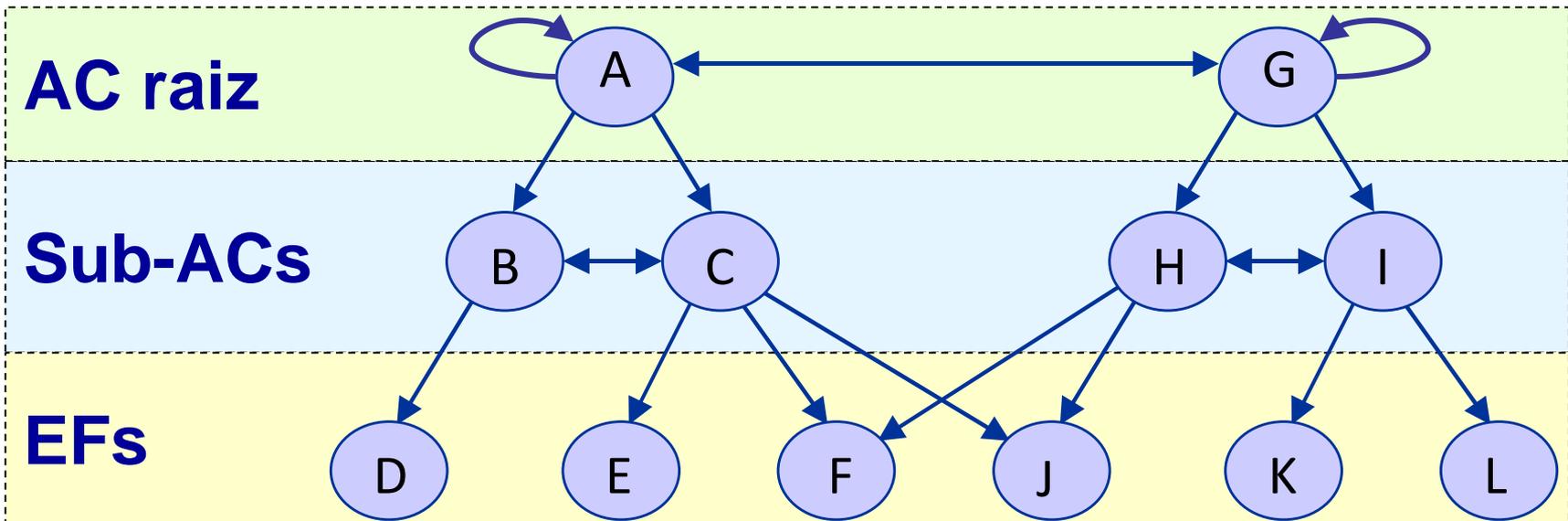


Alice usa K_U^{AC} para verificar a autenticidade do certificado

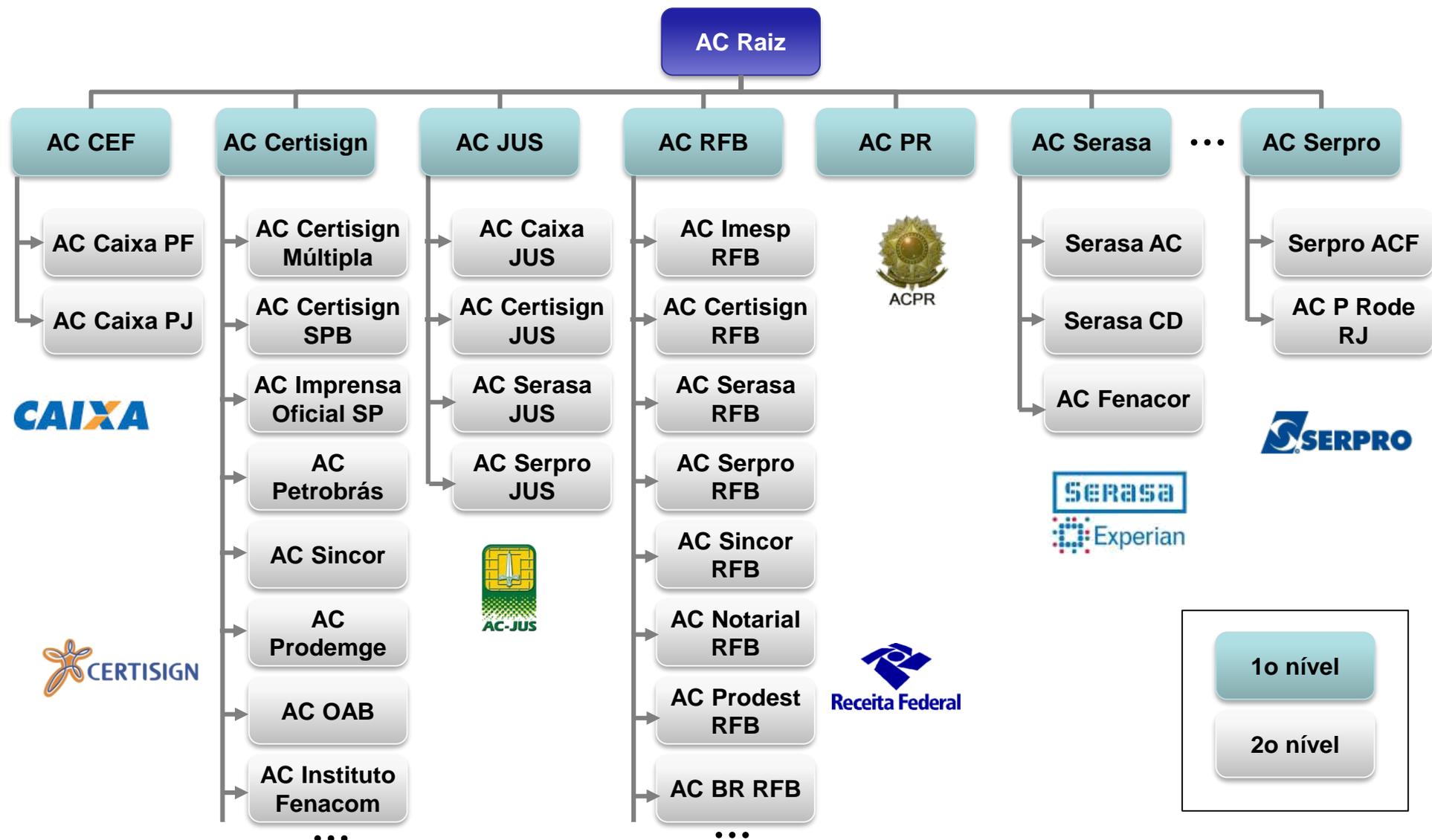


Certificados Digitais: ICP

- 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



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*

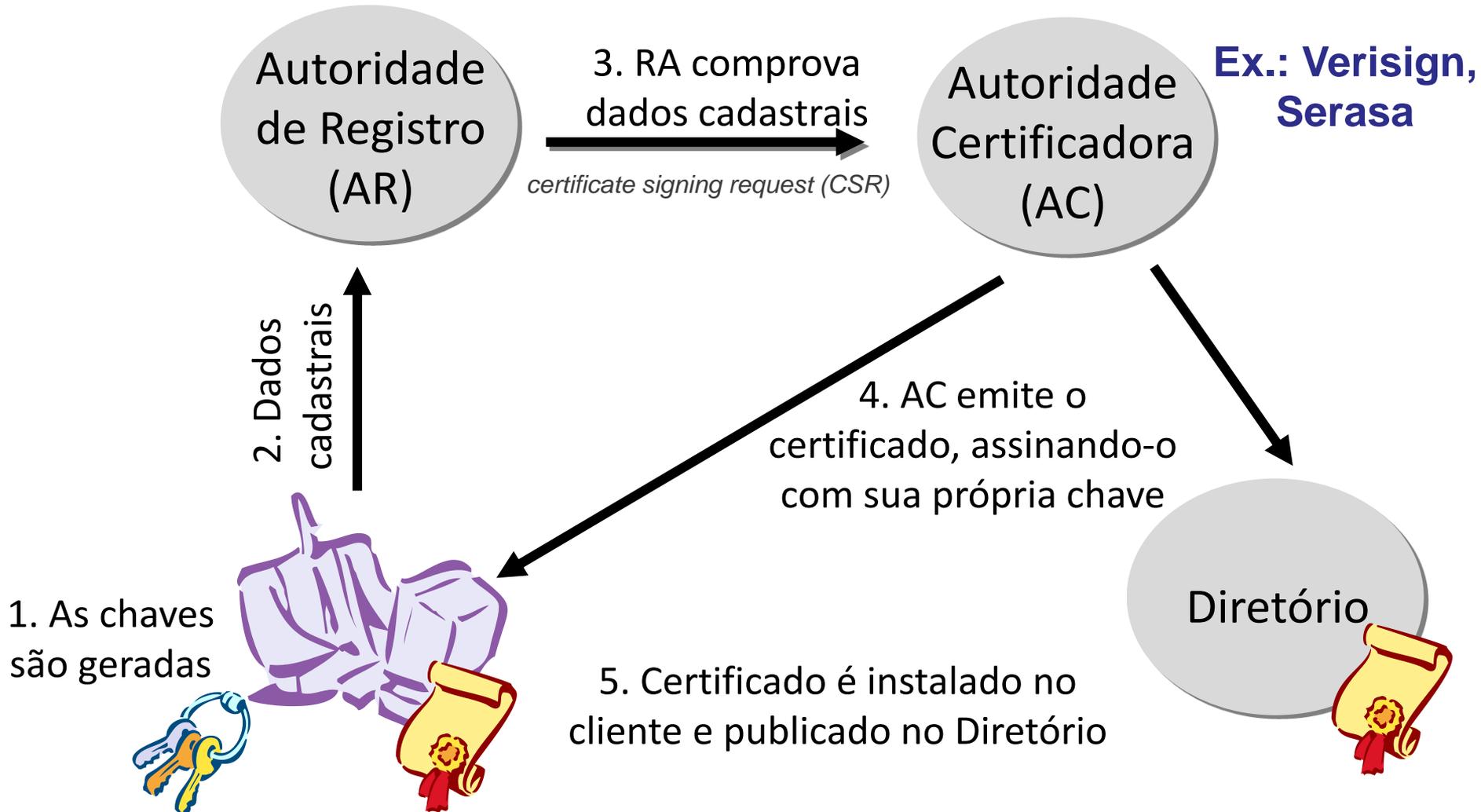
- **Outros (uso específico)**

- A CF-e-SAT: assinatura de Cupom Fiscal Eletrônico
- OM-BR: equipamentos de medição

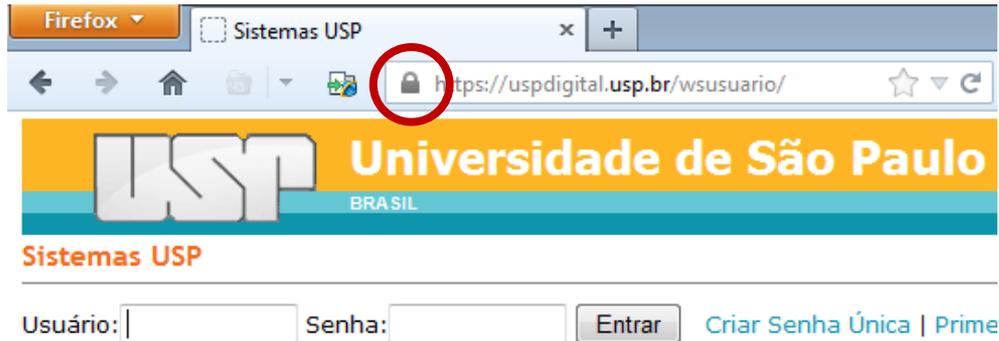
Certificados ICP-Brasil: tipos

- 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

Processo de certificação



Usando certificados (web)



**Autoridade
Certificadora**

[3.1. Consulta OCSP: revogação]

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



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



1. Requisita Certificado

2. Fornece certificado
assinado por AC

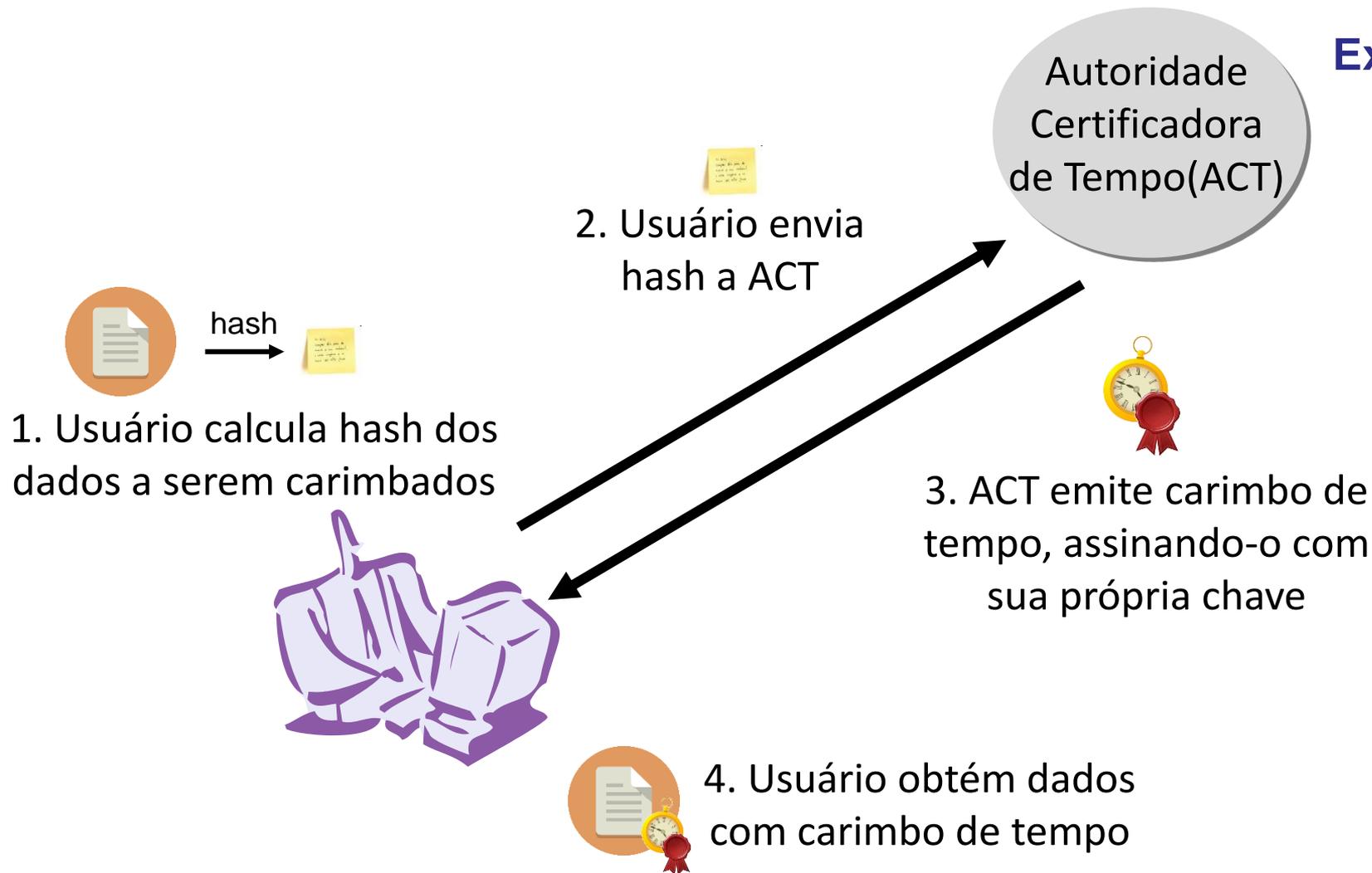


USP

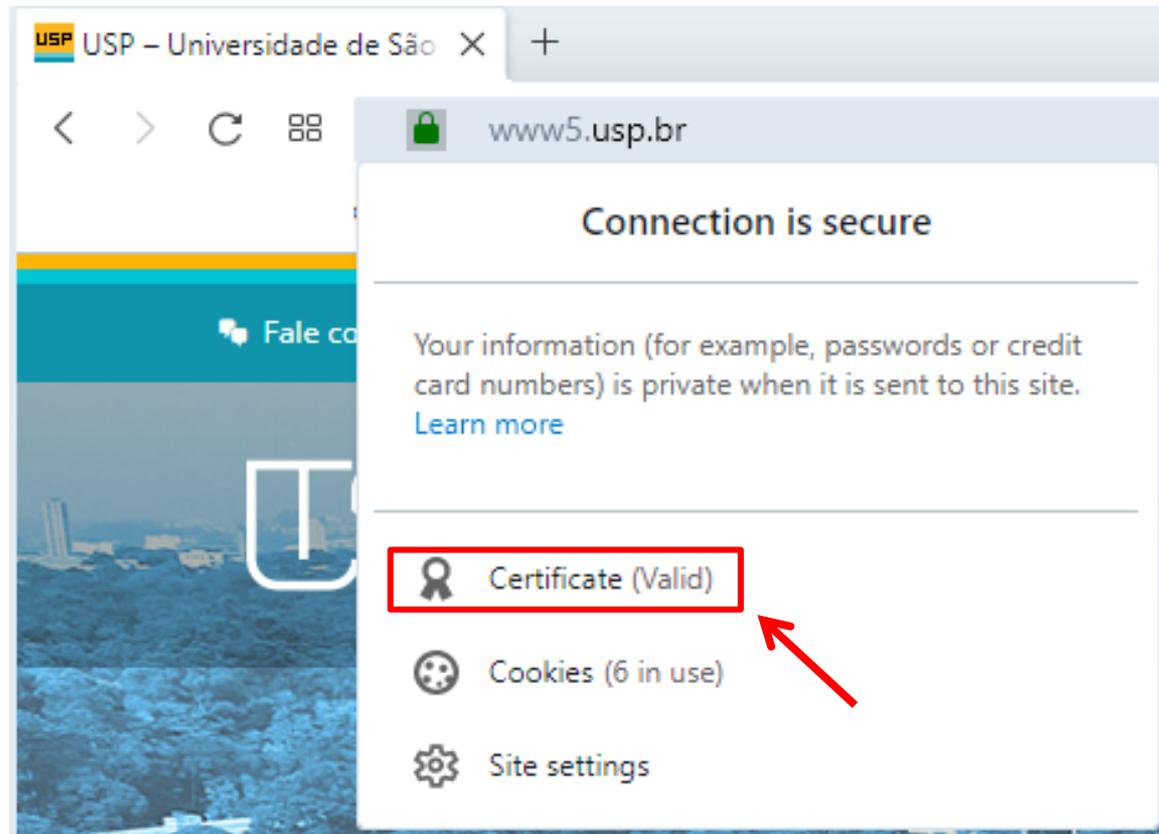


Processo de Carimbo de Tempo

Ex.: Caixa,
Serpro

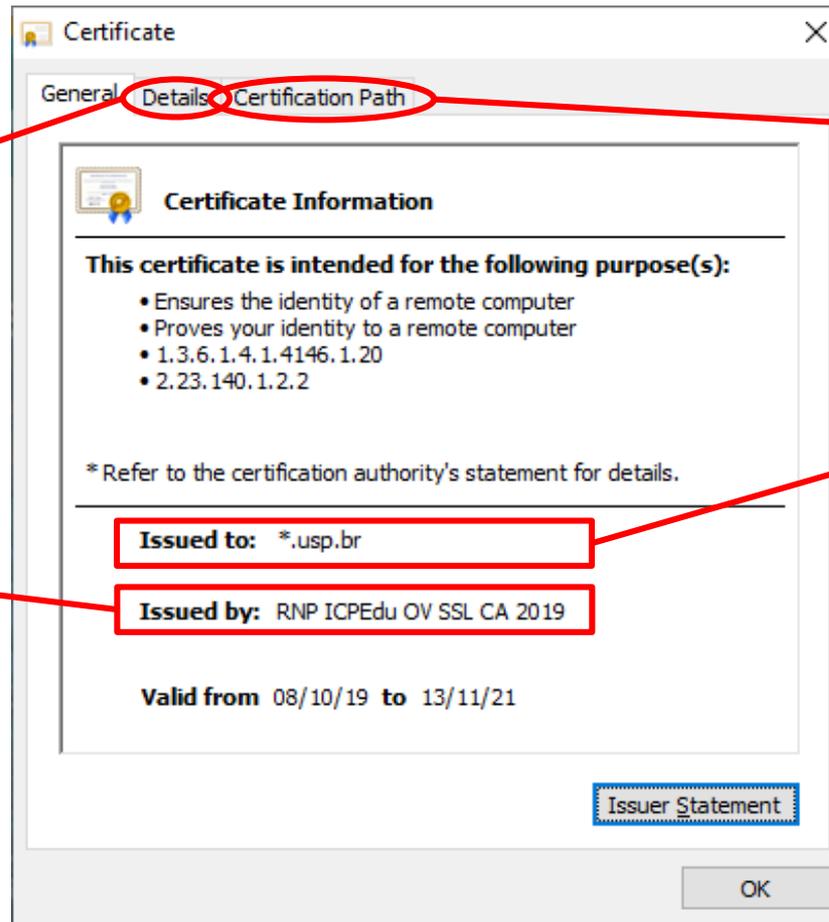


Exemplo: Certificado USP (X.509)



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)

The screenshot shows a Windows 'Certificate' dialog box with the 'Certification Path' tab selected. The path is displayed as a tree structure:

- GlobalSign Root CA - R3 (Root CA)
- Trusted Root CA SHA256 G2 (Intermediate CA)
- RNP ICPEdu OV SSL CA 2019 (Intermediate CA)
- .usp.br (End Entity)

Red annotations highlight the 'AC raiz' (Root CA) and the 'Cadeia de certificados' (Certificate chain).

AC raiz

Cadeia de certificados

View Certificate

Certificate status:
This certificate is OK.

OK

Exemplo: Certificado USP (X.509)

Field Value

Valid to	Saturday, November 13, 2021...
Subject	*.usp.br, UNIVERSIDADE DE S...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=End Entity, Pat...
CPI Distribution Points	[1]CPI Distribution Point: Distr...

```
30 82 01 0a 02 82 01 01 00 a1 b4 9f 7b ff
76 69 c5 0a de 1b ce 65 10 3d f0 22 6b e9
cd e9 6f 25 ba 12 03 e0 08 76 26 0a 36 f8
79 21 a9 d5 ad 3e 66 28 f2 6b 1c cf 65 dd
7a e5 9a 0f 39 79 a6 69 f8 d1 95 da 7f 11
56 49 db a2 2b 8d f6 c0 35 eb c2 02 b9 e0
47 59 b1 d0 92 fa b7 e8 bf 35 44 8d 34 3a
4f ed 95 fa 2d a2 1c ce aa 2c 83 48 97 90
c9 87 1e d7 8b e7 ad b4 08 e1 87 12 76 d8
```

Edit Properties... Copy to File...

OK

**Chave pública
(RSA 2048 bits)**

Field Value

Serial number	53f278b58ab9d0a2fc35d87b
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RNP ICPEdu OV SSL CA 2019, ...
Valid from	Tuesday, October 08, 2019 1...
Valid to	Saturday, November 13, 2021...
Subject	*.usp.br, UNIVERSIDADE DE S...
Public key	RSA (2048 Bits)

sha256RSA

Edit Properties... Copy to File...

OK

**Algoritmo de assinatura:
RSA+SHA-256**

Field Value

Version	V3
Serial number	53f278b58ab9d0a2fc35d87b
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RNP ICPEdu OV SSL CA 2019, ...
Valid from	Tuesday, October 08, 2019 1...
Valid to	Saturday, November 13, 2021...
Subject	*.usp.br, UNIVERSIDADE DE S...

53f278b58ab9d0a2fc35d87b

Edit Properties... Copy to File...

OK

**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)



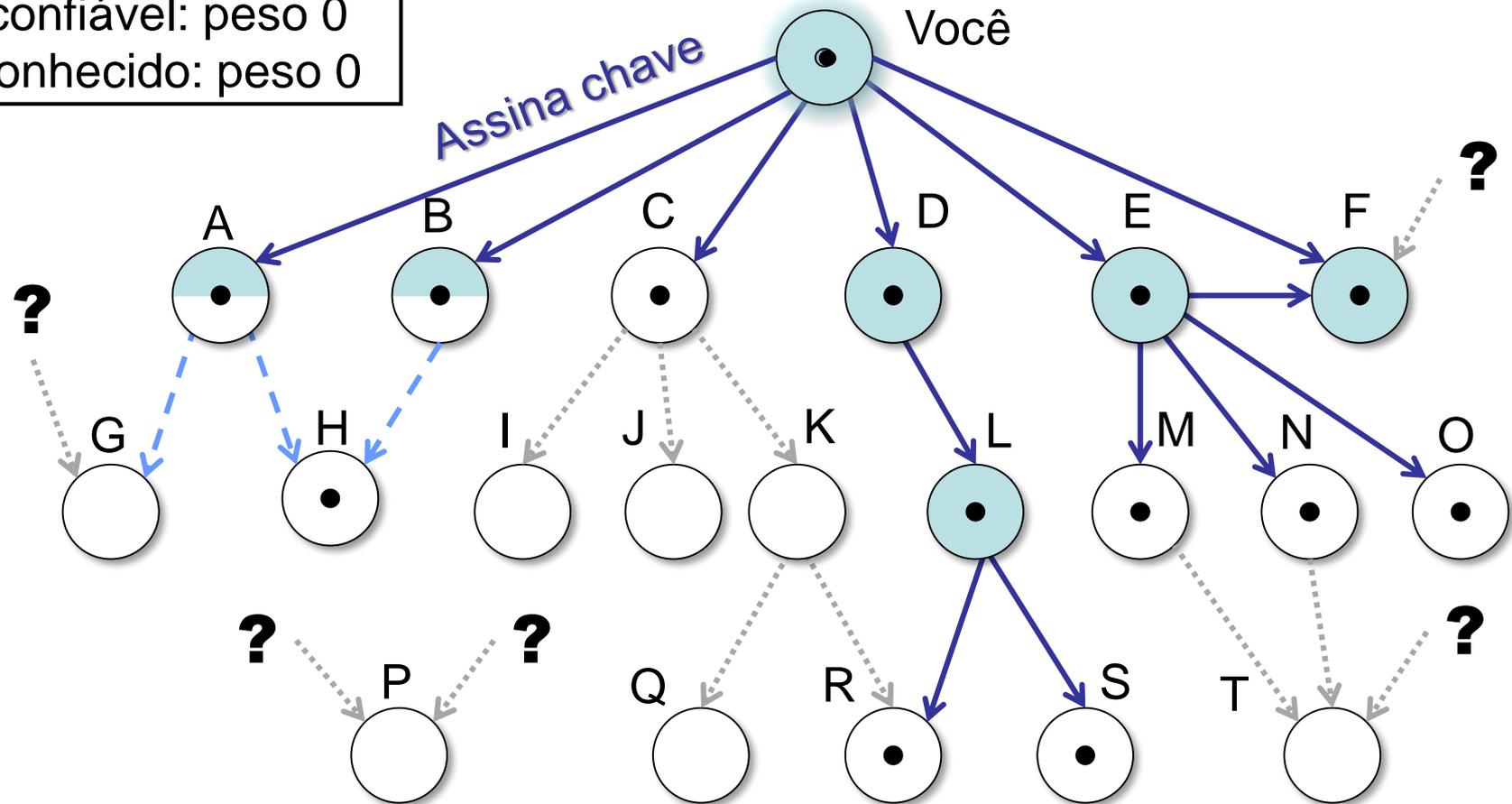
- Objetivo: prover um mecanismo de cifração forte e de uso fácil para todos
 - Foco: e-mails (cifração e assinatura)
 - Lançado por Phil Zimmermann em 1991
 - Versões abertas: OpenPGP e GNUPG
- Usa conceito de “molho de chaves”: elevada **descentralização** (Web of Trust)
 - Usuários usam **certificados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



Web of Trust (PGP)

- Confiável: peso 1
- ◐ Semi-confiável: peso 1/2
- Não confiável: peso 0
- ? Desconhecido: peso 0

⦿ Chave considerada legítima



Exemplo: PGP no Thunderbird

Enigmail

From Marcos Simplicio Reply Forward Archive Junk Delete More 19:26

Subject **Teste PGP**

To Marcos Simplicio

-----BEGIN PGP MESSAGE-----
Charset: UTF-8

hQGMxZ1M1ETQ+c0AQv/Q72cG1tYMgk4HBLbpSeMfuZyGsSBfIu+H3PPp6dWZ5Py
HjC8L5bAvN4Q89cfyL5yffZJwC0YEwCDMB71BioHin4ToZQ7hn/660gm0IF5PsdK
U9fHWZkqAZ1ovrxkFqhvAkSUysYbfZ2u1Gpw7+SBzksL7eZvg3lPZUrrhyXLZiYa
dgeB9lITPh20aQ4YF3b35QU6S1gSYAa62senNOUuFSRUGk9+Nam5eh8wn1YR2Zgs
THPwMhRj4AlaggDchPFw/sc0L6V10v/R+br1pk7NUqwx2rx/oNIrH4gLoz96HcaU
c8fnhaUvb8uG1xgihHu80zUMUZum21Vyrk2P+DhEbjt+GdsKG7hgbt050di+af+vs
q3BY8hPEp2MIDELQTKVnkBLV7CCj+a5h8mGvWibKkCcfQnr0ptg4mr
5nq9C888LhwJ17H30G4MKprh7YOUzjp9UqOMxgz9zzGZmFgNLvp1qyc
YeP2n/+SQwd704SMpxaJ0ukBy/Kh2PGWfsTqrrTiINj1dza/T9W1/e6
FDFM01id+KB+YbJ65WhZwszyrq863Nz6qcacvGYFTiKt8WPT+1YNTTj
5XtUAMCBg5zqww3igmCsvqtX5Yrd+MOF/gJqaIUrNaM0TwxR65f6
8h6XUz45/DQwN+8XgWcN62acXSolXrjVPqaw9rW8J6gk70S9Tzoei;
e3qQV7rRUwbre5DhcDai3lrHibQTMiELeLGKYT9Hb9LFF0mg/GV7XZ?
3Y4uGDCGJWKdb11ae4+th6WzUkS65nwT/pvIFs0nxtSf7YfVctC+CV?
TRYt11CYxisMXBIrblT7u+xzJs8CXLATLxjczYnFjrpRdt0smLBMHv
oLoskNGVzWjh3naXemv+oXx+3U8ZXXfi0sObueB4oEZ3afmxPQL2Nt\l
UNao1PK9if20zppPPfx1BvSV41+thCodIleJiFOIR1aAC9R+EVwxHa
06aTrCuXhtj6mB+oxr6x8i8f5pKMnwE/RsjfbgrxcwqzQ1Le693dV/4
mRh8B84sDcEds8KIBzLzncGXDE9pk2h457yAoSt5BFdjcpexIn2otsk
/cBE1t/zoBD5/K3mdM7lZ8r3eI+Kc/p021J3jv4tdiS0PpUCHnGx76;
nFe9GJIeodqy2fRxXwZavJjXarCeJcFfC220AFNP0oadJYWCzA1wgl
tJfY7UeHSk5GVT5F4z2GstYioY03mZkicyIDcDByzv+J/gipNcJs?
tRZKxU5pwk5giITcketylhvple9E1DpXJvwayCoqLAL0MboT/jZg9l;
0USvLchpxKAuwDac/EQrD0h0ajdaHQHsz0L7gFoN61uwC0JICwjurol
9W6J55CNJ4BXJWK3XdZokZvQpDZ20/Y=
=hqmX
-----END PGP MESSAGE-----

Part of the message signed and encrypted; click on 'Details' button for more information
Key ID: 0x8B52D279803811B95FF8BE58167533511343E734 / Signed on: 10/25/19, 7:26 PM

Enigmail Details

From Marcos Simplicio Reply Forward Archive Junk Delete More 19:26

Subject **Teste PGP**

To Marcos Simplicio

***** *BEGIN ENCRYPTED or SIGNED PART* *****

Teste PGP

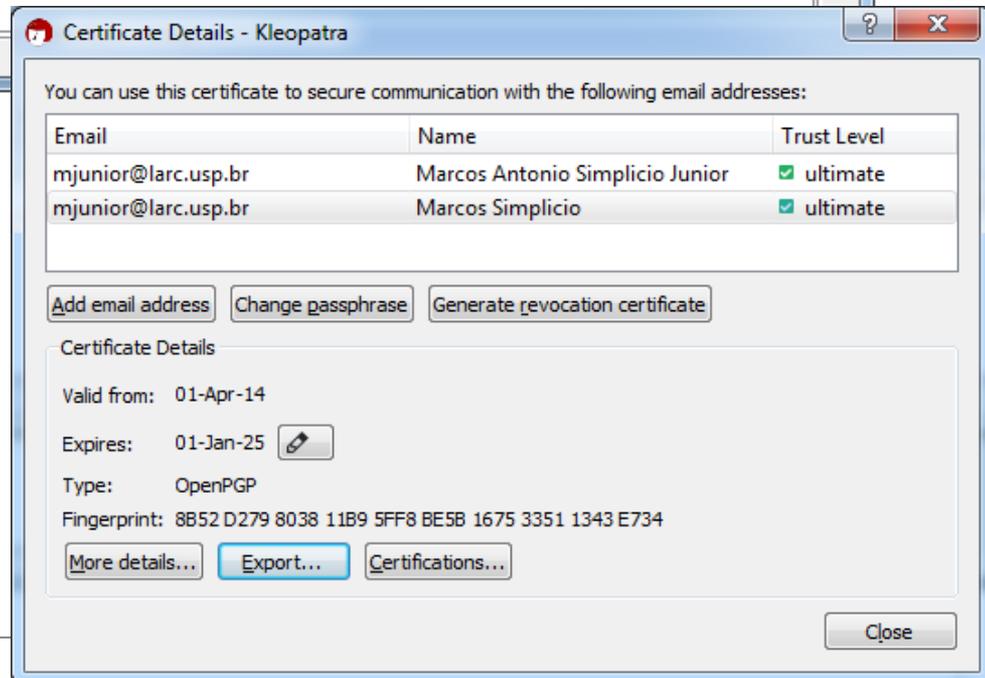
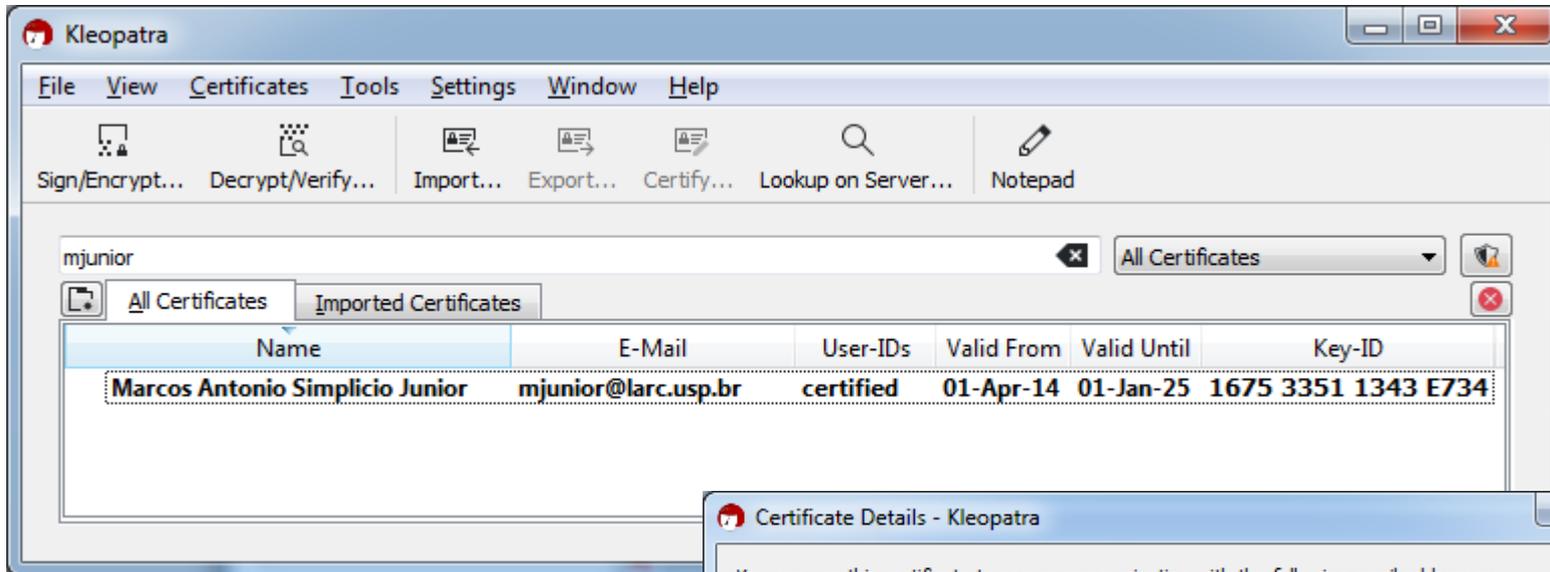
--
--
Prof. Dr. Marcos A. Simplicio Jr.
Escola Politecnica -- University of São Paulo (Poli-USP), Brazil
Laboratory of Computer Networks and Architecture (LARC)
https://www.researchgate.net/profile/Marcos_Simplicio
<http://lattes.cnpq.br/6874544707185541>

***** *END ENCRYPTED or SIGNED PART* *****

--
This email has been checked for viruses by Avast antivirus software.
<https://www.avast.com/antivirus>

1 attachment: 0x167533511343E734.asc 2.0 KB

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

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>