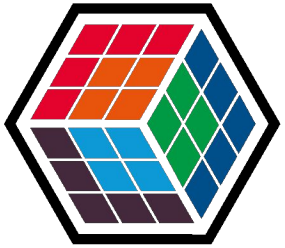


THE DEVELOPER'S CONFERENCE

Trilha – Segurança e Criptografia

James Miranda

O que é PKI e como essa estrutura é essencial para os negócios modernos.

Quem?

THE DEVELOPER'S CONFERENCE

James Miranda

Mestre em Engenharia de Software,
desenvolvedor nos últimos 7 anos.

MT4 Networks

O conteúdo apresentado aqui é de minha autoria e não representa, necessariamente, a opinião ou posicionamento de meu empregador.

Agenda

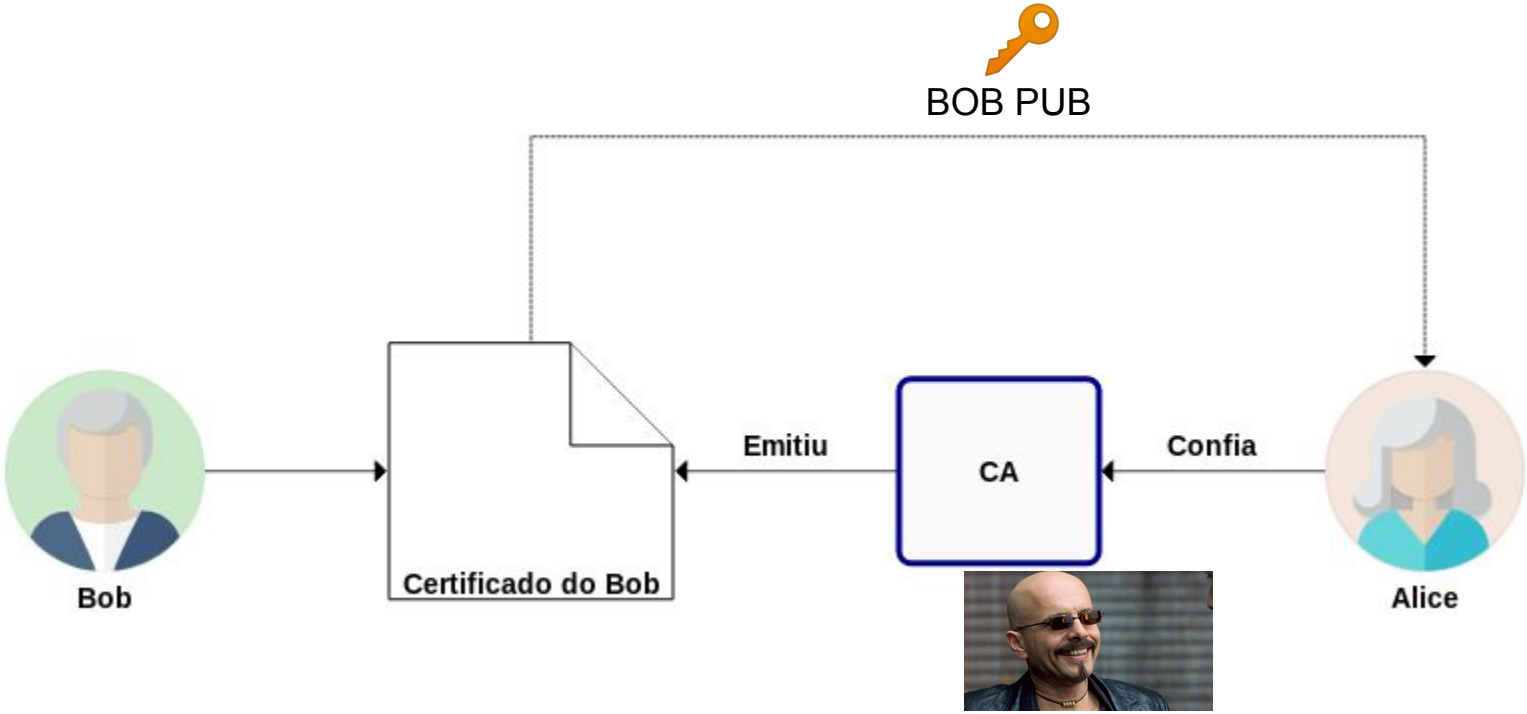
THE DEVELOPER'S CONFERENCE

- O problema da confiança
- Certificação
- O que é PKI?
- Problemas e alternativas
- E agora?

Photo by Chunlea Ju on Unsplash

O problema da confiança

Certificação



O que é um certificado?

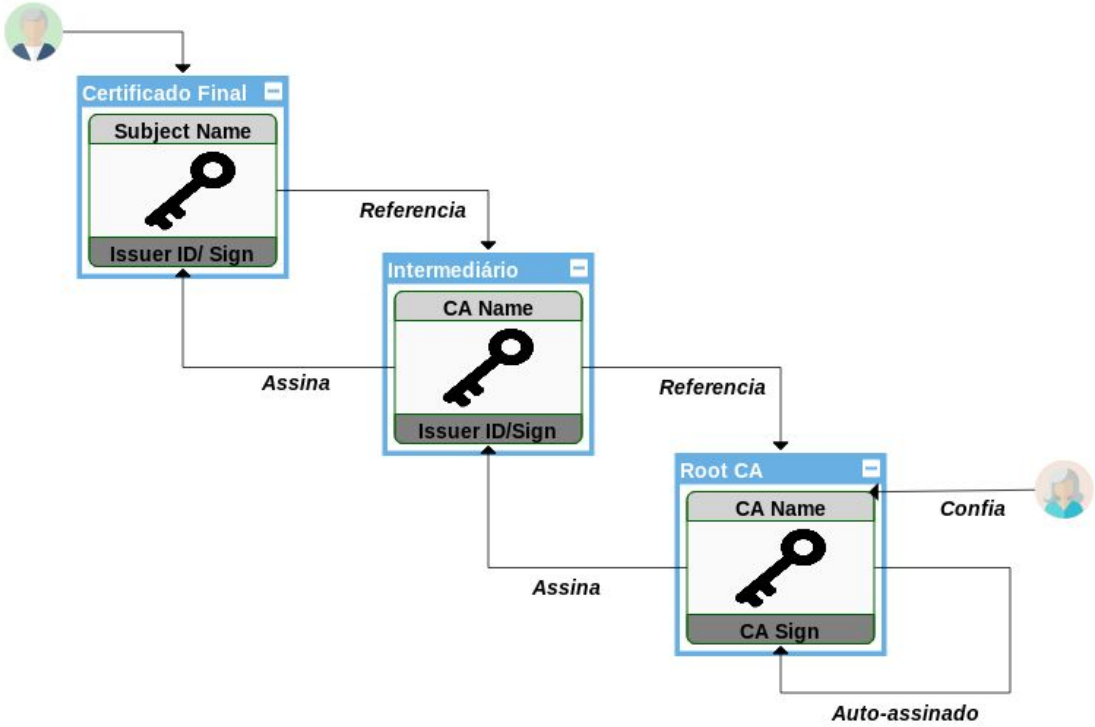
THE DEVELOPER'S CONFERENCE

Version (3)
Serial Number
Sign Alg
Issuer Name
Validity
Subject Name
Public key
Issuer ID
Subject ID
Extensions
Assinatura

- X.509
- RFC 5280 *
  - CRL
  - OCSP (2560)

*https://tools.ietf.org/html/rfc5280

Cadeia de Confiança



O que é PKI?

THE DEVELOPER'S CONFERENCE

- Framework/Infraestrutura
  Public Key Infrastructure

  - *Repositório de certificados de chave pública;*
  - *Revogação de certificados;*
  - *Publicação de certificados e de CRLs;*
  - *Atualização de chaves;*
  - *Backup de chaves;*
  - *Escrow de chaves;*

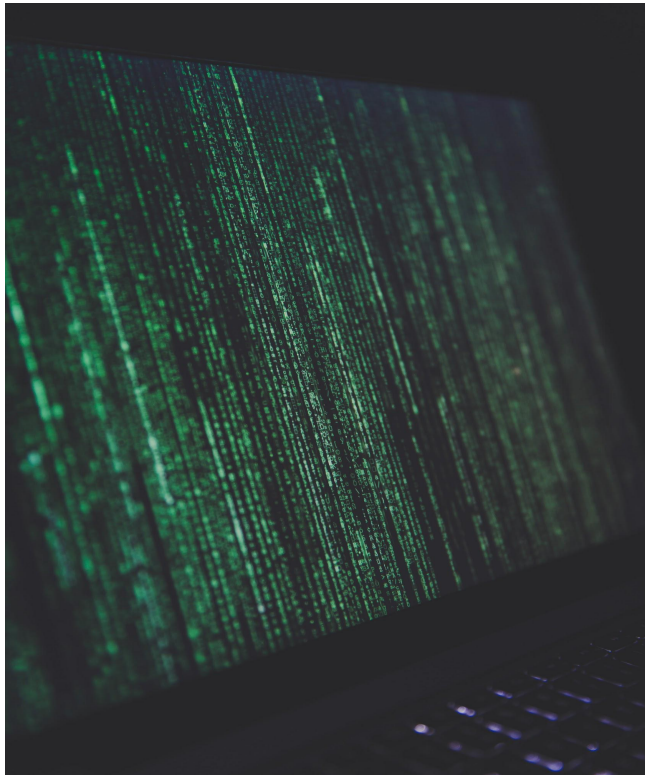
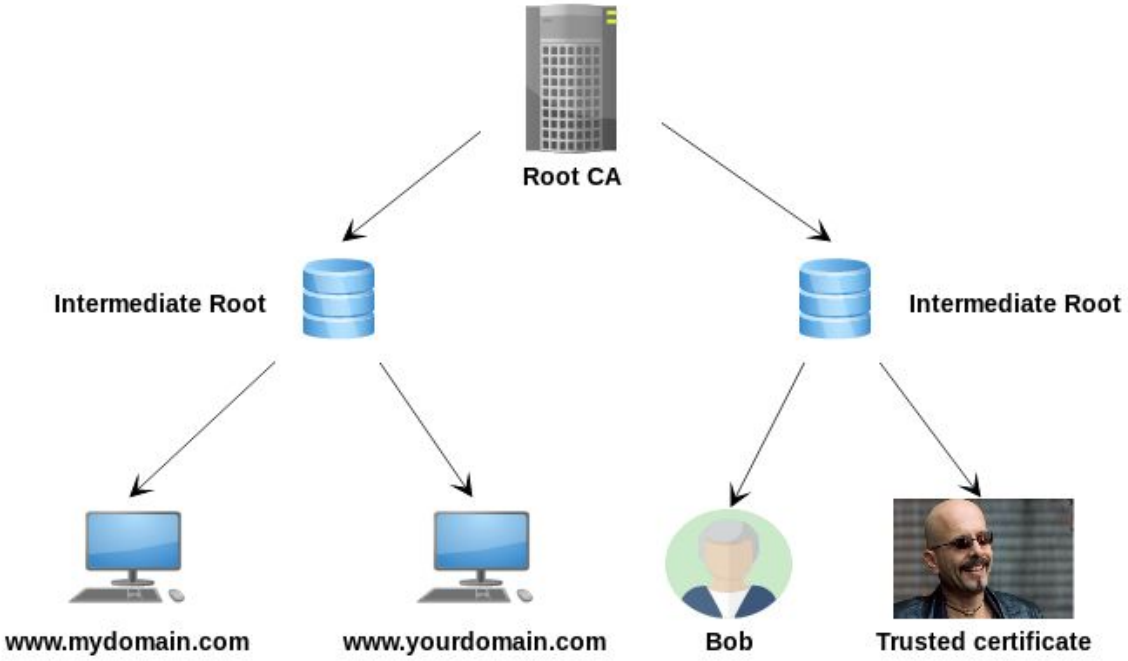


Photo by Markus Spiske on Unsplash

Agentes

THE DEVELOPER'S CONFERENCE



Arquitetura interna

- RA - Registration authority
- VA - Validation authority
- HSM - Hardware security module
- ...

Onde é usado?

THE DEVELOPER'S CONFERENCE

TLS

Autenticidade de domínios
Não repúdio de informações

S/MIME

Assinatura de e-mails
Não repúdio de informações.

NFS-e

Assinatura digital de notas fiscais.

Smart card

Pessoas físicas
Pessoas jurídicas
Cartões de acesso
...

Problemas e alternativas

Photo by Wesley Marçal on Unsplash

"Quem vigia os vigilantes?"

Problemas e alternativas

THE DEVELOPER'S CONFERENCE

- KDC (*Kerberos*);
  - Chaves simétricas
  - Centralizado
- PGP (*OpenPGP/GPG*)
  - Será que Bob é confiável, afinal?
  - Usado para envio de e-mails
  - Descentralizado
  - *Web of trust*
- Blockchain
  - Ainda muito experimental
  - Acadêmico

THE DEVELOPER'S CONFERENCE

E agora?

- Criar uma CA
  - OpenSSL
- Criar chave PGP
- Refletir sobre quem tem o controle da Web

Obrigado!!!

THE DEVELOPER'S CONFERENCE

Bibliografia

Stallings, W., Bressan, G., & Barbosa, A. (2008). *Criptografia e segurança de redes* . Pearson Educación.

Cooper, D. (2008). Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 5280.

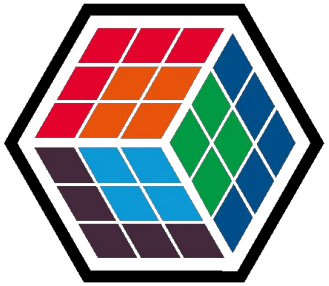
Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (1999). *X. 509 Internet public key infrastructure online certificate status protocol-OCSP* (pp. 01-14). RFC 2560.

Tutorial - Criar uma CA
https://gist.github.com/Soarez/9688998

THE DEVELOPER'S CONFERENCE

Créditos

Template da apresentação por TDC
Fotografias do Unsplash
Diagramas criados com yEd



THE DEVELOPER'S CONFERENCE