Certificação digital

Lucas Klüber
Silvia T. Lopes

Assinatura e Certificado Digital

Assinatura Digital e Certificado Digital agregam valor de confiança e segurança em operações veiculadas em ambiente virtual.

Assinatura Digital trabalha com **criptografia assimétrica**

- Criptografia de chaves públicas

Criptografia simétrica e assimétrica

- Criptografia Simétrica:
  - Mesopotâmia/Egito
  - Julio César - Guerras da Gália
  - Alfabeto Criptografado: veni, vidi, vici == YHQL, YLGL, YLFL
  - Chave única

Criptografia simétrica e assimétrica

- Criptografia assimétrica:
  - Anos 70 - Whitfield Diffie, Martin Hellman e Ralph Merkle
  - Chave Pública e Chave Privada (Privativa)

Certificado Digital

Agregar valor de confiança às comunicações virtuais.

Documento eletrônico assinado por uma terceira parte confiável, que associa nome e atributos confiáveis de uma pessoa à uma chave pública.

Direto do túnel do tempo

x.500 e x.509 - Padrões de serviço de diretório e autenticação com hierarquia

1988

PGP - Programa de criptografia baseado em Web of trust

1991

Signaturgesetz - Primeira Legislação de certificação digital implementada na Europa

1997

ICP-Brasil - Infraestrutura nacional para certificação digital criada

2001

X.500

- O X.500 é um conjunto de padrões abordando serviços de diretório
- Desenvolvido pela ITU-T (Telecommunication Standardization Sector) em 1988 com parceria da ISO
- O X.500 definiu os protocolos:
  - DAP (Directory Access Protocol)
  - DSP (Directory System Protocol)
  - DISP (Directory Information Shadowing Protocol)
  - DOP (Directory Operational Bindings Management Protocol)
- Originalmente utilizavam o modelo de rede OSI, porém foram feitas adaptações do DAP para o TCP/IP (LDAP).

X.509

- X.509 é um padrão que define certificados de chave pública.
- Utilizado em protocolos de rede
  - TLS/SSL
- Utilizado em assinaturas eletrônicas
- Define uma hierarquia baseada em autoridades certificadoras

X.509

- Certificado
  - Versão
  - Número Serial (Único)
  - ID do Algoritmo de assinatura
  - Nome do Emissor
  - Validade
    - Não Antes
    - Não Depois
  - Nome do proprietário
  - Informações da chave pública do proprietário
    - Algoritmo da Chave Pública
    - Chave Pública
  - Identificador Único do emissor (opcional)
  - Identificador Único do Proprietário (opcional)
  - Extensões (opcional, definem o propósito do certificado)
- Algoritmo de assinatura do certificado
- Assinatura do certificado

X.509

1. CSR (Certificate Signing Request) auto-assinada
    - Public key
    - Private key
2. A CSR contém a chave pública, DN (Distinguished name) e outras informações de identificação;
3. A CA (Autoridade Certificadora) então emite um certificado que vincula a chave pública com um DN ;
4. Como se baseia em hierarquia, o certificado raiz deve ser distribuído para que os certificados emitidos a partir dele sejam reconhecidos.
5. Navegadores vem com certificados das principais CA pré instalados.
6. Todo certificado deve conter o endereço de uma CRL (Certificate revocation List) da Autoridade Certificadora. Essa lista contém todos os certificados revogados.

PGP

- Pretty Good Privacy
- É uma forma de criptografia de comunicação e autenticação desenvolvida em 1991
- Diferente do padrão X.509, e baseado em uma Web of Trust
    - Certificados são assinados por outros certificados de entidades que confiam neste certificado.
    - Gradualmente cada certificado vai estar vinculado a diversos outros certificados que são considerados confiáveis, efetivamente criando uma “teia de confiança”
- Nas versões atuais do PGP foi adicionado suporte para a existência de Autoridades Certificadoras, tornando possível um funcionamento parecido com o do X.509

Secure Socket Layer

Protocolo HTTP com SSL:

Provê uma abstração de canal seguro de comunicação, ou *stream* seguro à interface HTML de maneira transparente.

- Autenticação de servidores através de certificados públicos (CA).
- sujeita às vulnerabilidades do protocolo TCP/IP.

OpenSSL

- O OpenSSL é uma implementação open source dos protocolos TLS e SSL.
- Disponibiliza várias funções de criptografia e pode ser utilizado para gerar certificados de autenticação de serviços.
- Disponível para Linux, BSD, MAC e Windows.

OpenSSL

Criar CSR

```
$ openssl req -new -sha256 -nodes -newkey rsa:4096 -keyout example.com.key -out example.com.csr
```

Criar certificado autoassinado

```
$ openssl req -x509 -sha256 -nodes -newkey rsa:4096 -keyout example.com.key -days 730 -out example.com.pem
```

Ver certificados e CSRs

```
$ openssl x509 -in example.com.pem -noout -text
```

```
$ openssl req -in example.com.csr -noout -text
```

OpenSSL

Criar um certificado AC

```
#arquivo x509.ext define as extensões
[ ca ]
# X509 extensions for a ca
keyUsage              = critical, cRLSign, keyCertSign
basicConstraints      = CA:TRUE, pathlen:0
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid:always,issuer:always

[ server ]
# X509 extensions for a server
keyUsage              = critical,digitalSignature,keyEncipherment
extendedKeyUsage      = serverAuth,clientAuth
basicConstraints      = critical,CA:FALSE
subjectKeyIdentifier  = hash
authorityKeyIdentifier  = keyid,issuer:always
```

OpenSSL

Criar um certificado AC

```
# Criar a chave privada e o certificado - Autoridade Certificadora

$ openssl req -new -sha256 -nodes -newkey rsa:4096 -keyout CA.key -out CA.csr

$ openssl x509 -req -sha256 -extfile x509.ext -extensions ca -in CA.csr -signkey CA.key -days 1095 -out CA.pem

# Criar certificado de servidor/cliente  e assinar pela AC

$ openssl req -new -sha256 -nodes -newkey rsa:4096 -keyout www.example.com.key -out www.example.com.csr

$ openssl x509 -req -sha256 -CA CA.pem -CAkey CA.key -days 730 -CAcreateserial -CAserial CA.srl -extfile x509.ext
-extensions server -in www.example.com.csr -out www.example.com.pem
```

Brasil

- A Infraestrutura de chaves Públicas Brasileira (ICP-Brasil) foi criada em 2001 e é o sistema nacional de certificações digitais;
- Utiliza o padrão X.509
- A Autoridade Certificadora Raiz é o ITI - Instituto de Tecnologia da Informação
- O ITI é responsável por credenciar e homologar as Autoridades Certificadoras que podem então emitir certificados para o contribuinte.

Uso

No Brasil, o certificado digital pode ser utilizado pelo contribuinte como um documento, CPF ou CNPJ eletrônicos, reconhecido pela receita federal.

Tipos de Certificados

Certificado A1:

Esse tipo de certificado digital é um arquivo (geralmente .pfx ou .p12) que pode ser instalado em qualquer computador.

Validade de 1 Ano.

Certificado A3:

É instalado em um token ou cartão que deve ser “espetado” na máquina para ser utilizado, por conta disso garante uma maior segurança.

Validade de 3 anos

Tipos de Certificados

Ambos podem ser utilizados tanto por pessoas físicas quanto jurídicas.

- O certificado de uma pessoa física é o e-CPF
- O certificado de uma pessoa jurídica é o e-CNPJ

e-CPF

Utilizado para:

- Declaração de imposto de renda
- Assinatura de documentos e email
- Acessar serviços online da secretaria da fazenda (Receita/PR, e-CAC)

e-CNPJ

Utilizado para:

- Emissão de documentos fiscais
- Transações bancárias
- Reconhecimento de firma
- Acessar serviços da SEFAZ
- Declaração de imposto de renda
- eSocial
- Assinatura de documentos

eNF-e

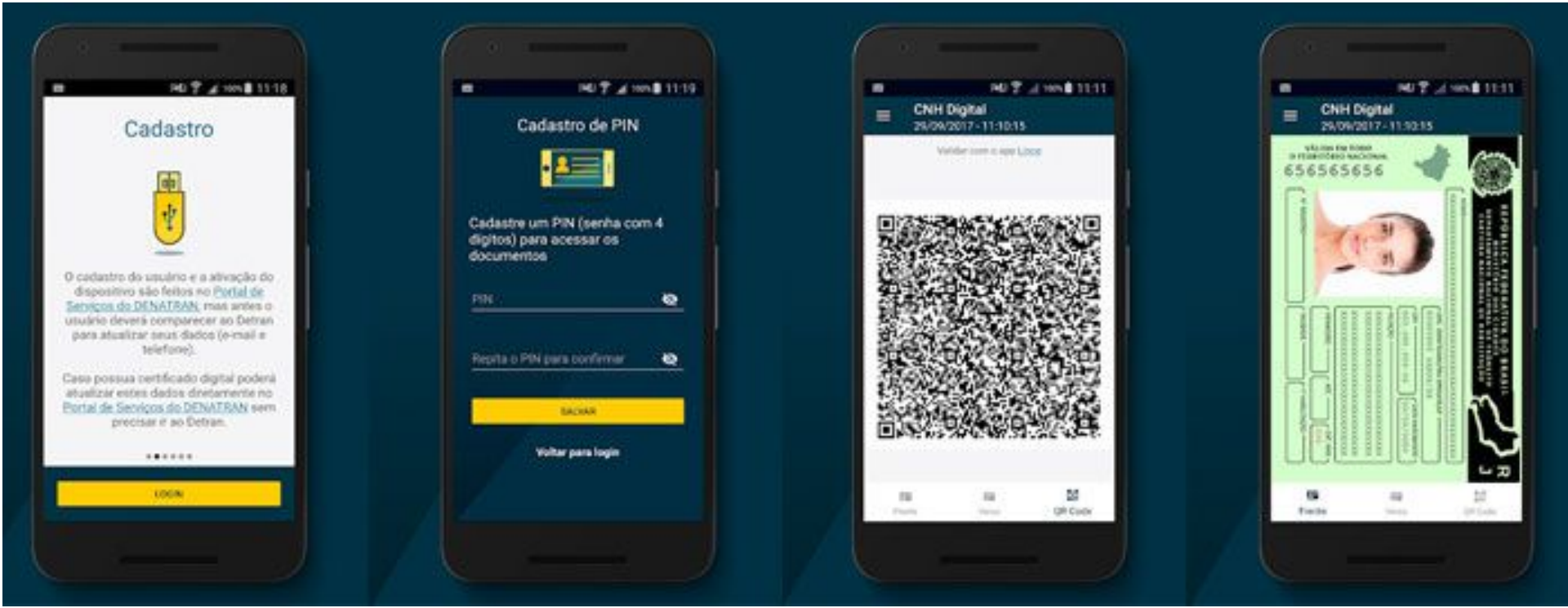
É um tipo de certificado para pessoa jurídica, mas que tem apenas a função de emitir documentos fiscais.

Enquanto o e-CNPJ é de propriedade do responsável legal da empresa, o eNF-e pode ser disponibilizado para uso dos funcionários.

Outros usos

- A partir desse ano é possível emitir a carteira de habilitação digital, processo facilitado para as pessoas que já possuem um certificado digital (podem fazer pelo próprio celular)

Outros usos


Cadastro
O cadastro do usuário e a ativação do dispositivo são feitos no Portal de Serviços do DENATRAN, mas antes o usuário deverá comparecer ao Detran para atualizar seus dados (e-mail e telefone).
Caso possua certificado digital poderá atualizar estes dados diretamente no Portal de Serviços do DENATRAN sem precisar ir ao Detran.
LOGIN
Cadastro de PIN
Cadastre um PIN (senha com 4 dígitos) para acessar os documentos
PIN
Repita o PIN para confirmar
SALVAR
Voltar para login
CNH Digital
29/09/2017 - 11:10:15
CNH Digital
29/09/2017 - 11:10:15
656565656

Outros usos

- e-Diploma: É um diploma completamente digital que pode ser utilizado da mesma forma que um diploma de papel. O documento é assinado digitalmente pelo proprietário e pelos responsáveis usando o certificado digital.

Referências

MENKE, Fabiano. **Assinatura Digital, Certificados Digitais, Infra-estrutura de chaves públicas brasileiras e ICP alemã**, 2003 - UFSC

POUW, Keesje Duarte; GEUS, Paulo Lício. **Desenvolvendo aplicações seguras em ambiente HTML/HTTPS**, 1999 - UNICAMP

Referências

Cryptoid
https://cryptoid.com.br/banco-de-noticias/26558-certificacao-digital/

https://cryptoid.com.br/certificacao-digital/diploma-na-parede-e-passado-entenda-as-vantagens-do-e-diploma/

FolhaZ
https://www.folhaz.com.br/noticias/certificado-digital/

Docusign
https://www.docusign.com.br/blog/assinatura-eletronica-x-assinatura-digital-voce-sabe-quais-as-diferencas/

Tecnoblog
https://tecnoblog.net/265343/cnh-digital-500-mil-motoristas/