HTTPS – O que muda no protocolo?

Conceitos básicos de segurança da informação

Criptografia por chave

Tipos

Assimétrica

- Chave privada
  - Assinatura - criptografia
- Chave pública
  - verificação de autenticidade

Simétrica

Chave única privada

- Conhecimento prévio da chave
- Como transferir a chave?
- Exemplo: Cifra de César
  - Bob, I love you. Alice
  - Ere, l oryh brx. Dolfh

Tipos:

- Cifra de fluxo
  - Sequência de bits pseudo-aleatório
  - Mapeamento 1 para 1
- Cifra de bloco
  - Blocos de bits
    - k= número de bits
    - Ex: k = 64

Certificado digital

O que é certificar uma chave?
Comprovar autenticidade

Quem comprova a autenticidade?
Entidade certificadora

- **Certification Authority - CA**

Entidade Certificadora

- Verificação de identidade
  - Alta confiabilidade
- Emissão de certificados
  - Vínculo entre chave e entidade

Padrões de autoridades certificadoras

- IETF - recomendação ITUX.509
  - Especificação de um serviço de autenticação e sintaxe de certificados
- RFC 1422

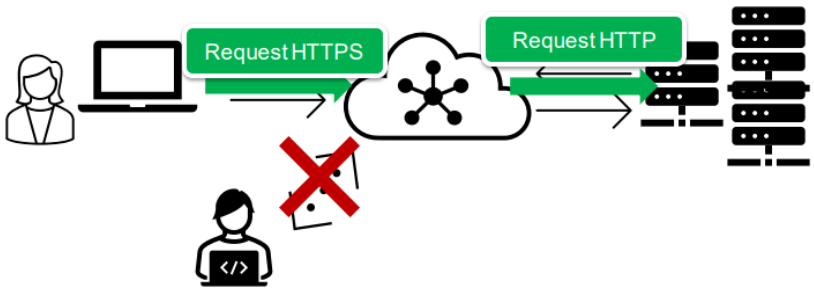
- Gerenciamento de chaves baseado em CA em e-mails seguros

Protocolo SSL – Secure Socket Layer

Segurança para conexões TCP

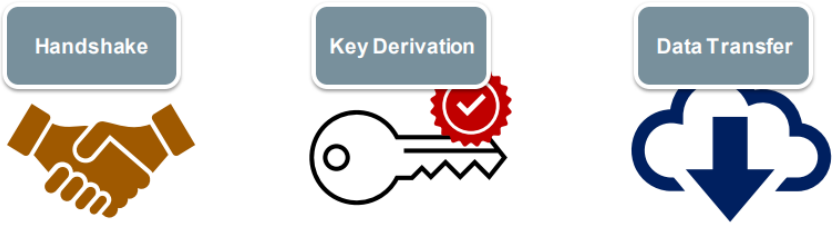
- Confidencialidade
- Integridade
- Autenticidade end-point

Importância



Operações do SSL & HTTPS

Temos 3 fases:



HTTPS e breve descrição da LGPD

HTTP + SSL

- Segurança na comunicação - HTTP
  - Over TCP
- Verificação da autenticidade por certificados digitais
  - Porta 443

Há sites que não utilizam?

- Maioria dos site utilizam a versão segura

LGPD – Lei Geral de Proteção de Dados

- Promulgada em 2018
- Entrou em vigor em Agosto de 2020
  - Lei de segurança da informação
- N° 13.709/2018

O que a lei protege?

- Dados de identificação dos usuários
- Dados sensíveis Religião, etnia, etc.
- Define o tratamento de dados
  - Diversos tipos de operações
- Livre conssentimento
- Direitos do titular das informações
- Sanções aos que descumprirem as regras

Criação da ANPD (Agência Nacional de proteção de dados)

- Zelar pela proteção dos dados;
- Elaboração de diretrizes para política nacional de proteção;

- Promover conhecimento das normas
- Editar regulamentos
- Realizar auditorias

Quem deve seguir a lei?

- Empresas que precisam manter um BD
- Funcionários e Usuários

Devem garantir ao titular sigilo das informações

GDPR – General Data Protection Regulation

- Legislação europeia
- Legislação do estado da Califórnia - EUA