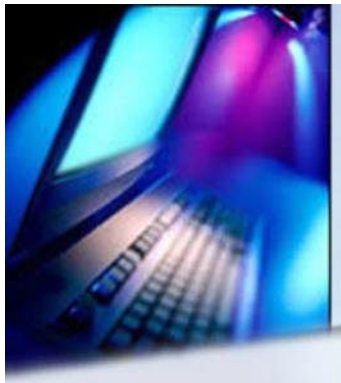

# Protocolo

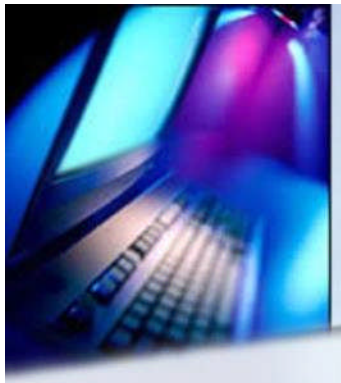
Autor : Marcelo Passos dos Santos



# Objetivo

Apresentar a estrutura do protocolo HTTP.

Quanto mais o desenvolvedor souber sobre este protocolo melhor, pois ele é utilizado em todas aplicações web.



# HTTP

- O que é o HTTP ? Pesquise na web ?

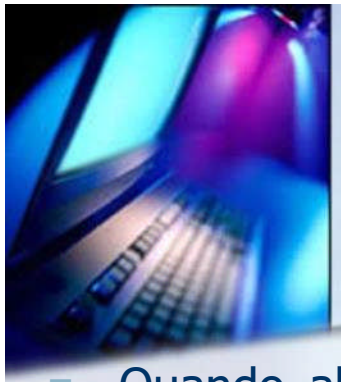
( ) - Heavy Transmission Text Protocol

( ) - Hypertext Transfer Protocol

( ) - Help Text Transfer Protocol

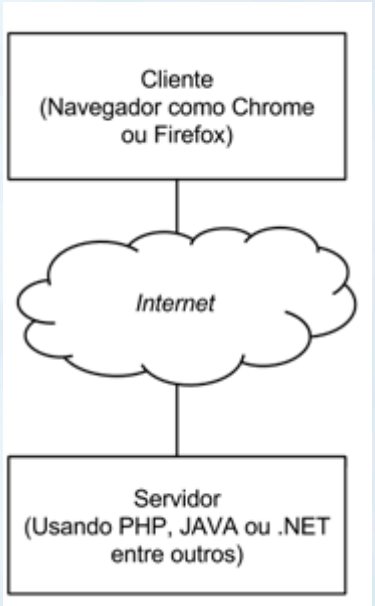
( ) - High Text Transmission Protocol

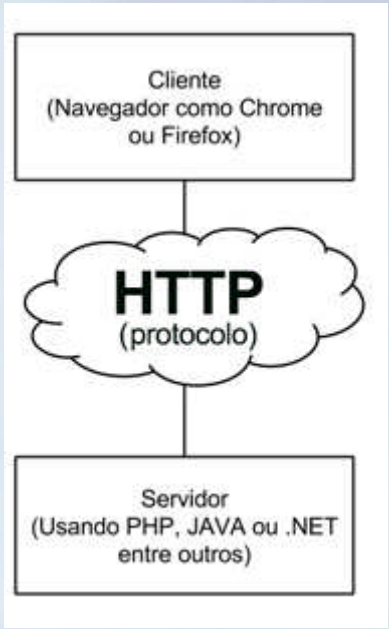
UniFOA
Centro Universitário de Volta Redonda



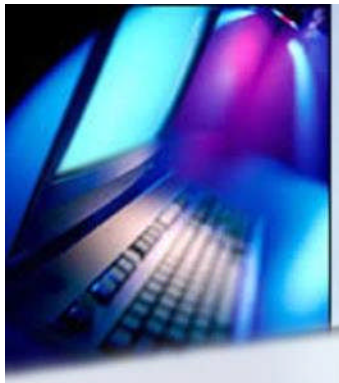
# Cliente - Servidor

- Quando alguma página na internet é acessada utiliza-se um navegador como Google Chrome, Mozilla Firefox ou Internet Explorer da Microsoft.
- O cliente pede informações e o servidor responde. Esse modelo de comunicação, ou essa arquitetura, é chamado de **Cliente-Servidor**, em inglês **Client-Server**.




**HTTP é um protocolo** que define as **regras de comunicação** entre **cliente e servidor** na internet.



# Cliente - Servidor

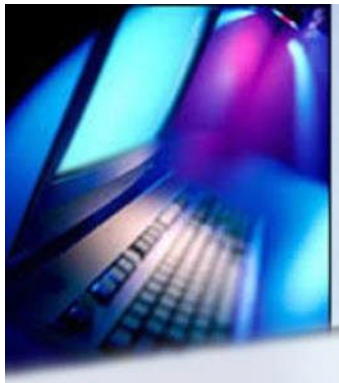
- O protocolo HTTP segue o modelo **Client-Server**.
- O que o navegador (como Chrome ou Firefox) representa nesse modelo? O cliente ou o servidor?

( ) - Nenhum dos dois

( ) - Servidor

( ) - Cliente

UniFOA
Centro Universitário de Volta Redonda



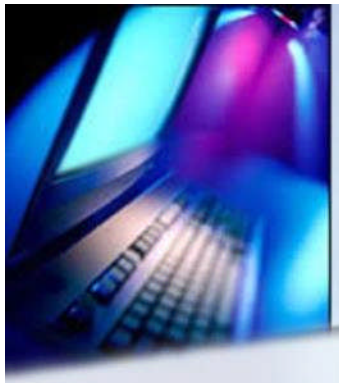
# Cliente - Servidor

- **PARABÉNS para quem respondeu :**

( ) - Nenhum dos dois

( ) - Servidor

( X ) - Cliente



# Cliente - Servidor

- **Papel do HTTP entre Cliente e Servidor**
- O cliente inicia a comunicação e o servidor responde. No entanto, qual é o papel do **HTTP** entre Cliente e Servidor?

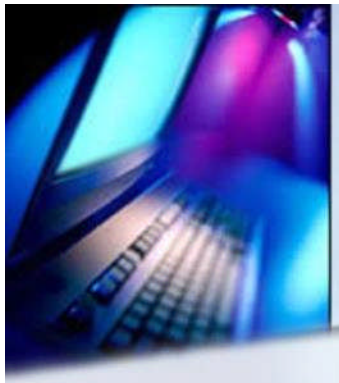
( ) - Estabelecer regras de comunicação

( ) - Definir uma estrutura de dados

( ) - Definir o melhor algoritmo de pesquisa

( ) - Comprimir os dados

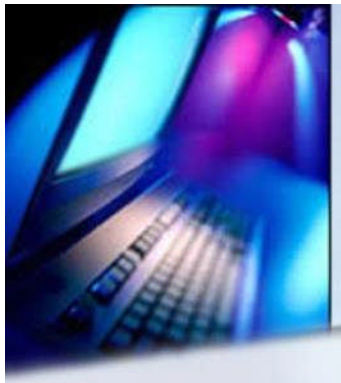
UniFOA
Centro Universitário de Volta Redonda



# Cliente - Servidor

- PARABÉNS para quem respondeu Estabelecer regras de comunicação.
- Se você compreende este texto, é porque você sabe português!
- Para que alguém consiga se comunicar com você, esse alguém deverá usar o português (supondo que você desconheça outro idioma, é claro).
- Isso significa que, sua regra (protocolo) de comunicação com o mundo é a língua portuguesa que define a forma com que as informações devem chegar até você (através do vocabulário, regras de gramática e etc).
- Uma outra pessoa que conheça português irá usar do mesmo formato, já que vocês possuem um idioma em comum.

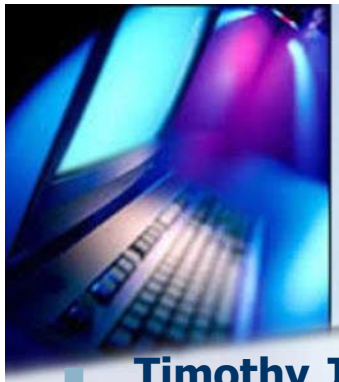
UniFOA
Centro Universitário de Volta Redonda



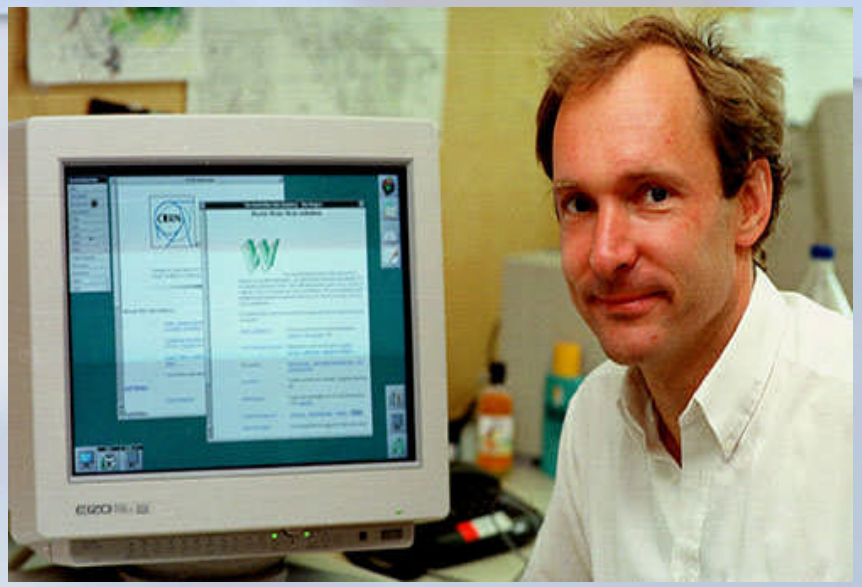
# Cliente - Servidor

- Na internet como já vimos, o idioma mais comum é o HTTP.
- Ele é responsável por definir a forma com que os dados são trafegados na rede através de várias regras.
- Portanto, todo mundo que conhece o idioma HTTP poderá receber e enviar dados e participar dessa conversa!

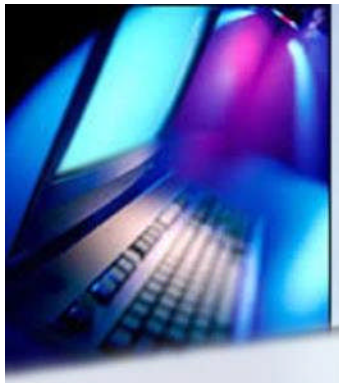
UniFOA
Centro Universitário de Volta Redonda



# Criador do Protocolo HTTP



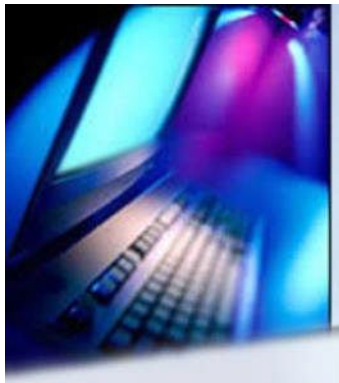
- **Timothy John Berners-Lee** (**TimBL** ou **TBL**) – nascido em (Londres, 8 de junho de 1955 ).
- É um físico britânico, cientista da computação e professor do MIT.
- É o criador da World Wide Web (Rede Mundial de Computadores - Internet), tendo feito a primeira proposta para sua criação a 25 de março de 1989.
- Em 25 de dezembro de 1990, com a ajuda de Robert Cailliau e um jovem estudante do CERN (centro de Pesquisa, implementou a primeira comunicação bem-sucedida entre um cliente HTTP e o servidor através da internet.



# Criador do Protocolo HTTP

- O primeiro website que Tim Berners-Lee construiu - inicialmente com uma página de texto - foi no Info.CERN.Ch, que foi posto online em 6 de Agosto de 1991.
- Oferecia uma explicação sobre o que a World Wide Web era, como se poderia criar um navegador (**Browser**), como instalar e configurar um web-server, etc.
- Foi também o primeiro diretório online do mundo, já que Berners-Lee fez uma lista de outras páginas de Internet que existiam na época.
- Mais tarde, esses simples diretórios iriam ser substituidos por motores de busca, como o Google.)

UniFOA
Centro Universitário de Volta Redonda

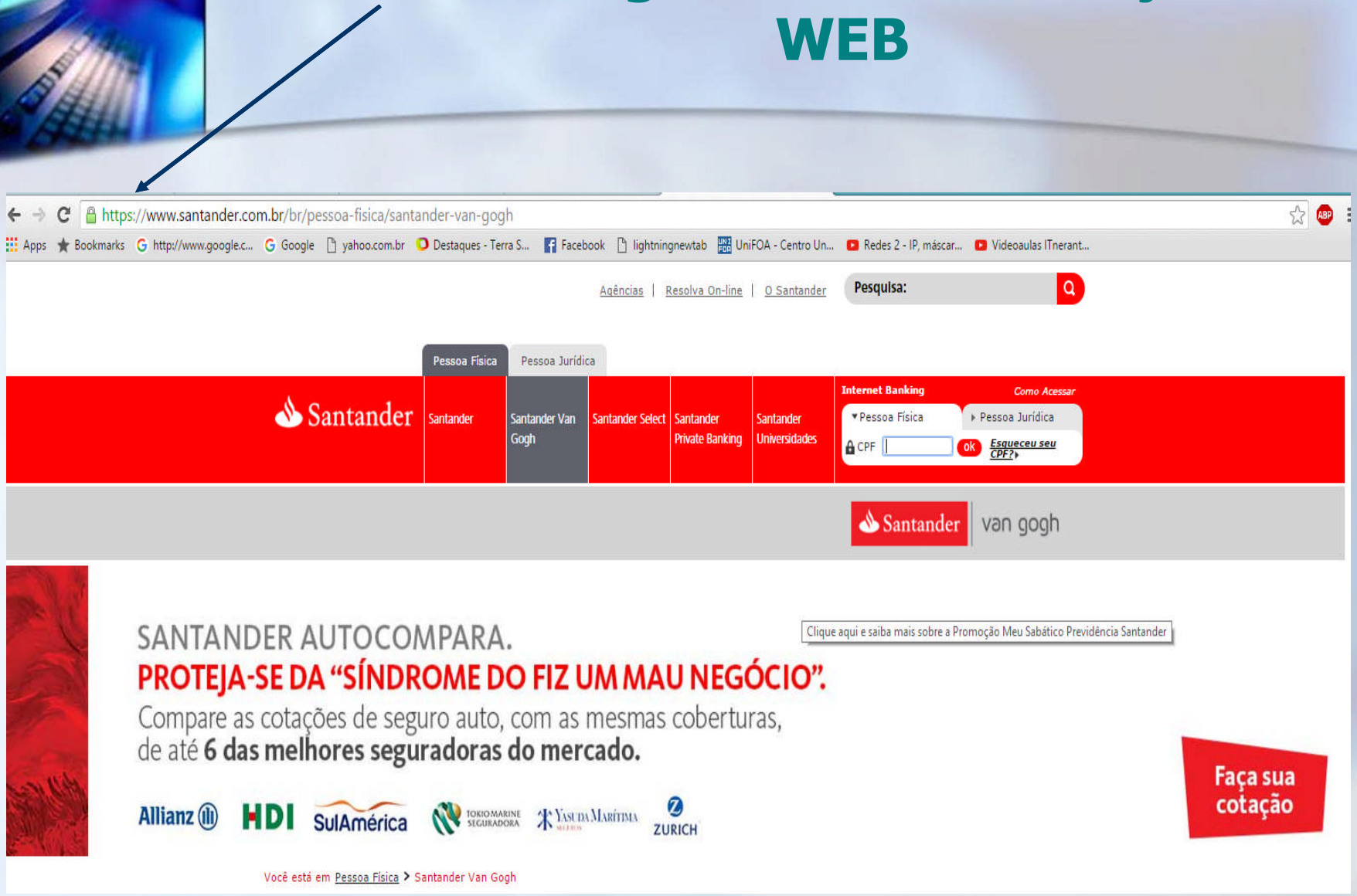


# http – É texto puro

- Quando usamos o HTTP (sem o **S** no final) todos os dados enviados entre cliente e servidor são transmitidos em texto puro, inclusive dados sensíveis como login e senha! Mas por que é importante sabermos isso?
- Bem, quando o navegador pede informações, nessa comunicação há vários intermediários. Por exemplo, usando uma conexão WIFI, os dados do navegador passam primeiro para o roteador WIFI e do roteador passam depois para o modem do provedor, do modem para algum servidor do provedor de internet, como Oi ou NET.
- É muito provável que existam outros servidores intermediários no provedor antes que os dados realmente cheguem no servidor que contém a página.
- Com a resposta é a mesma coisa, ela volta passando por esses servidores no meio antes de chegar até nosso navegador.  O problema é, quando usamos HTTP pode haver alguma tentativa de espionar os dados enviados.

UniFOA
Centro Universitário de Volta Redonda

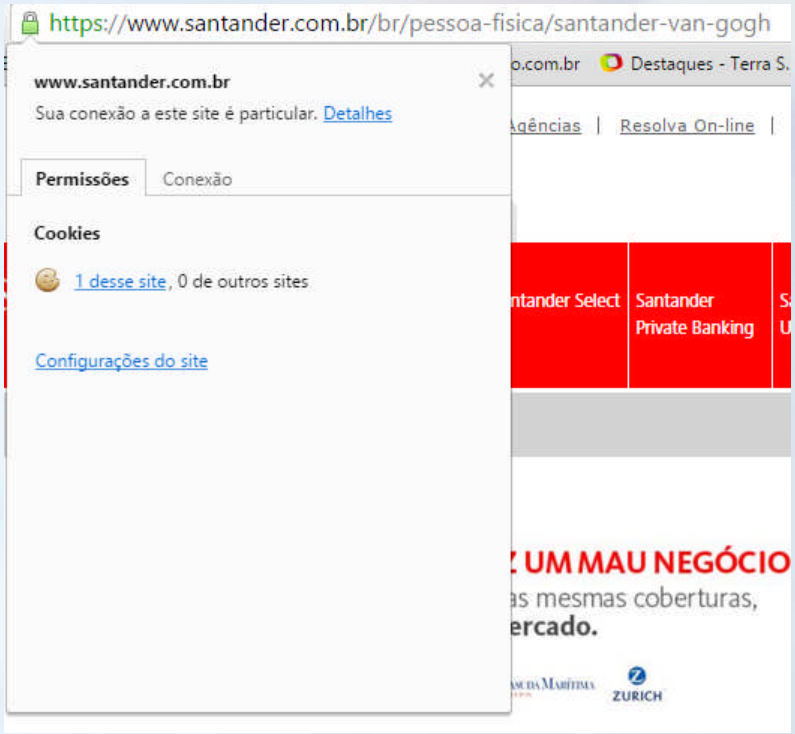
# Certificado Digital : a identificação na WEB

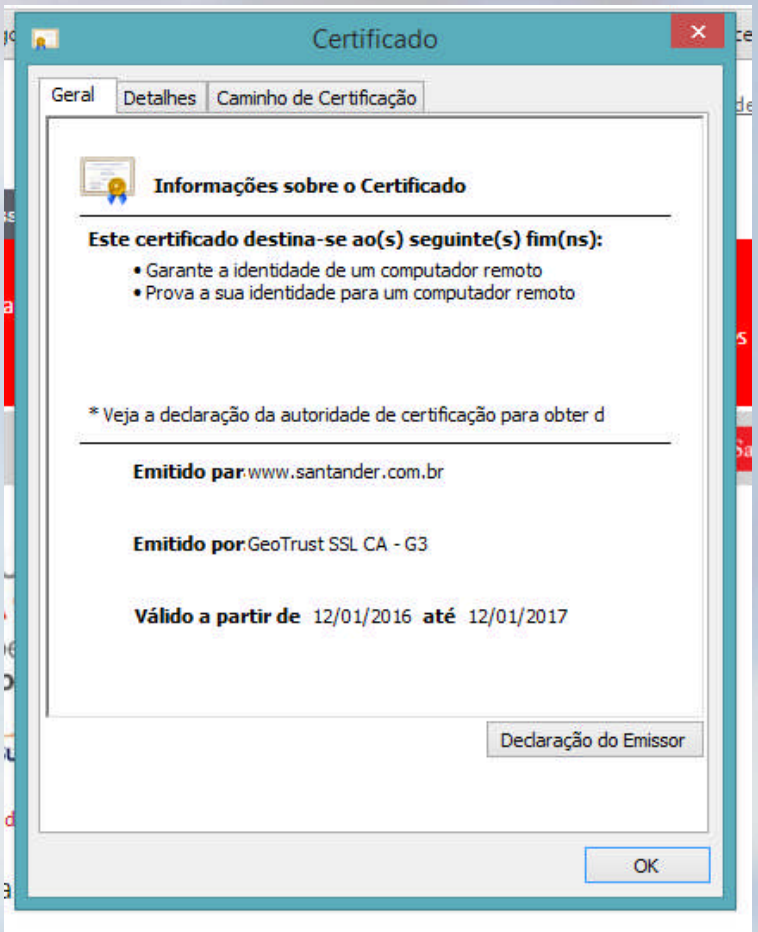


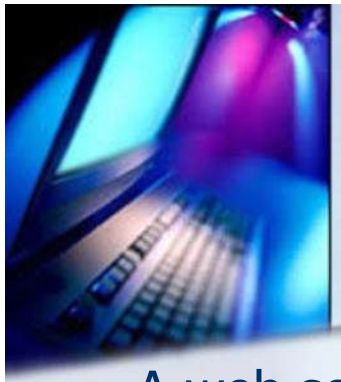
# Certificado Digital : a identificação na WEB

Ao clicarmos no cadeado podemos ver mais informações sobre HTTPS.

Repare que o SANTANDER possui uma identidade confirmada:





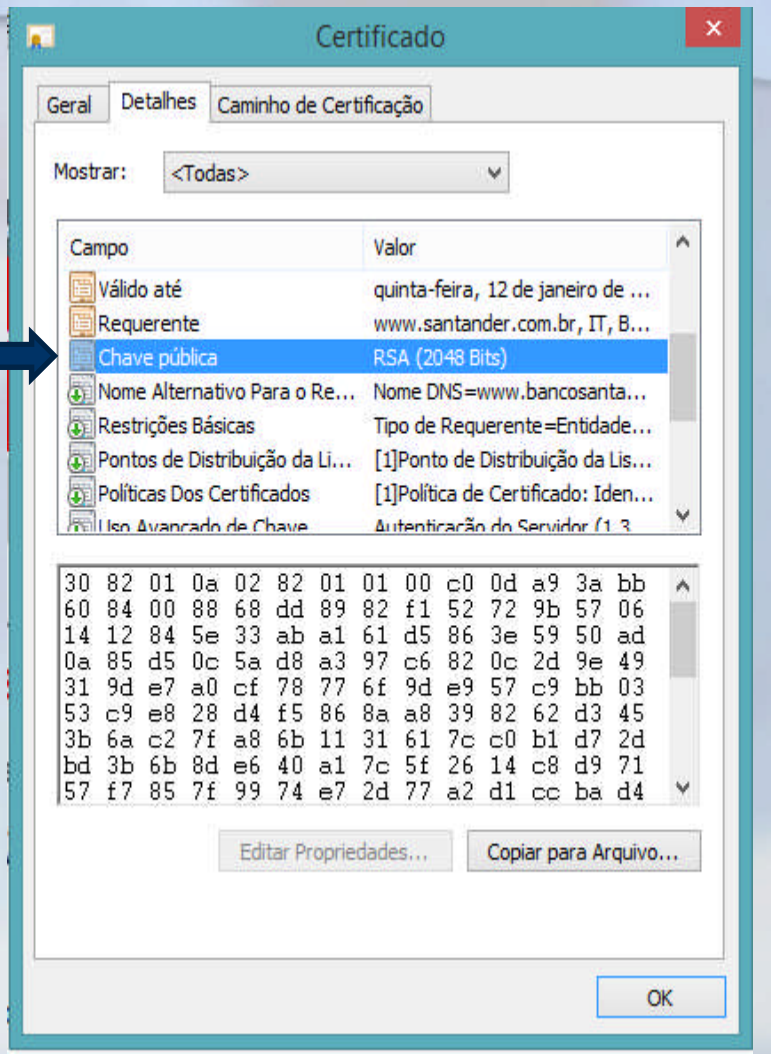
# Certificado Digital : a identificação na WEB

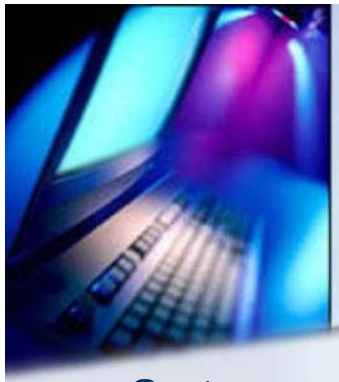
- A web segura trabalha bem parecida com a vida real.
- Uma pessoa possui uma identidade (RG ou Passaporte) para se identificar.
- Outras pessoas e organizações confiam nessa identidade, pois ela foi emitida por um órgão confiável.
- Se cada pessoa criasse o seu próprio RG não teríamos certeza da confiabilidade de seus dados e esta é a razão de solicitarmos o RG de um órgão especial do governo.
- Na web isso funciona bem parecido, só que a identidade é chamada de **certificado digital**.

UniFOA
Centro Universitário de Volta Redonda

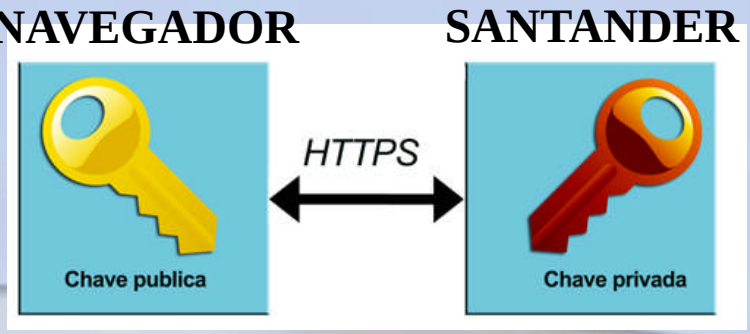
# Chave Pública

- Através do certificado o navegador consegue confirmar a identidade do site.
- No entanto, com isso não sabemos ainda como transmitir os dados de maneira segura.
- Para isso o certificado possui uma chave e essa chave é utilizada para criptografar os dados entre cliente e servidor. Ou seja, o certificado não só prova a identidade como também oferece uma chave para criptografar os dados!



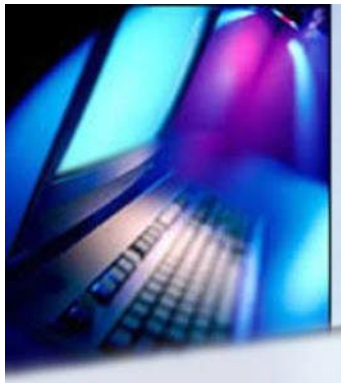


# Chave Privada




- Se tem uma chave pública tem que haver uma **chave privada**, certo? Mas cadê ela? Bom, a chave privada fica com o Santander. Jamais o servidor Santander pode oferecer essa chave para alguém, caso contrário toda comunicação se tornará insegura! Em geral, a chave publica é utilizada por qualquer um que queira se comunicar com Santander, pois faz parte do certificado. A chave privada só o Santander conhece, essa chave não é compartilhada com ninguém.
- Interessante é que os dados que foram criptografados com a chave pública só podem se descriptografados com a chave privada! As **chaves criam uma par** e devem ser utilizadas em conjunto (também chamadas de *chaves assimétricas*).
- O contrário também é verdadeiro: os dados criptografados com a chave privada só podem ser descriptografados pela chave pública. Ou seja, basta usar essa chave pública do certificado para enviar dados para o SANTANDER de maneira segura e teremos certeza que só SANTANDER pode ler estes dados!

UniFOA
Centro Universitário de Volta Redonda



# EXERCÍCIO

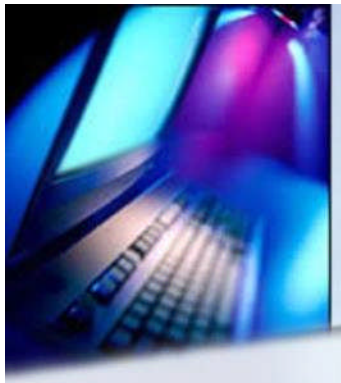
- **Enviando dados com HTTP**
- O que acontece com nossos dados quando usamos HTTP (sem s)?

(  ) - Os dados são criptografados para impedir a visualização por intermediários.

(  ) - Os dados são transportadores em texto puro para o servidor, visível para qualquer um.

(  ) - Usamos automaticamente um certificado digital para provar a identidade de um site.

UniFOA
Centro Universitário de Volta Redonda



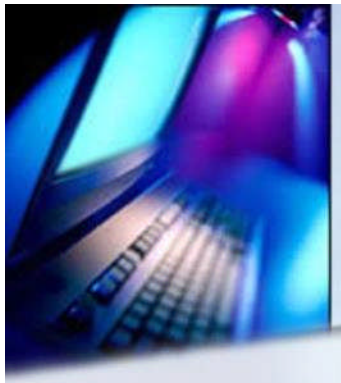
# RESPOSTA

- **Enviando dados com HTTP**
- O que acontece com nossos dados quando usamos HTTP (sem s)?

(  ) - Os dados são criptografados para impedir a visualização por intermediários.

( X ) - Os dados são transportadores em texto puro para o servidor, visível para qualquer um.

(  ) - Usamos automaticamente um certificado digital para provar a identidade de um site.



# EXERCÍCIO

- **Características do HTTPS**
- Qual das afirmações abaixo é **falsa**?

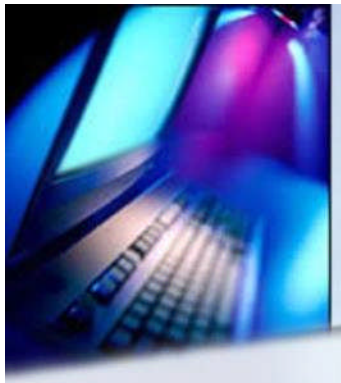
( ) - O certificado prova a identidade e tem validade.

( ) - HTTP significa usar um certificado digital do servidor.

( ) - O certificado guarda a chave pública.

( ) - A chave privada fica no lado do servidor apenas.

UniFOA
Centro Universitário de Volta Redonda



# EXERCÍCIO

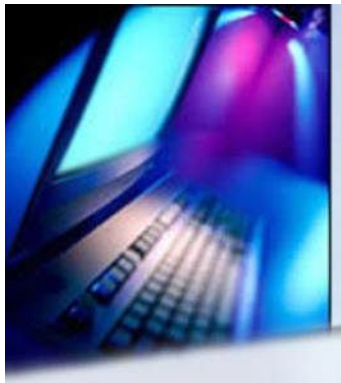
- **Características do HTTPS**
- Qual das afirmações abaixo é **falsa**?

( ) - O certificado prova a identidade e tem validade.

( x ) - HTTP significa usar um certificado digital do servidor.

( ) - HTTP significa usar um certificado digital do servidor.

( ) - A chave privada fica no lado do servidor apenas.



# EXERCÍCIO

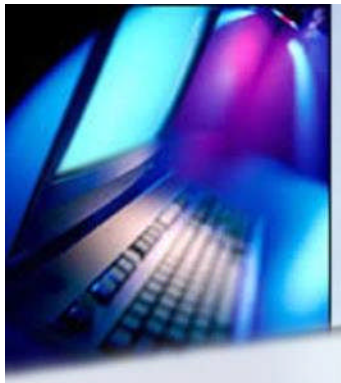
- **Autoridade certificadora**
- Qual o objetivo de uma *autoridade certificadora* ?

( ) - Importar/Exportar chaves publicas do servidor.

( ) - Garantir que podemos confiar naquele certificado (identidade).

( ) - Realizar a criptografia dos dados da requisição.

( ) - Usada para registrarmos nomes de domínio (DNS).



# RESPOSTA

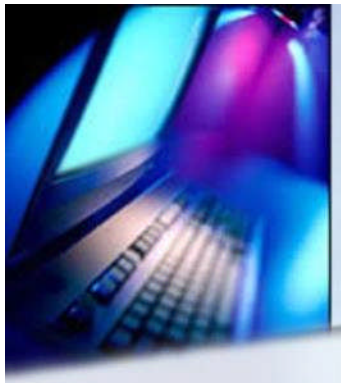
- **Autoridade certificadora**
- Qual o objetivo de uma *autoridade certificadora* ?

( ) - Importar/Exportar chaves publicas do servidor.

( X ) - Garantir que podemos confiar naquele certificado (identidade).

( ) - Realizar a criptografia dos dados da requisição.

( ) - Usada para registrarmos nomes de domínio (DNS).



# EXERCÍCIO

- **Faça uma busca na Internet e avalie as unidades certificadores dos seguintes sites.**

- **https://www.santander.com.br**
- **https://www.itau.com.br/**
- **https://www.google.com.br/**
- **https://www.microsoft.com/pt-br/**