Universidade Estadual de Londrina

KAUEE ROCHA PUERTAS

Segurança, TLS e Certificados Digitais

LONDRINA - PR
2023

Trabalho de Laboratório – 25/04/2023

Questão 01) Qual a função do protocolo TLS, apresente seu histórico, funções, camadas, em qual RFCs ele foi padronizado?

O protocolo TLS (Transport Layer Security) é uma tecnologia criptográfica que tem como principal função garantir a segurança da comunicação na internet. Ele foi projetado para proteger a integridade, autenticidade e confidencialidade dos dados transmitidos pela rede.

O TLS é o sucessor do protocolo SSL (Secure Sockets Layer) e foi desenvolvido em conjunto pela Netscape e pela Internet Engineering Task Force (IETF). A primeira versão do TLS foi publicada em 1999 e a versão atual é a TLS 1.3, que foi publicada em 2018.

O protocolo TLS é composto por duas camadas: a camada de Handshake e a camada Record. A camada de Handshake é responsável pela negociação dos parâmetros de segurança entre o cliente e o servidor, como a versão do TLS, os algoritmos de criptografia e autenticação, e a chave de sessão. Já a camada Record é responsável por encapsular os dados em pacotes criptografados antes de serem enviados pela rede.

Entre as principais funções do TLS, estão:

- Autenticação do servidor e, opcionalmente, do cliente
- Criptografia dos dados transmitidos entre o cliente e o servidor
- Garantia da integridade dos dados, impedindo que sejam alterados durante a transmissão
- Proteção contra ataques de replay, que consistem em retransmitir pacotes de dados antigos para tentar obter informações confidenciais

O TLS foi padronizado em diversas RFCs (Request for Comments) da IETF, incluindo:

- RFC 2246: TLS 1.0
- RFC 4346: TLS 1.1
- RFC 5246: TLS 1.2
- RFC 8446: TLS 1.3

As diferentes versões do TLS apresentam melhorias em relação às anteriores, como algoritmos mais seguros e eficientes e melhorias na negociação de parâmetros de segurança. O TLS é amplamente utilizado em aplicações que exigem segurança na transmissão de dados, como comércio eletrônico, serviços bancários online, correio eletrônico e outras aplicações web.

Questão 02) Qual a função de Certificados Digitais? Apresente seu histórico e funções.

Os certificados digitais são documentos eletrônicos que contêm informações de identificação de uma entidade, como uma pessoa, empresa ou servidor, e são usados para estabelecer a confiança na autenticidade e integridade das informações transmitidas pela Internet.

O uso de certificados digitais remonta aos anos 90, quando a necessidade de autenticação e criptografia de dados na Internet começou a se tornar mais evidente. O primeiro padrão para certificados digitais foi definido pela ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) em 1993, conhecido como X.509.

Os certificados digitais possuem algumas funções importantes, como:

- Autenticar a identidade de uma entidade: um certificado digital permite que uma entidade prove sua identidade para outras partes, estabelecendo a confiança necessária para a troca de informações.
- Proteger a privacidade: um certificado digital pode ser usado para criptografar dados, garantindo que somente o destinatário pretendido possa ler as informações.
- Garantir a integridade dos dados: ao assinar digitalmente um documento, um certificado digital assegura que o documento não foi alterado após a assinatura.

Os certificados digitais são emitidos por Autoridades Certificadoras (ACs), que são responsáveis por verificar a identidade da entidade que solicita o certificado e garantir que as informações contidas no certificado sejam precisas. A AC é uma terceira parte confiável que emite o certificado após verificar a identidade do titular, sendo a garantia de que o certificado é autêntico.

Os certificados digitais são amplamente utilizados em aplicações que exigem segurança na transmissão de dados, como comércio eletrônico, serviços bancários online, correio eletrônico e outras aplicações web. Eles permitem que os usuários confiem na autenticidade e integridade das informações transmitidas pela Internet, estabelecendo a base da confiança em transações eletrônicas.

Questão 03) Explique o padrão ITU X.509.

O ITU X.509 é um padrão internacional para certificados digitais emitidos por Autoridades Certificadoras (ACs). Ele define o formato de um certificado digital, as informações que devem ser incluídas no certificado e os procedimentos para verificar a autenticidade do certificado.

O certificado X.509 é um documento eletrônico que contém informações sobre a entidade que o detém, como nome, endereço, e-mail, número de identificação, entre outras informações relevantes. O certificado também contém a chave pública da entidade e uma assinatura digital da AC que emitiu o certificado.

A assinatura digital da AC garante a autenticidade do certificado, pois a AC é uma terceira parte confiável que verifica a identidade do titular do certificado e garante que as informações contidas no certificado são precisas. A AC usa sua própria chave privada para assinar o certificado, e essa assinatura é verificada usando a chave pública da AC, que é amplamente divulgada.

O padrão X.509 também define os procedimentos para verificar a autenticidade do certificado. Isso é feito por meio de uma cadeia de confiança, na qual um certificado é verificado por sua AC emissora e assim por diante, até chegar a uma AC de confiança (root). Uma AC de confiança é uma AC que é amplamente reconhecida como confiável, como as ACs de governo e as ACs de empresas especializadas em segurança da informação.

Em resumo, o padrão ITU X.509 define o formato de certificados digitais, as informações que devem ser incluídas neles, os procedimentos para sua emissão e verificação, e estabelece uma cadeia de confiança para garantir a autenticidade e a integridade das informações transmitidas pela Internet.

Questão 04) Quais são os campos do padrão X.509 para certificados digitais?

O padrão X.509 define um conjunto de campos que devem ser incluídos em um certificado digital. Esses campos são divididos em duas categorias principais: informações sobre o titular do certificado e informações sobre a AC emissora. Abaixo estão os principais campos definidos pelo padrão X.509:

Informações sobre o titular do certificado:

- Nome completo: nome completo da pessoa ou entidade que detém o certificado.
- Endereço: endereço físico da pessoa ou entidade que detém o certificado.
- Endereço de e-mail: endereço de e-mail da pessoa ou entidade que detém o certificado.
- Número de identificação: número de identificação da pessoa ou entidade que detém o certificado, como o número de CPF ou CNPJ.
- Chave pública: chave pública associada ao certificado.
- Período de validade: período de tempo durante o qual o certificado é válido.

Informações sobre a AC emissora:

- Nome da AC: nome da AC que emitiu o certificado.
- Endereço da AC: endereço físico da AC que emitiu o certificado.
- Endereço de e-mail da AC: endereço de e-mail da AC que emitiu o certificado.
- Chave pública da AC: chave pública da AC que emitiu o certificado.
- Assinatura da AC: assinatura digital da AC que emitiu o certificado.

Existem outros campos que podem ser incluídos em um certificado digital, dependendo do uso específico do certificado e dos requisitos de segurança da aplicação. No entanto, os campos acima são os principais definidos pelo padrão X.509 e são comumente encontrados em certificados digitais utilizados na Internet.

Questão 05) Explique o que é uma autoridade certificadora?

Uma Autoridade Certificadora (AC) é uma entidade confiável responsável por emitir e gerenciar certificados digitais. Certificados digitais são arquivos eletrônicos que contêm informações sobre a identidade de uma entidade (como um indivíduo, uma organização ou um dispositivo) e são usados para estabelecer conexões seguras pela Internet.

A AC é responsável por verificar a identidade da entidade que solicita um certificado digital, garantindo que as informações contidas no certificado sejam precisas e confiáveis. A AC usa técnicas de criptografia para proteger as informações contidas no certificado e, em seguida, emite o certificado digital para a entidade solicitante. O certificado digital é usado para estabelecer conexões seguras pela Internet, como por exemplo em transações financeiras, compras online, e-mails seguros, acesso a sistemas de informação, entre outros.

Questão 06) O que é ICP Brasil?

ICP-Brasil é a Infraestrutura de Chaves Públicas Brasileira, um conjunto de normas e procedimentos que regulam a emissão e a validação de certificados digitais no Brasil. Criada em 2001, a ICP-Brasil é responsável por garantir a autenticidade, integridade e confidencialidade dos dados que são transmitidos eletronicamente.

A ICP-Brasil estabelece os requisitos técnicos e legais que as Autoridades Certificadoras (ACs) devem atender para emitir certificados digitais válidos. Além disso, a ICP-Brasil é responsável por manter um diretório público com informações sobre todas as ACs e seus certificados emitidos.

Os certificados digitais emitidos pela ICP-Brasil são utilizados em diversas aplicações, como por exemplo em transações eletrônicas seguras, assinaturas digitais, envio de e-mails criptografados, acesso a sistemas de informação restritos, entre outros. O uso de certificados digitais emitidos pela ICP-Brasil é obrigatório em algumas situações, como por exemplo na emissão de notas fiscais eletrônicas.

Em resumo, a ICP-Brasil é responsável por garantir a segurança e a confiabilidade das transações eletrônicas no Brasil, por meio da regulamentação da emissão e validação de certificados digitais.

Questão 07) Como obter gratuitamente/comprar um certificado digital?

Existem diversas Autoridades Certificadoras (ACs) no Brasil que emitem certificados digitais, tanto para pessoas físicas como para empresas. Para obter um certificado digital, é necessário seguir os seguintes passos:

- Escolher uma AC.
- Identificação.
- Preencher formulário.
- Pagar a taxa.
- Instalar o certificado.

É importante lembrar que a obtenção de um certificado digital pode variar de acordo com a AC escolhida e o tipo de certificado desejado. Alguns tipos de certificados digitais, como os usados para assinatura digital, requerem validação presencial e, portanto, não podem ser emitidos de forma totalmente online.

Além disso, algumas instituições, como a Receita Federal, oferecem gratuitamente o Certificado Digital para acesso ao sistema de declaração de imposto de renda.

Questão 08) O que é Assinatura Digital?

Assinatura digital é uma técnica que utiliza criptografia para garantir a autenticidade e a integridade de documentos eletrônicos. A assinatura digital é uma forma de garantir que um documento eletrônico não foi alterado e que a pessoa que o assinou é realmente quem diz ser.

Para criar uma assinatura digital, é necessário usar um certificado digital emitido por uma Autoridade Certificadora (AC). O certificado digital contém informações sobre a identidade da pessoa ou empresa que o possui e é usado para gerar uma chave criptográfica que será usada para assinar o documento eletrônico.

Ao assinar um documento eletrônico com uma assinatura digital, é gerado um hash (um código numérico que representa o conteúdo do documento) que é criptografado com a chave privada do certificado digital. Esse hash criptografado é adicionado ao documento eletrônico, formando assim a assinatura digital. Qualquer alteração no documento eletrônico após a assinatura será detectada, pois o hash criptografado não corresponderá mais ao conteúdo atual do documento.

REFERÊNCIAS

https://www.gta.ufrj.br/grad/06_1/ssl/func_tls.htm

https://www.infowester.com/assincertdigital.php

https://pt.theastrologypage.com/x-509

https://tecnoblog.net/responde/o-que-e-uma-assinatura-digital/