Questão 1.1:

TLS is an encryption protocol designed to secure Internet communications. A TLS handshake is the process that kicks off a communication session that uses TLS encryption. During a TLS handshake, the two communicating sides exchange messages to acknowledge each other, verify each other, establish the encryption algorithms they will use, and agree on session keys. TLS handshakes are a foundational part of how HTTPS works.

Na autenticação do servidor é utilizado um esquema de chaves públicas nomeadamente um esquema de assinatura digital. Não poderia ser substituído por um MAC, devido ao problema de non repudiation em que o emissor não consegue confirmar que foi o mesmo quem mandou a mensagem o que faz com que a autenticação seja impossível.

Questão 1.2:

São as chaves de longo termo que tornam possível a desencriptação da chaves de sessão e posteriormente de todas as mensagens trocadas

How to get them

o A client or server being attacked by some other attack vector, and

the private key retrieved.

o A long-term key retrieved from a device that has been sold or

otherwise decommissioned without prior wiping.

o A long-term key used on a device as a default key [Heninger2012].

o A key generated by a trusted third party like a CA, and later

retrieved from it either by extortion or compromise

[Soghoian2011].

o A cryptographic break-through, or the use of asymmetric keys with

insufficient length [Kleinjung2010].

o Social engineering attacks against system administrators.

* Collection of private keys from inadequately protected backups.

Questão 2

O Salt é uma string de 8 bits gerada aleatoriamente e é usado para proteger as senhas no seu armazenamento, pois permite a defesa contra ataques de dicionário.

A salt in password-based cryptography has traditionally served the

purpose of producing a large set of keys corresponding to a given

password, one of which is selected at random according to the salt.

An individual key in the set is selected by applying a key derivation

function KDF, as

DK = KDF (P, S)

where DK is the derived key, P is the password, and S is the salt.

This has two benefits:

1. It is difficult for an opponent to precompute all the keys, or

even the most likely keys, corresponding to a dictionary of

passwords. If the salt is 64 bits long, for instance, there

will be as many as 2^64 keys for each password. An opponent

is thus limited to searching for passwords after a password-

based operation has been performed and the salt is known.

2. It is unlikely that the same key will be selected twice.

Again, if the salt is 64 bits long, the chance of "collision"

between keys does not become significant until about 2^32 keys

have been produced, according to the Birthday Paradox. The

fact that collisions are unlikely addresses some concerns

about interactions between multiple uses of the same key that

may arise when using some encryption and authentication

techniques.

In password-based encryption, the party encrypting a message can gain

assurance that these benefits are realized simply by selecting a

large and sufficiently random salt when deriving an encryption key

from a password. A party generating a message authentication code

can gain such assurance in a similar fashion.

Questão 3

Questão 4.1

O objetivo do parâmetro scope é de limitar o acesso da aplicação aos dados do utilizador, para isso é apresentado um ecrã onde o utilizador tem de dar o seu consentimento para a aplicação utilizar os seus dados.

Questão 4.2

O cliente\_id é o identificador do utilizador para a aplicação. É um código único e é suposto ser difícil descobrir este identificador. Ao contrário do client\_id que é um identificador público, o cliente\_secret é um identificador secreto que só a aplicação conhece.

Desta forma podemos concluir que o client\_id é possível ser descoberto pelo atacante, mas no entanto, o client\_secret não tem estas propriedade.

Questão 4.3

Não.

Questão 5

O id\_token é usado para guardar em cache informações acerca do perfil do cliente (claims) e disponibilizá-las para as aplicações permitindo uma melhor performance.