* 2.1

O protocolo handshake impede que o S1 se autentique como C porque S1 apenas tem a chave pública de C que o possibilita a verificar se o certificado que foi enviado foi assinado por C, no entanto, não o deixa forjar a assinatura digital do cliente C. Assim sendo, como S1 não tem a chave privada de C não se consegue fazer passar pelo mesmo.

* 2.2

São usadas assinaturas digitais no contexto de TLS/SSL com o objetivo de autenticar clientes em servidores e de ao mesmo tempo os proteger contra roubo de “identidade” visto que a assinatura digital é efetuada com a chave privada de cada cliente mas a verificação é feita com a chave pública o que dificulta bastante a ocorrência de assinaturas forjadas.

* 3.1

O salt pode ser guardado em texto em claro, visto que todo o seu objetivo é prevenir a pré-computação do hash que permite aceder aos dados privados de cada utilizador.

* 4.2

Ele não se autentica visto que já pediu ao utilizador para se autenticar antes e este lhe enviou um código de autenticação que comprova o seu consentimento no pedido aos recursos.

* 4.3

O grande problema dos bearer tokens está no facto de estes conterem informações privadas que no caso de serem acedidos por terceiros podem ser usados para obter recursos protegidos. Daí que os principais problemas se prendem com o envio destes tokens e a segurança dos canais em que são transmitidos, bem como os sítios onde são armazenados.