Segurança Informática

Fábio Parreirinha Nº39329 Tejal Amratlal Nº40605

Índice

Questão 1

1.1

O material criptográfico que tem de ser configurado do lado do cliente caso seja necessária autenticação de cliente e servidor usando o protocolo TLS é o certificado do cliente. Na autenticação do cliente o servidor usa a chave publica existente no certificado do cliente para decifrar a informação que foi enviada anteriormente. Na Figura 1 podemos observar o esquema de autenticação do protocolo Handshake que mostra o envio e verificação do protocolo nos pontos 4 e 5 com o envio da chave publica existente no certificado e o próprio certificado no ponto 5.

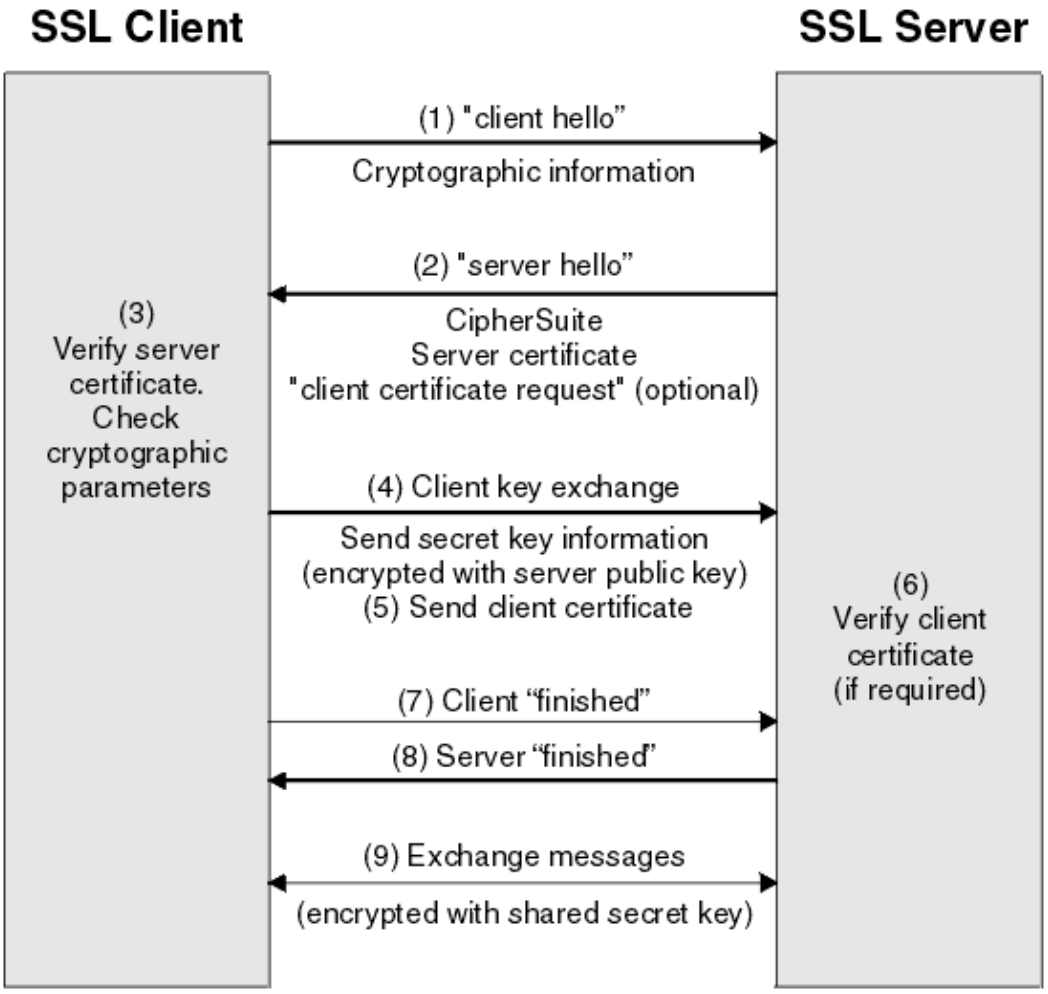

FIGURA 1 - ESQUEMA HANDSHAKE

Fábio Parreirinha Nº39329 Tejal Amratlal Nº40605

1.2

O esquema simétrico utilizado no Handshake do TLS é o MAC. O TLS, mais concretamente o Record Protocol utiliza o MAC como forma de autenticação da informação enviada através de um canal TCP. O Record protol trata da fragmentação, compressão, confidencialidade e autenticidade das mensagens enviadas usando o MAC para este último aspecto.

1.3

A característica que torna o record protocol vulnerável ao ataque de Vaudenay é o downgrade de versões do SSL através do POODLE attack (Padding Oracle On Downgraded Legacy Encryption). Este ataque tira partido da negociação de versões do protocolo do SSL, entre o cliente e o servidor, para forçar o uso da versão 3.0 que é vulnerável ao ataque de Vaudenay. Existe uma vulnerabilidade a um ataque Man-In-The-Middle na versão 3.0 deste protocolo que use o modo CBC.

Este ataque tira partido do facto de que quando uma ligação segura falha os servidores realizam um downgrade de versões para tentar manter compatibilidade com o máximo de utilizadores possíveis.

Questão 2

2.1

O cliente acede ao recurso especificando o Acess Token ao resource server que contem o recurso. O resource server terá de validar este token e conferir a sua validade.

Um exemplo de um pedido de um relying party a um recurso é:

GET /resource/1 HTTP /1.1
Host: exemplo.pt
Authorization: Bearer SlAV32hkKG

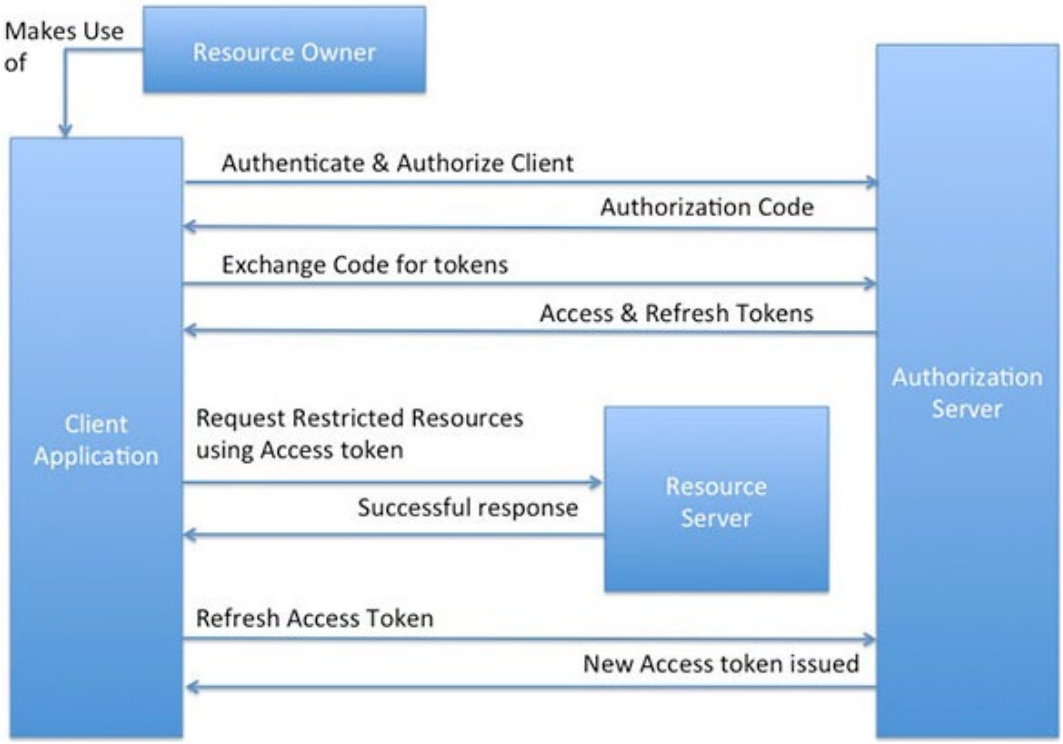

FIGURA 2 - PEDIDO ACESSO A RECURSO

2.2

Questão 3

3.1

O ID Token é um token de segurança que contém informação de autenticação de um cliente que se pretende autenticar num Identity Provider. O ID Token tem como propósito servir de base para gerar um autenticador para um utilizador que faz um pedido de autenticação para acesso a recursos. Este ID Token não é utilizado directamente para autenticação, mas sim o autenticador gerado por si.

3.2

A entidade que desempenha o papel de relying party é a aplicação cliente, pois é esta que trata dos redireccionamentos dos pedidos de autorização entre o browser e o Identity Provider (IP). A Figura 3 mostra o fluxo do OpenID Connect onde podemos observar a aplicação cliente que trata de desencadear o pedido de autenticação entre o utilizador e o IP.

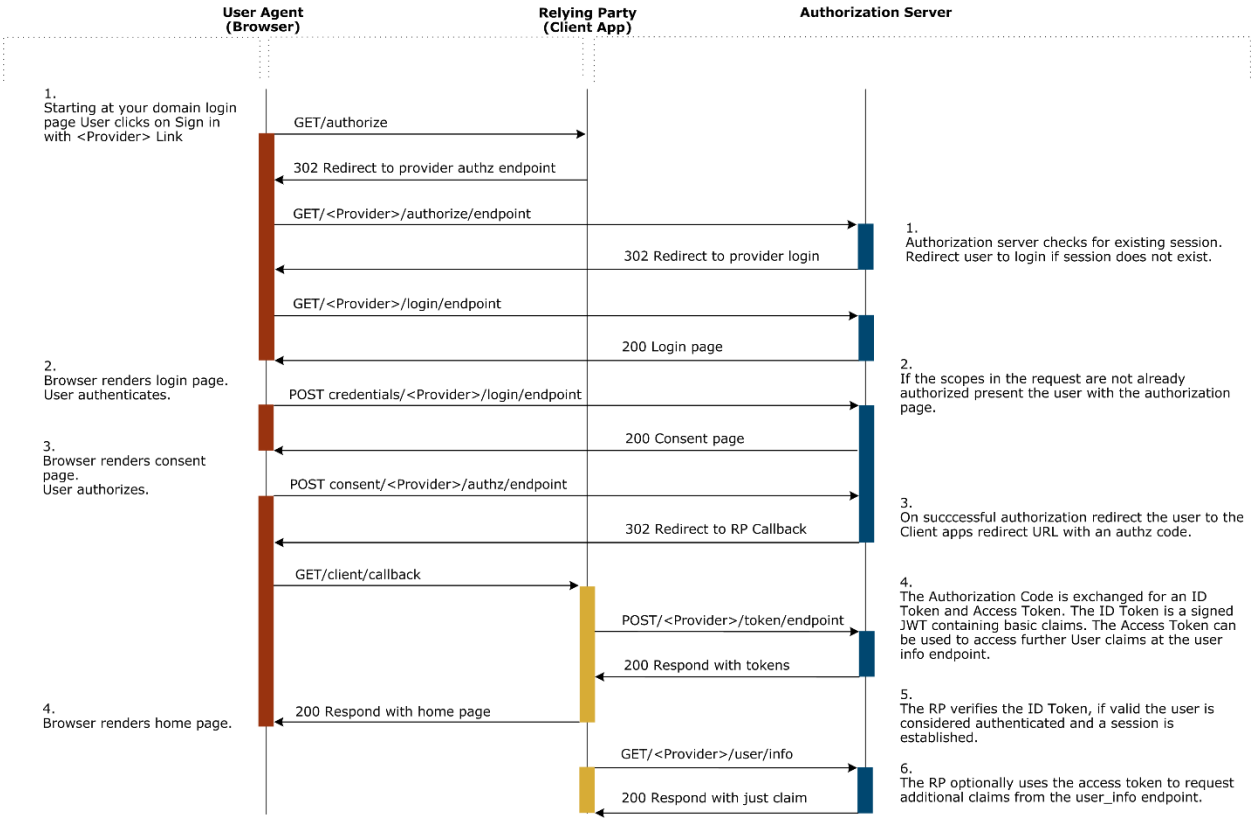

FIGURA 3 - OPENID CONNECT FLOW

Fábio Parreirinha Nº39329 Tejal Amratlal Nº40605

Questão 5

Código em anexo.

Questão 6

Código em anexo.

O código entregue apresenta duas lacunas relativamente ao pretendido:

1. Não faz a verificação da assinatura no final da desencriptação.
2. Na desencriptação no método *doFinal()* existe um problema com o *padding* dando excepção.

Questão 7

Código em anexo. Não foi possível cumprir com o objectivo proposto.

Bibliografia

IBM - Security concepts and mechanisms. Disponível em
<**Erro! A referência da hiperligação não é válida.**https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10630_.htm> acesso em: novembro 2018

OAuth 2.0 - The Good, The Bad & The Ugly. Disponível em:
<https://code.tutsplus.com/articles/oauth-20-the-good-the-bad-the-ugly--net-33216> acesso em: novembro 2018

OpenID Connect flow. OpenID Connect flow
<https://docs.axway.com/bundle/APIGateway_762_OAuthUserGuide_allOS_en_HTML5/page/Content/OAuthGuideTopics/OpenidImport/openid_flow.htm> acesso em: novembro 2018