Tech-invite

http://www.tech-invite.com

SSL Time-Diagram

First Variant: Generation of a Temporary 512-bit RSA Key

V1.0 – March 2, 2005

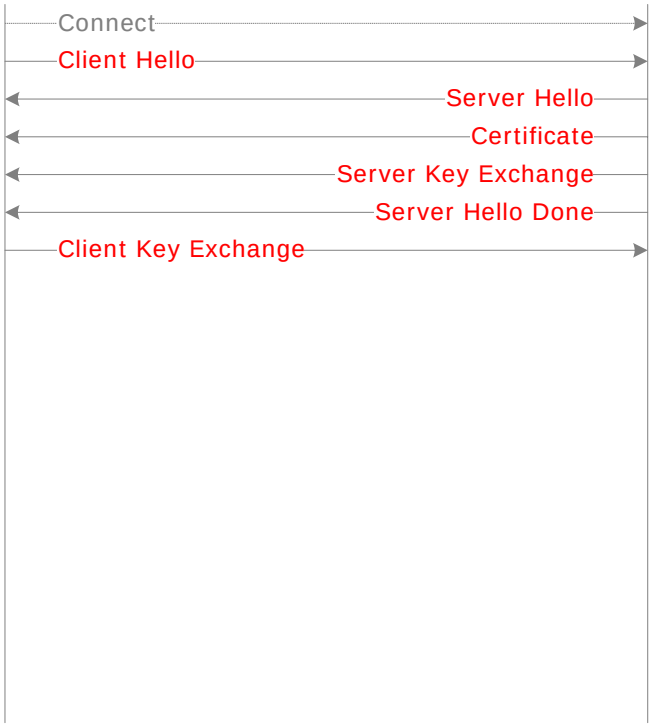
This document provides a detailed description of the sequence of first exchanges between an SSL Client and an SSL Server. This is the first variant to the main scenario described in another document. It reflects an Export situation entailing the generation of a temporary 512-bit RSA key for enabling the transport of the pre-master key.

The type of encryption algorithm used is "block cipher" in CBC mode, with this scenario.

Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

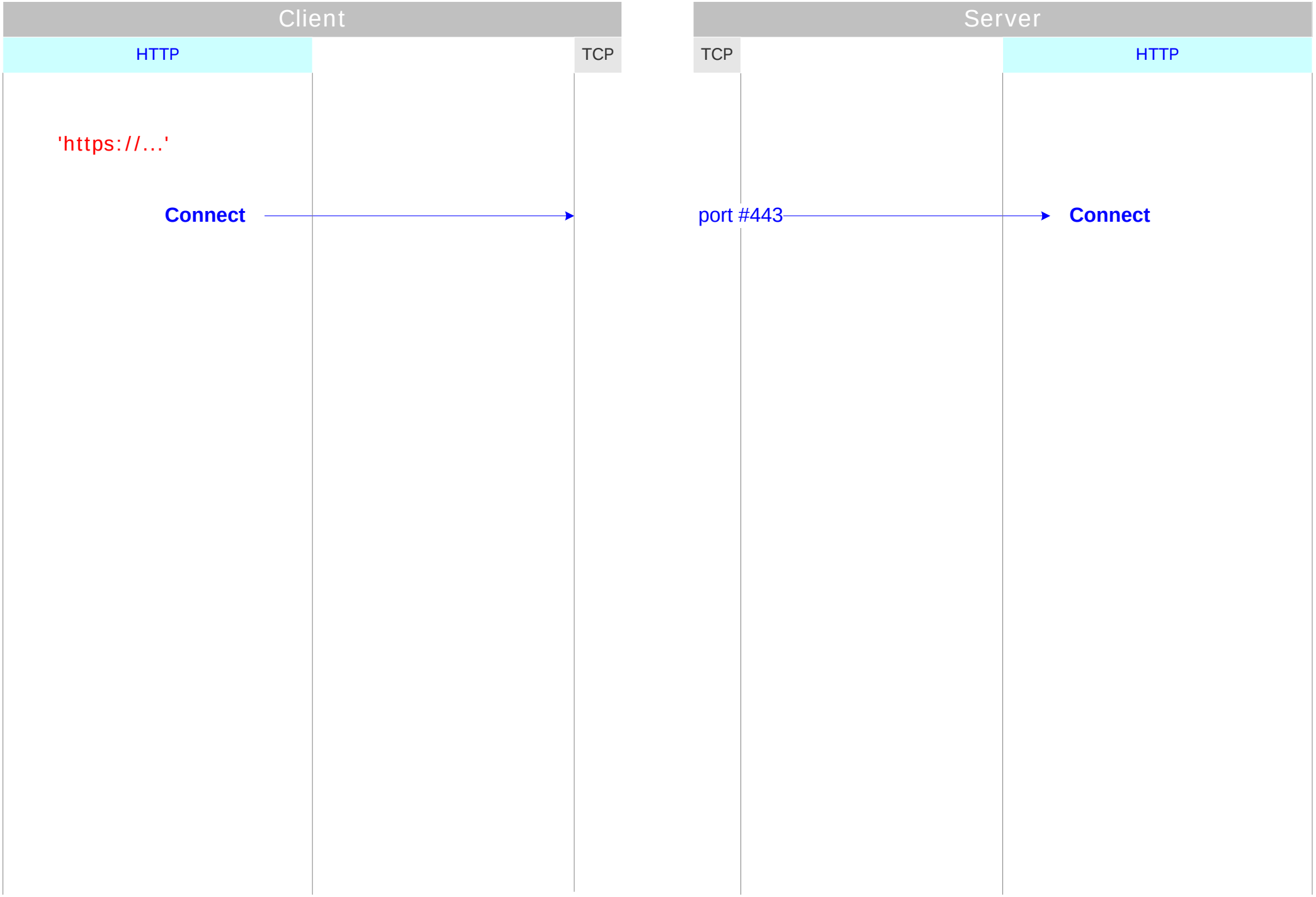
7 pages

Summary of Exchanges



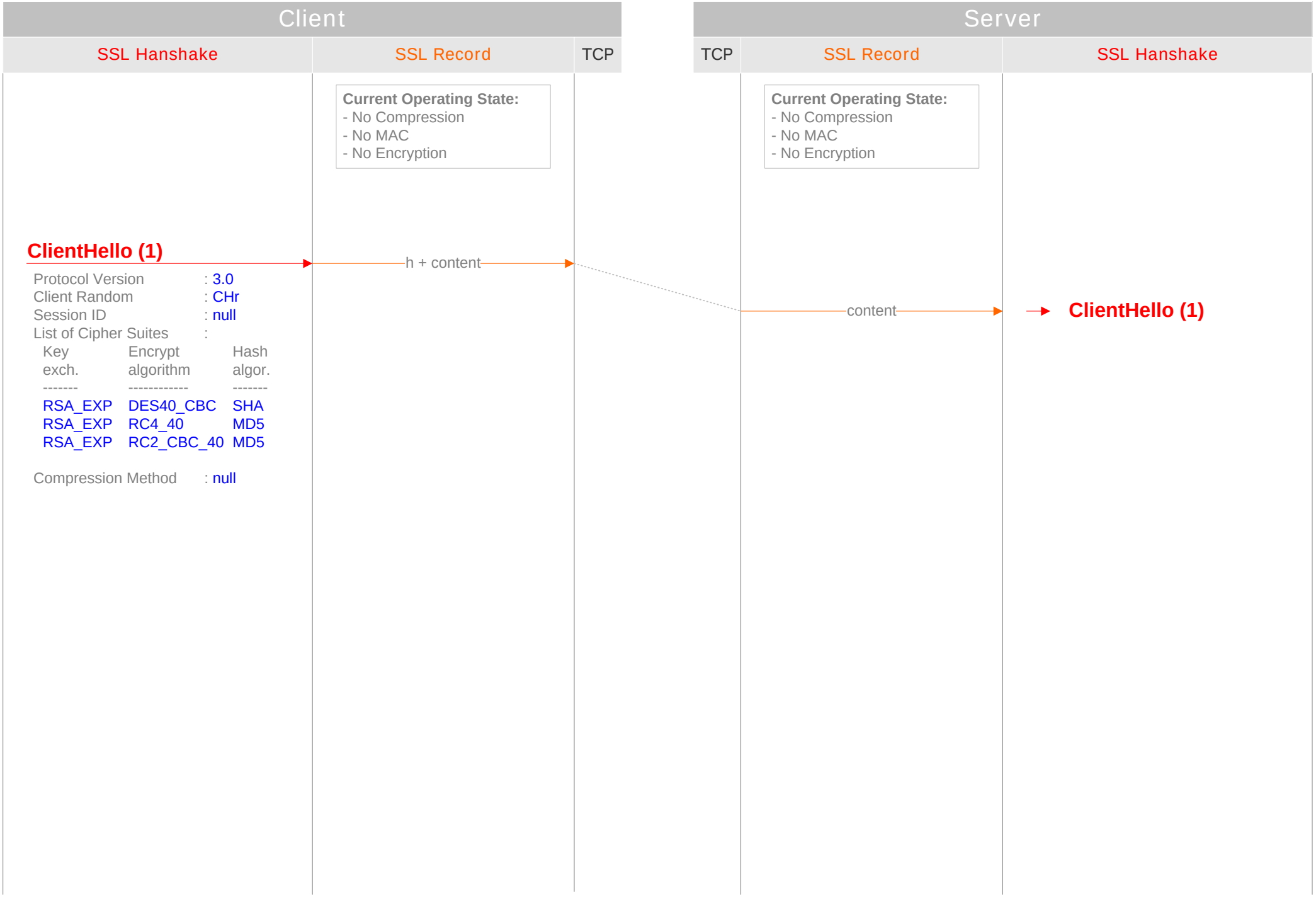
Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

(1) Export Situation – TCP Connection



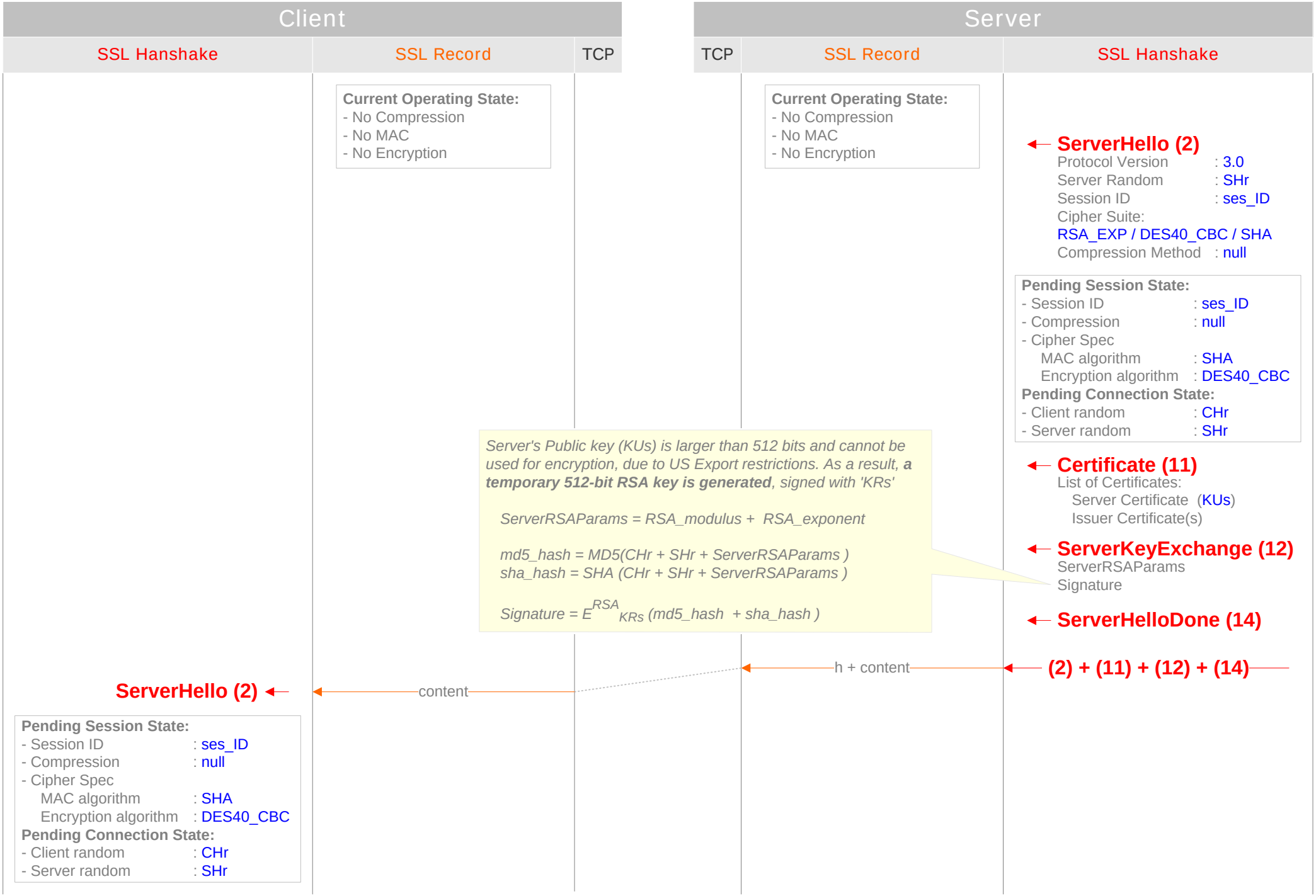
Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

(2) Export Situation – Client Hello



Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

(3) Export Situation – Server Hello & Server Key Exchange



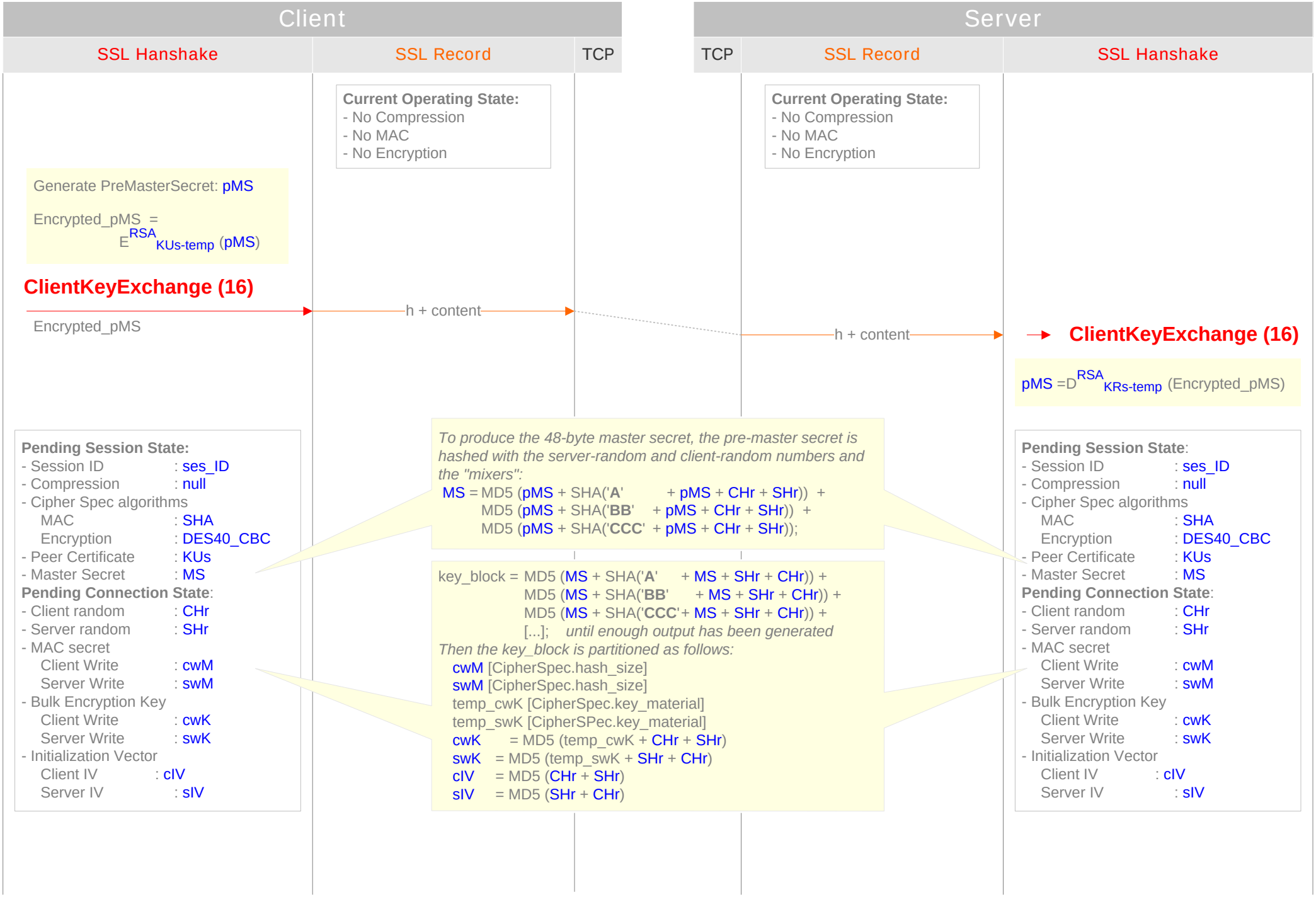
Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

(4) Export Situation – Authentication of Temporary RSA Key

Client				Server	
SSL Hanshake	SSL Record	TCP	TCP	SSL Record	SSL Hanshake
	Current Operating State: - No Compression - No MAC - No Encryption			**Current Operating State:** - No Compression - No MAC - No Encryption	
Certificate (11) ←					
Validate Server's Certificate: KUs					
Pending Session State: - Session ID : ses_ID - Compression : null - Cipher Spec MAC algorithm : SHA Encryption algorithm : DES40_CBC - Peer Certificate : KUs **Pending Connection State:** - Client random : CHr - Server random : SHr					
ServerKeyExchange (12) ←					
Check "KUs-temp" signature with KUs					
ServerHelloDone (14) ←					

Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.

(5) Export Situation – Transport of Encrypted PreMasterKey



Copyright © 2005-2007 Tech-invite.com Joël Repiquet. All Rights Reserved.