Réseaux et technologie Internet

# Les travaux de l'évaluation 6 : client-serveur sécurisé en Java et complément caddie virtuel en Java

|  |  |
| --- | --- |
| Nom de la fonction | But de la fonction |
| traiterConnect(Socket, ConsoleServeur ,PublicKey) | Recevoir digest, valider l’utilisateur en envoyant la liste des vols, envoi clé publique et effectuer handshake |
| Handshake (Socket) | Réception de deux clés : HMAC et clé symétrique |
| AchatTickets(Socket, ConsoleServeur) | Réserve le vol pour l’utilisateur |
| Confirm(Socket, ConsoleServeur) | Signale que le paiement a été effectué |

# Explication du contenu des différents keystores

Le différents keystore sont :

|  |  |
| --- | --- |
| Keystore | Type de chiffrement |
| Serveur\_Payment | RSA (certificat) |
| Tour\_Operator | RSA (certificat) |
| Vince | DES |
| Thibauth | DES |
| Serverweb | RSA (certificat) |
| Thib | DES |
| Vinceauth | DES |
| Serveur | RSA (certificat) |

# Diagramme du handshake pour l'échange des clés publiques

