Pour qu’un serveur WS puisse envoyer des informations au serveur AS, il faut qu’il obtienne une clef symétrique :

* WS envoie à AS :
  + Non crypté : son identifiant (‘WS1’ par exemple)
  + Crypté (RSA avec clef publique AS) : son identifiant (‘WS1’ par exemple), avec un nombre aléatoire appelé « nonce » r1.
* AS envoie à WS :
  + Crypté (RSA avec clef publique WS) : son identifiant (‘AS’ par exemple), avec le nombre r1 reçu juste avant, ainsi qu’un nouveau nombre aléatoire r2.
* WS envoie à AS :
  + Non crypté : le nombre aléatoire r2.
* AS envoie à WS :
  + Crypté (RSA avec clef publique WS) : une clef symétrique venant d’être générée et valide durant un temps t, avec le nonce r1.
* WS et AS peuvent désormais communiquer avec la clef de session.

Les utilisateurs (qui sont déjà dans la bdd) exécutent le protocole suivant pour avoir accès à un WS :

* Client envoie à AS :
  + Non crypté : son identifiant de client et l’identifiant du serveur WS auquel il veut accepter (par exemple ‘WS1’)
  + Crypté (RSA avec clef publique AS) : son identifiant de client, l’identifiant du serveur WS auquel il veut accepter, et un nonce r3.
* AS envoie à Client :
  + Crypté (RSA avec clef publique Client) : son identifiant (‘AS’ par exemple), l’identifiant du serveur WS auquel le client veut se connecter, le nonce r3 et un nonce r4.
* Client envoie à AS :
  + Non crypté : le nonce r4.
* AS envoie à Client :
  + Crypté (RSA avec clef publique client) : une clef symétrique venant d’être générée et valide durant un temps t donné (transmettre ce temps t), avec le nonce r3.
* AS envoie à WS :
  + Non crypté : son identifiant (‘AS’ par exemple)
  + Crypté (avec clef symétrique obtenue grâce au protocole ci-dessus WS-AS) : l’identifiant du client, la clef symétrique qui vient d’être générée pour lui et le temps t pendant lequel elle est valide. (fin du protocole)
* Client envoie à WS :
  + Non crypté : l’identifiant du client
  + Crypté (avec clef symétrique du client-WS) : la request
* WS envoie à client :
  + Crypté avec la clef symétrique : la réponse à la demande du service.