Infos sur le serveur :

domain et port ⇒ pdp-evernet.ddns.net:50000

Dictionnaire:

-alias = Pseudo
-certificat = objet pour obtenir la clef public
-private key = la clé privé
-password = le mot de passe
-phoneNum = le numéro de téléphone (10 chiffres ou +33 suivi de 9 chiffres)
-invitation_key = clef d'invitation nécessaire pour rejoindre le réseau (s'authentifier sur le serveur) obtenable via la commande get_invitation_key (accessible que au personne authentifié sur le serveur)
-n_numbers = le nombre de numéros que l'utilisateur veut recevoir

Elément séparateur (pôtô) entre données transmises : "_|_"

Vous pouvez split les données reçues avec ce séparateur.

Elément de début de communication serveur/client et client/serveur : "BEGIN_COMMUNICATION"

Elément de fin de communication serveur/client et client/serveur : "END_COMMUNICATION"

Vous recevrez donc des message depuis le serveur de la forme :
..._|_BEGIN_COMMUNICATION_|_……..._|_END_COMMUNICATION
Tout ce qui est avant _|_BEGIN_COMMUNICATION_|_ est considéré comme parasite et ne doit pas être considéré

Lors de chaque ouverture de socket avec le serveur, il vous enverra : "BEGIN_COMMUNICATION_|_You are connected._|_END_COMMUNICATION" pour acquiescer la connexion.

Toujours envoyer la requête “_|_BEGIN_COMMUNICATION_|_FIN_|_END_COMMUNICATION” pour faire la poignée de main de fermeture du socket

Requête au serveur possible:

- “**getPhoneNum**_|_*alias*”
  - description : retourne le numéro et le certificat correspondant à *alias*
  - format de retour : _|_BEGIN_COMMUNICATION_|_*numéro*_|_*certificat*_|_END_COMMUNICATION
  - format de retour d’erreur :
    - si non authentifié/connecté via signIn ou logIn : "_|_BEGIN_COMMUNICATION_|_ERROR 2_|_Permission denied!_|_END_COMMUNICATION"

- “**signIn**_|_*alias*_|_*password*_|_*phoneNum*_|_*invitation Key*”
  - decription : s’authentifier sur le réseau la première fois
  - Format de retour: _|_BEGIN_COMMUNICATION_|_*certificat_client*_|_*private_key_client*_|_*certificat_serveur*_|_END_COMMUNICATION
  - format de retour d’erreur :
    - si mauvais formatage de la requête (trop ou pas assez d’ arguments) : "_|_BEGIN_COMMUNICATION_|_ERROR 3_|_Wrong input format: signIn *alias* *password* *phoneNum* *invitationKey*_|_END_COMMUNICATION"
    - si déjà log (via signIn ou logIn) : "_|_BEGIN_COMMUNICATION_|_ERROR 1_|_Already logged my friend!_|_END_COMMUNICATION"
    - si alias déjà existant : “_|_BEGIN_COMMUNICATION_|_ERROR 5_|_Alias already exists_|_END_COMMUNICATION”
    - si Numéro déjà existant : “_|_BEGIN_COMMUNICATION_|_ERROR 5_|_Number already exists_|_END_COMMUNICATION”
    - si erreur format numéro de téléphone : “_|_BEGIN_COMMUNICATION_|_ERROR 3_|_Number format incorrect_|_END_COMMUNICATION”
    - si l’”invitation key” est incorrect : “_|_BEGIN_COMMUNICATION_|_ERROR 8_|_Wrong invitation key_|_END_COMMUNICATION”

- “**logIn**_|_*alias*_|_*password*”
    - description : se connecter sur le réseau (déjà authentifié)
    - format de retour : "_|_BEGIN_COMMUNICATION_|_Authentified_|_END_COMMUNICATION"
    - format de retour d’erreur :
        - si déjà log (via signIn ou logIn) : "_|_BEGIN_COMMUNICATION_|_ERROR 1_|_Already logged my friend!_|_END_COMMUNICATION"
        - si mauvais formatage de la requête : "_|_BEGIN_COMMUNICATION_|_ERROR 3_|_Wrong input format: logIn *alias* *password*_|_END_COMMUNICATION"
        - si mauvais alias ou mot de passe : “ERROR 4_|_Wrong alias or password_|_END_COMMUNICATION”

- “**getPhoneNumList**_|_*n_numbers*”
    - description : retourne une liste de numéros intermédiaires (random) ainsi que leur certificat (duquel est extrait la clef publique) associé.
    - format de retour : “_|_BEGIN_COMMUNICATION_|_*phoneNum1*_|_*certif1*_|_*phoneNum2*_|_*certif2*..._|_END_COMMUNICATION”
    - format de retour d’erreur :
        - si non authentifié/connecté via signIn ou logIn : "_|_BEGIN_COMMUNICATION_|_ERROR 2_|_Permission denied!_|_END_COMMUNICATION"
        - si mauvais formatage de la requête : "_|_BEGIN_COMMUNICATION_|_ERROR 3_|_Wrong input format: getPhoneNumList *n_numbers*_|_END_COMMUNICATION"
        - si la base de donnée est vide : "_|_BEGIN_COMMUNICATION_|_ERROR 7_|_Database error: Data base empty_|_END_COMMUNICATION"
        - si il n’y a pas assez de numéros dans la base de données : "_|_BEGIN_COMMUNICATION_|_ERROR 7_|_Database error: Not enough numbers in database_|_END_COMMUNICATION"
        - autre erreur potentielle dans la base de données : "_|_BEGIN_COMMUNICATION_|_ERROR 7_|_Database error: error on database side_|_END_COMMUNICATION"

- “**getInvitationKey_|_*end_date(jj-mm-yyyy)*_|_*nbOfUse***”
    - description : renvoie une clé d’invitation pour rejoindre le réseau
    - format de retour : “_|_BEGIN_COMMUNICATION_|_*invitation_key*_|_END_COMMUNICATION”
    - format de retour d’erreur :
        - si non authentifié/connecté via signIn ou logIn : "_|_BEGIN_COMMUNICATION_|_ERROR 2_|_Permission denied!_|_END_COMMUNICATION"

        - si mauvais format : "ERROR 3_|_Wrong input format: getInvitationKey_|_*end_date(jj-mm-yyyy)*_|_*nbOfUse*" end_date et nbOfUse peuvent être mis à 0 pour faire une clef infini dans le temps ou en nombre d'utilisation ou les deux
        - si l'alias a déjà un invitation key : "ERROR 9_|_you already have an invitation key"
        - si le format de date est incorrect : "ERROR 9_|_Date format incorrect"
        - si nbOfUse est négatif : "ERROR 9_|_nbOfUse can't be negative"
        - si nbOfUse n'est pas un entier : "ERROR 9_|_number of uses should be an integer"

- **"FIN"**
    - description : poignée de main de fermeture du socket avec le serveur
    - format de retour : "_|_BEGIN_COMMUNICATION_|_FIN_|_END_COMMUNICATION"
    - format de retour d'erreur : aucun

Pour toutes les requêtes au serveur, si une erreur empêche le serveur de répondre à la requête, il renverra au client "ERROR"

- **"getAllAlias_|_*admin_password*"**
    - description : renvoie la liste de tous les alias inscrit sur l'appli (exepté les utilisateurs bannis)
    - format de retour : _|_BEGIN_COMMUNICATION_|_*alias1*_|_*alias2*_|_..._|_END_COMMUNICATION
    - format de retour d'erreur :
        - si la base de donnée est vide : "_|_BEGIN_COMMUNICATION_|_ERROR 6_|_BDD empty_|_END_COMMUNICATION"
        - si mauvais format: "ERROR 3_|_Wrong input format: getAllAlias_|_*password*"