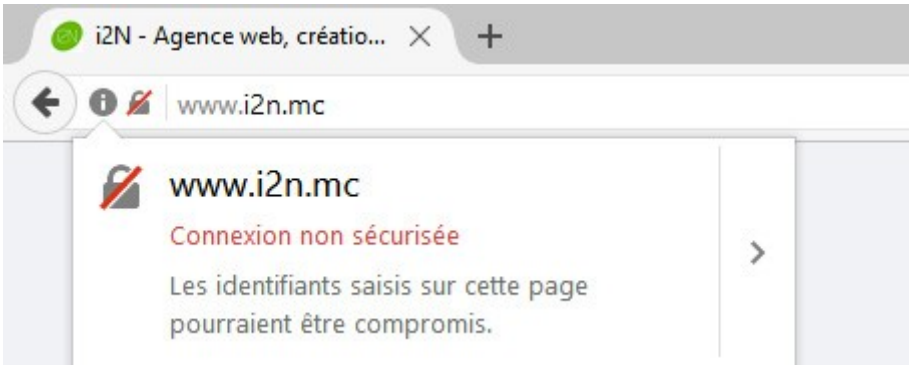
TP Certificat 2

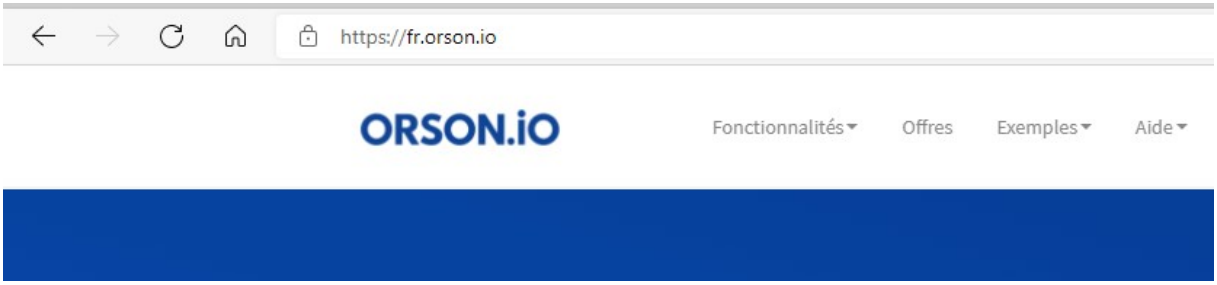
A. Un utilisateur souhaiterait se connecter à ce site



1. Quels sont les risques liés lors de la connexion à ce site internet ?
   Accès facile aux données par un attaquant dues aux données non chiffrées.

2. Quelles solutions pouvez-vous proposer au propriétaire de ce site ?
   Mettre en place un certificat SSL

B. Il souhaiterait à nouveau se connecter cet autre site



1. Ce site est-il sécurisé ? Si oui comment le savez-vous ?
   Oui il est sécurisé à l'aide du protocole https

2. Décrire les différentes étapes de connexion entre l'utilisateur et ce site ?

   a. Faire une demande de connexion auprès du serveur
   b. Le serveur renvoie son certificat au client qui contient sa clé publique et l'utilisateur vérifie la validité du certificat (validité de la clé pub)
   c. Si le certificat du serveur valide, le navigateur génère une clé de session et la crypte avec la clé pub du serveur
   d. Le serveur décrypte la clé de session avec sa clé privée
   e. Le serveur vérifie le certificat de l'utilisateur s'il est valide
   f. Etablissement d'un tunnel sécurisé

3. Quels sont les avantages de ce type de connexion ?
   La confidentialité, données chiffrées, authenticité, intégrité, non-répudiation