Résumé

Domaine de recherche relativement sensible, la protection de la vie privée et particulièrement l'anonymat constitue un axe de recherche crucial en sécurité dans les environnements mobiles.
L'anonymat consiste à protéger les informations secondaires telles que l'identité des entités impliquées dans une transaction mais aussi à protéger les méta-informations qui découlent des interactions entre entités d'un système. Etant donné que les réseaux mobiles sont plus vulnérables à l'écoute, un intrus peut avoir accès à des informations sensibles concernant la vie privée des utilisateurs. Les messages échangés durant la procédure d'authentification peuvent révéler des informations privées à des ennemis écoutant le médium de communication. Il devient alors possible de pister l'usager.
En nous intéressant au problème d'anonymat, nous nous sommes confrontés à un domaine sensible. En effet, d'un point de vue social, les communications anonymes semblent être désirées seulement par une minorité de gens concernés par le problème de préserver confidentielles les informations privées et souvent non acceptées par les gouvernements ou organisations. C'est pourquoi, les solutions pour les communications anonymes ne sont pas intégrées dans des produits existants ou infrastructures. Notons que l'anonymat assuré par GSM n'est que partiel et à ce jour les travaux de UMTS ne considèrent pas un anonymat complet. Il est également important de noter que même les travaux de recherche ne considèrent pas un anonymat complet.

Dans ce contexte, nous proposons un protocole d'authentification dans un environnement mobile qui assure l'anonymat complet. Le protocole est basé sur la technique de signature aveugle pour assurer l'intraçabilité de l'utilisateur mobile même par son domaine d'affiliation. Ce dernier ne pourra pas connaître les différents déplacements de son abonné. Le protocole, ainsi défini, garantit la confidentialité des messages échangés durant l'authentification et permet de résister aux attaques par rejeu.
L'anonymat complet peut sembler contradictoire avec la tarification des services demandés. Pour cela, nous intégrons un moyen de paiement électronique sans compromettre l'anonymat.