

## Problématique

L'utilisation des codes mobiles soulève plusieurs questions du domaine de la sécurité :

1. Le contrôle d'accès : est-ce que l'exécution de ce code est permise ?

2. L'authentification : l'utilisateur est-il un utilisateur valide ?

3. L'intégrité des données : pour assurer que le code est reçu intact.

4. La non-répudiation : l'utilisation de ce code doit être reconnue par le serveur et par le client, en particulier si son utilisation est payante.

5. La confidentialité des données : pour protéger les parties sensibles du code.

6. L'audit : il doit être possible de tracer l'exécution de codes mobiles. Les techniques pour garantir ces points sont bien connues. Leur mise en place devient délicate dans le cadre de la mobilité car ces notions peuvent varier localement : est à dire qu'un agent mobile peut disposer de droits différents mais aussi contrôler différemment ces droits en fonction de la plate forme d'accueil, dans la mesure où par exemple certaines d'entre elles mettent en jeu des mécanismes de cryptographie différents. Les points 2, 3 et 4 sont garantis par les mécanismes de signatures cryptographiques tandis que le point 5 relève de la cryptographie pure.

La question intéressante sera donc plutôt de se demander comment garantir la sécurité du système lors de l'exécution du code, une fois celui-ci validé et délivré à l'utilisateur final.