Cahier des charges

Face Key

# Situation initiale

## Problème des mots de passe

De nos jours on observe une augmentation du nombre de sites qui nécessite la création d’un compte : réseaux sociaux, diffèrent compte mail, opérateur téléphonique, journaux en ligne … Il devient difficile d’avoir un mot de passe différent par site, qu’il soit assez complexe pour être sécurisé et qu’on n’ait pas besoin de la noter quelque part. La plupart des utilisateurs utilise donc un seul mot de passe, souvent très simple, en dépit de la sécurité. Leur compte et informations qu’ils contiennent deviennent donc facilement hackable et comme les comptes sont souvent liés, on risque un hackage en chaine de beaucoup de ses comptes.

Une solution développée pour pallier ce problème est le gestionnaire de mot de passe (GMDP). Le principe est simple : l’utilisateur n’a qu’un seul gros mot de passe à connaitre et c’est le GMDP qui s’occupe des combinaisons login/mot de passe sécurisé pour chaque site. L’un des problèmes de cette solution est qu’il faut toujours retenir un mot de passe compliquer pour déverrouiller le GMDP et donc ce déverrouillage peut prendre plus de temps. Avec cette méthode il peut aussi être fastidieux, non intuitif et peu sécurisé de partager l’accès à un compte (partager son compteur d’opérateur téléphonique avec son conjoint par exemple).

## Maturation de la technologie

Avec l’émergence du deeplearning et d’autres technique de traitement d’image et de machine learning, les techniques de reconnaissance faciale deviennent de plus en plus performante. Certain algorithme arrive même à battre l’humain dans certaines conditions (Chaochao Lu et Xiaou Tang 2014). De plus beaucoup de grands acteurs économiques s’attaquent au problème, obtiennent d’excellents résultats et en sortent des applications, par exemple Facebook avec deepFace en 2014, Microsoft avec Hello en 2015 et enfin très récemment Apple avec FaceID (en 2017).

Il a également été prouvé que la reconnaissance faciale pouvait être plus difficilement hackable que des mots de passe de par la complexité et l’unicité du visage humain.

# Notre solution : Face Key