Authentification par notification Push

L'authentification par notification Push suppose que le client possède un smartphone sur lequel il aura installé une application spéciale mise au point par son institut financier et sur laquelle il recevra des notifications Push via une connexion Internet chiffrée.

Voici les points à tenir en considération si vous utilisez la méthode d'authentification par notification Push :

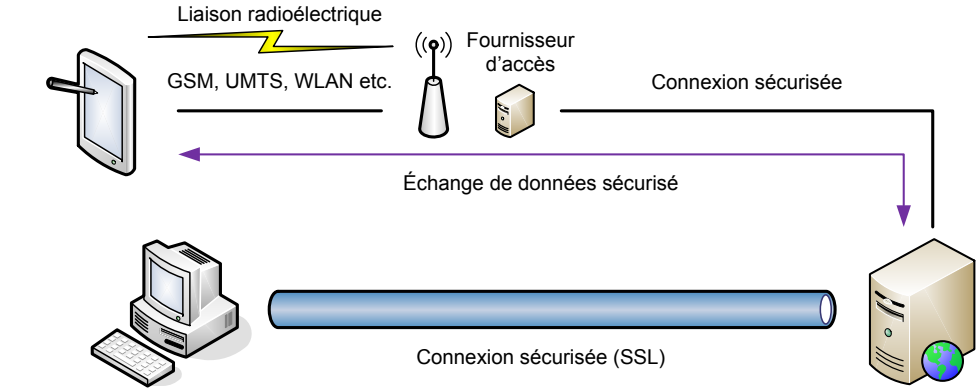
- Vérifiez soigneusement toutes les données saisies avant de confirmer vos transactions.
- Refusez toute demande de connexion parvenue en retard et contactez votre institut financier si vous en recevez sans les avoir sollicitées.
- Conservez vos identifiants de connexion ailleurs que sur votre téléphone portable.
- Ne notez aucun mot de passe ni code PIN, à moins de conserver ces notes sous clé.
- Respectez toutes les recommandations de sécurité concernant l'utilisation des smartphones (https://www.ebas.ch/fr/les-applications-de-banque-mobile-mobile-banking/) .
- Veillez à bien saisir votre numéro d'identification et votre mot de passe ou code PIN dans les champs correspondants sur la page de connexion du site d'e-banking
- Tapez votre code Appli-PIN personnel uniquement sur votre smartphone.

Fonctionnement

Une fois que le client a saisi son numéro d'identification et son mot de passe ou code PIN, l'institut financier lui transmet un code à usage unique sur son téléphone portable via une notification Push. Pour obtenir ce code, le client doit démarrer une application et s'identifier en saisissant son code PIN. Le processus d'authentification ne peut être validé et l'accès au compte autorisé qu'après la saisie de ce deuxième code d'accès.

Ce mécanisme d'identification doit être également utilisé pour confirmer certaines transactions considérées comme potentiellement à risque, comme des virements de sommes inhabituelles. De nombreux systèmes mémorisent les destinataires récurrents d'un même client, de sorte que ce dernier n'ait pas à confirmer chaque virement.

Ce procédé protège l'utilisateur contre les risques de piratage des transactions (p. ex. attaques « Man-in-the-Browser »), puisque le client de la banque a la possibilité de vérifier les données de la transaction qui s'affichent sur l'écran avant de confirmer cette dernière.



(https://www.ebas.ch/wp-content/uploads/2019/09/Push-TAN_fr.svg)