Lancement de la solution FIDO d'IST : de l'authentification par carte au serveur cryptographique sécurisé

Deux nouvelles solutions pour réduire le recours aux mots de passe, renforcer la sécurité et aider les banques et les commerçants à lutter contre la fraude.

 # PAIEMENT

POSTÉ LE 05.04.26

IDEMIA Secure Transactions (IST) redéfinit l'authentification grâce à deux nouvelles solutions indépendantes basées sur la norme FIDO, conçues pour renforcer la sécurité digitale tout en simplifiant l'expérience utilisateur. La nouvelle **applet FIDO** d'IST transforme la carte de paiement EMV en un dispositif de connexion sécurisé et sans mot de passe, faisant ainsi d'un outil de paiement quotidien une clé de confiance pour accéder aux services digitaux. Parallèlement, le **serveur FIDO** d'IST apporte une authentification forte et transparente aux acteurs des secteurs bancaire et du commerce électronique en stockant les clés publiques et en gérant les demandes d'authentification sans mot de passe via des méthodes cryptographiques sécurisées.

Ces deux solutions sont développées selon les normes de la FIDO Alliance afin de mieux protéger les comptes financiers et les transactions contre les tentatives de phishing et de piratage. L'objectif est simple : réduire la dépendance aux mots de passe tout en améliorant la sécurité, la compatibilité avec les systèmes existants et la confiance des utilisateurs.

FIDO (Fast IDentity Online) est une norme d'authentification ouverte et reconnue à l'échelle internationale qui remplace les mots de passe par des méthodes sécurisées et résistantes au phishing, telles que la biométrie, des clés de sécurité ou des codes PIN, évitant la transmission de mots de passe en ligne. Elle permet d'utiliser une carte de paiement comme moyen d'authentification sécurisé. Il suffit d'un tap de leur carte sur leur smartphone pour permettre aux utilisateurs se connecter ou de valider une transaction.

Cette approche répond directement à la croissance rapide de la fraude aux paiements en ligne. Selon Finance Magnates, les pertes liées à la fraude sans présentation de la carte (CNP) devraient augmenter de 40 % cette année.

L'applet FIDO transforme une carte EMV en moyen d'authentification

L'applet FIDO, destinée à l'authentification forte est directement installée par défaut sur la puce de la carte. Au lieu de saisir un mot de passe, les utilisateurs valident leur identité avec leur carte. Les cas d'utilisation les plus courants incluent la connexion à des sites web, la récupération de comptes ou la validation d'opérations sensibles. La carte de paiement devient un moyen d'authentification sécurisé que le client a toujours avec lui dans son portefeuille.

Le rôle du serveur FIDO dans le secteur bancaire et le commerce électronique

Le serveur FIDO fonctionne comme un serveur d'authentification traditionnel, mais s'appuie sur une sécurité cryptographique sans mot de passe. Déployé dans une infrastructure standard, le serveur stocke les clés publiques et les certificats et expose des APIs qui déterminent si l'accès à un service doit être accordé.

Le serveur FIDO peut être partagé entre plusieurs fournisseurs de services, agissant comme un socle de confiance commun. Le serveur valide tous les messages d'authentification et garantit la conformité aux spécifications FIDO. Chaque fournisseur de services conserve le contrôle total de sa propre logique métier et de l'expérience utilisateur, tout en s'appuyant sur le serveur pour une authentification sécurisée et fiable.

Avec ce serveur, IST intègre FIDO aux cas d'usage des secteurs bancaires et du commerce électronique et permet à ses clients (réseaux domestiques et les émetteurs inclus) d'offrir des expériences d'authentification fluides aux utilisateurs finaux.

Des solutions certifiées assurant une intégration parfaite à l'écosystème FIDO

IST a obtenu la **certification FIDO** pour l'applet **Solvo Fly 80** et son **serveur FIDO.** Cette étape importante confirme la conformité aux spécifications FIDO et atteste qu'IST répond aux exigences de sécurité et de compatibilité définies par l'Alliance.