Comment les systèmes ievo protègent vos données

**La biométrie fait référence à des caractéristiques humaines distinctives et mesurables, propres à chaque individu.
En les mesurant et en les analysant, vos données biométriques peuvent alors devenir vos codes d'accès personnels ultra sécurisés.**

INTRODUCTION

Considéré comme le lecteur biométrique le plus fiable et le plus avancé sur le marché, Iévo offre de nombreux avantages et bénéfices en termes de sécurité.
Utiliser la biométrie vous permet de dire adieu au vol ou au clonage de vos cartes ou badges d'accès, ou encore en cas d'oubli de vos codes ! Les menaces de piratage ne seront plus qu'un mauvais souvenir !
Vous gagnez en temps, en efficacité et surtout en niveau de sécurité sur tous vos systèmes de contrôle d'accès.

Ievo protège non seulement les bâtiments et tous types de locaux, mais également le résidentiel et permet d'améliorer la gestion des horaires et des présences.

Dans la mesure où les données biométriques sont uniques, cela ouvre de nombreuses perspectives de sécurité accrues, à des fins d'identification encore plus fiables, précises et efficaces.

Il est essentiel de comprendre aujourd'hui comment Iévo utilise et stocke les données afin de donner l'assurance aux utilisateurs que leurs informations sont totalement protégées.

Poursuivez votre lecture pour en savoir plus ...

VOS DONNÉES

Lors de l'enregistrement d'une empreinte digitale, le système ievo va scanner et extraire des données en utilisant un algorithme qui identifie des caractéristiques spécifiques à cette empreinte, appelées minuties.

Ces minuties, une fois identifiées, sont classées en groupes, incluant bifurcations de lignes et extrémités de crêtes, entre autres groupes de données.

Après un scan enregistré, le lecteur ievo envoie une trame chiffrée à la carte de contrôle ievo, où un algorithme avancé identifie et compare le type et la position des points caractéristiques de cette trame (Fig.1). L'image origine de l'empreinte digitale N'est ni stockée ni enregistrée.

Lors de l'utilisation d'un lecteur pour l'accès, un processus similaire à celui décrit ci-dessus commence. En revanche, cette fois-ci, l'algorithme de correspondance sera utilisé pour comparer les nouvelles données de minuties avec les modèles stockés.

Si un matching s'opère, l'identité de l'utilisateur sera confirmée. Cette confirmation sera transmise au système de contrôle d'accès.

DONNÉES PROTÉGÉES

Une fois qu'une empreinte digitale a été scannée, l'image originale n'est NI stockée NI enregistrée. Les seules données enregistrées sont les minuties de l'empreinte, transférées et stockées dans la carte contrôle dans un format chiffré de modèle propriétaire unique.

Les systèmes ievo utilisent un algorithme AFIS (Automated Fingerprints Identification System) de pointe pour les processus d'enregistrement, d'extraction et de comparaison des données. Ces données ne peuvent pas faire l'objet d'une ingénierie inverse pour recréer une image de l'empreinte digitale originale.

Pour obtenir plus d'information sur les lecteurs d'empreintes digitales ievo et la protection des données, veuillez nous contacter.

Un algorithme d'extraction avancé est utilisé pour créer un modèle à partir de données d'empreintes digitales spécifiques capturées après un scan. Ces données (Fig.2) sont stockées dans un format chiffré de modèles propriétaire unique. Toutes les autres informations **ne sont ni stockées ni enregistrées.**
Il est IMPOSSIBLE de reconstruire l'image d'une empreinte digitale à partir des données stockées.

SECURITE

AUCUNE information ou donnée n'est stockée localement sur les unités de lecture elles-mêmes.

Les lecteurs ievo ne contiennent aucun mécanisme De verrouillage ou relais de porte, ce qui signifie que si un lecteur était retiré, votre point d'accès Resterait sécurisé et vos données, en sécurité. L'unité de lecture deviendrait alors inutile pour Toute personne malveillante, car vide de toute donnée.

Fig.1: Image montrant ce qu'un lecteur ievo scanne et les minuties présentes

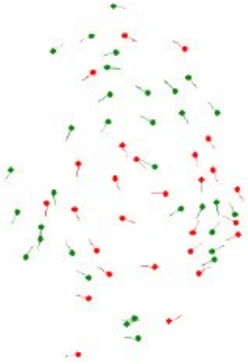

Fig.2: Image montrant les points de minuties extraits de l'empreinte, stockés en tant que modèle

RGPD

CDVI ne détient ni ne contrôle AUCUNE donnée personnelle relative aux lecteurs ievo, et n'a qu'un accès à distance à ces données que lorsqu'il fournit un support aux utilisateurs finaux.

Les installateurs et les utilisateurs finaux d'un système ievo doivent s'assurer qu'ils sont en totale conformité avec le Règlement général sur la Protection des Données (RGPD) 2016/679, car ils contrôlent la collecte des données et les finalités du traitement.