CDVI
Security to Access

ievo

Comment les systèmes ievo protègent vos données

La biométrie fait référence aux caractéristiques humaines distinctives et mesurables qui marquent et décrivent un individu. En mesurant et en analysant ces caractéristiques biologiques, les données peuvent être utilisées à des fins d'identification unique de sécurité.

INTRODUCTION

Considérée comme la forme la plus fiable et la plus sûre de sécurité de haut niveau, l'empreinte biométrique ievo offre de nombreux avantages et bénéfices par rapport aux solutions de sécurité habituelles. L'avantage de l'utilisation de la biométrie est que les problèmes courants tels que la perte, le vol ou la copie de cartes ou de badges, l'oubli de codes d'accès ou de codes pin, les menaces de piratage ou toute autre forme d'interaction inutile avec l'utilisateur sont tous résolus. Cela permet d'économiser du temps et des ressources tout en améliorant la sécurité des systèmes de contrôle d'accès.

Les systèmes ievo protègent non seulement les bâtiments et les locaux, mais aussi les individus et augmentent la productivité dans la gestion du temps et des présences.

SÉCURITÉ

La nature des données biométriques étant unique à un individu, elle ouvre de nombreuses options pour des niveaux de sécurité accrus à des fins d'identification, qui sont plus fiables, plus précis et plus efficaces que les niveaux de sécurité plus traditionnels.

Il est essentiel de comprendre comment les systèmes biométriques ievo utilisent et stockent ces données, afin de donner l'assurance aux utilisateurs que ces informations sont totalement protégées.

Veuillez tourner la page pour en savoir plus sur la façon dont ievo utilise et stocke vos données.

CAPTURER VOS DONNÉES

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

Les points de minuties identifiés sont classés en groupes, qui incluent les bifurcations de lignes et les extrémités de crêtes, entre autres groupes de données. Après un scan enregistré, le lecteur ievo envoie une image de l'empreinte digitale à la carte de contrôle ievo, où un algorithme avancé identifie le type, la direction et la distance entre les principales caractéristiques des points caractéristiques d'une empreinte digitale (Fig.1). Ces données sont converties en un modèle et stockées dans une base de données sur la carte de contrôle ievo. L'image originale 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. Cependant, cette fois, l'algorithme de correspondance sera utilisé pour comparer les nouvelles données de minuties avec les modèles stockés dans la base de données. Une fois qu'un nombre prédéfini de points de minuties a été comparé à un modèle stocké, l'identité de l'utilisateur sera confirmée, cette confirmation sera transmise au système de contrôle d'accès ou au système de "temps et de présence" pour l'entrée et/ou l'enregistrement des données.

DONNÉES PROTÉGÉES

Une fois qu'une empreinte digitale a été scannée, l'image originale n'est pas stockée ou enregistrée. Les seuls détails enregistrés sont les points clés de l'empreinte digitale qui sont transférés et stockés sur une carte de contrôle ievo dans un format de modèle propriétaire unique. Le modèle stocké est unique pour un individu et le modèle est uniquement accessible à des fins d'identification par la carte de contrôle ievo. Les données ne sont pas accessibles à d'autres fins et ne peuvent être visualisées à l'aide de logiciels courants.

Les systèmes ievo utilisent un algorithme AFIS (Automated Fingerprint 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'informations sur les lecteurs d'empreintes digitales ievo et la protection des données, veuillez nous contacter.

VOS DONNÉES

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 en utilisant un format de modèle propriétaire unique. Toutes les autres informations ne sont ni stockées ni enregistrées. Les données NE PEUVENT PAS être utilisées pour reconstruire l'image d'empreinte digitale originale.

SÉCURITÉ

ievo, ce qui signifie qu'aucune information ou donnée n'est stockée localement sur les unités de lecture elles-mêmes. Pour plus de sécurité, la carte de contrôle ievo doit toujours être installée sur le côté sécurisé d'un point d'entrée, loin des unités de lecture.

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 resteraient en sécurité. L'unité de lecture serait considérée comme inutile pour l'attaquant, car elle ne contient aucune donnée.

Fig.1 : Image illustrant ce qu'un lecteur ievo scanne et les principales caractéristiques des minuties.

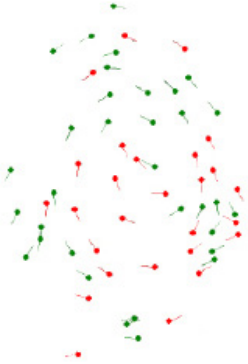

Fig.2 : Image représentant les données des caractéristiques clés qui sont extraites, transférées et stockées comme un modèle.

GDPR

CDVI Benelux ne détient ni ne contrôle aucune donnée personnelle relative aux lecteurs ievo et n'aura qu'un accès à distance à ces données personnelles lorsqu'elle fournira un support aux utilisateurs finaux, auquel cas elle agira en tant que processeur de données et agira sur les instructions d'un contrôleur de données.

En tant que contrôleur de données, les installateurs et les utilisateurs finaux d'un système ievo doivent s'assurer qu'ils sont pleinement conformes au règlement général sur la protection des données 2016/679, car ils contrôlent la collecte des données et les finalités du traitement afin d'identifier l'empreinte digitale de l'utilisateur et d'accorder l'accès ou d'enregistrer le temps de présence.