

RECONNAISSANCE FACIALE DANS LE CONTRÔLE D'ACCÈS.

UN **WHITEPAPER** RENDU POSSIBLE PAR BOON EDAM


BOON EDAM
YOUR **ENTRY** EXPERTS.



INTRODUCTION.

Ce whitepaper explique le fonctionnement du contrôle d'accès basé sur la reconnaissance faciale. Il aborde également les points auxquels il convient de prêter attention lors du choix d'un système de contrôle d'accès utilisant la reconnaissance faciale. Étant donné que la reconnaissance faciale est une technologie relativement récente sur le marché, vous vous demandez sans doute quels aspects sont à considérer avant de mettre en place un tel système. Après lecture de ce whitepaper, vous aurez une compréhension claire de ce que la reconnaissance faciale implique dans le cadre du contrôle d'accès et des éléments à prendre en compte lors de l'acquisition d'un tel système.

TYPES DE BIOMÉTRIE

Biometrische kenmerken zijn alle meetbare eigenschappen van het menselijk lichaam. Biometrie wordt steeds vaker ingezet binnen toegangscontrole. De vier meest gebruikte vormen zijn:

SCAN DE L'IRIS

Chaque iris humain possède des caractéristiques uniques. Lors d'un scan de l'iris, les creux, lignes et sillons sont analysés et convertis en un code d'iris. Ce code est ensuite comparé à une base de données pour permettre l'accès.

VEINES DE LA PAUME

À l'aide de la lumière infrarouge, le réseau unique de veines est cartographié. Certains lecteurs de paume enregistrent également les lignes et épaississements de la main. Ces données constituent un profil unique qui peut être associé à une personne autorisée.

EMPREINTE DIGITALE

Il existe différents types de lecteurs d'empreintes digitales. Tous ces lecteurs mesurent le motif unique des lignes de la peau. Les données enregistrées peuvent ensuite être utilisées pour déterminer si l'accès est autorisé.

RECONNAISSANCE FACIALE

La dernière forme de biométrie appliquée au contrôle d'accès est la reconnaissance faciale. Un algorithme extrait le visage humain d'une photo ou d'une image vidéo. En quelques millisecondes, les caractéristiques uniques du visage sont capturées et converties en un code unique.

Le logiciel de reconnaissance faciale compare ensuite ce code à une base de données. Lorsqu'une correspondance est trouvée, il est possible de déterminer l'identité de la personne sur l'image et de décider si l'accès doit être accordé ou non.





RECONNAISSANCE FACIALE

La reconnaissance faciale peut être utilisée de différentes manières. Ce whitepaper se concentre sur son utilisation dans le cadre du contrôle d'accès. Vous trouverez ci-dessous un bref aperçu des différentes applications:

SURVEILLANCE DE MASSE

Dans le cadre de la surveillance de masse, la reconnaissance faciale est utilisée pour identifier des individus au sein d'une foule. Pour ce faire, du matériel spécialisé et des logiciels puissants sont nécessaires.

PERSONNEL

Cette forme de reconnaissance faciale, souvent utilisée sur des appareils mobiles comme les smartphones, repose sur un logiciel et un matériel relativement simples. L'objectif est d'utiliser le visage comme alternative à un code PIN.

IDENTIFICATION JUDICIAIRE

La reconnaissance faciale peut également être utilisée pour reconstituer le parcours d'une personne à partir d'images vidéo enregistrées. Ces données permettent, par exemple, de déterminer où une personne recherchée s'est trouvée au cours des dernières 24 heures.

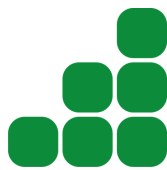
CONTRÔLE D'ACCÈS

Enfin, la reconnaissance faciale peut être appliquée dans le cadre du contrôle d'accès. Il est important que le logiciel fonctionne en temps réel, en comparant les images des caméras provenant de différents emplacements à une base de données. En fonction de la taille de cette base, un serveur suffisamment puissant est choisi pour déterminer rapidement si une personne est autorisée, après quoi le portique d'accès peut s'ouvrir.

DANS CE WHITEPAPER:



AVANTAGES DE LA RECONNAISSANCE FACIALE



COMPOSANTS DE LA RECONNAISSANCE FACIALE



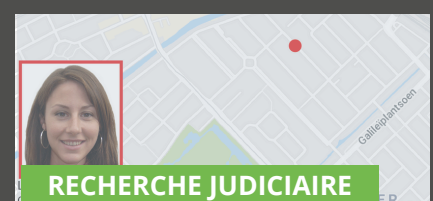
ASPECTS TECHNIQUES



EN PRATIQUE



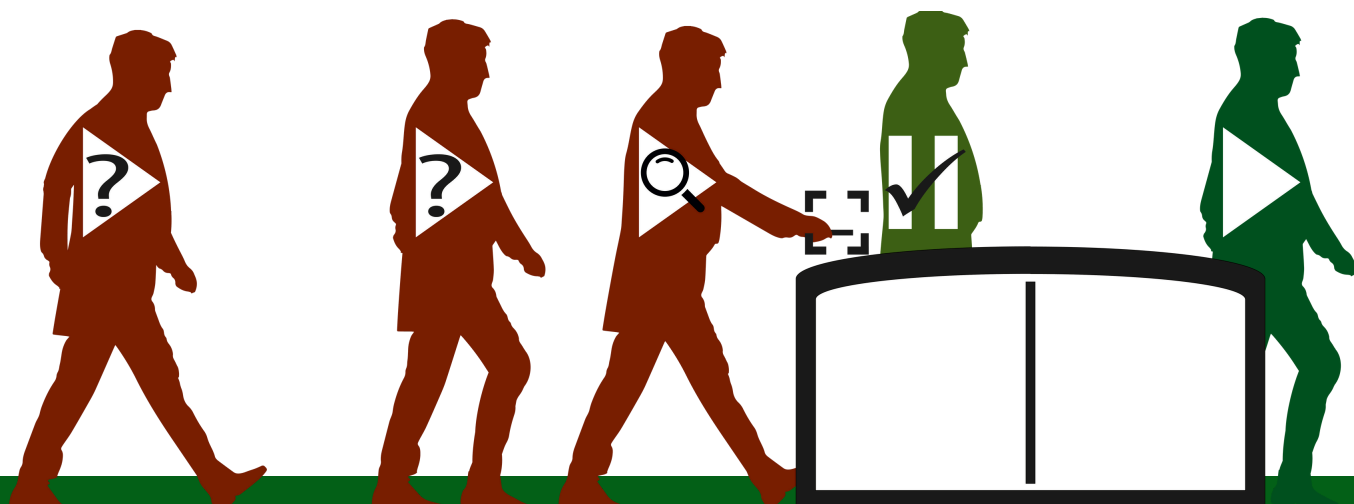
SÉCURITÉ NUMÉRIQUE



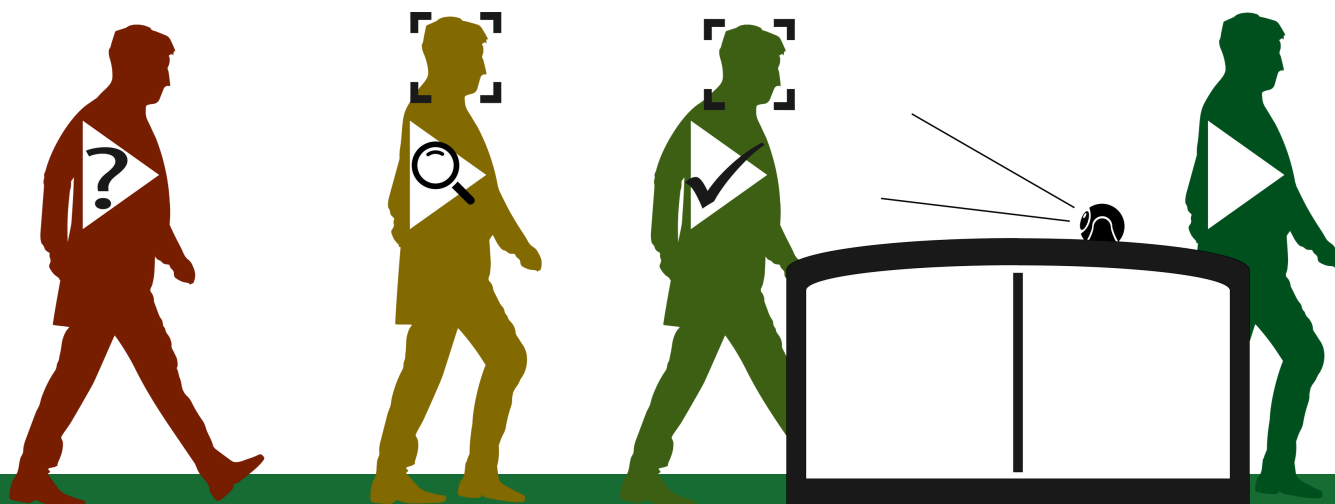


AVANTAGES DE LA RECONNAISSANCE FACIALE

LECTEUR DE CARTE 'CLASSIQUE'



RECONNAISSANCE FACIALE



FLUIDITÉ AMÉLIORÉE

L'un des principaux avantages de la reconnaissance faciale dans le cadre du contrôle d'accès est que la personne souhaitant entrer ne subit aucun temps d'attente au point d'accès. Le logiciel enregistre le visage d'une personne approchant avant même qu'elle n'atteigne le portique. Lors de l'approche, il est ainsi possible de déterminer si la personne est autorisée à entrer dans le bâtiment. Lorsque la personne autorisée se trouve juste devant ou dans le portique, le système s'ouvre automatiquement. Cela empêche qu'une autre personne pénètre de manière non autorisée. Le résultat : un passage fluide, sécurisé et sans contact à travers le contrôle d'accès.



ACCÈS RAPIDE À TOUT MOMENT

Comme la reconnaissance faciale biométrique repose sur un élément que vous portez toujours sur vous – votre visage –, vous ne vous retrouverez jamais face à une porte fermée. Le fait que chaque visage soit unique permet d'utiliser les caractéristiques faciales pour différencier et identifier correctement les personnes.

Un avantage supplémentaire est que l'utilisateur n'a pratiquement plus besoin d'intervenir activement à l'approche d'un point de contrôle d'accès. Dès que votre visage entre dans le champ de vision de la caméra, le logiciel vérifie automatiquement si vous êtes autorisé. Les badges d'accès deviennent ainsi superflus et ne peuvent plus être oubliés. De plus, vous n'avez plus à attendre qu'un collègue retrouve son badge parmi ses affaires et vous avez les mains libres pour, par exemple, porter votre manteau et votre sac.

AUCUN BADGE TRANSMIS

Un problème fréquent dans le contrôle d'accès est le partage d'un badge personnel avec un collègue. Cet usage inapproprié permet à des personnes non autorisées d'accéder au bâtiment. Grâce à la reconnaissance faciale, un individu inconnu ne peut plus franchir le contrôle d'accès.

De plus, la reconnaissance faciale empêche le vol ou la copie des badges d'accès. Le résultat: un renforcement net du niveau global de sécurité.



LA BIOMÉTRIE EST SANS CONTACT

De nombreuses personnes hésitent lorsqu'on leur demande de scanner leur iris ou leur doigt. Cette hésitation (souvent inconsciente) provient généralement d'un manque de familiarité avec le système ou d'un inconfort lié au fait de devoir placer une partie du corps contre un scanner. Cela nuit non seulement à la fluidité du passage, mais affecte également la perception de convivialité du contrôle d'accès.

Un grand avantage de la reconnaissance faciale est qu'une caméra enregistre l'utilisateur à distance. Ainsi, il n'est pas nécessaire d'adopter une posture inconfortable ni d'entrer en contact physique avec le portique d'accès. Dès que la personne entre dans le champ défini de la caméra, elle est automatiquement vérifiée et l'accès peut être accordé, sans le moindre retard.



COMPOSANTS DE LA RECONNAISSANCE FACIALE

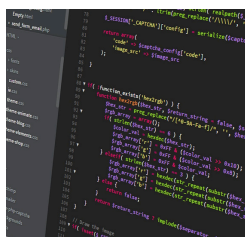
Lors du choix de la reconnaissance faciale dans le cadre du contrôle d'accès, il faut tenir compte du fait que le système se compose de plusieurs composants. Ces composants proviennent souvent de différents fournisseurs et doivent être correctement coordonnés entre eux. Il est donc important d'identifier clairement les parties capables de mettre en place un système fluide et fiable. En général, les composants suivants interagissent entre eux:



CAMÉRA ET AUTRES CAPTEURS

La caméra est un maillon crucial pour le bon fonctionnement du logiciel de reconnaissance faciale. Il existe différentes caméras de haute qualité sur le marché. L'expérience montre qu'un choix réfléchi, tant sur le plan technique qu'esthétique, contribue à la convivialité et à l'acceptation par les utilisateurs.

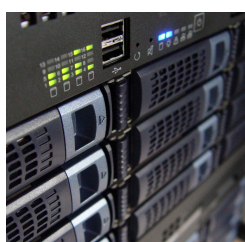
Le processus de sélection ne se limite pas au nombre de mégapixels: la sensibilité à la lumière, le type d'objectif et la puissance de calcul de la puce sont également des facteurs importants. Il est également possible d'opter pour des capteurs supplémentaires capables de distinguer un vrai visage d'une image, par exemple sur une photo.



LOGICIEL DE RECONNAISSANCE FACIALE

Également appelé le cœur du système, le logiciel de reconnaissance faciale convertit les visages en un code, qui est ensuite comparé à une base de données prédéfinie. Cette reconnaissance s'effectue via une série d'algorithmes. Le logiciel de reconnaissance faciale fonctionne souvent indépendamment d'un autre logiciel de contrôle d'accès. Il est donc possible de mettre en place un système autonome dans lequel le logiciel tourne sur un processeur externe.

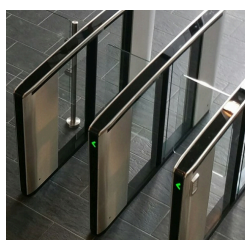
Il est essentiel que tant le logiciel que le système soient conformes au Règlement général sur la protection des données (RGPD) et utilisent les standards de chiffrement appropriés.



SYSTÈME DE CONTRÔLE D'ACCÈS

Un système de contrôle d'accès se compose souvent de plusieurs solutions logicielles. Celles-ci font généralement partie intégrante d'un système de gestion de la sécurité ou d'un système de gestion technique du bâtiment. Il est donc possible que le logiciel de reconnaissance faciale doive être intégré à une telle plateforme.

En pratique, cela signifie que différents modules sont connectés entre eux et peuvent ensuite être gérés de manière centralisée via un programme unique. Le module «logiciel de reconnaissance faciale» est alors intégré via une API.



ACCÈS PHYSIQUE

Lorsque la reconnaissance faciale est utilisée dans le cadre du contrôle d'accès, elle est toujours combinée à un produit d'accès physique. Sans cette barrière, il est en effet impossible d'empêcher efficacement l'entrée de personnes non autorisées. Il existe différents types de barrières, chacune offrant un niveau de sécurité spécifique.

Les composants peuvent être configurés de différentes manières. Il est possible d'intégrer complètement la reconnaissance faciale dans un seul produit physique, mais il est également possible d'utiliser les composants séparément.



ASPECTS TECHNIQUES.



CONDITIONS D'ÉCLAIRAGE

L'un des aspects les plus importants pour une mise en œuvre correcte de la reconnaissance faciale est la quantité de lumière dans la pièce où la caméra est installée. Dans le cadre du contrôle d'accès, la reconnaissance faciale se fait souvent à l'intérieur, ce qui permet de maîtriser dans une certaine mesure les conditions d'éclairage.

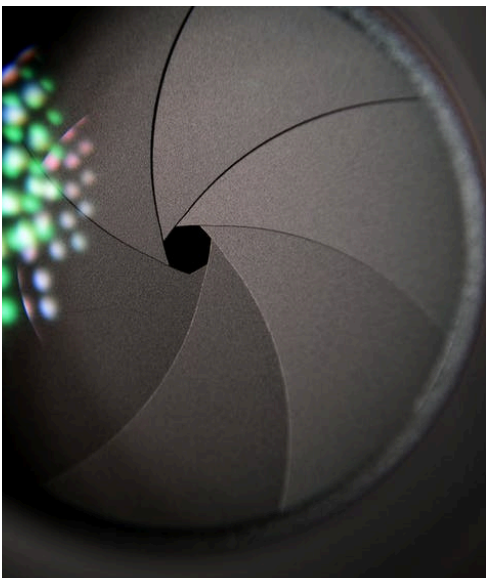
La surexposition représente un défi majeur. Pensez à un soleil intense, aux reflets sur les vitres ou aux espaces dotés d'un atrium élevé. Les variations de lumière sollicitent fortement la caméra et le logiciel de reconnaissance faciale. La sous-exposition, en revanche, est plus facile à corriger. Dans de nombreux cas, un simple ajustement des paramètres de la caméra suffit pour permettre une reconnaissance correcte des visages. Il est recommandé de faire appel à un expert pour effectuer les réglages appropriés.

POSITION DE LA CAMÉRA

Lors de l'installation de la caméra, il est important de bien réfléchir à l'image qu'elle enregistrera. Plus la caméra est proche de la personne souhaitant accéder, meilleure sera généralement la qualité de l'image.

La position de la caméra par rapport à l'utilisateur joue également un rôle crucial. Idéalement, elle doit être placée à un endroit vers lequel l'utilisateur regarde naturellement en approchant du contrôle d'accès. Ainsi, aucune action supplémentaire n'est nécessaire pour être reconnu.

Enfin, pour des raisons esthétiques, il est possible d'intégrer la caméra dans le produit d'accès ou de l'installer à un emplacement externe.



MISE AU POINT DE LA CAMÉRA

Lors de l'installation de la caméra, il est crucial de bien réfléchir à la mise au point. Celle-ci doit être dirigée vers la zone où le visage sera scanné. Le point de focalisation ne doit pas être trop éloigné du contrôle d'accès (pour éviter que les personnes soient reconnues trop tôt), ni trop proche (afin que les utilisateurs n'aient pas à attendre l'ouverture).

La mise au point de la caméra détermine également la zone de détection dans laquelle un visage peut être reconnu avec succès. Cela peut être configuré dans le logiciel en sélectionnant une partie spécifique de l'image de la caméra où la reconnaissance faciale est active.

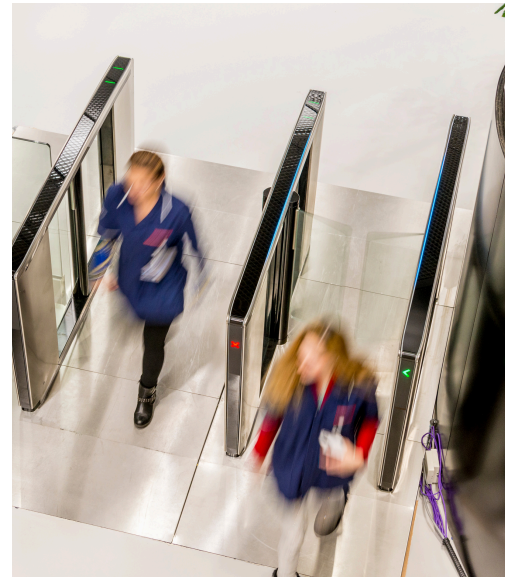


EN PRATIQUE.

FLUX DES UTILISATEURS

Dans la pratique, l'utilisation de sas de sécurité assure une posture naturelle vers l'avant pour l'utilisateur. Les personnes se déplacent en ligne droite, le visage orienté vers l'avant, à travers le produit d'accès. Il en résulte une zone relativement compacte où tous les visages sont bien visibles pour la reconnaissance.

Un avantage important de la reconnaissance faciale dans une solution de contrôle d'accès est qu'elle optimise le flux des utilisateurs. Comme tous se déplacent dans la même direction et que le sas est franchi comme un flux continu, la circulation reste fluide. La reconnaissance faciale garantit une vitesse d'authentification suffisante pour soutenir ce flux sans effort.



PRÉSENTATION DU VISAGE

Comme indiqué précédemment dans ce whitepaper, l'utilisateur n'a pas besoin d'effectuer d'actions supplémentaires lorsque la reconnaissance faciale est utilisée dans le cadre du contrôle d'accès. Une condition importante est cependant que l'utilisateur soit conscient que le logiciel de reconnaissance faciale doit pouvoir scanner correctement le visage.

En pratique, cela signifie que le visage doit être en grande partie découvert et clairement visible pour la caméra. Il n'est donc pas possible d'accéder au système, par exemple, en portant un masque buccal ou en regardant ailleurs. Une coopération minimale de l'utilisateur est donc nécessaire pour garantir le bon fonctionnement du système.

INTERACTION AVEC L'UTILISATEUR

Lors de l'utilisation de la reconnaissance faciale, ainsi que dans le cadre du contrôle d'accès en général, il est important de fournir un retour clair à l'utilisateur. Lorsque plusieurs personnes utilisent successivement un point d'accès, des signaux visuels et sonores peuvent clarifier la décision prise par le logiciel.

La reconnaissance faciale est particulièrement adaptée aux environnements comptant de nombreux utilisateurs réguliers. Un enregistrement unique suffit pour accorder l'accès à un utilisateur pendant une période prolongée. De plus, les utilisateurs fréquents se familiarisent rapidement avec l'interaction avec le système de contrôle d'accès.





SÉCURITÉ NUMÉRIQUE.



CRYPTAGE

Pour éviter que les données et images transmises via un réseau puissent être facilement piratées, le logiciel de reconnaissance faciale utilise le cryptage. Le cryptage consiste à coder ou crypter les informations numériques (comme les images). Sans connaissance de la méthode de cryptage utilisée, il est impossible pour des tiers non autorisés de lire ces informations.

Il existe différentes méthodes pour chiffrer les données. Selon l'infrastructure existante et la plateforme de gestion vidéo en place, une solution appropriée est choisie. On examine notamment si les données sont transmises via un réseau ouvert ou fermé.

DÉTECTION DE FRAUDE

La technologie de reconnaissance faciale progresse rapidement dans le domaine de la détection de fraude. Des recherches sont constamment menées pour éviter que le système soit trompé, par exemple en présentant une photo devant la caméra. Actuellement, deux méthodes permettent de détecter la fraude et de prendre des mesures préventives :

- **Détection matérielle:** via des capteurs 3D qui scannent la structure du visage. Une méthode alternative utilise des capteurs qui analysent la réflexion d'un motif de faisceaux lumineux colorés projetés sur le visage.
- **Détection logicielle:** en identifiant de légères différences dans les images vidéo. Cette approche nécessite une puissance de calcul (vidéo) importante, ce qui implique l'utilisation de serveurs plus grands et plus performants.



RGPD

Comme mentionné précédemment dans ce whitepaper, la reconnaissance faciale utilise des données biométriques. Dans le cadre de la loi d'exécution du Règlement général sur la protection des données (RGPD), il est important de savoir que les données biométriques font partie d'une catégorie particulière de données à caractère personnel. Celles-ci ne peuvent être utilisées à des fins d'identification que sous des conditions strictes.

Les données doivent être traitées exclusivement à des fins d'authentification ou de sécurité. De plus, l'administrateur du système doit être en mesure de démontrer que le traitement de ces données est entièrement conforme à la législation en vigueur.

L'utilisation de la reconnaissance faciale dans le cadre du contrôle d'accès est donc légalement autorisée, à condition que toutes les exigences soient respectées.



CONCLUSION.

L'objectif de ce whitepaper est de vous offrir une première compréhension claire de ce que la reconnaissance faciale implique dans le cadre du contrôle d'accès et des points auxquels il convient de prêter attention lors du choix du système adapté à votre organisation. Nous avons expliqué la distinction entre les différentes formes de biométrie et les applications de la reconnaissance faciale. De plus, vous avez reçu un aperçu des principaux avantages par rapport aux systèmes de contrôle d'accès classiques.

Nous vous avons également familiarisé avec les différents composants d'un système de reconnaissance faciale ainsi que les facteurs techniques et pratiques influençant son bon fonctionnement. Enfin, une brève présentation de la sécurité numérique et de la réglementation applicable relative au RGPD a été fournie.

RECOMMANDATIONS

Avec ce whitepaper, Boon Edam souhaite vous offrir une compréhension claire des conditions et points d'attention liés à l'utilisation de la reconnaissance faciale dans le cadre du contrôle d'accès. Nous sommes convaincus que la reconnaissance faciale a largement fait ses preuves ces dernières années et que cette technologie sera de plus en plus utilisée à l'avenir. Elle est adaptée à presque tous les niveaux de sécurité.

Selon vos besoins et la situation dans laquelle la reconnaissance faciale est mise en œuvre, tels que le nombre de personnes à reconnaître, les lieux d'application et le niveau de sécurité souhaité, nous vous accompagnons volontiers dans le choix et l'implémentation d'une solution adaptée.

Vous souhaitez obtenir plus d'informations sur la reconnaissance faciale dans le contrôle d'accès? N'hésitez pas à contacter Boon Edam. Nos Entry Experts se feront un plaisir de vous rendre visite pour une consultation sans engagement.

QUESTIONS FRÉQUENTES.

Si je souhaite passer par un portique équipé de reconnaissance faciale, le système convertira des points de mon visage en un code et le comparera à une base de données. Cela signifie-t-il qu'une photo de moi est enregistrée?

Lors de la création de la base de données, il n'est pas nécessaire de stocker les visages des utilisateurs. Une liste de codes hash suffit. Même lors de l'utilisation d'une solution d'accès, aucune photo n'a besoin d'être enregistrée pour effectuer une comparaison. Dans la pratique, il peut arriver que les systèmes de reconnaissance faciale conservent temporairement des images afin d'optimiser les performances du logiciel. Ces images sont alors stockées localement sur un serveur autonome et ne sont pas accessibles à des tiers.

D'autres données sont-elles enregistrées en plus de ce code hash?

Dans les systèmes de contrôle d'accès traditionnels, le moment où une personne autorisée entre dans le bâtiment est généralement enregistré. Cela s'applique en grande partie également aux systèmes de reconnaissance faciale. Il est toutefois possible de modifier ces paramètres afin que ces données ne soient pas enregistrées.

Est-il possible d'utiliser cette forme de reconnaissance faciale sur d'autres solutions d'accès que les portiques?

Il est possible d'appliquer le logiciel de reconnaissance faciale à différentes autres solutions d'accès. Vous y intéressez-vous? Nous serons ravis de discuter avec vous des possibilités.

UN RAYONNEMENT INTERNATIONAL.

Depuis 150 ans, nous fabriquons des solutions d'entrée sécurisées haut de gamme et élégantes aux Pays-Bas, aux États-Unis et en Chine. Forts de nos filiales établies dans les grandes villes du monde entier, nous pouvons affirmer en toute confiance que nous couvrons tous les points du globe. En outre, notre service d'exportation à l'international travaille non seulement en partenariat avec nos distributeurs mais il commercialise aussi nos produits et services en direct partout dans le monde. Ce vaste réseau nous permet d'occuper une solide position dans le monde et de bien comprendre les marchés locaux ainsi que leurs exigences uniques.

Pour trouver votre expert Boon Edam le plus proche, rendez-vous sur le site: www.boonedam.be/fr-be/contact



Boon Edam Belux BV
T +32 (0) 14 21 67 17
E be.info@boonedam.com
I www.boonedam.be/fr-be


BOON EDAM
YOUR ENTRY EXPERTS.