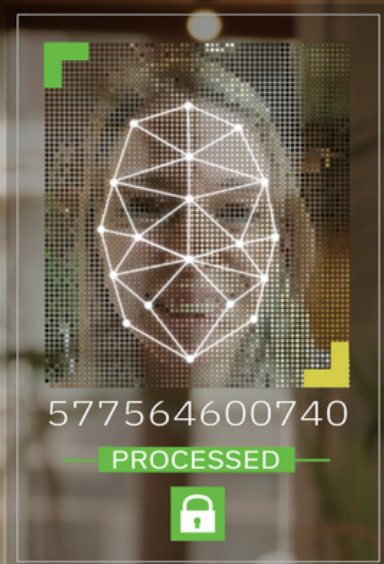




ADGANGSKONTROLL MED ANSIKTSGJENKJENNING.

WHITE PAPER UTARBEIDET MED STØTTE FRA BOON EDAM


BOON EDAM
YOUR **ENTRY** EXPERTS.



INNLEDNING.

Denne brosjyren forklarer hvordan adgangskontroll med ansiktsgjenkjenning fungerer. Det diskuterer også hvilke faktorer man bør ta hensyn til når man velger et adgangskontrollsystem med ansiktsgjenkjenning.

Siden ansiktsgjenkjenning er en relativt ny teknologi på markedet, lurer du kanskje på hvilke aspekter som kan spille en rolle i bruken av det. Denne brosjyren gir bedre innsikt i nøyaktig hva adgangskontroll med ansiktsgjenkjenning innebærer, og hva man må overveie når man går til innkjøp av et slikt system.

TYPER BIOMETRI

Biometriske identifikatorer er alle de målbare karakteristikkene som kan brukes til å beskrive mennesker. Biometri blir mer og mer populært innen adgangskontroll. Dette er de fire vanligste typene:

IRISSKANNING

Iris eller regnbuehinnen har unike kjennetegn hos hvert menneske. En irisskanner identifiserer fordypninger, furer og striper i iris, og konverterer dem til en iriskode. Deretter kan denne koden sammenlignes med en database for å avgjøre om adgang skal gis.

VENER I HÅNDFLATEN

Nær infrarød belysning blottlegger det unike mønsteret av vener og kapillarrør i håndflaten. Noen håndflateskannere måler også karakteristikk som rynker og klumper. Denne informasjonen gir en unik profil som kan knyttes til en autorisert enkeltperson.

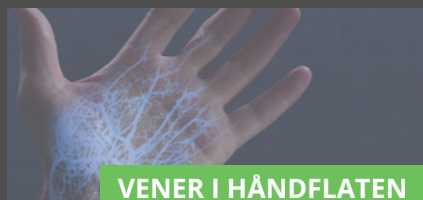
FINGERAVTRYKK

Det finnes ulike typer fingeravtrykksskannere. Alle fungerer ved å registrere det unike linjemønsteret i huden. Disse dataene kan brukes til å avgjøre om det skal gis adgang.

ANSIKTSGJENKJENNING

Den sistevtypen biometrisk adgangskontroll bruker ansiktsgjenkjenning. En algoritme brukes til å filtrere et menneskes ansikt fra en video eller et fotografi. Ansiktets særtrekk blir registrert og konvertert til en unik kode på bare noen millisekunder.

Deretter sammenligner ansiktsgjenkjenningsprogramvaren koden med en database. Hvis den finner en match, kan den brukes til å identifisere personen på bildet og avgjøre om adgang skal gis eller avslås.





ANSIKTSGJENKJENNING

Ansiktsgjenkjenning kan være nyttig i ulike bruksområder. Dette notatet fokuserer på adgangskontroll. Forskjellene på de ulike bruksområdene er kort omtalt nedenfor.

MASSEOVERVÅKING

Masseovervåking bruker ansiktsgjenkjenning til å plukke ut enkeltpersoner i en folkemengde. Dette krever spesialisert maskinvare og kraftig programvare for å fungere effektivt.

PERSONLIG GODKJENNING

Denne typen ansiktsgjenkjenning brukes ofte på mobilenheter, for eksempel smarttelefoner, med relativt enkle krav til programvare og maskinvare. Her brukes ansiktet som et alternativ til et passord eller en kode.

KRIMINALITETSETTERFORSKNING

Ansiktsgjenkjenning kan også brukes til å rekonstruere en persons bevegelser basert på videobilder.

Slike data kan for eksempel bidra til å identifisere hvor en rømling har vært de siste 24 timene.

ADGANGSKONTROLL

Til slutt kan ansiktsgjenkjenning brukes innen adgangskontroll. Det er viktig å sette opp programvaren slik at informasjon fra flere kameraer sammenlignes med databasen i sanntid. Basert på databasens størrelse installeres det en server som kan kontrollere godkjenningen raskt nok, og adgangspunktet kan deretter åpnes.

I DETTE **WHITE PAPER**:



**FORDELER
MED
ANSIKTSGJENKJENNING**



**KOMPONENTENE
I ANSIKTSGJENKJENNING**



**TEKNISKE
ASPEKTER**



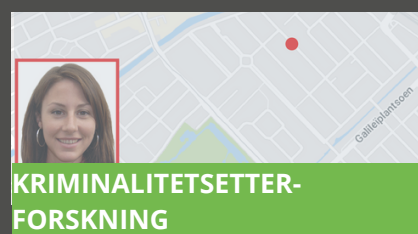
**I
PRAKSIS**



**DIGITAL
SIKKERHET**



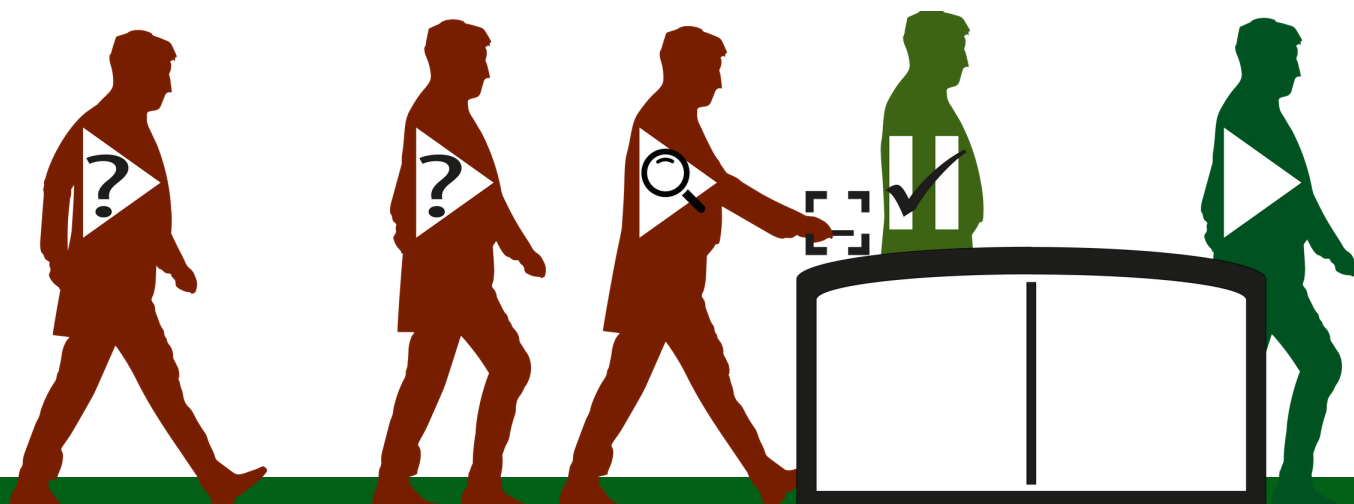
ADGANGSKONTROLL



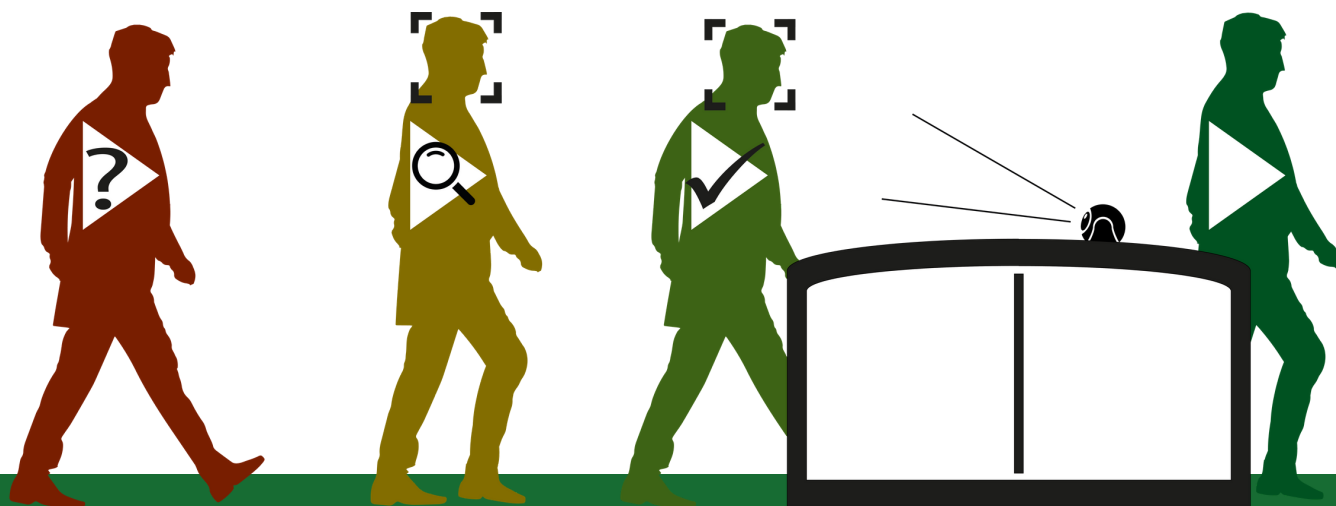


FORDELER MED ANSIKTSGJENKJENNING.

‘«TRADISJONELL» KORTLESER



ANSIKTSGJENKJENNING



HØYERE KAPASITET

En av de store fordelene ved adgangskontroll med ansiktsgjenkjenning er at det ikke er ventetid ved adgangspunktet. Programvaren registrerer en persons ansikt når vedkommende nærmer seg, og kan avgjøre om adgang skal gis i løpet av tiden det tar å gå frem til porten. Systemet åpner porten når den godkjente personen er nær eller ved adgangspunktet. Dette hindrer at uautoriserte personer smetter inn gjennom den åpne porten. Personen kan også gå gjennom adgangspunktet uten å stanse.



ALLTID RASK TILGANG

Fordi biometrisk ansiktsgjenkjenning er basert på noe vi mennesker alltid har med oss, slipper man å møte en stengt dør. Siden alle ansikter er unike, kan ulike personer skilles fra hverandre og identifiseres via ansiktstrekkene.

En annen fordel er at det krever bare et minimum av aktivt samarbeid fra brukeren ved adgangskontrollpunktet. Programvaren kan kontrollere godkjenningen så snart et ansikt kommer inn i kameraets fokusområde. Man slipper situasjoner der noen har glemt adgangskortet, siden det ikke lenger er nødvendig. I tillegg slipper man å vente på at en kollega skal grave gjennom tingene sine for å finne adgangskortet, og man har hendene fri til å bære vesker og annet.

INGEN DELING AV ADGANGSKORT

Personlige adgangskort som deles med kolleger er et vanlig problem ved adgangskontroll. Slik uriktig bruk kan føre til at uautoriserte personer får adgang til lokalene. Med ansiktsgjenkjenning hindres ukjente personer automatisk i å passere gjennom adgangskontrollen.

Adgangskontroll med ansiktsgjenkjenning gjør det dessuten umulig å stjele eller kopiere et adgangskort. Resultatet er at det generelle sikkerhetsnivået blir forbedret.



BIOMETRI ER BERØRINGSFRI

Mange nøler et lite øyeblikk før de skanner øyet eller fingeren. Denne (ubevisste) nølingen skyldes at man ikke er kjent med systemet eller er motvillig til å holde en kroppsdel aktivt mot skanneren. I tillegg til at det forstyrrer gjennomstrømningen, kan dette føre til at adgangskontrollen oppleves som mindre brukervennlig.

En annen stor fordel med ansiktsgjenkjenning er det faktum at brukerne registreres på avstand via et kamera. Brukerne trenger ikke å stille seg i en uvant posisjon eller berøre adgangspunktet fysisk. Identiteten kontrolleres så snart de kommer innenfor kameraets rekkevidde, og de kan gå gjennom adgangspunktet uten å stanse.



KOMPONENTENE I ANSIKTSGJENKJENNING.

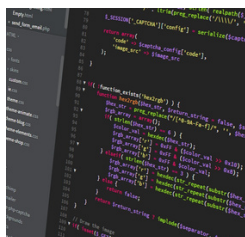
Når man velger adgangskontroll med ansiktsgjenkjenning må man ta hensyn til at systemet består av flere komponenter. Disse komponentene kommer ofte fra ulike leverandører, og de må fungere sammen. Derfor er det viktig å undersøke hvilke leverandører som kan bygge opp et velfungerende system. Generelt må følgende komponenter fungere sammen:



KAMERA OG ANDRE SENSORER

Kameraet er et viktig element ved pålitelig bruk av ansiktsgjenkjenningsprogramvare. Det finnes ulike kameraer med høy kvalitet på markedet. Erfaringen har vist at et omhyggelig valg basert på både tekniske og estetiske faktorer kan bidra til at brukerne opplever systemet som brukervennlig, og tar det i bruk.

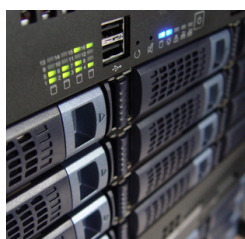
Valgprosessen handler om mer enn bare antall megapiksler; lysfølsomhet, linsetype og databrikkens prosesseringskraft er også viktige hensyn. Det er også mulig å velge flere sensorer, slik at et ansikt for eksempel kan skilles fra et fotografi.



PROGRAMVARE FOR ANSIKTSGJENKJENNING

Programvaren er hjertet i ansiktsgjenkjenningssystemet, og konverterer ansiktstrekk til en kode som kan sammenlignes med en eksisterende database. Gjenkjenningen skjer ved hjelp av en rekke algoritmer. Ansiktsgjenkjenningsprogramvaren fungerer uavhengig av andre typer adgangskontrollprogramvare. Dette gjør det mulig å opprette et frittstående system der programvaren kjøres på en ekstern prosessor.

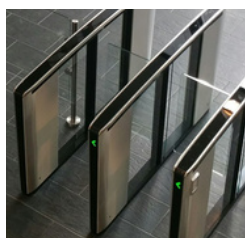
Det er viktig å forsikre seg om at programvaren og systemet samsvarer med EUs personvernforordning (GDPR) og har de riktige krypteringsstandardene.



ADGANGSKONTROLLSYSTEM

Adgangskontrollsystemer kombinerer ofte flere programvareløsninger. Disse løsningene er ofte integrert med et sikkerhetssystem eller et bygningssystem. Derfor må ansiktsgjenkjenningsprogramvaren også være kompatibel med slike systemer.

I praksis betyr det at ulike moduler kobles sammen for deretter å kontrolleres av ett enkelt, sentralt program. I slike tilfeller blir programvaremodulen for ansiktsgjenkjenning integrert ved hjelp av et API.



FYSISK ADGANG

Innen adgangskontroll brukes ansiktsgjenkjenning alltid i kombinasjon med et fysisk adgangskontrollprodukt. Det er tross alt ikke mulig å nekte uautoriserte personer adgang uten at en fysisk sperre er på plass. Det finnes ulike sperrealternativer, hvert med sin innvirkning på sikkerheten.

Komponentene kan konfigureres på ulike måter. Det finnes for eksempel fysiske produkter med fullt integrert ansiktsgjenkjenning, men komponentene kan også kjøpes separat.



TEKNISKE ASPEKTER.



LYSFORHOLD

En av de viktigste faktorene for vellykket ansiktsgjenkjenning er lysforholdene der kameraet er plassert. Ansiktsgjenkjenning for adgangskontroll finner ofte sted innendørs, og det er lett å tilpasse lysforholdene.

Overeksponering kan være en utfordring. Eksempler på dette er sterkt sollys eller gjenskinns fra refleksjoner eller høye glasstak. Variasjoner i belysningen kan være vanskelig å håndtere for kameraet og ansiktsgjenkjenningsprogramvaren.

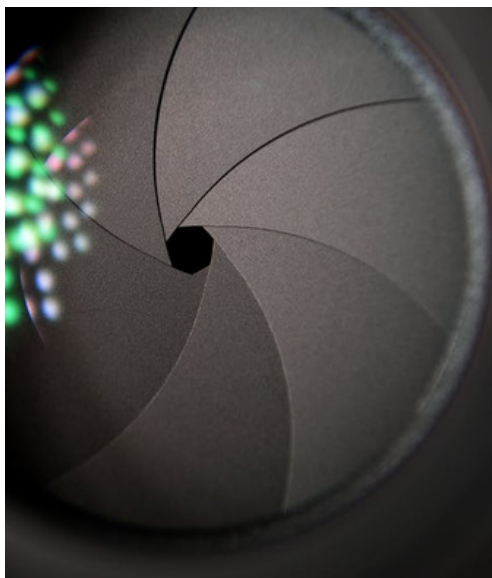
Undereksponering er mye lettere å korrigere. Ofte er det nok å justere kamerainnstillingene for å oppnå god gjenkjenning. Det anbefales å engasjere en ekspert for å få riktige innstillinger.

KAMERAPLASSERING

Vurder kamerabildet nøye når kameraet skal monteres. Jo kortere avstand det er mellom kameraet og personen som ønsker adgang, desto høyere blir bildekvaliteten.

Kameraets plassering i forhold til brukeren er også relevant. Det er best å plassere kameraet slik at brukerne allerede ser i kameraets retning når de forbereder seg på å passere gjennom adgangspunktet. På den måten trenger de ikke å foreta noen ekstra bevegelser for å bli gjenkjent.

Til slutt kan det være ønskelig å integrere kameraet i adgangskontrollproduktet eller montere det eksternt av estetiske årsaker.



KAMERAFOKUS

Fokus må vurderes nøye når kameraet installeres. Kameraet må fokusere på stedet der ansiktsgjenkjenningen finner sted. Fokuspunktet kan ikke være for langt fra adgangspunktet (for å hindre at personer smetter inn), og heller ikke for nær (noe som fører til venting).

Kameraets fokus avgjør også området der ansikter blir gjenkjent. Dette kan justeres ved å velge et bildeområde der ansiktsgjenkjenning skal finne sted i programvaren.

Våre eksperter hjelper deg gjerne å velge de riktige tekniske spesifikasjonene for din situasjon.



I PRAKSIS.

BRUKERGJENNOMSTRØMNING

Speed gates oppmuntrer i praksis brukerne til å se forover på en naturlig måte. Personene beveger seg gjennom produktet i rett linje, og ser forover. Resultatet er en relativt liten sone som alle brukernes ansiktet passerer gjennom.

En annen stor fordel ved adgangskontroll med ansiktsgjenkjenning er den økte brukergjennomstrømningen. Dette skyldes at alle brukerne er på vei i samme retning, og beveger seg gjennom speed gaten i en jevn strøm. Ansiktsgjenkjenning sikrer at godkjenningsprosessen går raskt nok til å opprettholde rask gjennomstrømning.



WISE ANSIKTET

Tidligere i dette white paper ble det nevnt at brukerne ikke trenger å foreta noen ekstra bevegelser ved adgangskontroll med ansiktsgjenkjenning. Dette avhenger imidlertid av at brukeren er oppmerksom på at ansiktsgjenkjenningsprogramvaren må kunne skanne vedkommendes ansikt.

I praksis betyr det at brukerne må vise ansiktet mer eller mindre uhindret for kameraet. De kan ikke gå gjennom adgangspunktet med ansiktsmaske eller mens de for eksempel ser bakover. Brukerne må samarbeide for at systemet skal fungere.

INTERAKSJON MED BRUKEREN

Gode tilbakemeldinger til brukeren er viktig ved bruk av ansiktsgjenkjenning og adgangskontroll generelt. Hvis flere personer bruker et adgangspunkt i rask rekkefølge, kan visuelle signaler og lydsignaler indikere programvarens konklusjoner for brukeren.

Ansiktsgjenkjenning er velegnet i situasjoner med mange tilbakevendende brukere. En bruker kan gis tilgang i så lang tid som er nødvendig etter å ha registrert seg én gang. Tilbakevendende brukere blir også vant til interaksjonen med adgangskontrollproduktet.





DIGITAL SIKKERHET.



KRYPTERING

Ansiktsgjenkjenningsprogramvaren bruker kryptering for å hindre hacking av data og bilder som sendes via et nettverk. Kryptering innebærer koding av digital (bilde-) informasjon. Det er umulig for utenforstående å lese dataene uten å kjenne krypteringsprosessen på forhånd.

Ulike datakrypteringsmetoder er tilgjengelige. Hvilken løsning som er best egnet, avhenger av den eksisterende infrastrukturen og videoprogramvaren. Det spiller for eksempel en rolle om dataene sendes over et åpent eller et lukket nettverk. Våre eksperter besvarer gjerne spørsmålene dine om dette emnet.

PÅVISNING AV SVINDEL

Når det gjelder påvisning av svindel, er ansiktsgjenkjenning i konstant utvikling. Målet er å hindre at systemet blir «lurt», for eksempel ved at man holder opp et fotografi til kameraet. Det finnes for øyeblikket to metoder for å påvise og hindre svindel:

- Maskinvarebasert deteksjon med 3D-sensorer som skanner ansiktsstrukturen. Én versjon innebærer en sensor som registrerer mønsteret av fargede lysstråler som reflekteres fra et ansikt.
- Programvarebasert deteksjon som registrerer svært små avvik i videobildet. Dette krever mye videoprosesseringskraft, slik at man trenger større og kraftigere servere.



EUS PERSONVERNFORORDNING

Tidligere i dette white paper ble det nevnt at ansiktsgjenkjenning benytter biometriske data. Når det gjelder EUs personvernforordning (GDPR) er det viktig å være oppmerksom på at biometriske data tilhører en spesiell kategori av personopplysninger. Data i denne kategorien kan brukes til personlig identifisering under bestemte betingelser. Dataene kan kun brukes til godkjennings- eller sikkerhetsformål. Dessuten må systemadministratoren kunne dokumentere at databehandlingen skjer i samsvar med denne forordningen. Bruk av ansiktsgjenkjenning til adgangskontroll er derfor lovlig.



KONKLUSJON.

Målet med dette white paper er å gi noen basiskunnskaper om hva adgangskontroll med ansiktsgjenkjenning innebærer, og hvilke hensyn som må tas for å finne det best egnede ansiktsgjenkjenningssystemet for din virksomhet. Det forklarer forskjellene mellom ulike metoder for biometrisk gjenkjenning og ansiktsgjenkjenning. I tillegg beskriver det fordeler med ansiktsgjenkjenning sammenlignet med tradisjonelle adgangskontrollsystemer.

Vi introduserer også de ulike komponentene av ansiktsgjenkjenningssystemer som brukes til adgangskontroll, samt de viktigste tekniske og praktiske aspektene ved ansiktsgjenkjenningssystemer. Til slutt omtaler dette white paper kort bruken av ansiktsgjenkjenning med tanke på digital sikkerhet og gjeldende personvernregler.

ANBEFALINGER

Med dette white paper har Boon Edam forsøkt å gi litt innsikt i betingelser og krav som er forbundet med ansiktsgjenkjenning. Vi mener at ansiktsgjenkjenningsteknologien har vist sin verdi de siste årene, og at den kommer til å bli mer utbredt i fremtiden. I tillegg ønsker vi å påpeke at ansiktsgjenkjenning er egnet for adgangskontroll på nesten alle sikkerhetsnivåer. Vi hjelper deg gjerne å velge og implementere et optimalt system basert på dine egne behov når det gjelder innføring av ansiktsgjenkjenning og dine spesifikke omstendigheter (for eksempel antall personer som systemet skal gjenkjenne, adgangspunktenes plassering osv.).

Kontakt forfatteren av dette white paper eller en av våre andre eksperter hvis du ønsker mer informasjon om adgangskontroll med ansiktsgjenkjenning. Vi kommer gjerne på et uforpliktende besøk.

VANLIGE SPØRSMÅL.

Hvis jeg som bruker nærmer meg et adgangspunkt med ansiktsgjenkjenning, blir ansiktstrekkene mine kodet og sammenlignet med en database. Betyr det at bildet av meg bli lagret?

Nei, databaseoppretting krever ikke at brukernes ansikter blir lagret; en liste over hash-koder er tilstrekkelig. Bruk av adgangsprodukter krever heller ikke at fotografier blir lagret for sammenligningsformål. I praksis kan imidlertid installasjoner med ansiktsgjenkjenning lagre fotografier (midlertidig) av og til for å optimere programvaren. Disse bildene lagres på en frittstående server, og kan ikke deles med tredjeparter.

Blir det lagret andre data i tillegg til hash-koden?

Tradisjonelle adgangskontrollsystemer registrerer generelt tidspunktet da en autorisert person går inn i et lokale, og dette gjelder også installasjoner med ansiktsgjenkjenning. Det er mulig å tilpasse innstillingene for å unngå lagring av slike data.

Er denne typen ansiktsgjenkjenning egnet for bruk med andre inngangsløsninger enn porter?

Ja, denne typen ansiktsgjenkjenning er også egnet for ulike andre inngangsløsninger. Vi diskuterer gjerne mulighetene med deg.

VI HAR GLOBAL REKKEVIDDE.

Vi produserer adgangsløsninger med førsteklasses utseende og sikkerhet i Nederland, USA og Kina, og har vært i bransjen i mer enn 140 år. Vi har datterselskaper i større byer over hele verden, og kan trygt si at vi dekker alle verdenshjørner. Vår globale eksportdivisjon samarbeider ikke bare med våre distributører, men tilbyr også direktesalg og service over hele verden. Dette store nettverket gir oss en sterk, global tilstedeværelse og gode kunnskaper om lokale markeder med unike krav til adgangskontroll.

Finn din nærmeste Boon Edam-ekspert her:
www.boonedam.no/touchless



Boon Edam AS
T +47 67 10 33 40
E info@boonedam.no
I www.boonedam.no


BOON EDAM
YOUR **ENTRY** EXPERTS.