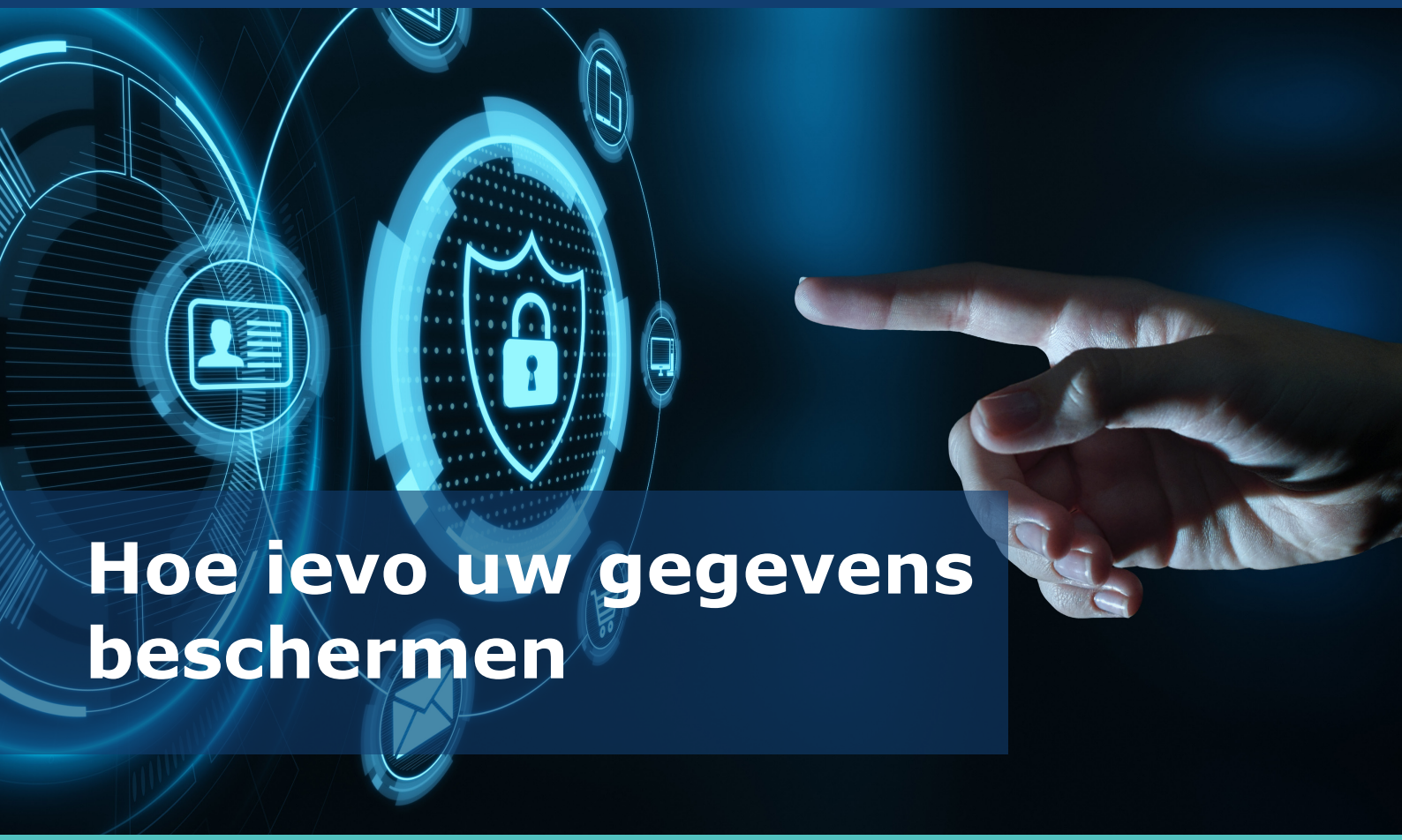
CDVI
Security to Access

ievo



Hoe ievo uw gegevens beschermen

Biometrie heeft betrekking op onderscheidende, meetbare menselijke kenmerken die een individu kenmerken en beschrijven. Door deze biologische kenmerken te meten en te analyseren kunnen de gegevens worden gebruikt voor unieke veiligheidsidentificatie.

INLEIDING

Biometrische vingerafdrukken van ievo worden beschouwd als de meest betrouwbare en betrouwbare vorm van hoogwaardige beveiliging en bieden veel meer voordelen dan de gebruikelijke beveiligingsoplossingen. Het voordeel van het gebruik van biometrie is dat veelvoorkomende fouten zoals verloren, gestolen of gekopieerde kaarten/fobs, vergeten pincodes en/of toegangscodes, bedreigingen door hackers of andere vormen van onnodige gebruikersinteractie allemaal worden opgelost. Dit bespaart tijd en middelen terwijl de veiligheid van toegangscontrole systemen wordt verbeterd.

ievo systemen beschermen niet alleen gebouwen en lokalen, maar ook individuen en verhogen de productiviteit in tijd- en aanwezigheidsbeheer.

VEILIGHEID

Omdat biometrische gegevens uniek zijn voor een individu, biedt dit veel mogelijkheden voor verhoogde beveiligingsniveaus voor identificatiedoeleinden, die betrouwbaarder, nauwkeuriger en efficiënter zijn dan de meer traditionele beveiligingsniveaus.

Het is van vitaal belang te begrijpen hoe de biometrische systemen van ievo deze gegevens gebruiken en opslaan, om de gebruikers de zekerheid te geven dat deze informatie volledig beschermd is.

Lees hier meer over hoe ievo uw gegevens gebruikt en opslaat.

CDVI
Security to Access

ievo

VASTLEGGEN VAN UW GEGEVENS

Bij het registreren van een vingerafdruk scant een ievo-systeem en extraheert gegevens met behulp van een extractiealgoritme dat specifieke kenmerken binnen een vingerafdruk identificeert, de zogenaamde minutiae.

Geïdentificeerde minutiae punten worden gecategoriseerd in groepen, die lijn bifurcaties en ridge eindigingen omvatten onder andere gegevensgroepen. Na een geregistreerde scan stuurt een ievo-lezer een beeld van de vingerafdruk naar het ievo-besturingspaneel, waar een geavanceerd algoritme het type, de richting en de afstand tussen de belangrijkste minutiae-kenmerken van een vingerafdruk vaststelt (fig.1). Deze gegevens worden omgezet in een sjabloon en opgeslagen in een database op het ievo controlebord. Het originele vingerafdrukbeeld wordt niet opgeslagen of geregistreerd.

Bij gebruik van een lezer voor toegang begint een soortgelijk proces als hierboven beschreven. Dit keer wordt echter het matching-algoritme gebruikt om de nieuwe minutiaegegevens te vergelijken met de opgeslagen sjablonen in de databank. Zodra een vooraf ingesteld aantal minutiae-punten met een opgeslagen sjabloon is vergeleken, wordt de identiteit van de gebruiker bevestigd; deze bevestiging wordt doorgestuurd naar het toegangscontrolesysteem of het "tijd- en aanwezigheids"-systeem voor invoer en/of registratie van gegevens.

GEGEVENS BEVEILIGD

Zodra een vingerafdruk is gescand, wordt het originele beeld niet opgeslagen of bewaard. De enige geregistreerde gegevens zijn de belangrijkste datapunten van een vingerafdruk die worden overgebracht en opgeslagen op een ievo controlekaart in een uniek, gepatenteerd sjabloonformaat. Het opgeslagen sjabloon is uniek voor een individu en het sjabloon is alleen toegankelijk voor identificatiedoeleinden door het ievo-controlebord. De gegevens zijn voor geen enkel ander doel toegankelijk en kunnen ook niet met gewone software worden ingezien.

ievo systemen maken gebruik van een geavanceerd Automated Fingerprint Identification System (AFIS) algoritme voor gegevensinvoer, extractie en matching processen. Deze gegevens kunnen niet worden omgekeerd om een beeld van de originele vingerafdruk te reconstrueren.

Voor meer informatie over ievo vingerafdruklezers en gegevensbescherming kunt u contact met ons opnemen.

UW GEGEVENS

Een geavanceerd extractiealgoritme wordt gebruikt om een sjabloon te maken van specifieke vingerafdrukgegevens die na een scan worden vastgelegd. Deze gegevens (fig.2) worden opgeslagen in een uniek, gepatenteerd sjabloonformaat. Alle andere informatie wordt niet opgeslagen of bewaard. De gegevens KUNNEN NIET worden gebruikt om het originele vingerafdrukbeeld opnieuw te reconstrueren.

BEVEILIGING

ievo-systemen werken met een afzonderlijk bedieningspaneel dat een ievo-lezer aanstuurt, wat betekent dat er geen informatie of gegevens lokaal op de lezer zelf worden opgeslagen. Voor extra veiligheid moet de ievo control board altijd aan de beveiligde kant van een toegangspunt worden geïnstalleerd, uit de buurt van de lezerunits.

ievo-lezers bevatten geen vergrendelingsmechanismen of deurrelais, wat betekent dat als een lezer zou worden verwijderd, uw toegangspunt veilig zou blijven en uw gegevens veilig zouden blijven. De lezers zou voor de aanvaller nutteloos zijn, omdat deze geen gegevens bevat.

Fig.1: Afbeelding van wat een ievo-lezer scant en de belangrijkste minutiae-kenmerken.

Fig.2: Image depicting key feature data which is extracted, transferred and stored as a template.

GDPR

CDVI Benelux bezit of beheert geen persoonsgegevens met betrekking tot de ievo-lezers en zal alleen op afstand toegang hebben tot dergelijke persoonsgegevens wanneer het ondersteuning biedt aan eindgebruikers, in welk geval het optreedt als een gegevensverwerker en handelt in opdracht van een Data Controller.

Als gegevensbeheerder moeten installateurs en eindgebruikers van een ievo-systeem ervoor zorgen dat zij volledig voldoen aan de Algemene Verordening Gegevensbescherming 2016/679, aangezien zij het verzamelen van gegevens en de doeleinden van de verwerking controleren om de vingerafdruk van de gebruiker te identificeren en toegang te verlenen of tijd & aanwezigheid te registreren.