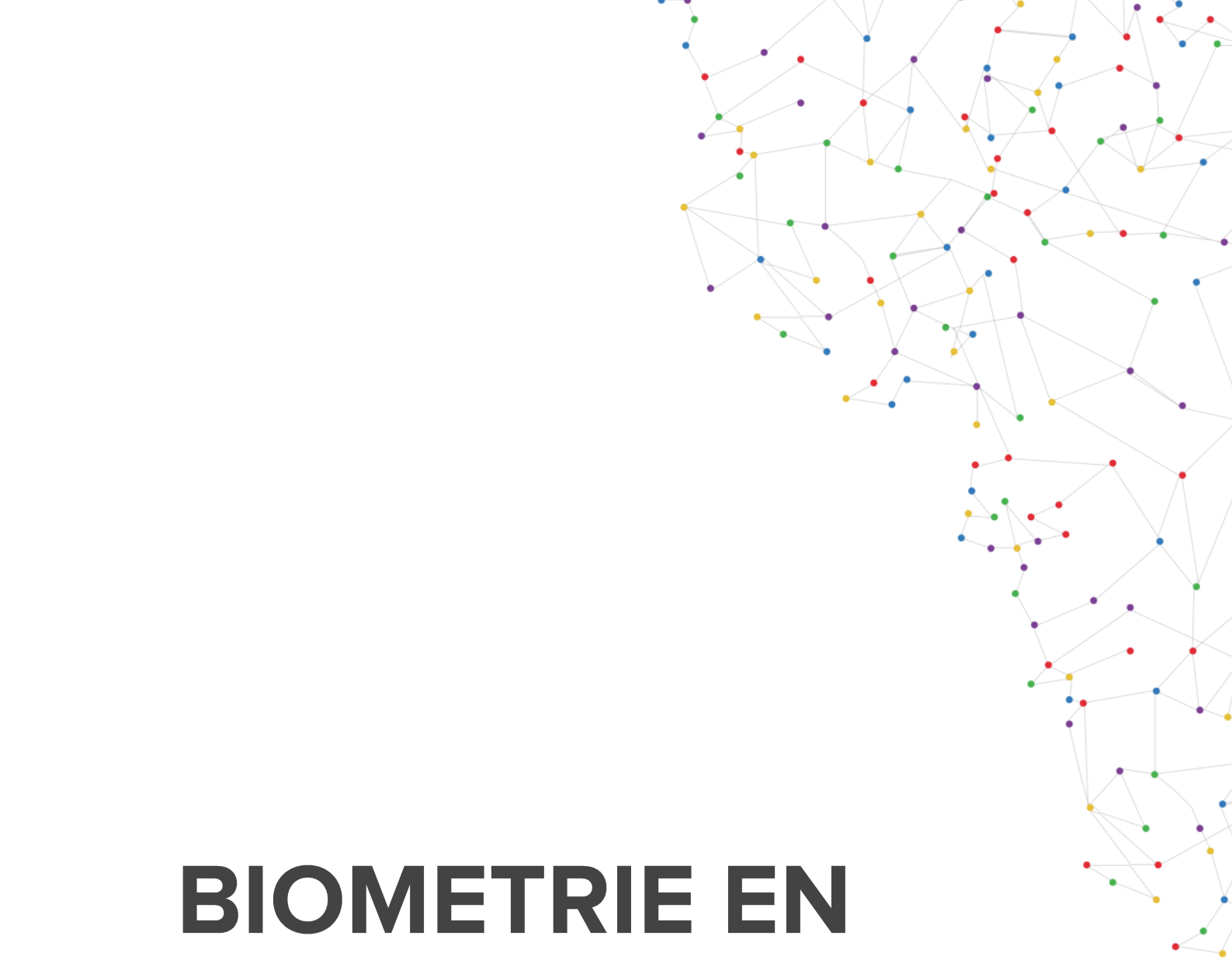

BIOMETRIE EN URENMANAGE-MENTSYSTEMEN

Overwegingen voor het veilig en privacy-vriendelijk toepassen van biometrische hulpmiddelen

Tijdplein.nl, een ledennetwerk van Nederland ICT, in samenspraak met de VVBI (vvbi.nl)

Augustus 2016

Voor de digitale economie

NEDERLAND ICT

INLEIDING

Biometrie is de kunde die zich bezighoudt met het vaststellen van identiteit op basis van unieke waarden van biologische eigenschappen van mensen. Steeds vaker worden urenmanagementsystemen (workforce management systemen) voor aan- en afwezigheidregistratie (tijdregistratie) voorzien van boekingsterminals met een biometrische lezer (vingerscan). Omdat een vingerafdruk een uniek kenmerk is van een persoon, kan het gebruik daarvan voor toegangs- en aanwezigheidsregistratie de veiligheid en betrouwbaarheid maar ook het gebruiksgemak enorm vergroten. Tegelijkertijd groeien de zorgen bij gebruikers of er niet te veel van de eigen identiteit 'weggegeven' wordt en of het wel veilig is.
De leveranciers van urenmanagement- en tijdregistratiesystemen, verenigd Tijdplein.nl, een ledennetwerk van Nederland ICT, willen graag met deze whitepaper duidelijkheid geven over de mogelijkheden van biometrie en de factoren die van invloed zijn op privacy en veiligheid.
Deze whitepaper behandelt eerst de basis van de inzet van biometrie, de verschillende technieken en opslagmethoden en de voor- en nadelen hiervan. Vervolgens wordt aangegeven welke relatie dit met privacy(wetgeving) heeft en met welke privacyaspecten er rekening gehouden moet worden. Tot slot wordt een aantal overwegingen meegegeven aan bedrijven die willen starten met het gebruik van biometrie.

DE BASIS VAN BIOMETRIE: INZET IN TWEE FASEN

Het succesvol invoeren van biometrie als hulpmiddel voor urenregistratie bestaat uit twee fasen:

1. **Enrollment**

   In deze fase worden de gebruikers in het systeem ingevoerd om later te kunnen worden herkend. Dit gebeurt door een nulmeting te doen die leidt tot een eerste vast te leggen meetwaarde (template of referentiewaarde). Dit gebeurt meestal op een boekingsterminal zelf of via een aparte inlees-unit die met de software verbonden is. Deze referentiewaarde wordt op een persoonlijk opslagmedium (een token, badge of smartcard), of in een centrale database opgeslagen.

2. **Gebruik**

   Hierin zijn drie stappen te onderscheiden:

   - Collection: het aanbieden van de vinger op de boekingsterminal, zodat de biometrische eigenschap gemeten kan worden en het omzetten ervan in een digitale representatie. Op dit grensvlak van analoge en digitale techniek, op de grens van hardware en software, biedt vrijwel iedere leverancier zijn eigen standaard aan;
   - Comparison: de vergelijking van de digitale representatie met de opgeslagen referentiewaarde. Als de referentiewaarde is opgeslagen op een persoonlijk opslagmedium, dan is dit een snel proces. Als echter matching moet plaatsvinden in een (grote) centrale database kan dit langer duren. Het eerst vragen van een user-id (een nummer of een pas) kan het zoeken aanzienlijk versnellen;
   - Pass/fail: de beslissing of de gemeten vingerafdruk voldoende nauwkeurig overeenkomt met de meest passende, of op basis van aangedragen user-id gevonden referentiewaarde, op basis waarvan de persoon al dan niet wordt toegelaten.

CENTRALE EN DECENTRALE OPSLAG

Zoals kort genoemd, kunnen we onderscheid maken tussen toepassingen die zijn gebaseerd op een (centrale) database met biometrische gegevens en toepassingen met een persoonlijk opslagmedium, waarbij de referentiewaarde in een token, badge of smartcard is opgeslagen. Dit onderscheid heeft theoretische en praktische consequenties.

Vergelijkbaarheid

Een centrale database heeft het voordeel van het centraal bijeen hebben van biometrische en andere gegevens, die daardoor eenvoudig onderling vergelijkbaar zijn en blijven. Dit maakt zowel het schonen van de database mogelijk (ontdubbelen, op basis van naam of op basis van extreem nauwkeurig overeenkomende biometrie) alsook het vaststellen van de toegestane of vereiste foutmarge in de meting.

Infrastructuur

In het geval van centrale opslag is er dataverkeer nodig tussen de boekingsterminal en de centrale database. Het gebruik van centrale opslag stelt dan ook andere eisen aan de infrastructuur en beveiliging van deze infrastructuur. Het is bijvoorbeeld aan te raden gebruik te maken van een versleutelde verbinding.

Kwetsbaarheid hacken

Het centraal verzamelen van gegevens op één centrale database verhoogt het risico van derden die zonder toestemming willen inbreken op de database systemen (hacken). Decentrale opslag is hiervoor onaantrekkelijk. Eén van de belangrijkste mogelijkheden om de veiligheid inherent te verhogen is de wijze van aanmaken van de referentiewaarde, zodat de referentiewaarde niet terug te herleiden is tot een persoon. Indien de referentiewaarden alleen op een persoonlijk opslagmedium staan, dan kunnen niet alle gegevens tegelijk gestolen worden.

MODERNE OPSLAGTECHNIEKEN

Veel systemen van de overheid (justitie, paspoort etc.) gebruiken een systeem waarbij men letterlijke kopieën of plaatjes opslaat van de vingerafdruk. Dit wordt AFIS (Automated Fingerprint Identification System) genoemd. Deze plaatjes kunnen, als zij in verkeerde handen vallen of verkeerd gebruikt worden, misbruikt worden en privacy van mensen schenden.

Het is vanuit een beveiligings- en privacy-optiek beter om voor tijdregistratie en toegangscontrole gebruik te maken van een algoritme dat de vingerafdruk middels een slimme rekenmethode omzet in een one-way code. Deze code bestaat uit een lange reeks cijfers. De code kan niet worden ‘teruggerekend’ naar een daadwerkelijke vingerafdruk. De code kan dan ook niet zo maar worden gekoppeld aan een persoon. Een dergelijke encryptiemethode verhoogt de veiligheid van zowel opslag op een persoonlijk medium als in een centrale database met referentiewaarden dan ook enorm.

BETROUWBAARHEID EN NAUWKEURIGHEID

Een belangrijke factor die telkens weer opduikt, is de betrouwbaarheid van biometrische systemen. Die is uit te drukken in de technische maten False Rejection Rate en False Acceptance Rate. Vrij vertaald wil je niet teveel mensen afwijzen bij registratie doordat de lezer té nauwkeurig afgestemd staat, of omgekeerd te veel mensen accepteren die niet geautoriseerd zijn.

De False Rejection Rate

Dit is de kans dat een aanmelder ten onrechte wordt afgewezen op basis van de biometrische meetwaarde. Het doel is deze zo laag mogelijk te houden, om te voorkomen dat gebruikers klagen over onterechte afwijzingen. Dit vraagt om zo ruim mogelijke meetmarges, zeker omdat rekening moet worden gehouden met veranderlijkheid van persoonlijke biometrische kenmerken in de tijd en wegens klimaatomstandigheden.

De False Acceptance Rate

Dit is de kans dat een aanmelder ten onrechte wordt geaccepteerd op basis van de biometrische meetwaarde. Het doel is deze zo laag mogelijk te houden, omdat uniciteit van de identificatie en authenticiteit wordt nagestreefd. Dit betekent een streven naar zo klein mogelijke meetmarges, ondanks de veranderlijkheid van biometrische karakteristieken.

De Failed to Enroll Rate

Bij vingerherkenning komt ook de FER (Failed to Enroll Rate) aan de orde. Dit zegt iets over het percentage van medewerkers dat niet ingelezen kan worden. (Eind-)gebruikers dienen zich te realiseren dat er van een beperkt percentage (2 á 3 %) van de medewerkers geen bruikbare vingerafdruk is te maken.

Per geval verschillend

Per organisatie kan het verschillen hoe de software of de lezers ingesteld moet worden. Ook is van belang of met een aanvullende ID-methode, zoals een code, ID-card of persoonlijk opslagmedium, dan wel alléén met een biometrische methode en een centrale database wordt gewerkt. De keuzes daarin hangen af van de mate van beveiliging die binnen een bedrijf nodig en gewenst is. Stel je het systeem te strak af dan worden er wellicht meer mensen geweigerd dan je zou willen. Stel je het systeem te ruim af dan worden door het systeem wellicht twee medewerkers door elkaar gehaald of worden onbevoegden mogelijk toegelaten.

EEN VOORBEELD UIT DE PRAKTIJK

De smartcard waarop de referentiewaarde staat, wordt dicht bij een leesapparaat gehouden en uitgelezen. De ter plekke gemeten biometrische waarde kan meteen worden gecontroleerd op voldoende overeenkomst met slechts die ene waarde. Dit systeem werkt sneller dan controle via een centrale database. Daarbij verlaat de data de boekingsterminal niet. Na de controle kan de informatie meteen van de boekingsterminal verwijderd worden. Er wordt dan verder niets opgeslagen. Tot slot laat de vergelijking in dit geval vaak een wat grotere tolerantie in de matching toe omdat sprake is van authenticatie in combinatie met de smartcard(user-id) en dus nauwelijks verwarring met andere gebruikers mogelijk is (zie onder 'betrouwbaarheid voor meer informatie over meettoleranties).

VOORDELEN VAN VERSCHILLENDE VORMEN VAN OPSLAG

De voordelen van alléén een biometrische methode en een centrale database zijn:

- Geen aanschaf van badges (kaarten) of tags (druppels/sleutelhangers).
- Geen administratie bijhouden van wie welke pas heeft.
- Pasjes kunnen uiteraard niet zoek of beschadigd raken en ze kunnen uiteraard niet meer vergeten worden.
- Medewerkers kunnen niet voor een ander klokken.

De voordelen van een biometrische methode in combinatie met een persoonlijk opslagmedium zijn:

- De identificatie gaat sneller.
- De False Rejection Rate is lager.
- Er is een hogere inherente veiligheid voor bedrijf en medewerker omdat er geen dataverkeer wordt uitgewisseld en er geen centrale database is.

PRIVACY EN BIOMETRIE

Wetgeving

De Wet bescherming persoonsgegevens (Wbp) stelt regels voor de verwerking van persoonsgegevens door een bedrijf. Een biometrisch kenmerk, zoals een vingerafdruk, is een persoonsgegeven omdat het herleidbaar is tot een persoon. Als plaatjes van de vingerafdruk worden opgeslagen, dan geldt dat als een verwerking van persoonsgegevens en zijn op die verwerking alle regels uit de Wbp van toepassing.

De bij Nederland ICT aangesloten leveranciers van deze systemen zijn zich bewust van hetgeen voorgeschreven wordt in de Wbp ten aanzien van omgang met persoonsgegevens binnen de door hen geproduceerde en geleverde systemen.

Behandelen als persoonsgegeven

Indien het biometrische kenmerk wordt omgezet in een one-way code zoals hierboven beschreven, dan is maar de vraag of die code nog wel een persoonsgegeven is. Immers, het is niet meer herleidbaar tot het biometrisch kenmerk en dus niet meer tot de persoon. Voor de zorgvuldigheid is het verstandig zowel het biometrisch kenmerk als de code te behandelen als een persoonsgegeven, zodat de Wbp daarop van toepassing is. Zo wordt een zorgvuldige omgang met al deze gegevens alleen maar vergroot. Aangezien er bij de toepassing van urenmanagementsystemen en de toepassing van biometrische gegevens sprake is van verwerking van persoonsgegevens, moet de klant zich als verantwoordelijke voor die verwerkingen aan de Wbp houden. Hieronder zullen we aan een aantal specifieke aspecten van de Wbp aandacht besteden. Naast deze specifieke aspecten moet een bedrijf zich natuurlijk aan alle verplichtingen uit de Wbp houden bij iedere verwerking van persoonsgegevens.

Informeren personeel

Persoonsgegevens moeten op een behoorlijke en zorgvuldige wijze worden verwerkt. Een onderdeel daarvan is dat het personeel voorafgaand aan de introductie van een urenmanagement (tijdregistratie)systeem geïnformeerd wordt over deze verwerkingen en het doel ervan. Indien er een OR is, heeft deze zelfs instemmingsrecht. Voor de implementatie van de scanners moet deze procedure dus afgerond zijn.

One way code

Een belangrijke methode om de privacy te vergroten is het gebruik van een opslagmethode van de referentiewaarden waarbij geen plaatjes worden opgeslagen maar waarbij van het biometrisch kenmerk een one way code wordt gemaakt. Het adviesorgaan voor de privacy van de EU, de 'artikel 29 werkgroep', zegt daarover in haar rapport over biometrische toepassingen: *"The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template"* . Deze werkwijze biedt belangrijke extra privacywaarborgen, omdat een hacker of onbevoegde de code niet kan herleiden naar een persoon en de code op zichzelf ook niet kan gebruiken om zichzelf toegang te verschaffen tot systemen of plaatsen.

Niet-gekoppelde databases

Een andere waarborg die gesteld wordt is dat de medewerkerdata in bijvoorbeeld het HR-systeem separaat wordt gehouden van de database met referentiewaarden. Zo kan de code ook niet eenvoudig gekoppeld worden aan een persoon. Indien de leverancier onderhoudswerkzaamheden of tests moet uitvoeren op het urenregistratiesysteem kan hij dan in principe niet bij de HR-systemen zelf, maar alleen bij de - niet herleidbare - referentie-waarden. Ook dit levert een extra privacywaarborg op.

Medewerker houdt zeggenschap

Op grond van de privacywetgeving behoudt de medewerker zeggenschap over zijn gegevens. De code moet dan ook vernietigd worden zodra de medewerker uit dienst is.

Bewerkers in de cloud

Voor systemen die in de cloud werken (online of saas-applicaties) geldt dat de beveiliging van dit specifieke onderdeel valt onder dezelfde wijze van beveiliging als voor het systeem in zijn geheel, inclusief de hiervoor geldende certificeringen etc. In dat geval kan de leverancier gezien worden als bewerker van persoonsgegeven in de zin van de Wbp. Klanten moeten een zogenaamde bewerkersovereenkomst sluiten met hun bewerkers. De bij het Tijdplein.nl aangesloten leveranciers kunnen hiervoor de standaard bewerkersovereenkomst van Nederland ICT gebruiken.

Meldplicht datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Op basis van deze meldplicht zijn organisaties die persoonsgegevens verwerken verplicht ‘datalekken’ te melden aan de Autoriteit Persoonsgegevens. In het geval van systemen die in de cloud werken betekent dit dat er extra afspraken gemaakt moeten worden tussen klanten en leveranciers over het melden van datalekken. De voorbeeld bewerkersovereenkomst van Nederland ICT houdt hier rekening mee.

PRAKTISCHE PRIVACYOVERWEGINGEN EN VRAGEN

Het volgende geeft een kort overzicht van de overwegingen en vragen die bij de selectie en implementatie van biometrische systemen aan bod zouden moeten komen:

1. Is een biometrisch hulpmiddel nodig? Wellicht kan bij nader inzien volstaan worden met een bestaande vorm van registratie.
2. Is er een onderzoek uitgevoerd onder de uiteindelijke gebruikers en wat zijn daarvan de resultaten? Tenminste zal moeten worden onderzocht hoe de opslag

van biometrische en eventueel andere gegevens eruit gaat zien. Eerlijke voorlichting zal essentieel zijn voor uiteindelijke acceptatie. Als het gebruik van biometrie simpel wordt voorgesteld en later een zware belasting blijkt, zal de acceptatie laag zijn.

3. Wie gaat het systeem onderhouden? Is dat de externe leverancier, of wordt het beheer bij interne functionarissen ondergebracht?
4. Hoe wordt toegang tot biometrische gegevens beveiligd en waar? Het systeem op zich dient ook te worden beveiligd. Goede beveiliging is altijd een combinatie van techniek, organisatie en bewustzijn bij medewerkers. Duidelijk moet zijn welke gegevens de ronde doen en waar die zich bevinden; in database(s), datacommunicatie, smartcards, etc.
5. Wat is het beste moment voor enrollment? Bij het beste moment voor enrollment dient te worden nagegaan of de gebruikers er apart voor moeten komen of dat het mogelijk is de enrollment te doen als de gebruikers zich melden voor diensten. Ook hier zal gemak voor de medewerker de acceptatie verhogen.
6. Welke (potentiële) juridische aspecten spelen een rol? Dit kan betrekking hebben op de privacy rond de biometrische gegevens en/of de ermee samenhangende opgeslagen gegevens, zowel in opslag (al of niet afhankelijk van de opslag in een centrale database of decentraal op smartcards, etc.) als tijdens transport over netwerken.
7. Welke meetmarges zijn acceptabel? Met andere woorden: welke balans tussen false acceptance en false rejection is wenselijk (zie het onderdeel ‘Betrouwbaarheid en nauwkeurigheid’)? Dit zal afhangen van het doel van het systeem en de mogelijke impact van te ruim of juist te klein geformuleerde meetmarges.

AFSLUITEND

Samenvattend kan worden gesteld dat de biometrische hulpmiddelen technisch volwassen genoeg zijn geworden om een betrouwbare extra beveiliging te kunnen bieden. Behalve enige duidelijkheid die soms nog moet worden geschapen over juridische aspecten, zal het erop aankomen, zoals altijd, de selectie en implementatie consciëntieus te doen. Dit geldt niet alleen voor de technische implementatie maar ook voor het implementeren van het privacybeleid rondom een dergelijke nieuwe toepassing. Vervolgens zal dan het beheertraject netjes moeten zijn ingericht om tot een succes te komen.

Biometrie moet niet omdat het een hype is. Biometrie kan wel worden overwogen als extra hulpmiddel naar een vergrote veiligheid.

Alle leden van het netwerk Tijdplein.nl kunnen desgewenst de technische procedure in hun eigen systeem documenteren en een eigen protocol daarvoor formuleren en beschikbaar stellen.

Bij de totstandkoming van deze whitepaper heeft het netwerk Tijdplein.nl overleg gevoerd met de VVBI (Vereniging Voor Biometrie & Identiteit – www.vvbi.nl).