Van: Riemen, John (J.A.J.M.)
Aan: 5.1.2.e
Onderwerp: RE: regime Havank?
Datum: maandag 27 november 2017 14:33:57

Hoi 5.1.2.e

Bewaartermijn zijn complex en er is relatie tussen het delict en de bewaartermijnen van de sporen.

https://zoek.officielebekendmakingen.nl/stb-2016-171.html

http://njb.nl/wetgeving/staatsbladen/bewaren-dna-gegevens-en-vingerafdrukken.12856.lynkx

TP moeten we per batch kunnen schonen aangezien wij dat alleen op aangeven van JUSTID doen

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Operationeel Specialist Biometrie
Beheerder HAVANK en CATCH
Landelijke Eenheid
DLOS/LFSC/Forensisch Biometrie Onderzoek

(+31) 06 5.1.2.e

Europaweg 45
2711 EM Zoetermeer

Van: 5.1.2.e
Verzonden: donderdag 23 november 2017 12:45
Aan: Riemen, John (J.A.J.M.) 5.1.2.e @politie.nl>
Onderwerp: FW: regime Havank?

Hoi John,

Ik probeer te kijken of ik in het PvE de eisen en wensen ten aanzien WPG en AVG en andere wet en regelgeving mbt bewaartermijnen helder kan krijgen. Het gaat erom dat de leverancier hier een beeld bij krijgt en dan met name wanneer dit complex is.

Kun jij me op weg helpen?

Groet 5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 23 november 2017 12:36
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: regime Havank?

Hoi 5.1.2.e
Ik weet onvoldoende van de regelgeving rondom Havank. Er zijn ook bijzondere regels geldend omdat er ook een rol voor identificatie van onbekende doden is weggelegd vvor Havank. Ik zou even

bij 5.1.2.e op de lijn gan om te vernemen wie je het beste kan adviseren.
Zelf denk ik aan 5.1.2.e .

Met vriendelijke groet,

5.1.2.e
Operationeel Specialist

Politie | Landelijke Eenheid | DLos|LFSC|Forensisch Biometrie Onderzoek
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 23 november 2017 11:55
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: regime Havank?

Hoi 5.1.2.e

Ten aanzien WPG en AVG eisen en wensen is het van belang hoe we thans Havank zien.
Beschouwen we het als een art 13 omgeving inclusief protocol? Of moeten we per incident kijken wat het regime is art 8, 9, 10, …?
Of is het nog ingewikkelder en moeten we naar incident en biometrisch kenmerk apart kijken?
Zaakgegevens kunnen al geschoond zijn terwijl dactygegevens nog bewaard mogen worden.

5.2.1

Kun je mij op weg helpen hiermee?

Groet 5.1.2.e

Met vriendelijke groet,

5.1.2.e
IV-Expert RA

Politie | Dienst Informatiemanagement | IM-Advies

Doelwater 5, 3011 AH Rotterdam
Postbus 70023, 3000 LD Rotterdam
5.1.2.e @politie.nl
M 06 5.1.2.e

SAFRAN
MorphoTrak

CONTRACT CHANGE ORDER APPROVAL

MorphoTrak
1250 N. Tustin Ave.
Anaheim, CA 92807

Program Manager: 5.1.2.e
Telephone No.: 1 5.1.2.e
Fax No.:

Customer: Netherlands Police Agency
Europaweg 45
2711 EM Zoetermeer

Attention: 5.1.2.e
Telephone No.: 06-5.1.2.e
Fax No.:

Change Order No.: 1
Date: 5 Dec 2017
MorphoTrak Contract No.: PF0111A

Netherlands Police Agency Projectcode: G130005 Budgetcode: LE0000L

1. Pursuant to the Section entitled "CHANGE ORDERS" in the above described contract, Customer hereby directs Seller to immediately adopt and implement the changes set forth in this document hereto.
2. This change order is a part of and is governed by the provisions of the Contract. This Change Order is valid only if signed by an authorized MorphoTrak representative.
3. Except as expressly modified by this Change Order, all other terms and conditions of the contract, as amended to date, remain in full force and effect.
4. This Change Order becomes binding at the time that both parties have executed the Change Order.

This document must be executed below in order to be effective.

MorphoTrak

By 5.1.2.e
Signature

Date: 5 Dec 2017

Netherlands Police Agency

By C. Man 13-12-17
Signature

Date: 5.1.2.e

5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 31 januari 2018 15:02
Aan: 5.1.2.e; 5.1.2.e; 5.1.2.e; Riemen, John (J.A.J.M.); 5.1.2.e
CC: 5.1.2.e; 5.1.2.e; 5.1.2.e
Onderwerp: Aanpassingen PvE informatiebeveiliging
Bijlagen: Bijlage X Specificatie-van-de-opdracht-Biometrie 0.86 MdH.docx

Hallo 5.1.2.e -en, John, 5.1.2.e en 5.1.2.e

Ik heb een aantal aanpassingen gedaan in het document op versie 0.86.

H3: Juridisch kader @5.1.2.e heeft volgens mij geen aanpassing nodig omdat raamovereenkomst een clausule bevat die zegt dat er voldaan moet worden aan NL wet- en regelgeving. De AVG en WPG kunnen dan in H6 en H9 blijven staan.
H6: Bewaartermijn, ik heb de wet- en regelgeving aangepast omdat de WBP na 25 mei 2018 vervangen wordt door AVG
H6.18: Ik heb de eisen rond autorisatie hier wel laten staan (functioneel) maar in eis en wens geformuleerd. SSO is een wens geworden. Ik heb ook RuleBased Access Control als wens toegevoegd, zie toelichting. @John is dit wenselijk of noodzakelijk?
H8.1: Ik heb SSO verwijderd omdat dit geen beheer taak is en beheertaken al eerder genoemd worden inclusief (de)blokkeren gebruiker. @5.1.2.e is dit OK?
H9.1: Aangepast doordat autorisatiedeel naar IAM aansluiting herschreven is en paar uitgangspunten overgeheveld zijn
H9.2 (was 9.1.1): Autorisatie verwijderd en vervangen door aansluitvoorwaarden IAM zoals deze in de blauwdruk IAM zijn opgenomen. Dit is een wens geworden. @5.1.2.e is dit OK?

Overweging is om 9.1 beveiliging wat later in H9 op te nemen waar compliancy en kwaliteit ook genoemd worden.

Met vriendelijke groet,

5.1.2.e
Adviseur informatiebeveiliging

Politie | Politie Dienstencentrum | Dienst IM |Gegevensgebruik en -beheer | Team Informatiebeveiliging
Ringbaan West 232, 5038 KE Tilburg
Postbus 8050, 5004 GB Tilburg
M +31 (0)6 5.1.2.e
E 5.1.2.i @politie.nl (loket informatiebeveiliging)
I 5.1.2.i (intranetpagina)

Werkdagen: maandag, dinsdagochtend, woensdag, donderdag tot 16 uur, vrijdag

BIJLAGE X – Specificaties van de opdracht

Behorende bij : ?

Versie : 0.86
Datum : 22 januari 2024~~31 januari 2018~~

INHOUDSOPGAVE

Hoofdstuk 1. Doel van dit document

Dit document beschrijft de eisen en wensen die de aanbestedende dienst stelt in het kader van de Europese aanbesteding. Dit document maakt integraal onderdeel uit van Inschrijvingsleidraad.

1.1. Eisen en wensen

Voor het indienen van de inschrijving zal onderhavige bijlage van de Inschrijvingsleidraad integraal als Word-document ter beschikking worden gesteld zodat Inschrijvers op eenvoudige wijze de tabellen kunnen invullen waarin de eisen en wensen zijn opgenomen.

De aanbestedende dienst heeft geen voorkeur voor bepaalde Inschrijvers, noch voor bepaalde merken, types, fabricaten, herkomst e.d. Als er wordt gerefereerd aan bepaalde fabricaten, merken, typen, specifieke standaarden en dergelijke, dan dient dit te worden gelezen met de toevoeging “of daaraan gelijkwaardig”.

Aan eisen móét worden voldaan. Het niet voldoen aan een eis betekent uitsluiting van verdere beoordeling en wordt de inschrijving terzijde gelegd (knock-out criterium).

De wensen worden inhoudelijk beoordeeld door een beoordelingscommissie.

Inschrijvers dienen te voldoen aan alle opgenomen eisen en wensen die de aanbestedende dienst heeft geformuleerd ten aanzien van de te leveren Dienst. Eisen en wensen worden als volgt weergegeven:

EIS 1	**Gunningseisen** Aan een gunningseis moet worden voldaan. Als niet is voldaan aan een gunningseis dan wordt tot uitsluiting overgegaan.

W 1	**Wensen** Wensen maken onderdeel uit van subgunningscriteria op basis waarvan de economisch meest voordelige Inschrijver wordt bepaald.

UE 1	**Uitvoeringseisen** Voorwaarden waar Inschrijver zich bij de uitvoering van de opdracht aan dient te houden zijn uitvoeringseisen. De uitvoeringseisen zijn opgenomen in dit document. Door het indienen van een inschrijving gaat u onvoorwaardelijk akkoord met het voldoen aan de uitvoeringseisen gedurende de uitvoering van de overeenkomst.

Hoofdstuk 2. Uitvoeringseisen

In dit hoofdstuk zijn specifieke uitvoeringseisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbesteedde opdracht.

2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden

UE 1.	Inschrijvers dienen bij het opstellen van hun inschrijving rekening te hebben gehouden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: - de Belastingdienst, www.belastingdienst.nl - het Ministerie van Infrastructuur en Milieu, www.rijksoverheid.nl/ministeries/ienm - het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.

2.2. Sociale Voorwaarden

Op deze opdracht zijn de generieke sociale voorwaarden van toepassing. De ingevulde en ondertekende bijlage Sociale Voorwaarden maakt onderdeel uit van de Raamovereenkomst.

UE 2.	Inschrijver zal de Sociale Voorwaarden (Bijlage G van de Inschrijvingsleidraad) op eerste verzoek van de aanbestedende dienst, maar niet eerder dan na het mededelen van de gunningsbeslissing, invullen en ondertekend aanleveren.

2.3. Verzekering

UE 3.	Gezien de aard van de werkzaamheden acht de Politie het noodzakelijk dat Inschrijver verzekerd is tegen beroeps- en bedrijfsaansprakelijkheid, dan wel bereid en in staat te zijn om bij gunning zich voor beroepsfouten te verzekeren voor een bedrag van minimaal €500.000.- per schadeveroorzakende gebeurtenis en minimaal €1.000.000.- per jaar of equivalente tegenwaarde, gedurende tenminste de looptijd van de opdracht. Op daartoe strekkend verzoek verstrekt de winnende Inschrijver bewijs van adequate verzekering dan wel een verklaring waaruit blijkt dat deze hiertoe bereid en in staat is de bij gunning af te sluiten.

2.4. Milieu

UE 4.	Inschrijver voldoet gedurende de gehele looptijd van de Raamovereenkomst aantoonbaar aan alle vigerende milieu en arbo wet- en regelgeving.

Hoofdstuk 3. Juridische kaders

In dit hoofdstuk zijn specifieke juridische eisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbesteedde opdracht.

EIS 1	De in Bijlage E van de Inschrijvingsleidraad opgenomen concept Raamovereenkomst kan - alvorens deze door Inschrijver(s) wordt ondertekend - door de aanbestedende dienst worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Inschrijver gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 5.1. (Nota van Inlichtingen, nadere inlichtingen of vragen over de Aanbestedingsstukken). De wijzigingen en/of de aangepaste Raamovereenkomst zullen/zal de Inschrijvers per Nota van Inlichtingen kenbaar worden gemaakt.

EIS 2	De als Bijlage E bij deze Inschrijvingsleidraad opgenomen concept Raamovereenkomst bevat uitsluitend voorwaarden die door Politie dwingend worden voorgeschreven. Inschrijver gaat met het bepaalde in de concept Raamovereenkomst akkoord.

Met opmerkingen [MdH1]: Opmerking van 25/1 is om hier wet- en regelgeving neer te zetten. In de raamovereenkomst staat al dat er aan de NL wetgeving voldaan moet worden check 5.1.2.e , de AVG ten aanzien van het contract en uitvoering valt hieronder.

Voor de verwerking van gegevens in de voorziening kan hier de WPG en AVG (voorheen WBP) genoemd worden. De vraag is of dit valt onder juridische kaders? De leverancier moet software leveren zodat wij aan wet- en regelgeving kunnen voldoen. Zie H6 en H9.

Hoofdstuk 4. Financiële afspraken

In dit hoofdstuk zijn specifieke financiële afspraken opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbesteedde opdracht.

4.1. Prijsstelling

De eisen en wensen met betrekking tot het gunningscriterium prijs zijn:

EIS 3	Alle met de Diensten gemoeide kosten zijn verwerkt (inclusief reis en verblijfskosten) in de prijs, tenzij anders vermeld. Vermeld in de inschrijving alle geldbedragen in Euro's (afgerond op hele € (euro's)) en exclusief omzetbelasting (BTW).

EIS 4	De opgegeven prijzen en tarieven dienen realistisch en marktconform te zijn.

EIS 5	Het is niet toegestaan met de ingediende prijzen de gehanteerde formule te frustreren; negatieve prijzen of prijzen van € 0,- zijn in ieder geval niet toegestaan.

EIS 6	Inschrijver gaat akkoord dat er in de nadere offerteprocedure geen hogere tarieven geoffreerd worden dan aangeboden in het prijzenformulier.

De door inschrijver geoffreerde prijzen en tarieven, zoals opgegeven in bijlage C, formulier F – Prijsblad mogen jaarlijks per 1 september worden geïndexeerd op basis van de tabel 'Dienstenprijzen (DPI); commerciële dienstverlening en transport; indexcijfers 2010 = 100', (CPA2008, kwartaalindex) conform de volgende webpagina:
http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=81530NED&D1=0&D2=0&D3=46-49,51-54,56-59&HDR=T,G1&STB=G2&VW=T.

Inschrijver dient, voor 1 juni voorafgaande aan de genoemde momenten van tarief indexering, een schriftelijk verzoek in bij de aanbestedende dienst, met bijbehorende onderbouwing om voor indexering in aanmerking te komen.

Het uitgangspunt voor de tariefstijging is de ontwikkeling van de betreffende index gedurende de eerste vier kwartalen van de zes kwartalen voorafgaand aan de genoemde datum voor de tarief indexering. Het percentage van de tariefstijging wordt afgerond op één decimaal achter de komma.

Tariefstijging	Ontwikkeling Index		
per	ultimo		ultimo
1 januari 2018	Q3 2016	t/m	Q3 2017
1 januari 2019	Q3 2017	t/m	Q3 2018
1 januari 2020	Q3 2018	t/m	Q3 2019
1 januari 2021	Q3 2019	t/m	Q3 2020

EIS 7	Inschrijver is akkoord met de indexering voor de Diensten conform de geoffreerde prijzen in bijlage C, formulier F – Prijsblad, en dient voor 1 juni voorafgaande aan de genoemde momenten van tarief indexering, een schriftelijk verzoek in met bijbehorende onderbouwing om voor de indexering in aanmerking te komen.

EIS 8	Kosten die niet in de inschrijving genoemd worden en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van de Diensten, conform de in de Inschrijvingsleidraad gestelde eisen, zijn voor rekening van Inschrijver.

EIS 9	Indien de Politie, in aansluiting op EIS 8, kosten moet maken die noodzakelijk blijken te zijn voor een goed functioneren van de Diensten, zijn deze kosten voor rekening van Inschrijver.

EIS 10	De facturering dient na uitvoering van de Diensten plaats te vinden. Inschrijver dient een betalingstermijn van 30 dagen na ontvangst van de factuur te accepteren.

4.2. DigiInkoop - Elektronisch bestellen en factureren (EBF)

Algemene informatie DigiInkoop
De overheid heeft als doelstelling om te komen tot administratieve lastenverlichting voor het bedrijfsleven en de Rijksdienst door bedrijfsprocessen te optimaliseren. DigiInkoop ondersteunt deze doelstelling. DigiInkoop is een op aangeven van de Politie door de Inschrijver verplicht te gebruiken transactiegerichte digitale voorziening die de verwerving van goederen en diensten voor het Rijk en het bedrijfsleven ondersteunt.

Bij de toepassing van DigiInkoop als inkoopsysteem geldt de verplichting dat voor de uitwisseling van inkoop gerelateerde berichten door de Rijksoverheid vastgestelde berichtformaten toegepast worden. Op deze wijze kunnen tussen bedrijfsleven en de Rijksdienst op uniforme wijze digitale inkoopberichten aangemaakt, verzonden en verwerkt worden.

De Rijksoverheid berekent geen kosten aan leveranciers voor aansluiting op en communicatie met DigiInkoop. Bij een directe aansluiting op DigiInkoop komen alle kosten vanaf het koppelvlak aan leverancierszijde voor rekening van Inschrijver.

Nagenoeg alle operationele beheeractiviteiten, waaronder ook het ondersteunen van deelnemers en leveranciers bij het aansluiten op DigiInkoop zijn belegd bij Logius. Als onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties vormt Logius de digitale “e-overheid” schakel met klanten, partners en leveranciers. Meer informatie over Logius kunt u lezen op de website www.Logius.nl.

Gebruik van DigiInkoop
Er zal een geautomatiseerde uitwisseling van gestructureerde berichten door aansluiting op de berichtenverkeervoorziening, Digipoort, van DigiInkoop plaatsvinden. De berichtstandaard die van toepassing is op deze productcategorie is UBL 2.0 voor alle inkoopopdrachten.

De Inschrijver maakt vanaf de ingangsdatum van de Raamovereenkomst gebruik van de huidige factuur procedure (email naar factuur loket) van de Politie.

Inschrijver start het aansluitproces op DigiInkoop direct na het beschikbaar komen van DigiInkoop voor de Politie.

Bij geautomatiseerde uitwisseling van berichten meldt de inschrijver zich na gunning aan voor een aansluiting bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties: via telefoon 0900 555 4555, per e-mail servicecentrum@logius.nl of op www.logius.nl. Op het aansluiten op DigiInkoop zijn de algemene gebruiksvoorwaarden Digipoort en de algemene voorwaarden van Logius van toepassing. Deze voorwaarden treft u eveneens aan op voornoemde website. Het uitbrengen van een inschrijving (offerte) impliceert dat voornoemde voorwaarden door de Inschrijver worden geaccepteerd.

EIS 11	Inschrijver zorgt voor de implementatie van een aansluiting op DigiInkoop na het beschikbaar komen van DigiInkoop bij de Politie.

EIS 12	De Rijksoverheid berekent geen kosten aan leveranciers voor aansluiting op en communicatie met DigiInkoop. Bij een directe aansluiting op de Digipoort van DigiInkoop komen alle kosten vanaf het koppelvlak aan leverancierszijde voor rekening van de Inschrijver. De kosten die Inschrijver in dit verband nu (en in de toekomst) maakt, zijn voor eigen rekening.

Hoofdstuk 5. Kwaliteit

5.1. Algemeen (voor alle Diensten)

5.1.1. Offerteprocedure

Inschrijver ontvangt via Commerce-Hub de offerteaanvraag.

Inschrijver maakt een concept offerte, heeft een intake met contactpersoon (interne Politie) genoemd in de offerteaanvraag, hetzij telefonisch hetzij in een intakegesprek. Dit gesprek maakt het mogelijk om eventuele onduidelijkheden (o.a. inhoud, technische vragen, aantal dagen, beschikbaarheid systemen enz.) weg te nemen en details af te stemmen. Inschrijver stuurt op basis van de intake, binnen de genoemde termijn in de offerteaanvraag een Offerte aan de Politie. De Offerte wordt na ontvangst beoordeeld op de in de offerteaanvraag meegegeven eisen. Indien een Offerte op de gestelde eisen passend is en de prijs marktconform is, kan Politie besluiten een Inkoopopdracht te verstrekken die als Nadere Overeenkomst onder de Raamovereenkomst zal vallen.

UE 5.	Inschrijver verklaart akkoord te gaan met de offerteprocedure.

5.1.2. Personeel van Inschrijver/Sleutelfiguren

Het Personeel van de van Inschrijver dat belast is met de daadwerkelijke levering van de Diensten en waarvoor geldt dat zij over voldoende deskundigheid en ervaring beschikt om op een goede wijze invulling te geven aan de opdracht, wordt gezien als Sleutelfiguren.

UE 6.	Inschrijver conformeert zich bij de uitvoering van de Raamovereenkomst aan bovenstaande.

Het is te verwachten dat gedurende looptijd van de Raamovereenkomst en/of Nadere Overeenkomst er veelvuldig contact is tussen Personeel van Inschrijver en Politie. Om een optimale samenwerking te kunnen creëren is het noodzakelijk dat er vanuit Inschrijver een beperkt aantal vaste Contactpersonen, contacten heeft met Politie. Dit voorkomt dat er meer afstemming en overdracht van lopende zaken nodig is. Daarbij is de verwachting dat in de samenwerking er sneller en efficiënter gehandeld kan worden, dan in een situatie waarbij veel wisselende contacten zijn.

UE 7.	Inschrijver stelt een Contactpersoon en een team van Sleutelfiguren samen dat belast wordt met de levering van Diensten ten behoeve van Politie.
UE 8.	Inschrijver dient bij aanvang van de Raamovereenkomst het team van Sleutelfiguren op te geven inclusief vermelding van de specialismen per Sleutelfiguur en levert daartoe de CV's aan van het team van Sleutelfiguren.
UE 9.	Inschrijver informeert Politie tijdig bij voorgenomen vervanging van Sleutelfiguren.
UE 10.	Inschrijver is verplicht om bij vervanging en uitbreiding van Sleutelfiguren de competenties van het team van Sleutelfiguren op minimaal hetzelfde niveau te behouden. Politie zal voorafgaand aan vervanging en uitbreiding een CV-toets uitvoeren alvorens akkoord te gaan met de vervanging/uitbreiding. Inschrijver houdt periodiek rapporteren aangaande de vervanging en uitbreiding.
UE 11.	Voor al het personeel van Inschrijver, dat wordt ingezet voor deze opdracht geldt: **Screening** Voor de screening van het Personeel van Inschrijver en Personeel van Onderaannemers die betrokken raken bij werkzaamheden in het kader van deze opdracht geldt dat deze gescreend dienen te zijn. Daarbij geldt het volgende: 1. Personeel van Inschrijver dient bij iedere uit te voeren opdracht in het bezit te zijn van een recente Verklaring Omtrent Gedrag (VOG) voor Natuurlijke Personen welke niet ouder is dan 6 maanden en waaruit blijkt er geen

bezwaren zijn voor de uitvoering van de opdracht. Inschrijver zal periodiek rapporteren aangaande de VOG.
2. Personeel van Inschrijver dient bij iedere uit te voeren opdracht waarbij sprake is van Gegevens geclassificeerd als Politie Intern of Politie Confidentieel minimaal te beschikken over een positief advies op basis van de Protocol Betrouwbaarheids- en geschiktheidsonderzoek Politie 2015 (BGO) of een Verklaring van Geen Bezwaar (VGB) niveau B (van de AIVD) welke niet ouder is dan 12 maanden en waaruit blijkt dat er geen bezwaren zijn voor de uitvoering van de opdracht. Inschrijver zal periodiek rapporteren aangaande de BGO en de VGB.

Een negatieve uitslag van een screening resulteert automatisch in uitsluiting van het betreffende Personeelslid van de Dienstverlening of werkzaamheden bij of voor Politie. Inschrijver garandeert in dat geval dat dergelijk Personeel van Inschrijver op geen enkele wijze ingezet zal worden voor uitvoering van de Opdracht ten behoeve van Politie. Inschrijver sluit dit Personeel uit van alle of iedere kennisname van gegevens van en over Politie. Inschrijver zal zijn Personeel verplichten mee te werken aan de screening en draagt zorg voor het vrijmaken van tijd die voor een screening benodigd is (bijvoorbeeld het invullen van een formulier en mogelijk het voeren van persoonlijke gesprekken). Hiervoor worden geen kosten in rekening gebracht bij Politie.

Inschrijver zorgt ervoor dat hij binnen 5 maanden na inwerkingtreding van de Overeenkomst maar ook gedurende de duur van de Overeenkomst over voldoende Personeel beschikt dat over een positieve screeningsuitslag (BGO of VGB) beschikt, om de dienstverlening te kunnen uitvoeren. Let op: u dient dit proces zelfstandig te doorlopen en de kosten hiervoor te dragen. Zie www.aivd.nl

Geheimhouding

Behoudens wettelijke verplichtingen zullen Inschrijver en zijn Personeel strikte geheimhouding in acht nemen met betrekking tot de gebouwen, de interne organisatie van de Politie, de identiteit van het Personeel van de Politie en alle overige informatie waarvan het Personeel van Inschrijver weet of kan weten dat deze vertrouwelijk is.

Met Inschrijver en eventuele Onderaannemers zal een geheimhoudingsverklaring worden overeengekomen. Inschrijver zal ervoor zorg dragen dat ook op de individuele basis Personeel van Inschrijver en Onderaannemers deze geheimhoudingsverklaring aangaan.

Inschrijver garandeert dat informatiegegevens van de Politie uitsluitend worden gedeeld met Personeel van Inschrijver of Onderaannemers die direct betrokken zijn bij de uitvoering van de Opdracht voor Politie en dat deze informatie de gegevens niet in handen van derden komen.

Deze geheimhoudingsplicht blijft ook na beëindiging van de Overeenkomst van kracht. Inschrijver zal, zonder voorafgaande schriftelijke toestemming van Politie, in geen enkel geval melding doen aan derden van zijn Overeenkomst met Politie. Personeel van Inschrijver dat de politielocaties van Politie betreedt, dient na Gunning een door Politie aangeleverde geheimhoudingsverklaring te ondertekenen. Deze geheimhoudingsverklaring blijft ook van kracht nadat de arbeidsrelatie tussen het Personeelslid en Inschrijver is beëindigd.

Registratie geheimhoudingsverklaringen en screening

Inschrijver houdt een lijst van zijn Personeelsleden en van medewerkers van Onderaannemers bij:

1. Die een geheimhoudingsverklaring hebben getekend (voorzien van datum ondertekening en eventuele looptijd van de geheimhoudingsverklaring);
2. Aan wie een geheimhoudingsverklaring ter ondertekening is aangeboden, maar die nog niet is ondertekend (voorzien van aanbiedingsdatum en status);
3. Die een door de Politie gevraagde screening hebben afgerond (waarin ook is opgenomen het type, screening, het resultaat, de datum van afgifte en de datum en de geldigheidsduur);
4. Die een door de Politie gevraagde screening nog niet hebben afgerond (voorzien van type screening, aanmeldingsdatum en status);

	5. Die over de door de Politie gevraagde Verklaring Omtrent Gedrag (VOG) beschikken (voorzien van datum afgifte en de geldigheidsduur); 6. Die de door de Politie gevraagde VOG hebben aangevraagd, maar nog niet hebben ontvangen (voorzien van aanvraagdatum en status). Deze lijst van ingezette medewerkers wordt elk kwartaal op uiterlijk de 10e Werkdag volgend op het vorige kwartaal (de kwartalen eindigen op 31 maart, 30 juni, 30 september en 31 december van elk jaar) aan de Politie verstrekt door Inschrijver. Indien tussentijds gegevens van deze lijst wijzigen voorziet Inschrijver de Politie van een aangepaste versie van het overzicht.

UE 12.	Voor al het personeel van Inschrijver, dat wordt ingezet voor deze opdracht geldt: **Legitimatieplicht** Het Personeel van Inschrijver dient conform de vigerende regelgeving in het bezit te zijn van een geldig identiteitsbewijs en een geldig bewijs van het resultaat van de screening en deze op verzoek van de beveiliging of receptie te tonen, alvorens de gebouwen van Politie te betreden. **Toegang Personeel van Inschrijver tot locaties van Politie** Toegang tot de locaties van Politie wordt alleen verleend aan Personeel van Inschrijver of van medewerkers van Onderaannemers, die door Inschrijver daartoe uitdrukkelijk opdracht hebben gekregen en die tijdig voorafgaande aan hun komst aangemeld zijn bij Politie.

W 3	**Screening** Hoe heeft Inschrijver de aanvullende eis aangaande de minimale verklaring van geen bezwaar AIVD niveau P in geval van Staatsgeheim Confidentiële Gegevens in zijn organisatie geborgd? Beoordeling vindt o.a. plaats op: - reeds aanwezige screening van Personeel op dit vlak. - aantal Sleutelfiguren die deze verklaring van geen bezwaar niveau C reeds in bezit hebben. - proactieve houding om deze screening te verkrijgen en te behouden.

5.1.3. Eisen en wensen uit te voeren opdrachten

EIS 13	Inschrijver garandeert strikte vertrouwelijkheid ten aanzien van de uit te voeren opdrachten voor Politie.

UE 13.	Inschrijver draagt er middels zijn e-mail systeem zorg voor dat alle e-mails tussen de Politie en Inschrijver veilig worden uitgewisseld.

Hoofdstuk 6. Functionele eisen

In dit hoofdstuk zijn de functionele eisen en wensen opgenomen die de aanbestedende dienst stelt in het kader van de Europese aanbesteding.
Daarbij zijn onder het kopje Specifiek de specifieke eisen en wensen ten aanzien van deze biometrische modaliteiten beschreven. Daarnaast zijn binnen de verschillende processen generieke functies gedefinieerd welke onder het kopje Algemeen geplaatst zijn.
Waar noodzakelijk geacht is de context rond een eis of wens geschetst om Inschrijver een beter beeld te geven en de gelegenheid te bieden, rekening houdend met de eisen, zelf zo goed mogelijk invulling te geven aan de wensen.

6.1. Inleiding

De biometrievoorziening Politie is een verzameling componenten ten behoeve van de ondersteuning van het operationele werkproces waarbij vreemdelingen, justitiabelen, verdachten, veroordeelden, getuigen en/of slachtoffers geïndividualiseerd en/of geverifieerd kunnen worden, dan wel in bepaalde mate herkend worden. De componenten en software die nodig zijn om de afname van de biometrische kenmerken te verzorgen behoren niet tot de scope van deze aanbesteding.

Bij de Politie zijn individualisatie, identificatie en verificatie en/of het in bepaalde mate herkennen van personen aan de hand van biometrische kenmerken de kerntaken van de afdeling Forensisch Biometrie Onderzoek (FBO)- onderdeel van het Landelijk Forensisch Service Centrum van de Politie en de Forensische Opsporing in de eenheden. Deze taak wordt ondersteund met een geautomatiseerd vergelijkingssysteem voor vingerafdrukken, handafdrukken, sporen en gelaatsafbeeldingen (nu Havank en Catch).

Op dagelijkse basis handelt de afdeling een groeiend aantal individualisaties en verificaties van onder andere de Politie, andere Nederlandse overheidsdiensten en internationale partners af.

Het doel van de (nieuwe) biometrievoorziening is om personen en sporen met biometrische kenmerken te individualiseren c.q. te verifiëren of in bepaalde mate te herkennen. Hierbij is performance (duur van het individualisatieproces) in balans is met accuratesse. De voorziening is optimaal in gericht voor de verschillende biometrische werkprocessen van individualisatie en verificatie.

Het systeem wordt ingezet om de taken van de afdeling Forensisch Biometrie Onderzoek en die van de Forensische Opsporing van de Nationale Politie te ondersteunen. Dit zijn:

1. Identiteitsonderzoek met behulp van 1 of meer dactyloscopische vingerafdrukken en/of 1 of meer gelaatsafbeeldingen. Tijdens dit onderzoek wordt bekeken of dezelfde vingerafdrukken en/of gelaatsafbeelding in de databank(en) voorkomen;
2. (Forensische) opsporingsonderzoeken met vingerafdruksporen, handpalmafdruksporen en/of gelaatsafbeelding met als doel een donor van het spoor te achterhalen middels gehanteerde criteria;
3. Opsporingsonderzoeken met operationele gelaatsafbeeldingen, die zowel gecontroleerd als ongecontroleerd zijn vastgelegd, met als doel een mogelijke herkenning van de persoon.

Er zijn meerdere categorieën gegevensverzamelingen waarmee vergeleken kan worden:

- De referentiebestanden die onderdeel uitmaken van de scope van dit traject;
- (Inter)nationale registers: er zijn diverse (inter)nationale registers die door middel van koppelingen geraadpleegd worden in het identificatieproces;
- Door aanvrager aangeleverde referentiebestanden.

Ook zijn er meerdere vergelijkingsmogelijkheden:

- Er wordt 1:1 vergeleken – dat wil zeggen dat gekeken wordt of er overeenkomstige biometrische kenmerken zijn tussen de (aangehouden) persoon en de genoemde referentiebestanden;
- Er wordt 1:n gezocht – dat wil zeggen dat er gezocht wordt op overeenkomstige biometrische kenmerken tussen de (aangehouden) persoon en de referentiebestanden op de database;
- Er wordt 1:s gezocht – dat wil zeggen dat er gezocht wordt op overeenkomstige biometrische kenmerken tussen de (aangehouden) persoon en de referentiebestanden in een (beperkte) referentieset op de database.

6.2. Modaliteiten

Biometrie is een verzameling van technieken waarmee de identiteit van een persoon kan worden vastgesteld of gecontroleerd. Het gaat daarbij om fysieke eigenschappen of gedragskenmerken die voor ieder natuurlijk persoon uniek zijn.
De politie maakt gebruik van een aantal biometrische modaliteiten welke in deze paragraaf kort toegelicht worden.

6.2.1. Vingerafdrukken

De bekendste en meest gebruikte vorm van biometrie is de vingerafdruk. Hierbij worden van het vingerafdrukpatroon unieke kenmerken vastgelegd. Deze kenmerken zijn de punten waar een papillairlijn begint, stopt of zich splitst. Er wordt onderscheid gemaakt in 'platte' vingerafdrukken en 'gerolde' vingerafdrukken.

6.2.1.1. Invoer

Invoer van vingerafdrukken zal mogelijk zijn door middel van:

- Camera, 1:1 gecallibreerd 1000 ppi, overruled door callibratie op meetlat in afbeelding;
- Live-scan;
- Flatbed scanner;
- Handmatig file importeren, usb-drive of folder;
- Vanuit koppeling als NIST pakket, met bekende-resolutie 500 ppi of 1000 ppi;
- Vanuit een app/web-service/web-omgeving;
- Portaal in de voorziening waar politiemedewerkers en externe ketenpartijen afbeeldingen en gegevens kunnen uploaden/bevragen/downloaden.

6.2.1.2. Proces

- Er zal een 2 vingers plat verificatie proces zijn met binnenkomende platte vingerafdrukken die vergeleken worden met alle platte vingerafdrukken in de referentieset van de betrokken persoon;
- Er zal een 10 vingers plat identificatie proces zijn met binnenkomende platte vingerafdrukken van alle vingers die vergeleken worden met alle platte vingerafdrukken in de referentieset en binnenkomende biografische gegevens die vergeleken worden met alle biografische gegevens in de voorziening.
- Er zal een 10 vingers plat/10 vingers gerold identificatie proces zijn met binnenkomende platte en gerolde vingerafdrukken van alle vingers die vergeleken worden met alle platte en/of gerolde vingerafdrukken in de referentieset en binnenkomende biografische gegevens die vergeleken worden met alle biografische gegevens in de voorziening.

Alle in de voorziening geregistreerde vingerafdrukken dienen als referentieset voor sporen vergelijking.

- Er zal een identificatie proces zijn met alle binnenkomende platte en/of gerolde vingerafdrukken die vergeleken worden met alle openstaande sporen.

Vingerafdrukken kunnen ook internationaal vergeleken worden bij partner landen. Bijvoorbeeld met behulp van de Prüm koppeling.

- Er zal een uitgaand identificatie proces zijn om vingerafdrukken internationaal te vergelijken met referentiesets in andere landen;
- Er zal een binnenkomend identificatie proces zijn om vingerafdrukken internationaal te vergelijken vanuit andere landen met de referentieset van de Politie.

Vingerafdrukken kunnen ook nationaal vergeleken worden bij ketenpartners. Bijvoorbeeld met behulp van de BVV of ID-zuil koppeling.

- Er zal een uitgaand identificatie proces zijn om vingerafdrukken nationaal te vergelijken met referentiesets van ketenpartners;
- Er zal een binnenkomend identificatie proces zijn om vingerafdrukken nationaal te vergelijken vanuit ketenpartners met de referentieset van de Politie.

6.2.1.3. Type zoekingen

Er wordt bij zoeken met sporen gewerkt met 4 levels:

- Level 1: één automatisch gecodeerde zoeking;

- Level 2: één automatisch en één handmatig gecodeerde zoeking door één onderzoeker;
- Level 3: één automatisch en drie handmatig gecodeerde zoekingen door drie verschillende onderzoekers;
- Level 4: één automatisch en drie handmatig gecodeerde zoekingen door drie verschillende onderzoekers.

Het is een trapsgewijs systeem, waarbij ieder level volgt op het voorgaande level. In totaal kunnen er 8 verschillende zoekingen verricht worden.

Met vingerafdrukken worden de volgende type zoekingen verricht:

- A - Referentie vs referentie;
- B - Referentie vs sporen;
- Biografische zoeking.

6.2.2. Handafdrukken

Bij handafdrukken worden net als bij vingerafdrukken het patroon van unieke kenmerken vastgelegd. Deze kenmerken zijn de punten waar een papillairlijn begint, stopt of zich splitst.

6.2.2.1. Invoer

Invoer van handafdrukken zal mogelijk zijn door middel van:

- Camera, 1 :1 gecallibreerd 1000 ppi, overruled door callibratie op meetlat in afbeelding;
- Live-scan;
- Flatbed scanner;
- Handmatig file importeren, usb-drive of folder;
- Vanuit koppeling als NIST pakket, met bekende-resolutie 500 ppi of 1000 ppi;
- Vanuit een app/web-service/web-omgeving;
- Portaal in de voorziening waar politiemedewerkers en externe ketenpartijen afbeeldingen en gegevens kunnen uploaden/bevragen/downloaden.

6.2.2.2. Proces

- Er zal een identificatie proces zijn met binnenkomende handafdrukken die vergeleken worden met alle handafdrukken in de referentieset en binnenkomende biografische gegevens die vergeleken worden met alle biografische gegevens in de voorziening.

Alle in de voorziening geregistreerde handafdrukken dienen als referentieset voor sporen vergelijking.

- Er zal een identificatie proces zijn met alle binnenkomende handafdrukken die vergeleken worden met alle openstaande sporen.

Handafdrukken kunnen ook internationaal vergeleken worden bij partner landen. Bijvoorbeeld met behulp van de Prüm koppeling.

- Er zal een uitgaand identificatie proces zijn om handafdrukken internationaal te vergelijken met referentiesets in andere landen;
- Er zal een binnenkomend identificatie proces zijn om handafdrukken internationaal te vergelijken vanuit andere landen met de referentieset van de Politie.

6.2.2.3. Type zoekingen

Met vingerafdrukken worden de volgende type zoekingen verricht:

- A - Referentie vs referentie;
- B - Referentie vs sporen;
- Biografische zoeking.

6.2.3. Sporen

Sporen identificatie is het proces waarbij een dactyloscopisch expert een spoor afbeelding vergelijkt met een referentie afbeelding (Vingerafdruk, handafdruk, gelaatsafbeelding of een andere spoor afbeelding) en concludeert of deze van dezelfde donor afkomstig zijn of niet.

6.2.3.1. Invoer

Invoer van sporen zal mogelijk zijn door middel van:

- Camera, 1 :1 gecallibreerd 1000 ppi, overruled door callibratie op meetlat in afbeelding;
- Live-scan;
- Flatbed scanner;
- Handmatig file importeren, usb-drive of folder;
- Vanuit koppeling als NIST pakket, bij voorkeur op 1000 ppi;
- Vanuit een app/web-service/web-omgeving;
- Portaal in de voorziening waar politiemedewerkers en externe ketenpartijen afbeeldingen en gegevens kunnen uploaden/bevragen/downloaden.

6.2.3.2. Proces

Het sporen proces doorloopt de volgende stappen: Invoer, automatische zoeking, verificatie door een of meer dactyloscopisch experts, handmatige aanpassing, verificatie door een of meerdere dactyloscopisch experts, handmatige aanpassing door een of meer andere dactyloscopisch experts, verificatie door een of meerdere dactyloscopisch experts, parallel identificeren door twee dactyloscopisch experts (Double blind ACE), optioneel controle door coördinator t.b.v. meervoudige procedure (MVP), identificatie door 3 andere dactyloscopisch experts.

Meervoudige procedure:
Parallelle identificatie door 3 dactyloscopisch experts (ACE) die nog niet betrokken zijn geweest in het proces.

6.2.3.3. Type zoekingen

Met vingerafdrukken worden de volgende type zoekingen verricht:

- C - Sporen vs referentie
- D - Sporen vs sporen

6.2.4. Gelaatsafbeeldingen

Geautomatiseerde gezichtsherkenning is een relatief nieuwe methode die in een aantal situaties goed kan worden gebruikt. Een aantal karakteristieke afstanden van het gezicht wordt gemeten, zoals de afstanden tussen de ogen, oren, mond en kin.

6.2.4.1. Invoer

Invoer van gelaatsafbeeldingen zal mogelijk zijn door middel van:

- Live-scan;
- Flatbed scanner;
- Handmatig file importeren, usb-drive of folder;
  - Vanuit koppeling als afbeelding;
- Vanuit een app/web-service/web-omgeving;
- Portaal in de voorziening waar politiemedewerkers en externe ketenpartijen afbeeldingen en gegevens kunnen uploaden/bevragen/downloaden.

6.2.4.2. Proces

Het gelaatsafbeeldingen proces doorloopt de volgende stappen: Invoer, automatische zoeking, verificatie door een of meer experts, handmatige aanpassing, verificatie door een of meerdere experts, handmatige aanpassing door een of meer andere experts, verificatie door een of meerdere experts, parallel identificeren door twee experts (Double blind ACE), optioneel controle door coördinator t.b.v. MVP, identificatie door 3 andere experts.

6.2.4.3. Type zoekingen

Met gelaatsafbeeldingen worden de volgende type zoekingen verricht:

- A - Referentie vs referentie
- B - Referentie vs probes
- C – Probes vs probes
- D – Probe vs referentie
- Biografische zoeking

6.2.5. Speciale kenmerken

De Politie wil met de nieuwe voorziening ook een aantal speciale biometrische kenmerken volwaardig kunnen verwerken, zoals:

- Voetafdrukken;
- Teenafdrukken;
- Dieren (pootafdrukken).

Specifiek deel eisen en wensen

[Multimodaliteit]

De politie wenst ter ondersteuning van een vingerafdrukken of handafdrukken vergelijking ook parallel hieraan een gelaatsafbeeldingen vergelijking uit te voeren.

UE 14.	De voorziening zal parallel aan een vingerafdrukken of handafdrukken zoeking ook een zoeking met een gelaatsafbeelding uit kunnen voeren. (indien beschikbaar)

[Biografische zoeking]

Een belangrijk aspect van de nieuwe voorziening is de mogelijkheid om inconsistent naamgebruik bij betrokken personen te detecteren. Betrokken personen kunnen of willen niet altijd een valide identiteitsbewijs tonen en kunnen een valse naam gebruiken. Om dit te detecteren wordt in sommige processen naast een biometrisch vergelijk ook een vergelijk op biografische gegevens uitgevoerd op de door de betrokken persoon opgegeven gegevens.

UE 15.	De voorziening zal parallel aan een vingerafdrukken of handafdrukken zoeking ook een zoeking met biografische gegevens uit kunnen voeren. (indien beschikbaar)

[TP]

UE 16. De voorziening zal ten aanzien van vingerafdrukken tenminste de volgende data entries kunnen verwerken:

Beschrijving	Afbeeldingen	Vingers	Impressie
Rechts index	1	1	plat
Links index	1	1	plat
Links en rechts index	2	2	plat
Identificatie plat	3	10 (4; 4; 2)	plat
Tien vingers gerold	10	10	gerold
Tien vingers plat	4	10 (4; 4; 1; 1)	plat
Links/rechts plat	8	8 (4; 4)	plat

De Politie werkt met afbeeldingen met verschillende resoluties (ppi) en wil niet gebonden zijn aan een opgelegde resolutie.

UE 17.	Registratie van vingerafdruk met minimaal 500 ppi, standaard 1000 ppi. Hoger is toegestaan.

[PP]

UE 18. De voorziening zal ten aanzien van handafdrukken tenminste de volgende data entries kunnen verwerken:

- Upper palm;
- Lower palm;
- Writerspalm;
- Full palm;
- Other palm;
- Segmented palm.

De Politie werkt met afbeeldingen met verschillende resoluties (ppi) en wil niet gebonden zijn aan een opgelegde resolutie.

UE 19.	Registratie van handafdruk standaard 1000 ppi. Andere waarden ook toegestaan.

[LT]

UE 20.	De voorziening zal ten aanzien van sporen tenminste de volgende data entries kunnen verwerken: • Vingerafdrukken; • Handafdrukken; • Gelaatsafbeeldingen.

De Politie werkt met afbeeldingen met verschillende resoluties (ppi) en wil niet gebonden zijn aan een opgelegde resolutie.

UE 21.	Registratie van LT sporen standaard 1000 ppi. Andere waarden ook toegestaan.

[FC / PR]

UE 22.	De voorziening zal ten aanzien van sporen tenminste de volgende data entries kunnen verwerken: • Frontale foto; • Meerluiks foto; • 3D; • Compositietekeningen; • Video frame; • Video.

UE 23.	De voorziening zal feedback geven over de kwaliteit van de gelaatsafbeelding. Bijvoorbeeld slechte belichting, te weinig pixels.

UE 24.	De geautoriseerde gebruiker zal bij een vergelijking met een videoframe het bijbehorende videofragment kunnen raadplegen (afspelen binnen voorziening).

Ten behoeve van (foto)confrontaties, zowel opsporingsconfrontatie als bewijsconfrontatie, zal de voorziening twee taken kunnen ondersteunen:

- Het kunnen registreren en raadplegen van meerluik foto's;
- Het kunnen samenstellen en presenteren van confrontaties ten behoeve van de opsporing van onbekende en bekende daders op basis van signalementskenmerken.

W 5	[Midden] De geautoriseerde gebruiker zal het volgende kunnen: • Kunnen zoeken met zij aangezichten (gelaatsafbeelding uit 3 luik, 5 luik, 3D enz.); • Kunnen zoeken met een deel van het gelaat (uitsnede uit een gelaatsafbeelding); • Van een 3 luik of 5 luik gelaatsafbeelding een 3D afbeelding kunnen genereren; • Het kunnen samenstellen en presenteren van fotoconfrontaties op basis van signalementskenmerken. In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaande punten voorziet.

[TP / PP]

De Politie zal van personen ook de zogenaamde "Major Case Collection" registreren in de voorziening. Onder een "Major Case Collection" verstaan we: Volledig uitgerolde afdrukken, d.w.z. 1ste, 2de en derde lid, van individuele vingers en duimen.

UE 25.	De voorziening zal van een persoon de "Major Case Collection" kunnen registreren.

Segmenteren: Onder segmenteren verstaan we een uitsnede maken van de bruikbare delen van een afbeelding.

UE 26.	De geautoriseerde gebruiker zal afbeeldingen kunnen segmenteren.

UE 27.	De geautoriseerde gebruiker zal in bij het segmenteren van afbeeldingen kunnen beschikken over flexibele boxen/segmenten.

[TP / PP / LT]

UE 28.	De voorziening zal de “mated minutiae” kunnen tonen tussen de gematchte afbeeldingen.

UE 29.	De voorziening zal ten aanzien van specials tenminste de volgende data entries kunnen verwerken: • Voetafdrukken; • Teenafdrukken; • Dieren (pootafdrukken).

W 6	[Midden] De Politie wenst de komende jaren kennis en ervaring op te doen met de volgende (biometrische) modaliteiten: • DNA; • Iris; • Oren; • Aderen; • Motoriek (gait); • Stem; • Tattoo. In hoeverre biedt uw oplossing daartoe de gelegenheid? Beoordeling vindt o.a. plaats op basis van de mate waarin uw oplossing hierin voorziet.

Algemeen deel

6.3. Gebruikersinterface

De Politie gaat uit van het principe Het Nieuwe Werken (HNW): werken op zelfgekozen tijd en plaats met gebruikmaking van technologische hulpmiddelen, zoals draadloos internet, smartphone, tablet en laptop. De nieuwe biometrie voorziening moet dit principe ondersteunen en over een op web technologie gebaseerde interface beschikken.
Biometrie experts, zoals dactyloscopisch experts, kunnen bij hun werkzaamheden gebruik maken van vaste werkplekken, standaard Politie werkplek (WBT) of standaard werkstation (PC), met kwalitatief hoogwaardige beeldschermen.

UE 30.	De voorziening zal over een op web technologie gebaseerde interface beschikken die rechtstreeks via HTML 5 ondersteunende webbrowsers te gebruiken is.

Het geniet de voorkeur dat de voorziening op alle devices dezelfde interface heeft. Daarbij is het toegestaan dat de voorziening de functies op een andere wijze aanbiedt als dat vereist is voor een goede werking.

UE 31.	De gebruikersinterface zal adaptief zijn. Hiermee wordt bedoeld dat de webpagina’s zich aanpassen aan het device waarop de webpagina wordt opgeroepen. Dit kunnen o.a. de volgende devices zijn: WBT, PC, laptops, tablets en smartphones. Ook moet het mogelijk zijn dat de voorziening meerdere beeldschermen kan ondersteunen.

UE 32.	De voorziening zal een meertalige gebruikersinterface hebben en de gebruiker minimaal de keuze bieden uit Engels en Nederlands.

UE 33.	De vastlegging van soortgelijke velden zoals (geboorte)datum zal door de gehele voorziening op identieke, met een vast formaat, manier plaatsvinden. [ISO8601 o.i.d. benoemen]

W 7	[Midden] De voorziening zal ten aanzien van de gebruikersinterface over de volgende functionaliteit beschikken: • De Politie zal eigen, context afhankelijke, documentatie toe kunnen voegen aan de helpfunctionaliteit van de voorziening. Bijvoorbeeld werkinstructies en handleidingen; • Verzamelen van statistische data m.b.t. het gebruik van de interface. Denk hierbij aan actieve tijd per pagina en een heatmap. In hoeverre biedt uw oplossing daartoe de gelegenheid? Beoordeling vindt o.a. plaats op basis van de mate waarin uw oplossing hierin voorziet. Soorten informatie, gemak van uploaden dan wel configureren, het kunnen gebruiken van linken naar andere externe bronnen (bv files).

6.4. Registreren

De voorziening moet gegevens van verschillende biometrische kenmerken kunnen registreren en deze gegevens kunnen combineren met biografische en zaak gerelateerde gegevens (databronnen).
Onder registratie verstaan we: Het vastleggen van ingewonnen en verzamelde gegevens waarbij gecontroleerd wordt (= zoek- of identificatiefunctie) of deze voorkomen in de verzameling van biometrische, zaak gerelateerde en biografische gegevens die eerder in de tijd zijn verzameld en geregistreerd.
Het doel van de biometrievoorziening is een natuurlijk persoon te kunnen individualiseren en verifiëren, dan wel met bepaalde mate herkennen, met behulp van zijn biometrische kenmerken. En gebruikers te voorzien van middelen om dit proces te kunnen laten plaatsvinden en hierin te ondersteunen.
In de voorziening wordt van een persoon meer vastgelegd dan alleen de biometrische kenmerken. Het betreft hier de biografische gegevens, waaronder naam, geboortedatum, geslacht en signalementskenmerken. Daarnaast worden, ten behoeve van de samenhang met het operationele werkproces, ook de aan de persoon of het spoor gekoppelde zaakgegevens geregistreerd.

UE 34.	De voorziening zal tenminste de volgende algemene gegevens kunnen verwerken:
	• **Biometrische templates**
	  o Vingerafdrukken
	  o Handafdrukken
	  o Gelaatsafbeeldingen
	• **Zoekinggegevens**
	  o Gegevens met betrekking tot uitgevoerde zoekingen
	• **Zaakgegevens**
	  o Diverse gegevens met betrekking tot het gerelateerde incident
	• **Biografische gegevens**
	  o Diverse gegevens met betrekking tot de gerelateerde persoon. Waaronder signalementskenmerken.

Binnen de voorziening worden verschillende type gegevens geregistreerd (biometrische gegevens, persoonsgegevens, zaakgegevens, spoorgegevens, enz.) Om deze gegevens aan elkaar te kunnen koppelen wordt gebruik gemaakt van identifiers per gegevenstype. Denk hierbij aan de volgende identifiers:

- Een ID voor één biometrische kenmerkenset
- Een ID voor één spoor
- Een ID voor één persoon
- Een ID voor één zaak

De administratieve lastenverlichting voor de gebruiker is daarbij ook van groot belang. Deze zal bij voorkeur zo weinig mogelijk registreren „om het registreren", zoveel mogelijk gebruik maken van gegevens die al

bekend zijn bij de Politie. Op basis van unieke sleutels gegevens automatisch overnemen uit basis voorzieningssystemen.

UE 35.	De voorziening zal biometrische kenmerken, spoorgegevens, zaakgegevens en biografische gegevens een uniek registratienummer toekennen c.q. koppelen als secundaire key. Elke toevoeging krijgt daarbij een eigen uniek nummer toegekend.
UE 36.	De voorziening zal voor 1 registratie de templates en het biometrienummer bij elkaar opslaan in het eigen referentiebestand waardoor 1:n zoeken en 1:1 verificatie mogelijk is.
UE 37.	De voorziening zal expliciete kenmerken van biometrische kenmerken, spoorgegevens, zaakgegevens en biografische gegevens registeren (bijvoorbeeld in metadata).
UE 38.	De voorziening zal alle digitale bestanden voorzien van een geregistreerde hash om duplicaten te kunnen detecteren.
UE 39.	De voorziening zal diakrieten kunnen verwerken en tonen conform de ISO 8859-1 tekencoderingsstandaard. Bespreken met architecten, voorstel UTF32
UE 40.	De voorziening zal minimaal 1000 kenmerken onder één zaakregistratie kunnen registreren. (bijvoorbeeld: aantal sporen dat aan een zaak toegevoegd kan worden of het aantal gelaatsafbeeldingen van een persoon)

De Politie wil van personen ook de signalementskenmerken kunnen registreren in de voorziening. Vooral om hiermee in combinatie met biometrische kenmerken te kunnen zoeken.
Onder signalementskenmerken verstaan we: Een precieze beschrijving van een uiterlijk. Denk daarbij aan geslacht, leeftijd, lengte, schoenmaat, uiterlijk, postuur, enz.
Ter illustratie is het Landelijk Meldingsformulier Personen (LMF) als bijlage toegevoegd.

UE 41.	De voorziening zal van een persoon de signalementskenmerken kunnen registreren conform het LMF formulier.
UE 42.	De voorziening zal minimaal de volgende formaten als input kunnen registreren: • Jpg; • Png; • Tiff; • MP4; • NIST; • BMP • RAW • WSG

De voorziening zal gebruik maken van referentietabellen waardoor waarden kunnen worden gebruikt voor meerdere zaaktypen. Dit zorgt voor eenduidig gebruik van deze waarden en een centrale plaats om deze te beheren.

UE 43.	De geautoriseerde gebruiker zal referentietabellen kunnen wijzigen.

De Politie heeft de wens om vroeg in het werkproces een kwaliteitsoordeel te krijgen ten aanzien van een aangeleverde afbeelding op basis van een set kwaliteitseisen. Bij een te hoge of te lage kwaliteit kan voortijdig ingegrepen worden, teneinde fouten in opvolgende fases in het voortbrengingsproces te voorkomen. Het gaat om het geven van een kwaliteitsoordeel voor alle type biometrische kenmerken (vingerafdrukken, handafdrukken, sporen en gelaatsafbeeldingen). Hierbij is het wenselijk om, daar waar mogelijk, het kwaliteitsoordeel te baseren op de NFIQ2 standaard.

W 8	[Hoog] De voorziening zal ten behoeve van kwaliteitscontrole feedback geven over de kwaliteit van de ingevoerde afbeelding. Bijvoorbeeld slechte belichting, te weinig pixels. In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing hierin voorziet.

6.5. Raadplegen

De voorziening beschikt over een zoekfunctie waarmee op eenvoudige wijze gegevens en/of in combinaties van gegevens kunnen worden weergegeven. De aangeboden oplossing zal daarbij rekening houden met restricties bij het tonen van informatie, functionaliteit, schermen en zoekresultaten.
De voorziening biedt functionaliteit m.b.t. zoeken waarbij gebruikers zowel vrije (d.m.v. eigen invoer) als gestructureerde (d.m.v. selecties uit één of meer dropdown-/picklists) zoekopdrachten van één of meer "velden" (tekst, categorieën, datum, waarde / bereik, etc.) kunnen "samenstellen" om te kunnen zoeken in de voorziening.

UE 44.	De voorziening zal rekening houden met autorisaties en restricties bij het tonen van informatie, functionaliteit, schermen en zoekresultaten.
UE 45.	De geautoriseerde gebruiker zal in combinatie kunnen zoeken op biometrische kenmerken, zaakgegevens, biografische gegevens en zoekinggegevens.
UE 46.	De geautoriseerde gebruiker zal kunnen zoeken met zogeheten wildcards voor één of meer karakters.
UE 47.	De voorziening zal bij het zoeken ongevoelig zijn t.a.v. hoofdletters en diakrieten (zodanig dat bij zoeken op bijvoorbeeld *Dhr Sirac* of *dhr siraç* dezelfde resultaten worden gegeven).
UE 48.	De geautoriseerde gebruiker zal met een nieuwe zoekopdracht - incl. alle betreffende functionaliteiten - verder kunnen zoeken in de zoekresultaten (zoekresultaten verfijnen).
UE 49.	De geautoriseerde gebruiker zal het kwaliteitsoordeel van een afbeelding kunnen zien.
UE 50.	De geautoriseerde gebruiker zal binnen hetzelfde biometrisch dossier de complete set aan vingerafdrukken, handpalmenafdrukken, spoorafbeeldingen en gelaatsafbeeldingen kunnen raadplegen.
UE 51.	De voorziening zal alle afbeeldingen van een zaak gegroepeerd in een overzicht kunnen tonen.
UE 52.	De voorziening zal wanneer er sprake is van een relatie tussen meerdere zaken de bijbehorende afbeeldingen gegroepeerd per zaak kunnen tonen.
UE 53.	De geautoriseerde gebruiker zal de zoekresultaten kunnen sorteren doormiddel van kolommen. Zowel op- als aflopend kunnen sorteren op ten minste alfabet, datum en type biometrisch kenmerk.
UE 54.	De geautoriseerde gebruiker zal uit de kenmerken van een zaak kunnen zien van welke klant (eenheid, afdeling, buitenland) de gegevens afkomstig zijn. Dit moet dynamisch zijn in en uit te schakelen via opgave van een parameter middels gebruiker en- of webservice.

6.6. Zoekingen verrichten

De voorziening zal met de geregistreerde biometrische gegevens diverse type zoekingen kunnen verrichten en het zal ook mogelijk zijn om op zaakgegevens en/of biografische gegevens te kunnen zoeken.
Zoekingen kunnen geïnitieerd worden door de geautoriseerde gebruiker vanuit de gebruikersinterface of vanuit koppelingen met andere voorzieningen.

De voorziening zal vergelijken kunnen uitvoeren met vingerafdrukken, handafdrukken, sporen, gelaatsafbeeldingen, en wellicht op termijn nog meer biometrische kenmerken.
Tevens kent de voorziening mogelijkheden voor het individualiseren of herkennen op basis van op plaats delict aangetroffen sporen: vingerafdrukken, handafdrukken en/of gelaatsafbeeldingen.
Voor het zoeken in het kader van forensische opsporing, worden sporen vergeleken met een sporen referentiebestand of met individuele spoorafbeeldingen.

Alle hieronder staande type te kunnen verrichten zoekingen gelden uiteraard ook bij het werken met specifieke databases.

UE 55.	De voorziening moet in staat zijn om de volgende type zoekingen te kunnen verrichten: • Voor alle modaliteiten: ▪ A - Referentie vs referentie ▪ B - Referentie vs sporen ▪ C - Sporen vs referentie ▪ D - Sporen vs sporen • Biografische zoeking

UE 56.	De voorziening zal bij alle type biometrische kenmerken meerdere templates kunnen registreren. Bijvoorbeeld automatische codering, geoptimaliseerde codering, nieuw algoritme codering en handmatige codering(en).

UE 57.	De voorziening zal bij het wijzigen van biografische gegevens een historie bijhouden.

Het ABIS kan op twee manieren zoeken:

- Optie 1: Met 1 drempelwaarde waarboven een vergelijkingsscore een treffer is en daaronder niet. Bij uitstek geschikt voor lights-out zoekingen;
- Optie 2: Met 2 drempelwaarden. Eén waarboven een vergelijkingsscore een treffer is en één waaronder een vergelijkingsscore geen treffer is. Vergelijkingsscores tussen de twee drempelwaarden in zijn mogelijke treffers in het grijze gebied.

Het ABIS is zo ingesteld dat een vergelijkingsscore boven de drempelwaarde die een treffer bepaalt een zekere treffer is (kans op onterechte treffer < 1:10.000).

Bij zoek optie 1 is deze drempelwaarde voldoende om te bepalen of er een treffer of geen treffer is.
Voor zoekoptie 2 is het ABIS zo ingesteld dat vergelijkingsscores onder een tweede drempelwaarde zeker geen treffer zijn (kans op onterechte geen-treffer < 1:10.000).
De voorziening handelt het werkproces met de biometrisch expert af als er bij zoekoptie 2 een mogelijk treffer is.

UE 58.	De voorziening zal bij alle type zoekingen drempelwaarden kunnen gebruiken om het resultaat per respondent te bepalen.

UE 59.	De drempelwaarden van alle categorieën moeten variabel in te stellen zijn via opgave van een parameter. De parameter zal door een geautoriseerde gebruiker en/of een webservice ingesteld kunnen worden.

UE 60.	De lengte van de respondentenlijst die het ABIS teruggeeft moet variabel zijn via opgave van een parameter middels gebruiker en- of webservice.

UE 61.	De geautoriseerde gebruiker zal per zoeking de lengte van de respondentenlijst aan kunnen geven.

UE 62.	De voorziening zal de respondentenlijst flexibel en dynamisch kunnen rangschikken. Bijvoorbeeld op basis van de vergelijkingsscore van iedere respondent.

UE 63.	De geautoriseerde gebruiker zal alle type zoekingen in combinatie met biografische en/of signalementskenmerken kunnen uitvoeren.

UE 64.	De voorziening zal voor iedere zoeking een vergelijkingsrapport samenstellen en registreren. In dit rapport is minimaal opgenomen: • Identificerende nummers; • Ranking; • Totaal aantal gevonden afbeeldingen; • Vergelijkingsscores; • Afbeeldingen.

UE 65.	De voorziening zal bij het coderen van een afbeelding altijd minimaal de originele afbeelding voorzien van een hash en controleren of deze hash en ID niet eerder in een andere registratie is gebruikt.

6.7. Bewerken

Het bewerken (dan wel opwerken) biedt de geautoriseerde gebruiker visuele mogelijkheden om afbeeldingen te bewerken ter ondersteuning van de uit te voeren taak.

UE 66.	De geautoriseerde gebruiker zal tenminste de volgende handelingen uit kunnen voeren op afbeeldingen:
	• Brightness aanpassen;
	• Contrast aanpassen;
	• Roteren (Alleen 0,90,180,270 toegestaan, wel backend configurabel). Geldt voor TP/PP/LT;
	• Centreren;
	• Bijsnijden;
	• Positioneren;
	• Grootte van de afbeelding kalibreren op basis van een schaal in de afbeelding;
	• Overstappen op omgekeerd zwart/wit weergave. Witte pixels worden zwart/zwarte pixels worden wit. Geldt voor TP/PP/LT;
	• Afbeeldingen spiegelen;
	• Minutiae weergave aan/uit zetten. Geldt voor TP/PP/LT;
	• Zoom in en uit. (minimaal 4x de originele grootte inzoomen);
	• Beide afbeeldingen kunnen zoomen
	  ◦ tegelijkertijd (parallel continuous zoom)
	  ◦ onafhankelijk van elkaar;
	• Terug naar de originele afbeelding voor bewerking;
	• In lagen kunnen werken bij het bewerken van een afbeelding;
	• De geautoriseerde gebruiker zal een signalering aan kunnen brengen op basis van eigen kwaliteitsoordeel. Met de signalering wordt aangeven dat nieuw bronmateriaal moet worden afgenomen.

UE 67.	De voorziening zal iedere bewerkte afbeelding automatisch registreren inclusief bewerkingshistorie.

W 9	[Midden] De geautoriseerde gebruiker zal de volgende handelingen uit kunnen voeren op/met/bij afbeeldingen: • Gebieden semi-transparant afbakenen in kleur;

	• De thinned image kunnen raadplegen. (De afbeelding die de voorziening gebruikt om te coderen). Geldt voor TP/PP/LT. • Afbeeldingen aanpassen door aanpassing van het histogram; In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaande punten voorziet.

6.8. Charten

Functionaliteit ten behoeve van de analyse van een afbeelding. Een dactyloscopisch expert gebruikt dit onder anderen om een conclusie te onderbouwen.

UE 68.	De geautoriseerde gebruiker zal minimaal de volgende handelingen kunnen verrichten: • Plaatsen van een chartlijn voorzien van een nummer; • Verwijderen van een chartlijn; • Annotatie per chartlijn kunnen plaatsen.

UE 69.	De voorziening zal de chart als afbeelding registreren.

W 10	[Midden] De voorziening zal het volgende kunnen: • Kleur van de chartlijn kunnen aanpassen (per lijn); • Verbergen van een specifieke chartlijn (aan/uit). • Bij inzoomen moeten de uiteinden van chartlijnen in beeld blijven. (bijv. in de marge); • Helderheid van de chartlijn kunnen aanpassen (per lijn); • De geautoriseerde gebruiker zal bij het charten gelijktijdig een beoordelingsformulier in kunnen vullen. • De geautoriseerde gebruiker zal tijdens de chart gebruik kunnen maken van meerdere afbeeldingen in combinatie met elkaar. Alleen van afbeeldingen binnen hetzelfde biometriedossier. In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaande punten voorziet.

6.9. Notities

UE 70.	De geautoriseerde gebruiker zal één of meerdere notitie(s) toe kunnen voegen aan een transactie en/of een taak.

UE 71.	Geautoriseerde gebruikers zullen notities kunnen raadplegen.

UE 72.	Een notitie zal basic tekstverwerking ondersteunen en bestaan uit: • categorie; • titel; • bodytekst; • gebruikers ID; • datum; • tijd van creatie; • minimaal 25Mb aan karakters.

6.10. Analyseren t.b.v. verificatie

Deze functionaliteit wordt gebruikt indien gevonden resultaten ter visuele beoordeling voorgelegd dienen te worden aan de geautoriseerde gebruiker waarbij de geautoriseerde gebruiker moet kunnen aangeven of (een) bepaald (e) biometrisch(e) kenmerk(-enset) wel of niet bij de gezochte afbeelding hoort.

UE 73.	De voorziening zal met een visuele indicatie (kleur en- of icoon) in de gebruikersinterface aangeven welke respondenten van een respondentenlijst reeds beoordeeld zijn door de geautoriseerde gebruiker.

UE 74.	De geautoriseerde gebruiker zal bij een vergelijking met gelaatsafbeeldingen meerdere bronafbeeldingen binnen dezelfde zaak en respondenten binnen hetzelfde biometriedossier kunnen gebruiken.

W 11	[Hoog] De voorziening zal ten behoeve van analyse doeleinden over de volgende functionaliteit beschikken: • De voorziening zal een afbeelding in volledig scherm kunnen tonen; • De geautoriseerde gebruiker zal bij het analyseren gelijktijdig een vergelijkingsformulier in kunnen vullen. In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaande punten voorziet.

6.11. Vergelijken

UE 75.	De geautoriseerde gebruiker zal bij een identificatie alle beschikbare vingerafdruk-, handpalmsets en gelaatsafbeeldingen en sporen van dezelfde persoon/zaak kunnen gebruiken.

UE 76.	De geautoriseerde gebruiker zal de afbeelding waarmee de zoeking is uitgevoerd en de afbeelding uit de respondentenlijst naast elkaar kunnen vergelijken.

UE 77.	De voorziening zal de afbeelding waarmee de zoeking is uitgevoerd en de afbeelding uit de respondentenlijst tonen met dezelfde schaal, gelijke grootte, rotatie en positie.

Het zal mogelijk zijn om twee afbeeldingen met elkaar te vergelijken zonder dat deze in een referentieset zijn opgenomen of opgenomen zullen worden. Vergelijking met twee handmatig ingevoerde afbeeldingen waarbij wel de volledige functionaliteit van de voorziening beschikbaar is.

UE 78.	De geautoriseerde gebruiker zal een vergelijking uit kunnen voeren op twee handmatig ingevoerde afbeeldingen en daarbij over de volledige functionaliteit van de voorziening beschikken.

UE 79.	De geautoriseerde gebruiker zal de metagegevens van beide afbeeldingen kunnen inzien op basis van autorisaties.

UE 80.	De geautoriseerde gebruiker zal bij het vergelijken zowel de gezochte afbeelding als de referentieafbeelding onafhankelijk van elkaar kunnen schalen, zodat ze in dezelfde schaal in hetzelfde gebied naast elkaar worden getoond.

UE 81.	De geautoriseerde gebruiker zal het resultaat van een vergelijking voor alle modaliteiten vast kunnen leggen in de vorm van: • Oordeel: o Match; o Hard-to-match;

	o No-match o Non-match o Ident; o Individualisation; o Hard-to-ident; o Non-ident; o Inconclusive; • Kwaliteit: o Insufficient; o Incorrect;

6.12. (Her)coderen

Vingerafdrukken, handafdrukken, gelaatsafbeeldingen en sporen worden conform het algoritme gecodeerd. Alle afbeeldingen worden automatisch gecodeerd en gezocht. Indien aangegeven is dat een level 2, 3 of 4 zoeking gewenst is en de zoeking geen hit heeft opgeleverd dan is de vervolgstap hercoderen (ReEncode).

Voorwaarden:
Iedere zoekcyclus moet volledig worden verwerkt. Dit betekent dat een spoor (dacty/gelaat), indien geen herkenning), een of meerdere keren achter elkaar kan worden gecodeerd, gezocht en geverifieerd, dit is afhankelijk van de level die het spoor heeft meegekregen.
Bij al deze levels bevat de mogelijkheid tot handmatig coderen alvorens een zoeking te initiëren. Elke zoeking wordt gevolgd door een verificatie.

UE 82.	De voorziening zal elke afbeelding automatisch coderen en zoeken.

UE 83.	De geautoriseerde gebruiker zal de automatische codering handmatig kunnen aanpassen / wijzigen / toevoegen (hercoderen), waarbij bij voorkeur visueel onderscheid wordt gemaakt tussen het automatische en handmatige coderen.

6.13. Specifieke databases

In sommige gevallen is het nodig dat er gezocht kan worden in specifieke databases(1:s), bijvoorbeeld bij speciale evenementen, gebeurtenissen, getuigen of bij andere doeleinden.
Gebruikers moeten, op basis van autorisatie, toegang hebben tot een specifieke database en onderliggende gegevens. De gegevens in een specifieke database mogen op geen enkele andere wijze benaderbaar zijn dan binnen de specifieke database zelf. Zo mogen zij bijvoorbeeld niet meegenomen worden in reguliere raadplegen en zoekingen.
Een specifieke database moet gezien worden als een besloten omgeving met een beperkte duur en een gelimiteerd aantal gebruikers.
In voorkomende gevallen, daar waar dit wettelijk noodzakelijk is, zal de rechtmatigheid geregistreerd moeten worden. Vastleggen van gegevens waarvoor en in opdracht van wie de specifieke database is aangemaakt. Bijvoorbeeld officier van justitie of rechter-commissaris.

Werkzaamheden in specifieke databases zullen op dezelfde wijze inzichtelijk zijn als regulier werk. Waarbij wel rekening wordt gehouden met rechten.

UE 84.	De geautoriseerde gebruiker zal, specifieke database(s) van vingerafdrukken, handafdrukken, sporen en/of gelaatsafbeeldingen kunnen aanmaken.

UE 85.	De geautoriseerde gebruiker zal bij het werken met specifieke databases gebruik kunnen maken van de volledige functionaliteit van de voorziening.

UE 86.	De geautoriseerde gebruiker zal een selectie van referentiesets kunnen koppelen aan een specifieke database.

UE 87.	De voorziening zal alleen toegang tot een specifieke database verlenen aan hiervoor geautoriseerde gebruikers.

UE 88.	De geautoriseerde gebruiker zal meerdere (specifieke) databases kunnen selecteren voor een zoeking.

6.14. Processturing

De procesgang binnen de voorziening wordt ingericht door middel van vooraf gedefinieerde workflows op basis van autorisaties, mandaat en productgroepen en kan door medewerkers van de Politie zelf worden aangepast.

De voorziening zal de geautoriseerde gebruiker, maximaal ondersteunen. Deze ondersteuning omvat onder andere workflow functionaliteit, waarmee de procedures gevolgd en in acht genomen kunnen worden.
In de workflow kan worden vastgelegd dat bepaalde raadplegingen en werkzaamheden alleen conform het 'vier ogen principe' uitgevoerd kunnen worden.

De voorziening zal over een flexibel workflow systeem beschikken. Flexibel wil in dit geval zeggen dat het in te richten, aan te passen en te onderhouden is door medewerkers van de Politie. Het moet uitgebreid genoeg zijn en voorzien in koppelvlakken (bijv. email/exchange) zodat de huidige werkprocessen ondersteund kunnen worden.
Voor het opstellen van de specificaties van de workflows zelf (stappen, acties, enz.) gebruikt de Politie de Scrum methodiek, hetgeen in zichzelf inhoud dat detaillering van de workflows pas wordt vastgesteld gedurende het implementatieproces. Hiervoor zijn nu nog geen gedetailleerde beschrijvingen vastgelegd.

De Politie maakt op dit moment gebruik van de workflow functionaliteit in haar AFIS voorziening. Daarnaast gebruikt de Politie een externe workflowmanagement voorziening, waarmee opdrachten gegeven worden aan het AFIS en het resultaat wordt terug ontvangen.
Het is niet uitgesloten dat een dergelijke combinatie van intern en extern gebruik van workflow management functionaliteit voortgezet zal worden.

6.14.1. Algemeen

UE 89.	De opdrachtnemer zal de ontwikkeling en implementatie van de workflows in samenwerking met de gebruikers c.q. het DevOps team opleveren.

Onderstaande eisen dienen dan ook slechts als basis voor de nieuwe voorziening.

UE 90.	De voorziening zal de uitvoering van werkprocessen (geautomatiseerd) ondersteunen met workflowmanagement, waarbij het aantal te ondersteunen functionele processen kan oplopen tot boven de 100.

UE 91.	De geautoriseerde gebruiker zal door middel van configuratie (zero-coding) workflowprocessen kunnen aanmaken, aanpassen, parametriseren en beheren.

UE 92.	De voorziening zal minimaal de volgende workflowmanagement functionaliteit ondersteunen: • Stapelgewijze verwerking (= het achtereenvolgens uitvoeren van dezelfde taak voor verschillende zaken zonder terug te hoeven keren naar de taaklijst) • Taakgericht werken (= het achtereenvolgens uitvoeren van taken voor dezelfde zaak zonder terug te hoeven keren naar de taaklijst) • Het goedkeuren dan wel paraferen van een werkprocesstap. • Minimale, maximale, vaste en flexibele doorlooptijden voor een werkproces of werkprocesstap in te stellen. • Een taak of een stap in een taak is apart toe te wijzen aan een specifieke gebruiker of gebruikersgroep die daarvoor worden ingedeeld in een schema van gebruikersrollen en gebruikersgroepen specifiek voor deze voorziening. • Functiescheiding: bepaalde activiteiten binnen een werkproces mogen niet door dezelfde gebruiker worden uitgevoerd (functiescheiding in relatie tot de administratieve organisatie). • Routeringsvormen: o sequentiële routering

	o selectieve routering o parallelle routering o iteratieve routering o conditionele routering
UE 93.	De voorziening zal de mogelijkheid bieden tot routing langs verscheidene functionarissen voor mutatie en- of fiattering en biedt de mogelijkheid om binnen hetzelfde niveau of dezelfde rol door te sturen i.v.m. communicatie, werkoverdracht.
UE 94.	De voorziening zal functiescheiding kennen tussen invoer van gegevens enerzijds en goedkeuring van deze gegevens anderzijds en tussen raadpleeg- en muteerautorisaties
UE 95.	De voorziening zal bij een workflow het invullen van invulvelden kunnen verplichten.
UE 96.	Het DevOps team zal zelf invoervelden / metadata velden (vrije en gestructureerde) kunnen definiëren bij een workflow, object en document.

De voorziening biedt functionaliteit voor het inzichtelijk maken van de voortgang van transacties door middel van automatisch toe te kennen statussen. Welke soorten afhankelijkheid kunnen worden gedefinieerd, waarbij bijv. een type besluit, aanwijzing, resultaat, of document het verder vervolg van een transactie als het ware dicteren.

UE 97.	De geautoriseerde gebruiker kan nieuwe statusdefinities toevoegen en instellen voor alle transacties die systeem breed gebruikt worden.
UE 98.	De voorziening zal met betrekking tot processturing transacties door middel van een aantal opeenvolgende statussen naar een eindresultaat kunnen geleiden op basis van bedrijfsregels.

Automatische acties

UE 99.	De voorziening zal op basis van eerder ingestelde status van de transactie in de workflow automatisch mail kunnen versturen inclusief bijlage.
UE 100.	Per workflow zal instelbaar zijn of een status wijziging automatisch leidt tot het uitzetten van een actie (bv opstarten deel workflow). Bijvoorbeeld: als een statuswijziging X plaatsvindt dient automatisch de ketenpartner X te worden geïnformeerd.
UE 101.	De voorziening zal vanuit de workflow documenten / e-mails kunnen genereren o.b.v. sjablonen door de tags ervan te vullen met de overeenkomstige kenmerken uit de betreffende zaak / het betreffende object („parameters" t.b.v. documentcreatie) en/of eventuele andersoortige gegevens (zoals d.m.v. vrije tekst en/of snelkeuzelijsten), incl. de eventuele handelingen die gebruikers daartoe dienen uit te voeren.
UE 102.	De geautoriseerde gebruiker zal (visuele) workflow processchema's kunnen exporteren en/of printen.
UE 103.	De voorziening zal op basis van een actieknop een schermprint met bijbehorende sessie informatie, opmerkingen en categorie vastleggen en doorsturen naar een gedefinieerd systeem en- of gebruiker.
UE 104.	De voorziening zal transacties die veel resources gebruiken (op basis van parameters), kunnen afbreken of pauzeren en hiervan een bericht naar een geautoriseerd gebruiker sturen.

De eigenlijke "trigger" voor het starten van een flow kan buiten de voorziening plaatsvinden. Bijvoorbeeld een verzoek vanuit een externe applicatie of workflowsysteem. De wijze waarop de verzoeken binnenkomen betreft soms ook het kanaal waarlangs terug levering van informatie noodzakelijk of gewenst is. Dit stelt allerlei eisen en wensen aan de koppelbaarheid en integreerbaarheid van de aangeboden workflow oplossing.

UE 105.	De workflowmanagement component van de voorziening zal extern aan te sturen zijn en/of kunnen interacteren met een extern workflow systeem.

6.14.2. Prioriteren

Om bezig te zijn met de zaken die belangrijk zijn is een prioriteringssysteem van grote waarde. De nieuwe voorziening moet dan ook om kunnen gaan met prioritering van transacties.
Prioritering op gebruikersniveau: zichtbare transacties in de gebruikersinterface.
Prioritering op systeemniveau: afhandelen van transacties vanuit de gebruikersinterface versus afhandelen van transacties vanuit koppelingen (ID-Zuil, Prüm, enz.)

UE 106.	De geautoriseerde gebruiker kan types transacties definiëren.
UE 107.	De geautoriseerde gebruiker kan een prioriteit per type transactie definiëren.
UE 108.	De geautoriseerde gebruiker zal de type definiëring en te hanteren prioritering kunnen beheren (wijzigen of verwijderen).
UE 109.	De voorziening zal nieuwe transacties automatisch de vooraf vastgestelde prioriteit toekennen.
UE 110.	De geautoriseerde gebruiker zal de toegekende prioriteit van een transactie kunnen wijzigen.
UE 111.	De voorziening en- of gebruiker zal transacties op basis van gestelde prioriteit afhandelen.

De voorziening zal wanneer een transactie de hoogste prioriteit krijgt een notificatie sturen naar gedefinieerde gebruikers zodat zij er voor kunnen zorgen dat de transactie zo snel mogelijk opgepakt wordt.
De voorziening zal over een mechanisme beschikken om gedefinieerde gebruikers een bericht te sturen via Email of SMS.
Gedefinieerde gebruikers betekent een lijst met gebruikers geassocieerd met de categorie waartoe het bericht behoord.

6.14.3. Termijnbewaking

Voor type transacties zijn afspraken gemaakt met betrekking tot de doorlooptijd en deze moeten bewaakt worden.
De voorziening beschikt over een signaalfunctie waarmee gebruikers automatisch worden geïnformeerd over het overschrijden van bepaalde drempelwaarden, ten minste het naderen of passeren van de doorlooptijd van een transactie of taak. Deze signaalfunctie kan betrekking hebben op alle modules van de voorziening.

UE 112.	De geautoriseerde gebruiker zal de type definiëring en te hanteren doorlooptijd kunnen beheren (wijzigen of verwijderen).
UE 113.	De voorziening zal transacties een doorlooptijd toekennen.
UE 114.	De geautoriseerde gebruiker zal de doorlooptijd van een transactie aan kunnen passen.
UE 115.	De geautoriseerde gebruiker zal de doorlooptijden per type transactie kunnen definiëren.
UE 116.	De voorziening zal bij (dreigende) termijnoverschrijding van een transactie een notificatie sturen naar gedefinieerde gebruiker(s) en/of een groep.
W 12	[Hoog] De voorziening zal een (dreigende) termijnoverschrijding visueel weergeven in de actuele werkvoorraad (dashboard). In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaand punt voorziet.

6.14.4. Werkvoorraad

Om taken binnen de biometrische werkprocessen op een juiste en tijdige manier af te handelen is het van belang om inzicht te hebben op de werkvoorraad.
Hierbij wordt door de geautoriseerde gebruikers gedacht aan een (soort van) dashboard waarmee in één oogopslag de lopende en nog in behandeling te nemen taken zichtbaar zijn, ongeacht welk type biometrisch kenmerk (vingerafdrukken, handafdrukken, sporen en gelaatsafbeeldingen). Vanuit zo'n dashboard kan de geautoriseerde gebruiker dan aan de slag met een taak.

Definitie transactie: Een reeks van informatie uitwisselingen (voornamelijk bij koppelingen) en aanverwant werk (taken) dat wordt behandeld als een eenheid voor het voldoen aan een verzoek en voor het waarborgen van de integriteit van de database.

Definitie Taak: Hoeveelheid van werk die aangemaakt is in de voorziening maar nog niet gereed is. Dit kan zijn: het uitvoeren van een verificatie of identificatie, het bewerken van een spoor, het uitzetten van een Prüm verzoek, het opstarten van een meervoudige procedure, enz.

Definitie actuele werkvoorraad: De verzameling taken die op dit moment in behandeling zijn of in de wachtrij zitten om in behandeling genomen te worden.

UE 117.	De voorziening zal de actuele werkvoorraad zichtbaar maken door middel van een dynamisch dashboard.
UE 118.	De geautoriseerde gebruiker zal inzicht hebben in de actuele werkvoorraad.
UE 119.	De daartoe geautoriseerde gebruiker zal een taak/zaak kunnen toewijzen aan andere geautoriseerde (groep) gebruiker(s).
UE 120.	De voorziening zal een in behandeling genomen taak koppelen aan de geautoriseerde gebruiker.
UE 121.	De geautoriseerde gebruiker zal een in behandeling genomen maar niet afgeronde taak terug kunnen plaatsen in de actuele werkvoorraad.
UE 122.	De voorziening zal taken in de werkvoorraad tonen op basis van aflopende prioriteit.
UE 123.	De geautoriseerde gebruiker zal de aan een gebruiker gekoppelde taak kunnen ontkoppelen.
UE 124.	De voorziening zal vervolg taken in een werkproces automatisch koppelen aan de geautoriseerde gebruiker die de voorgaande taak heeft uitgevoerd. Mits dit toegestaan is in het werkproces.
UE 125.	De geautoriseerde gebruiker zal een afgehandelde transacties kunnen raadplegen.
UE 126.	De geautoriseerde gebruiker zal de actuele werkvoorraad kunnen monitoren.
UE 127.	De geautoriseerde gebruiker zal de actuele werkvoorraad kunnen filteren en sorteren om tot een selectie van taken te komen. Dit is te sorteren/filteren per gebruiker en soort workflow op elk gewenst niveau.
UE 128.	De geautoriseerde gebruiker zal, indien deze een selectie aan taken heeft gemaakt, na het afhandelen van een taak direct door kunnen gaan met de (eerst) volgende taak binnen deze selectie aan taken.
UE 129.	De voorziening zal een afgehandelde taak niet meer tonen in de actuele werkvoorraad.
UE 130.	De geautoriseerde gebruiker zal een taak kunnen verwijderen uit de actuele werkvoorraad.

Met opmerkingen [FvL2]: Het definitief terugplaatsen zou mijn inzien alleen na goedkeuring coördinator moeten kunnen.

UE 131.	De voorziening zal een verwijderde taak een specifieke eindstatus toekennen waardoor zichtbaar is dat deze is verwijderd.

UE 132.	De geautoriseerde gebruiker zal bij het verwijderen van een taak verplicht een reden moeten opgeven.

Er is informatie nodig om toezicht te kunnen houden op de kwaliteit van de uitvoering en om verantwoording te kunnen afleggen over de geleverde prestaties.
Statistische gegevens over bijvoorbeeld:

- Aantallen per soort taak en/of transactie die zijn afgehandeld binnen een nader aan te geven tijdsperiode.
- Aantallen per soort taak en/of transactie die zijn afgehandeld per tijdseenheid binnen een nader aan te geven tijdsperiode.
- Gemiddelde afhandelingstijd per soort taak en/of transactie die zijn afgehandeld binnen een nader aan te geven tijdsperiode. (bv 1000 transactie in de periode november)
- Gemiddelde afhandelingstijd per soort taak en/of transactie die zijn afgehandeld per tijdseenheid, binnen een nader aan te geven tijdsperiode. (bv gemiddeld afgehandeld 10 per uur binnen 00:00 – 12:00)
- Afhandelingstijd per soort taak en/of transactie die zijn afgehandeld weergegeven per tijdseenheid, binnen een nader aan te geven tijdsperiode. (bv afgehandeld in de periode 08:00 – 12:00)

UE 133.	De geautoriseerde gebruiker zal statistische gegevens kunnen raadplegen m.b.t. de verwerking van transacties/taken door gebruikers van de voorziening.

UE 134.	De geautoriseerde gebruiker zal een bericht kunnen versturen naar andere gebruikers of gebruikersgroepen. Bijvoorbeeld een geautoriseerd gebruiker die een bericht naar alle gebruikers stuurt.

6.15. Output

De aangeboden oplossing ondersteunt de opslag en ontsluiting van documenten uit alle gangbare formats. Tot gangbare formats verstaat de Politie onder meer Microsoft Office-documenten, ODF-bestanden, Pdf-bestanden, image- en vectorformats (JPG, WSQ, PNG, GIF, SVG), video-bestanden, enz. (niet-limitatieve opsomming).

Bij export van data (NIST en afbeeldingen)mag compressie en decompressie worden toegepast, mits geen verlies van informatie optreedt.

UE 135.	De voorziening zal formulieren van en gegevens over alle transacties kunnen genereren.

UE 136.	De voorziening zal afhankelijk van het type gegevens in de volgende formaten kunnen exporteren: • Daartoe geautoriseerde gebruikers kunnen gegevens exporteren als gestructureerde data; • Daartoe geautoriseerde gebruikers kunnen formulieren exporteren als pdf; • Gegevens uitwisseling in het kader van koppelingen met externe systemen c.q. organisaties zal minimaal NST en CSV/SQL formaat kunnen.

UE 137.	De voorziening zal de geautoriseerde gebruiker de mogelijkheid bieden om een afbeelding te printen of op te slaan.

UE 138.	De voorziening zal gegevens horende bij een biometrisch kenmerk, persoon of zoeking automatisch kunnen overnemen in formulieren in de vorm van een pdf.

Functionaliteit m.b.t. het creëren (ad hoc) en beheren van (management)rapportages en query's:

- Presentatiewijze (zoals taartdiagrammen, staafdiagram, tabellen, vrij te kiezen, etc.).
- Uitvoerwijzen zoals afdrukken, opslaan, exporteren (zoals CSV, XLS, XLSX, SQL), etc.
- Selecties en groepering per eenheid (buurt, stad)
- Selecties en groepering per type dienst
- Overige selecties en groeperingen (per gebruiker, per type transactie, etc.)
- Periodiciteit (per dag, week, maand, kwartaal, jaar, vrij te kiezen, etc.)
- Het gebruik van functies zoals sorteringen, (sub)totalen, etc.

Belangrijk daarbij is de mate waarin gebruikers rapportages zelfstandig kunnen creëren en beheren.

UE 139.	De voorziening zal ten behoeve van rapporteren over de volgende functionaliteit beschikken: • De voorziening zal automatisch en op verzoek rapportages kunnen genereren naar gelang de aanvraag en/of uitslag van een zoeking; • De geautoriseerde gebruiker zal zelf ontwikkelde rapportages en analyses kunnen toevoegen aan de voorziening; • De geautoriseerde gebruiker zal op een willekeurig tijdstip maatwerkrapportages (rapportengenerator) kunnen samenstellen met actuele gegevens. Bijvoorbeeld op basis van een selectie van biometrische en administratieve gegevens; • De daartoe geautoriseerde gebruiker zal een expertiserapport kunnen genereren van een vergelijking; • De voorziening zal periodiek rapportages kunnen genereren en deze naar gedefinieerde gebruikers mailen. Bijvoorbeeld naar de gebruiker of het management).

6.16. Alerts

Een persoon, incidentnummer of spoor kunnen voorzien van een alert ter ondersteuning van opsporing of in het kader van kwaliteitsbeheer. De alert is een notificatiefunctie. Bijvoorbeeld: indien de vingerafdrukken van een persoon met alert aangeboden worden ter verificatie c.q. identificatie dan gaat er een notificatie naar de belanghebbende.

UE 140.	De daartoe geautoriseerde gebruiker zal een alert kunnen plaatsen op: • Biometriedossier; • Incident (alle modaliteiten); • Spoor (alle modaliteiten); • Type of transaction; • Systeemstatus; • Biografisch gegeven; • Administratief gegeven; • Handeling in systeem.

Bewaartermijnen

De biometrische kenmerken worden voorzien van metadata, deze metadata kan onder meer gebruikt worden voor het schonen van de registers, conform wettelijke regimes per werkproces/keten. Daarbij dient aandacht besteed te worden aan de mogelijkheid dat in het ene wettelijk kader de gegevens vernietigd dienen te worden, terwijl in het andere wettelijk kader de gegevens bewaard mogen blijven.

De gegevensverwerking door de Politie wordt gereguleerd door verschillende algemene wetten en regelingen zoals de Wbp en de Wpg.
De Algemene Verordening Gegevensbescherming (AVG) ~~Wet bescherming persoonsgegevens~~ geeft aan onder welke voorwaarden persoonsgegevens mogen worden verwerkt. De Wet politiegegevens (WPG) bepaalt onder welke voorwaarden de politie gegevens mag verwerken.
Informatie-objecten worden bij opslag en verdere verwerking voorzien van kenmerken die nodig zijn om de juistheid en de rechtmatigheid van de gegevensverwerking te kunnen waarborgen.
Bij de binnenkomst of het ontstaan van gegevens in de organisatie en bij de opslag en verdere verwerking van gegevens moet de verwerkingsgrondslag worden bijgehouden.

Met opmerkingen [MdH3]: Hier de AVG noemen omdat deze 25 mei 2018 de WBP vervangt. Afkorting in de afkortingenlijst meenemen.

Met opmerkingen [MdH4]: Dit komt ook terug bij beveiliging, mag hier wel blijven staan als toelichting.

Wanneer gegevens niet langer verwerkt mogen worden dan worden deze in eerste instantie een wettelijk periode bewaard (logisch verwijderen) en vervolgens in tweede instantie vernietigd (onherroepelijk verwijderen).
Bewaarde gegevens mogen slechts voor specifieke redenen geraadpleegd (administratieve handelingen, klachtenafhandeling) c.q. verder verwerkt worden (voor identificatie van onbekende doden). De termijn van bewaren en vernietigen is mede gebaseerd op het delictskenmerk van het incident.

UE 141.	De voorziening zal biometrische kenmerken voorzien van de grondslag van de verwerking waarvoor de gegevens zijn verzameld c.q. verder verwerkt mogen worden.
UE 142.	De voorziening zal biometrische kenmerken voorzien van een bewaartermijn per wettelijk regime.
UE 143.	De geautoriseerde gebruiker zal een biometrisch kenmerk kunnen voorzien van een verjaringstermijn.
UE 144.	De geautoriseerde gebruiker zal de bewaartermijn en/of verjaringstermijn van een biometrisch kenmerk aan kunnen passen.
UE 145.	De voorziening zal transacties voorzien van een delictskenmerk.
UE 146.	De geautoriseerde gebruiker zal de het delictskenmerk van een biometrisch kenmerk aan kunnen passen.

De voorziening moet functionaliteit bieden voor het selectief kunnen verwijderen van (biometrische) gegevens op basis van de in de wet vastgestelde bewaartermijnen. Het niet langer mogen gebruiken van de biometrische kenmerken in zoekingen.

UE 147.	De voorziening zal een biometrische kenmerk waarvan de bewaartermijn verstreken kunnen markeren met een specifieke status en toegang.

De voorziening moet functionaliteit bieden voor het selectief kunnen vernietigen van (biometrische) gegevens op basis van de in de wet vastgestelde bewaartermijnen.
De voorziening dient zo te worden ontworpen en uitgevoerd dat de bewaartermijnen in acht worden genomen en gegevens die niet langer bewaard mogen worden automatisch worden vernietigd, na autorisatie door een daartoe geautoriseerde medewerker.

UE 148.	De voorziening zal een biometrisch kenmerk waarvan de bewaartermijn definitief is verstreken voorzien van een specifieke status en vernietigen.
UE 149.	De voorziening zal van ieder vernietigd biometrisch kenmerk een rapportage opmaken en registreren.

6.17. Documentatie

Alle documentatie voor de gebruikers van de voorziening is volledig Nederlandstalig en bovendien in zodanig “begrijpelijke” taal gesteld dat ook mensen die wat minder technisch onderlegd zijn e.e.a. kunnen begrijpen.
Systeem- en andere (technische) documentatie voor technisch beheerders van de voorziening is volledig Nederlands- en/of Engelstalig. Alle documentatie van de voorziening wordt door Inschrijver aan de Politie beschikbaar gesteld in aanpasbare bestandsformaten (dus niet (alleen) als PDF en dergelijke).

UE 150.	De voorziening zal voor geautoriseerde gebruikers en beheerders over een Nederlandstalige en- of Engelstalige handleiding beschikken.

UE 151.	De Politie zal het recht hebben om alle documentatie van de voorziening te dupliceren en te distribueren voor intern gebruik, alsmede aan uitvoeringsorganisaties en andere partijen die voor c.q. namens de Politie werkzaamheden verrichten.

Met opmerkingen [RH(5]: Let op! Kan zijn dat leveranciers dit zien als informatie leveren aan de concurrent bij afname van een SBC van een concurrent.

UE 152.	Inschrijver zal gedurende de looptijd van de overeenkomst (incl. eventuele verlenging) de beschikbaar gestelde documentatie actueel houden en voor iedere nieuwe en verbeterde versie van de voorziening opleveren.

6.18. Autorisaties

Met opmerkingen [FvL6]: Moet hier niets vermeld worden over IAM of verwezen naar de paragraaf hieronder?

Met opmerkingen [MdH7R6]: Ik zou IAM in de beheer en techniek hoofdstukken noemen en hier beperken tot de functionaliteit.

De voorziening bevat zeer vertrouwelijke gegevens over personen. De beveiliging van deze gegevens en de bescherming van de privacy van de betrokkenen is daarom van het grootste belang. Onderdeel daarvan is toegang tot deze gegevens en de autorisatie is rolgebaseerd en op basis van "need to know" principe.

UE 153.	~~Gebruikers hebben via single sign-on (SSO) toegang tot onderdelen van de voorziening (voor zover zij daartoe geautoriseerd zijn).~~ Binnen de voorziening moeten autorisaties op zowel rol als groep bepaald kunnen worden. Dit moet ook in combinatie mogelijk zijn. Rollen in de voorziening zijn vrij te definiëren. ~~en kunnen gekoppeld worden aan één of meer groepen in de active directory van Politie.~~

Met opmerkingen [MdH8]: Hier stonden meerdere eisen en wensen doorelkaar. Voor de functionaliteit is het belangrijk dat er rolbased en rulebased (is er doelbinding, locatie gebonden werken ivm eisen werkplek. Etc.) SSO is een hoge wens en wordt in de techniek verder uitgewerkt. Rulebased mogelijk in de toelichting op nemen: “Sommige verwerkingen mogen alleen uitgevoerd worden op bepaalde werkplekken die voldoen aan bepaalde eisen”.

W 13	[Hoog] Gebruikers hebben via single sign-on (SSO) toegang tot onderdelen van de voorziening (voor zover zij daartoe geautoriseerd zijn).
W 14	[Hoog] Binnen de voorziening kunnen autorisaties worden bepaald via toegangsregels (grondslag verwerking, locaties, etc.) en niet op basis van de rol van een gebruiker

Met opmerkingen [MdH9]: IAM doelstelling kent ook rules gedefinieerde toegang.
Doelstelling is om zo efficiënt mogelijk gebruikersaccounts te kunnen autoriseren en de-autoriseren voor vooraf gedefinieerde functionaliteit voor de betreffende personen en/of doelgroepen, waarin SSO en RBAC (RolBAC & RulBAC) worden ondersteund.

Hoofdstuk 7. Niet-functionele eisen

7.1. Inleiding

De uiteindelijke voorziening laat zich niet alleen kenmerken door functionele eisen, maar niet in de laatste plaats ook door de non-functionele eisen. Het is afhankelijk van de eisen van de use case waar biometrie voor wordt ingezet. Zo dient het individualisatieproces zorgvuldig te gebeuren en is accuratesse van groot belang. Bij verificatie bijvoorbeeld, is het daarentegen essentieel dat de beschikbaarheid en performance goed geregeld is om te voorkomen dat er grote wachttijden ontstaan.

Daarnaast moet het gehele werkproces zodanig zijn ingericht dat de authenticiteit van de gegevens geborgd is. Zo is het goed denkbaar dat het matchingsproces een rol vervult in een rechtszaak. De rechtsgang mag in dit geval niet gestoord worden door enig twijfel over de authenticiteit van de gegevens en de matchingsprocedure. Dit impliceert dat de correcte werking van het systeem glashelder kan worden aangetoond.

7.2. Capaciteit

De mate waarin de maximale limieten van een product- of systeemparameter voldoet aan de wensen.

UE 154. De voorziening moet in staat zijn om onderstaande volumes aan te kunnen bij een jaarlijkse groei van ongeveer 10%:
M = miljoen

File Type	Contract	NU	NIEUW	P/J prognose
Tenprint File (TPF) Flat	2,675M	1,20M		
Tenprint File (TPF) Roll/Flat	4,000M	2,60M		
Tenprint Files (TPF)	6,675M	3,80M	10M	+0,75M
Palm Print File (PPF)	1,175M		2M	+0,05M
Unsolved Latent File (ULF)	0,200M	0,26M	1M	+0,10M
Unsolved Latent Palm (ULP)	0,100M		0.5M	+0,03M
Latent Case Database	0,250M	0,34M	1M	+0,10M
Face Case Database			?	?
Face Reference Files	12,000M	7,5M	25M	+0,35M
Single Images		42M	100M	
Incident ID's		3,8M	?	
Biometric ID's		1,6M	?	

UE 155. De voorziening moet in staat zijn om verschillende typen zoekingen gelijktijdig te verwerken. Waarbij op jaarbasis onderstaande aantallen gelden:
M = miljoen

Type	Huidig aantal	Prognose	SR	VR	Anders	Piek p/u
TP vs TP	2.1M	5,25M	3,5M	1M	0,75M	500
TP vs LT	0.8M	1,75M	1M		0,75M	250
LT vs TP	0.4M					
LT vs TP/PP	0.42M	1,26M	1M	0,001M	0,25M	50
PP vs PP		0,01M	0,01M			10
PP vs LT	0.08M	0,01M	0,05M			10
LT vs PP	0.02M					10
LT vs LT	0.001M	0,03M	0,03M		0,001M	10
FC vs FC		2,1M	1M	0,001M	1M	200

	PR vs FC	?	2M	1M	1M		200
	FC vs PR		3M	1M	1M	1M	200
	PR vs PR		0,25M	0,25M			

UE 156.	De voorziening moet in staat zijn om onderstaande volumes aan inscannen van afdrukbladen te verwerken. Waarbij op jaarbasis onderstaande aantallen gelden:

Scans	**Aantal**
Afdrukbladen	20.000

UE 157.	De voorziening zal over faciliteiten beschikken om per ingestelde tijdseenheid, per aan te geven periode, de in deze paragraaf genoemde aantallen weer te geven. Dit dynamisch door middel van een dashboard en via een rapportage. Doelen: (1) Dynamisch monitoren van het systeem; (2) Mogelijkheden te hebben voor capaciteitsplanning: (a) year-to-date te controleren; (b) korte en middel lange termijn capaciteitsbehoefte te voorspellen; (c) trend analyse uit te voeren; (d) een basis te hebben om lange termijn capaciteitsplanning mogelijk te maken.

7.3. Performance

Deze paragraaf beschrijft de gewenste prestatie van de voorziening in verhouding tot het aantal resources, onder bepaalde condities.
De genoemde doorlooptijden gelden vanaf ontvangst door de ABIS vanuit het aanroepende proces tot verzenden van antwoord door de ABIS naar het aanroepende proces.

UE 158.	Responsetijden op schermen in de gebruikersinterface zijn gemiddeld minder dan 3 seconden voor elke gebruiker van de voorziening bij het schakelen tussen velden en schermen. Dit geldt niet voor het genereren van overzichten en rapportages, en uploaden van bestanden.

UE 159.	Voor alle type zoekingen gelden de volgende responstijden: • zoekingen met vingerafdrukken, handafdrukken of sporen maximaal 5 seconden; • zoekingen met gelaatsafbeeldingen maximaal 30 seconden.

UE 160.	De voorziening zal over faciliteiten beschikken om per ingestelde tijdseenheid, per aan te geven periode, de in deze paragraaf genoemde aantallen weer te geven. Dit dynamisch door middel van een dashboard en via een rapportage. Doelen: (1) Dynamisch monitoren van het systeem; (2) Mogelijkheden te hebben voor capaciteitsplanning: (a) year-to-date te controleren; (b) korte en middel lange termijn capaciteitsbehoefte te voorspelen; (c) trend analyse uit te voeren; (d) een basis te hebben om lange termijn capaciteitsplanning mogelijk te maken.

7.4. Beschikbaarheid

De biometrische voorziening dient in principe 24 uur per dag beschikbaar te zijn:

- De uptime van de voorziening is 24 uur per dag, 7 dagen per week, 365/366 dagen per jaar (24x7x365);
- Een gegarandeerde beschikbaarheid van 99%. Waarbij het streven is om tot een hogere beschikbaarheid te komen;

- Voor een maand van 30 dagen mag de voorziening bij elkaar opgeteld niet langer dan 8 uur ongepland onbeschikbaar zijn;
- De voorziening mag niet vaker dan 4 keer per maand ongepland onbeschikbaar zijn;
- De voorziening mag op één dag niet langer dan 4 uur ongepland onbeschikbaar zijn.

UE 161.	De inschrijver bevestigd dat het geleverde product voldoet aan de eisen en uitgangspunten zoals in bovenstaande paragraaf 7.4 Beschikbaarheid zijn vermeld.

7.5. Uitbreidbaarheid

Een onderdeel van het beter laten werken van de voorziening is zorg te dragen voor het toevoegen en/of verbeteren van biometrische modaliteiten. Zo kan er een behoefte ontstaan om een nieuwe systematiek van biometrisch matchen toe te voegen (iris, tattoo o.a.). In dit geval voorziet de oplossing er in dat er “relatief eenvoudig” een standaardcomponent kan worden toegevoegd zonder dat dit grote consequenties heeft voor de werking van de gehele biometrievoorziening.

- De voorziening zal het inpassen in de voorziening van aanvullende biometrische modaliteiten ondersteunen. Dit kunnen ook modaliteiten van derden zijn.

Ten behoeve van het toe kunnen voegen van extra biometrische modaliteiten (ook van derden) koppelt de ABIS van de voorziening met biometrische modaliteiten op basis van een vooraf gedefinieerde standaard interface conform ANSI/NIST-ITL 1-2011 Update:2015 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (verder aangeduid als de NIST-standaard). Iedere biometrische modaliteit heeft zijn eigen dataopslag ten behoeve van de biometrische functies.

- De voorziening zal (extra) biometrische modaliteiten kunnen koppelen op basis van de NIST-standaard.

UE 162.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 7.5 Uitbreidbaarheid zijn vermeld.

7.6. Compartimentering

De informatievoorziening binnen de voorziening wordt georganiseerd in gescheiden compartimenten met gecontroleerde koppelvlakken.
Zo bevat de voorziening bijvoorbeeld gelaatsafbeeldingen referentiesets afkomstig uit de strafrechtelijke en de migratie (vreemdelingen) keten, welke op basis van wet- en regelgeving strikt gescheiden gehouden moeten worden.

- De biometriegegevens worden gescheiden opgeslagen van de overige persoonsgegevens. Door middel van een nummer kan identiteit van een biometrie gegeven worden gekoppeld. Deze koppeling wordt alleen gemaakt wanneer dit noodzakelijk is;
- Het is mogelijk om datasets samen te stellen aan de hand van de grondslag van de verwerking zodat gegevens rechtmatig verwerkt worden. Deze grondslag bevat geen / zo minimaal mogelijk details van de context waarvoor de gegevens verwerkt worden;
- Data van verschillende privacy regimes zal gescheiden kunnen worden opgeslagen in de biometrievoorziening en mogen alleen gekoppeld/benaderd worden als dit rechtmatig is.

UE 163.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf Compartimentering zijn vermeld.

Hoofdstuk 8. Ontwikkeling en Beheer (DevOps)

De voorziening moet onderhouden, beheerd en geëxploiteerd worden.
Eisen t.a.v. dit beheer is dat alle beheerprocessen (incidentmanagement, lifecycle management, probleem management, capaciteitsmanagement en servicemanagement) goed worden/ zijn ingericht en er afspraken zijn gemaakt over de manier waarop gemeten en gerapporteerd wordt. Dit wordt vastgelegd in een Service Level Agreement (SLA) en een Dossier Afspraken en Procedures (DAP). Hiervoor zal de opdrachtgever als onderdeel van dit Programma van Eisen (bijlage), voor elk van de documenten een basis aan leveren die in de periode direct na gunning, concreet zal worden ingevuld in samenwerking met de opdrachtnemer.

Met opmerkingen [RH(10]: Check op SLA en DAP

Het technische en functioneel beheer van het systeem wordt uitgevoerd volgens het DevOps (Scrum) principe door medewerkers van de opdrachtgever. Ze voeren dit beheer uit via de standaard werkplekken van de opdrachtgever. Omdat de opdrachtgever standaard werkt met het Thin Client principe is voor het uitvoeren van de beheertaak uitdrukkelijk niet nodig om de beschikking te hebben over een fat cliënt.

UE 164.	De inschrijver garandeert dat het beheertaken van de voorziening volledig met Thin Cliënts kan worden uitgevoerd

Systeembeheer wordt gezamenlijk(shared) ingericht samen met andere afdelingen van de opdrachtgever. Uitgangspunt is dat het shared beheer op basis van strikte functie scheidingen wordt ingericht en op basis van het 4 ogen principe wordt uitgevoerd.

De voorziening dient ook onderhouden te worden. Het aanpassen van de voorziening behoort tot het werkterrein van het DevOps team en/of Inschrijver. Dit zal zonder onderbreking van de service plaats vinden met als uitzondering van de beschreven onderbrekingen in de DAP en SLA.

8.1. Gebruikersbeheer

Voor wat betreft gebruikersbeheer onderkennen;

- Gebruikers
  - De nieuwe voorziening zal gebruikersnaam, natuurlijke voornaam, achternaam, voorvoegsel en e-mail adres kunnen registreren
  - De gebruikersnaam zal gelijk kunnen zijn aan die gebruikt wordt in de kantoor infrastructuur van de opdrachtgever (Microsoft Windows gebaseerd)
  - Een gebruiker kan tot één of meerdere groepen behoren en één of meerdere rollen hebben
- Groepen
  - Een groep is een verzameling van één of meer gebruikers
  - Groepen zijn bedoeld om gebruikers binnen de nieuwe voorziening te structuren naar organisatie en of locatie
  - Een groep zal in de nieuwe voorziening bruikbaar zijn om alle gebruikers die tot die groep behoren, automatisch of handmatig een (e-mail) bericht te versturen vanuit de voorziening
- Rollen
  - Een rol is een verzameling van één of meerdere gebruikers
  - Rollen zijn bedoeld om gebruikers binnen de nieuwe voorziening te structureren naar functie binnen de werkprocessen van de opdrachtgever
  - Een rol zal in de nieuwe voorziening bruikbaar zijn om alle gebruikers die deze specifieke rol hebben automatisch of handmatig een (e-mail) bericht te versturen vanuit de voorziening

Voor wat betreft het beheer van de gebruikers, groepen en rollen kennen we de volgende bewerkingen;

- Aanmaken gebruikers, rollen en groepen;
- Onderhouden gebruikers, rollen en groepen;
- Blokkeren van gebruikers, rollen en groepen;
- Verwijderen van gebruikers, rollen en groepen.

Voor gebruikersbeheer wordt door de opdrachtgever gebruikt gemaakt van een Identity Access Management architectuur (IAM) met bijhorend systeem en systeem koppelingen naar applicatie en database servers. Gebruikers van de infrastructuur worden aangemaakt in het IAM en daarin geautoriseerd voor de voorziening. Er vindt in IAM een registratie plaats van gebruikersgegevens, groeps- en rol lidmaatschappen zoals eerder in dit hoofdstuk aangegeven.

UE 165.	De voorziening zal doormiddel van een automatische koppeling met IAM, in staat zijn het aanmaken, onderhouden, blokkeren en verwijderen van gebruikers vanuit het IAM systeem te ondersteunen en binnen de voorziening zelf, automatisch de juiste bijhorende bewerkingen op de interne autorisaties door te voeren.

UE 166.	De voorziening zal doormiddel van een automatische koppeling met IAM, in staat zijn het aanmaken, onderhouden, blokkeren en verwijderen van rollen en/of groepen vanuit het IAM systeem te ondersteunen en binnen de voorziening zelf, automatisch de juiste bijhorende bewerkingen op de interne autorisaties door te voeren. OF De voorziening zal functionaliteit bieden aan de beheerders om binnen de voorziening het aanmaken, onderhouden, blokkeren en verwijderen van rollen en/of groepen uit te voeren en binnen de voorziening automatisch de juiste bijhorende bewerkingen op de interne autorisaties door te voeren.

Zoals aangegeven wordt in het hoofdstuk over techniek zal de toegang tot de voorziening Single Sign-on moeten zijn. De gebruiker logt in op de netwerkinfrastructuur van de opdrachtgever en afhankelijk van de registraties in het Identity Access Management systeem verleent de voorziening algemene toegang tot de voorziening.

Met opmerkingen [MdH11]: Dit kan weg, SSO is geen beheer ding en al bij functie genoemd en in de techniek uitgewerkt.

Indien geen SSO (koppeling IAM) zal het beheer de hierboven beschreven handelingen in de voorziening zelf moet uitvoeren.

UE 167.	De algemene toegang zal de voorziening regelen op basis van de registratie van een gebruiker in het Identity Access management systeem. Bij de juiste registratie in het IAM wordt automatisch toegang tot de voorziening gegeven.

8.2. Beheer autorisatie programma functionaliteit

Om de in dit document genoemde scheiding van verantwoordelijkheden en uitvoeren van taken in werkprocessen te ondersteunen zal de voorziening een toegangs- en gebruiksautorisatiesysteem hebben die toegang en gebruik van de in de voorziening aanwezige functies en processen (workflows) regelt. Deze autorisatie zal hoofdzakelijk plaatsvinden op rol en/of groepslidmaatschap. De voorziening zal functionaliteit hebben waarmee dit beheer uitgevoerd kan worden.

UE 168.	De voorziening zal functionaliteit bieden aan de beheerders en gebruikers om autorisatie regelen op programma functies en transacties, enkelvoudig of als onderdeel van een workflow proces. Tevens zal er functionaliteit zijn waarmee workflow processen als geheel kunnen worden geautoriseerd.

UE 169.	De voorziening moet de functioneel beheerder de mogelijkheid bieden om de functionele werking van de voorziening te kunnen beheren. Hieronder wordt minimaal verstaan: • Genereren van rapportages m.b.t. autorisatie op de voorziening; • Genereren van rapportages m.b.t. gebruik van de voorziening; • Beheer van documenten, rapportages en analyses. • Een voor mensen leesbare inzage op logging t.b.v. analyse van gebruik en incidenten/problemen

UE 170.	De voorziening zal automatisch alle beheerhandelingen vastleggen in een logboek.

De voorziening zal diverse systeemfuncties hebben waarmee de gebruikersopdrachten in het systeem worden afgehandeld. Denk aan bericht communicatie van en naar andere systemen die via een interface

synchroon of asynchroon gekoppeld zijn maar ook aan verwerkingsrijen voor zoekopdrachten en de beschikbaarheid van systeem functies. Verder is het interessant wat de actuele systeembelasting is en hoe zich dat vertaald naar de gebruiker. Hierbij wordt bijvoorbeeld gedacht aan de actuele verwerkingstijden die de verschillende zoekopdrachten hebben gekost.
Voor deze en mogelijk nog andere nader te bepalen zaken, zal er een faciliteit zijn (monitor applicatie) waarmee deze dynamisch, real-time gevolgd kunnen worden in het actuele operationele systeem. Tevens zal het hierbij mogelijk zijn om bepaalde grenswaarden in te stellen ten behoeve van alarmeringen. De alarmeringen zijn visueel via de faciliteit zichtbaar maar kunnen tevens via te configureren e-mail en andere elektronische middelen zoals tekst berichten verspreid worden.

UE 171.	De voorziening zal functionaliteit bieden waarmee verwerkingsprocessen van de voorziening dynamisch gevolgd kunnen worden. Deze functionaliteit signaleert afwijkingen in de verwerkingsprocessen van de voorziening. (Signaleringen zullen dynamisch en real-time via beeldscherm een dashboard), e-mail en/of beeldscherm bericht worden gecommuniceerd. Afwijkingen zullen ook vastgelegd worden in een logboek met een duidelijk voor mensen leesbare teksten zodat die bijvoorbeeld bruikbaar zijn in managementrapportages. Of een bepaalde functionaliteit afwijkend, kan worden ingesteld via te configureren parameters in de vorm van drempel waarden. Aanbieder geeft aan of er standaard, te configureren faciliteiten aanwezig zijn of dat er een mogelijkheid is om dit op eenvoudige wijze te realiseren op basis van een aanwezige standaard voorziening binnen de voorziening.

Met opmerkingen [FvL12]: De monitor afdeling van de dienst ICT zal hierop ook moeten kunnen aansluiten en 7 * 24 uurs monitoring moeten kunnen uitvoeren. Of en wat hiervoor aanvullend nodig weet ik niet.

Met opmerkingen [CR(13]: Even opletten dat in de soc tabel bij de inschrijving een veld is waar deze info bij een eis kan worden verstrekt.

UE 172.	De inschrijver zal voor de operationele fase voor wat betreft release planning en bug fixing als ook de communicatie rondom dit beheer, nadere afspraken maken met de opdrachtgever. Dit wordt geformaliseerd in het overeenkomen van de SLA en DAP.

Met opmerkingen [HH14]: Ik zou zeggen in de periode vanaf de gunning eenmaal in de x weken. Het releasebeleid is gerelateerd aan het LCM van het platform dus moet daarmee worden geïntegreerd.

Met opmerkingen [KIL15]: Er is een verschil tussen operationeel en realisatie. Tijdens de realisatie fase gelden in de regel andere afspraken en een apart communicatie protocol voor dit soort zaken → project management.
Wat mij betreft er gewoon uit… wordt door SLA en DAP afgedekt (toch?)

Met opmerkingen [KIL16]: Er is een verschil tussen operationeel en realisatie. Tijdens de realisatie fase gelden in de regel andere afspraken en een apart communicatie protocol voor dit soort zaken → project management.

8.3. DevOps

Binnen de Politie IV organisatie werken we volgens de DevOps werkwijze die weinig afwijkt van de Scrum methode van werken. DevOps is een raamwerk voor het ontwikkelen, onderhouden en ondersteunen van complexe producten. Dit kan zijn eigenbouw zijn maar ook customisable-off-the-shellf installaties. Het raamwerk bestaat uit DevOps rollen, gebeurtenissen, artefacten en de regels die deze zaken samenbrengen zoals die algemeen in de markt bekend zijn. Binnen DevOps adresseren mensen complexe, adaptieve problemen en leveren tegelijkertijd op een productieve en creatieve wijze producten van de hoogst mogelijk waarde voor de organisatie.

Een DevOps team bestaat uit; een product owner, scrum master en ontwikkelaars waarbij de maximale bemensing uit negen personen bestaat (exclusief scrum master en product owner). Verder worden de normale (scrum) elementen als dagelijkse stand-ups, sprint planning, sprint review en retrospective gehanteerd.

Met opmerkingen [FvL17]: Een scrumteam van 11 personen is erg groot. Ik zou dit ergens tussen de 6 en 8 personen laten zijn.

In de productie fase zullen afhankelijk van de verdeling van taken tussen de gebruiksorganisatie en de meer technische mensen, één of meerdere DevOps teams worden ingericht. Initieel zal de productiefase gestart worden met één team.

Zoals aangegeven zullen na in productie name van de nieuwe voorziening ondersteuningsprocessen actief zijn. De aansluiting van de opdrachtnemer op deze processen zal vastgelegd worden in een nader uit te werken SLA en DAP en waarvan de basis requirements weergegeven zijn in de templates van deze documenten in de bijlage van dit document. Doel is uiteraard de optimale ondersteuning van de gebruikersorganisatie binnen de gestelde service levels zoals die zijn aangegeven eerder in dit document.

UE 173.	De inschrijver zal aansluiten op en meewerken in de ondersteuningsprocessen van het DevOps team van de opdrachtgever zoals die in basis worden beschreven en na gunning, in overleg vastgelegde SLA en DAP.

Met opmerkingen [RH(18]: check

UE 174.	De inschrijver zal duidelijk aangeven welke ondersteuningsprocessen ze hanteer, welke beschikbare servicelevels er geboden worden en welke voorwaarden hieraan voorbonden worden. De aanbieder zal daarbij duidelijk aangeven hoe het communicatie proces rondom meldingen van en naar haar organisatie verloopt.

Met opmerkingen [CR(19]: Onduidelijk wat nut/noodzaak is van deze eis.

UE 175.	De inschrijver geeft aan of en welke tools en/of middelen deze beschikbaar heeft voor de opdrachtgever voor het beheer van en communicatie over, uitstaande tickets bij de inschrijver. Denk hierbij aan een klant portaal waarmee uitstaande vragen, incidenten enz. gevolgd kunnen worden voor wat betreft het oppakken, verwerken enz. door de inschrijver. Indien de inschrijver een dergelijke faciliteit biedt, zal de inschrijver aangeven wat de mogelijkheden van deze faciliteiten zijn.

8.3.1. DevOps en realisatie

Voor de realisatie zal met 2 DevOps teams worden gewerkt. Eén die zich bezig houdt met de nieuwe voorziening (centrale team) en één team dat zich specifiek met migratie van de data bezig houdt.

Zie Hoofdstuk 10 voor de eis behorende bij de implementatie.

Centrale team

In het centrale team zullen de experts van de inschrijver naast de installatie en inrichting zich richten op het wegwijs maken en opleiden van de andere DevOps teamleden in het team zoals in dit programma van eisen is aangegeven. Het team houdt zich primair bezig met de realisatie van alle functionaliteit zoals beschreven in dit document. Dit team zal in totaal maximaal bestaan uit 9 personen (exclusief Scrummaster en product owner). Na de in productie name zal dit team blijven bestaan en de DevOps taak uitvoeren in de operationele fase.

Met opmerkingen [FvL20]: Zie eerdere opmerking hierover.

Migratie team

Het migratie team zal zich specifiek richten op de migratie van de data naar het nieuwe systeem volgens een door de Politie aangegeven strategie, methode en techniek. De leden van de opdrachtgever van dit team zijn niet exclusief voor het team en kunnen ook zitting hebben in het centrale team. Het migratie team heeft echter een aparte en duidelijke focus om een zo effectief mogelijke data migratie op te zetten met een zo minimaal mogelijke impact voor de lopende business. Dit team zal in totaal bestaan uit ongeveer 5 personen. Na in productie name zal dit team worden ontbonden. Mogelijk dat interne medewerkers van de opdrachtgever deel gaan nemen aan het centrale team wat wel blijft bestaan.

Met opmerkingen [FvL21]: Productowner, scrummaster, informatieanalist, ontwikkelaar en tester. Dat zijn er 5. Dat is erg mager. De ontwikkelaar en tester zou ik er twee van opnemen,

Inzet van de opdrachtnemer vanaf gunning tot aan de in productie name

De opdrachtnemer zal in beide teams deelnemen gedurende de realisatie fase van de nieuwe Biometrie voorziening

De taken voor de experts van de opdrachtnemer in het centrale team;

- Begeleiden en opleiden van de DevOps teamleden van de opdrachtgever (zie hoofdstuk opleidingen)
- Mede realiseren van oplossingen voor de in dit document genoemde functionaliteit

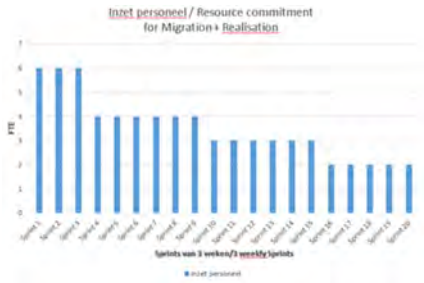
De taken voor de experts van de opdrachtnemer in het migratie team;

- Het realiseren van de data migratie zoals genoemd in dit document bij de paragraaf migratie, hoofdstuk implementatie

De (aantoonbare) vereisten voor wat betreft de door de opdrachtnemer in te zetten experts zijn;

- In vast dienstverband bij de opdrachtnemer
- Meerjarige ervaring met Biometrische systemen en implementaties hiervan
- Minimaal één jaar werk ervaring bij de opdrachtnemer
- Senior level medewerkers
- Voldoen aan de voorwaarden voor in te zetten extern personeel zoals gesteld in hoofdstuk 5

Bij het schrijven van dit document wordt er uitgegaan van een gemiddelde inzet van minimaal 3,5 FTE van de opdrachtnemer over beide teams. De volgende afbeelding geeft een beeld van hoe de verdeling er mogelijk uit kan zien. Na gunning zullen de opdrachtnemer en opdrachtgever een nadere invulling hieraan kunnen geven.



Bij de start van de realisatie zal de opdrachtnemer rekening dienen te houden met een grotere inzet van haar personeel dus met de inzet van meer mensen. In het verloop van de realisatie kan in overleg met de opdrachtgever de personele bezetting van haar mensen afgebouwd worden indien de situatie volgens de opdrachtgever dit toelaat.

Op dit moment gaan we uit van een inzet van 20 sprints over een periode van 15 maanden.

Met nadruk wijzen we de inschrijver erop dat er voor wat betreft het inzetten en plannen van personeel, rekening gehouden moet zijn met de veiligheidseisen voor personeel (zie hoofdstuk 5) en dat het doen van een veiligheidsonderzoek een langere periode van tijd in beslag neemt. Het niet hebben van voldoende door de Politie gescreend personeel zou kunnen resulteren in het niet na kunnen komen van de minimaal gewenste invulling van de opdracht door de opdrachtnemer. Denk hierbij aan het opvangen van ziekte of het niet voldoende functioneren van een persoon in het DevOps team.

UE 176.	De inschrijver zal aangeven hoe ze invulling gaat geven aan de DevOps team deelname, gegeven de in deze paragraaf gegeven beschrijving en rekening houdend met zaken beschreven in het hoofdstuk Implementatie. De inschrijver zal daarbij toelichten hoe eventuele bezettingsproblemen van haar personeel in het project, worden voorkomen.

8.3.2. DevOps en nazorg periode

Na in productie name door de opdrachtgever zal er een periode van nazorg zijn. In deze nazorg periode is er een verhoogd niveau van ondersteuning nodig van de opdrachtnemer om het DevOps te helpen bij het optreden van specifiek operationele problemen.

UE 177.	De inschrijver zal na de in productie name door de opdrachtgever voor een periode van 2 maanden, één van de senior experts die deelgenomen heeft in één van de realisatie teams, laten deelnemen in het operationele DevOps team van de opdrachtgever.

Met opmerkingen [FvL22]: Als je 24-uurs dekking wil is een geen optie.

8.3.3. DevOps en productie

Uiteindelijke doel van alle inspanningen binnen deze aanbesteding op beheergebied is het mogelijk maken voor het DevOps team van de Politie om, geheel zelfstandig en zonder tussenkomst van Inschrijver:

- De voorziening in hoge mate zelf aan te passen door configuratie en/of faciliteiten om door middel van programmering, functionaliteit van de voorziening aan te sturen. Denk hierbij aan de aansturing van de voorziening via RPC API technology.
- Door middel van openstandaarden zelf systeemkoppelingen met andere systemen te realiseren;
- Direct maar ook via tooling, dynamisch de werking van het operationele systeem te controleren op diverse functionaliteiten (technisch);

- Management rapportages samen te stellen e/o te ontwerpen en te laten genereren door de voorziening of de mogelijkheid cijfers voor management rapportages via een geautomatiseerde toegang zoals een RPC API of via geprogrammeerde database access uit de voorziening te halen;
- Het functioneren of het niet functioneren van programma onderdelen van de nieuwe voorziening te onderzoeken;
- Correcte en bruikbare probleem analyses en probleemrapportages te maken voor Inschrijver zodat deze problemen sneller kan oppakken;
- De dagelijks operationele functionele en technische bedieningen en beheer uit te voeren op de nieuwe voorziening;
- Kleinere, door Inschrijver opgeleverde systeem updates zelfstandig uit te voeren.

Met opmerkingen [FvL23]: Waarom niet alle update? Zo niet dan definieren wat klein is. Als de updates en de systeemdocumentatie van een goede kwaliteit zijn, dus duidelijk, volledig, dan is het uitvoeren van iedere update zonder hulp van inschrijver mogelijk

Van belang is dat de DevOps teamleden kennis hebben van alle nodige technische achtergrond, mechanismes en processen die horen bij bovengenoemde punten. De opdrachtnemer zal mede zorgdragen dat het DevOps team van de opdrachtgever in staat zal zijn zelf alle genoemde zaken, zelfstandig uit te kunnen voeren.

UE 178.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in dit hoofdstuk zijn vermeld.

8.4. Beheer koppelingen

De voorziening zal diverse systeem koppelingen hebben (zie hoofdstuk techniek). Over deze koppelingen worden diverse berichten uitgewisseld met andere interne en externe systemen. De berichten zijn onderdeel van simpele en meer complexere uitwisselingsprotocollen. Voor beheer is het belangrijk om operationeel inzicht te hebben in de uitwisseling en afhandelingen van die berichten volgens het afgesproken en vastgelegd protocol.

UE 179.	De voorziening zal functionaliteit hebben waarmee de operationele werking van de koppeling gevolgd en beheerd kunnen worden. Dit zal minimaal bestaan uit de mogelijkheid om dit via RPC API's uit te voeren. Inschrijver dient aan te geven of, en in welke mate de voorziening dit standaard ondersteunt.
UE 180.	De voorziening zal functionaliteit hebben waarmee berichten verwerking van en naar andere interne en externe systemen beheerd en gevolgd kunnen worden. Via deze functionaliteit is het mogelijk om real-time alle ingekomen en uitgestuurde berichten in te zien. Dit zal minimaal bestaan uit de mogelijkheid om dit via RPC API's te realiseren. Inschrijver dient aan te geven of, en in welke mate de voorziening dit standaard ondersteunt.
~~W 13~~W 1	[Hoog] De voorziening zal functionaliteit hebben waarmee een berichten uitwisselingssessie (van meerdere berichten) van en naar andere interne en externe systemen beheerd en gevolgd kunnen worden. Hierbij controleert het systeem of de set berichten behorende bij één van de te configureren uitwisselingsprotocollen compleet is In hoeverre voorziet uw oplossing hier in? Beoordeling vindt plaats op basis van de mate waarin uw oplossing in bovenstaand punt voorziet.

Met opmerkingen [CR(24]: Is dit een eis of wens?

Hoofdstuk 9. Technisch

De voorziening voor biometrie zal draaien op infrastructuur die door de beheerder wordt geleverd. De beheerder heeft bij verschillende leveranciers voorzieningen ingekocht:

- Generieke infrastructuur die alles behalve Oracle capaciteit levert op basis van Infrastructure as a service (IaaS) of op basis van Platform as a Service (PaaS). PaaS heeft de voorkeur, omdat de externe leverancier van het platform dan zelf verantwoordelijk is voor de inrichting van de platforms. De generieke infrastructuur kan bijvoorbeeld JBoss of PostgreSQL als een service leveren. In het geval van IaaS gaat het om een kale virtual machine. Deze wordt toegepast als de betreffende applicatie een platform nodig heeft dat niet tot de standaard-diensten van het platform behoort. Zie ook paragraaf 9.11.
  De voorziening wordt beheerd door de leverancier als een on-premises private cloud omgeving.
- Een voorziening die Oracle database- en middleware capaciteit biedt op basis van Platform as a service (PaaS). Ook in dit geval wordt de voorziening door de externe leverancier beheerd als een on-premises private cloud omgeving.

Nieuwe toepassingen mogen alleen op de bovengenoemde voorzieningen worden ingericht.
Als een toepassing gebruik maakt van zowel niet-Oracle als van Oracle producten zal de hosting deels plaatsvinden op de generieke infrastructuur en deels op het Oracle platform voor de betreffende onderdelen.
Voor het opslaan van foto's, films en andere multimedia-bestanden wordt een speciale multimedia-server ingericht die is geoptimaliseerd voor de opslag van grote bestanden en grote hoeveelheden kleine bestanden. Logging wordt geregeld via een centrale logging server op basis van graylog of elk. Het ABIS systeem moet gebruik maken van deze services.

De politie is bezig met het opzetten van kernregister waarmee uitvoering word gegeven aan het architectuurprincipe "eenmalig registreren, meervoudig gebruik". Praktisch betekend dat kerngegevens niet in de verschillende applicaties word opgeslagen, bewerkt en bevraagd, maar dat de applicaties daarvoor gebruik maken van een kernregister (middels een koppeling) Voor de biometrie-voorziening gaat het dan specifiek om de biografische gegevens, deze moeten hun plaats krijgen in een Kernregister Personen (KRP) Op termijn zouden hier ook de signalementskenmerken als een persoonskenmerk hun plek moeten krijgen (en evt. ook de gelaatsfoto's en vingerafdrukken, etc.)
Omdat het KRP nog in ontwikkeling is, zal de biometrievoorziening alleen voorzien in het kunnen koppelen met het KRP d.m.v. een unieke identifier. Dat wil zeggen, we willen een persoon in de biometrie-voorziening kunnen koppelen met een persoon in het KRP middels een unieke identifier (ID)

Verwerving

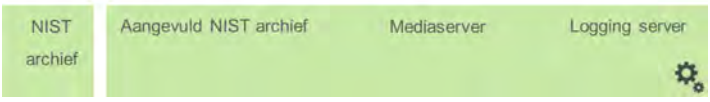


Diagram 9.1

In bovenstaande diagram wordt aangegeven binnen het blauwe vlak wat de componenten zijn die de politie wil verwerven met deze aanbesteding. Het gaat om de drie grijze blokken binnen het blauwe vlak:

- Een applicatie met bijbehorende workflow
- Een systeem voor vinger- en handafdrukken
- Een systeem voor gelaatsherkenning

De voorzieningen in de groene balk worden ingericht binnen de infrastructuur van de politie om voor alle toepassingen te worden ingezet (media- en loggingserver, Nist archief). Hiermee wordt ontkoppeling van gegevens en applicaties bereikt en kunnen gegevens gemakkelijk aan andere applicaties ter beschikking worden gesteld. Mocht de toegang tot de logging server (tijdelijk) geblokkeerd zijn, dan moeten de logging gegevens worden gebufferd tot deze weer bereikbaar is.

Uitbreidingsmogelijkheden
Het ABIS dat wordt verworven moet passen in een raamwerk waarbij uitbreiding met een extern workflow systeem of een extra biometrische component mogelijk is. Hiervoor is het nodig dat de politie inzicht heeft in de koppelvlakken tussen de verschillende componenten die samen het ABIS vormen.
Het gaat dan over:

- Het koppelvlak tussen het workflow systeem en de UI/de core applicatie (1),
- Een koppelvlak waarmee de UI/core toepassing als service is aan te roepen (2),
- Het koppelvlak waarmee de biometrische componenten, zoals de systemen voor vinger- en handafdrukken en het systeem voor gelaatsherkenning, aan te roepen als service (3).

Het is mogelijk dat de politie de koppelvlakken via een service-bus laat lopen, in de tekening hieronder ‘Motorblok’ genoemd. In paragraaf 9.3 komen we hier op terug.

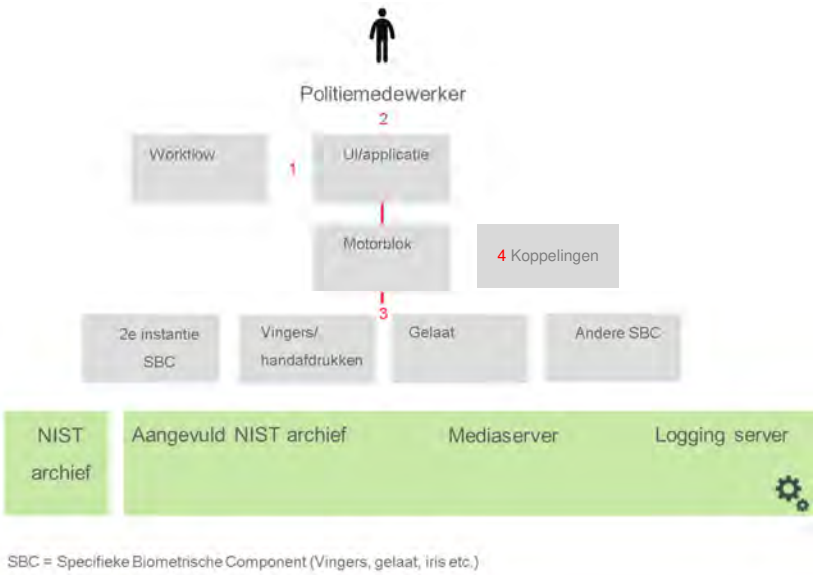


Diagram 9.2

Met opmerkingen [RH(25]: Koppelingen als nr 4 naast motorblok toevoegen?

Oracle

De Politie heeft een voorkeur voor applicaties die geen gebruik maken van Oracle middleware- en/of database producten. Dit heeft te maken met de licentie- en onderhoudskosten en met het schaalvoordeel dat de Generieke Infrastructuur biedt ten opzichte van de specifieke Oracle infrastructuur. In paragraaf 9.10 wordt een opgave gevraagd van alle benodigde software en licenties. Vanaf 2020 zal het gebruik van Oracle worden afgebouwd. In paragraaf 9.10 wordt ook gevraagd om een plan waarbij het eventuele gebruik van Oracle producten wordt afgebouwd.

Open source
De CIO van de Nationale Politie heeft op 26 juni 2016 de 'visie op open source' vastgesteld. Deze visie kan als volgt worden samengevat:
De Politie geeft de voorkeur aan de toepassing van open source oplossingen in haar informatievoorziening. Bij gebleken geschiktheid wordt gebruik gemaakt van open source oplossingen voor de realisatie van nieuwe voorzieningen en diensten. Bestaande voorzieningen worden aangepast om open source oplossingen te gebruiken als hiervoor een positieve (functionele- en/of financiële) business case is.

De Politie zal mede daarom naast Oracle ook voor andere door de opdrachtnemer toegepaste producten rekening houden met noodzakelijke licentiekosten. De Politie wil (in paragraaf 9.11) een opgave van alle andere producten, die benodigd zijn voor het hosten van de biometrische applicaties. Deze zullen weliswaar op de generieke infrastructuur worden gehost, maar verhogen toch de beheerlasten.

Bovengenoemde voorzieningen worden ingezet voor het ontwikkeling, opleiding en productie. De IaaS- en PaaS voorzieningen zijn zodanig gestandaardiseerd dat geen barrières worden opgeworpen om een applicatie te deployen in de complete Ontwikkel-, Test-, Acceptatie en Productie-straat (OTAP). De generieke infrastructuur is voorzien van een selfservice portaal waarmee gestandaardiseerde IaaS- en PaaS instanties kunnen worden aangevraagd of verwijderd.

Genoemde voorzieningen worden, met alle andere infrastructuur (in het schema hieronder archief), aangesloten op een intern netwerk. In dit netwerk zijn voorzieningen aanwezig als Active Directory. Voor de biometrievoorziening is de aangewezen landingsplaats het productie Windows-domein politie.local.
Voor ontwikkeling, test en acceptatie is een tweede domein ingericht: ota.local. Alle Identity- and Access management (IAM) vindt plaats tegen deze domeinen.

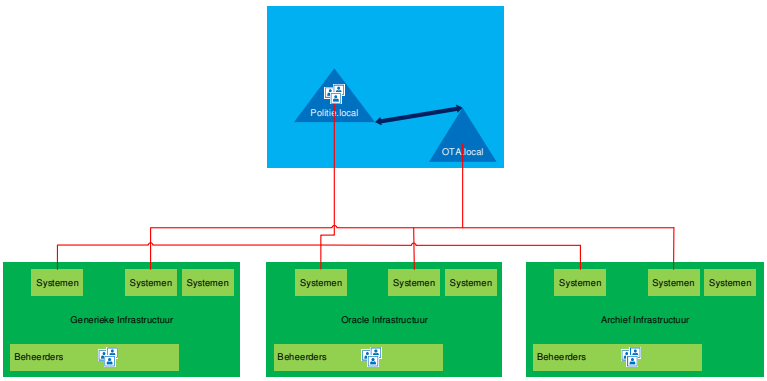


Diagram 9.3

De externe partijen die de platforms leveren zijn verantwoordelijk voor het life-cycle-management. Dat betekent dat de gebruikers of afnemers van de platformen regelmatig hun toepassingen geschikt moeten maken en testen voor gebruik op nieuwe versies van door de platformen geleverde services. Het is van belang dat de leveranciers van applicaties hun toepassingen onafhankelijk maken van de onderliggende platformen.

Doelstelling is dat een upgrade van het platform geen noodzakelijke wijzigingen op de applicatie noodzakelijk maken. In het geval dat bij een bepaalde update van het platform toch wijzigingen noodzakelijk zijn, is de leverancier van deze applicatie verantwoordelijk voor deze wijzigingen. In het DAP worden hierover afspraken vastgelegd.

9.1. Beveiliging

De voorziening wordt gebruikt voor verschillende bedrijfsprocessen. De verwerking van de biometrische persoonsgegevens dient te voldoen aan wet- en regelgeving in ieder geval aan onderstaande algemene wetten voor verwerking van persoonsgegevens:

- WPG: de wet Politiegegevens (en de opvolger hiervan aan de hand de Richtlijn (EU) 2016/680);
- AVG: algemene verordening gegevensbescherming internationaal aangeduid als general data protection regulation (GDPR), verordening (EU) 2016/679).

Met opmaak: Standaard, Geen opsommingstekens of nummering

De voorziening is in staat om te voldoen aan wet- en regelgeving:

- Het is te herleiden voor welk doel en door wie gegevens verwerkt zijn;
- De rechtmatigheid van de verwerking is controleerbaar;
- De gegevens worden bewaard zolang deze noodzakelijk zijn en deze gegevens kunnen geschoond, geanonimiseerd, voor verdere bewerking worden beperkt en/of gearchiveerd worden;
- Grondbeginselen voor privacy en security by design zijn toegepast bij de ontwikkeling van de voorziening:
  - Proactief en preventief, risico´s worden op voorhand aangepakt;
  - Privacy is de standaard: gegevens worden doelgericht verwerkt en worden zo minimaal mogelijk verzameld en opgeslagen en gebruikt;
  - Privacy is ingebed in het ontwerp: gedurende de ontwikkeling wordt rekening gehouden met privacy, wordt er gewerkt met standaarden en worden risico´s geanalyseerd en geminimaliseerd;
  - Volledige functionaliteit: privacy is geen doel op zich maar onderdeel van de algemene doelen;
  - End-to-end beveiliging en lifecycle beveiliging: gegevens zijn gedurende de gehele levensduur beveiligd en er wordt gebruik gemaakt van veilige protocollen, methoden en technieken;
  - Zichtbaar en transparant: er is inzicht op welke wijze gegevens verwerkt worden;
  - Respecteer de privacy van de betrokkene: door de gegevens rechtmatig en nauwkeurig te verwerken door geautoriseerde personen.
- De biometrische gegevens zijn gescheiden opgeslagen van de overige (persoons)gegevens en de relatie wordt alleen gelegd indien dit noodzakelijk (zie **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**);
- Wijzigingen in de autorisatiestructuur kunnen door geautoriseerde beheerders van de Politie worden aangebracht;
- Rechtstreekse toegang vanuit de ~~toepassing~~voorziening tot bestanden is niet toegestaan. Toegang is mogelijk vanuit het framework in de applicatieserver;
- ~~Remote access door Inschrijver tot de beheeromgeving wordt niet toegestaan.~~;

Met opmerkingen [MdH26]: Ik heb hier een link naar de compartimentering in H7

UE 181.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 9.1 Beveiliging zijn vermeld.

Met opmaak: Standaard, Geen opsommingstekens of nummering

~~9.1.1.~~9.2. ~~Autorisaties~~Identity & Access Management

Met opmerkingen [MdH27]: Ik heb de aansluitvoorwaarde tekst uit de blauwdruk IAM aangehouden. Hier wordt gesproken van applicaties in plaats van voorziening. Overweeg dit aan te passen in voorziening ivm consequent taalgebruik.

Met opmaak: Kop 2;Paragraaf;k2;Subkop;BP Heading 2;Tempo Heading 2;2scr;h2;Reset numbering;Bijlage;paragraaf;Numbered - 2;h 3;Chapter Title;052;Annex Kop 2;Vet + inhoudsopg-niveau 2;Paragraaf (1.1);ips_paragraaf;Paragrf 2;Bold 14;L2;Kapitel;Header 2

De Politie realiseert een Identity & Access Management (IAM) systeem. IAM is een omgeving waarbij er logisch centraal identiteitsgegevens worden beheerd en er één logische centrale toegangscontrole is. De biometrievoorziening zal aangesloten worden op het IAM-systeem. De hieronder genoemde aansluitvoorwaarden zijn van toepassing voor zowel COTS-producten als maatwerkproducten. Indien er niet voldaan wordt aan de aansluitvoorwaarden dan wordt er niet gekoppeld aan het IAM-systeem. De

applicatie wordt dan niet gekoppeld waardoor een gebruiker op de applicatie apart moet inloggen (geen SSO).

1. De applicatie & bronsystemen koppelen eenzijdig (single point of data exchange) aan de LDAP directory tbv authenticatie en autorisatie. Koppeling is op basis van open standaarden[1], standaard protocollen en uitwisselingsmechanismes, zoals LDAP of een op XML gebaseerde afspraak.
2. De applicatie koppelt aan één ID-repository welke gevoed wordt door het IAM-systeem.
3. Multi(klant)domeinfunctionaliteit wordt alleen gefaciliteerd door IAM. In de IAM kunnen ook gegevens worden vastgelegd m.b.t. gebruikers vanuit een ander klantomgeving om te federeren
4. Applicaties maken eenduidig gebruik van de centrale identity gegevensset (LDAP veldnamen) welke vanuit IAM (centrale ID-repository) wordt aangeboden.
5. Op technisch niveau wordt voor de applicaties SAML[2] en/of WS*[3] en/of Kerberos gebruikt, waarbij een PKI certificaat als identificatie wordt gebruikt.
6. Applicaties krijgen alleen leesrechten op de centrale ID gegevensset. Mutaties van deze gegevens worden alleen gedaan vanuit de IAM (beheer)tooling. Self-service voor gebruikersbeheer is vanuit de applicatie niet mogelijk, dit wordt gefaciliteerd door het IAM-systeem.
7. Bestaande en/of lokale ID-repository, voor applicatie- en functioneel beheer, moeten zijn opgenomen in centrale ID-repository.
8. Autorisaties zijn op basis van RBAC waarbij de rollen in de applicatie (bij voorkeur 1/n op 1) matchen met op de rollen in IAM.
9. Logging betreffende authenticatie en autorisatie van de OTAP omgevingen worden verwerkt in de centrale logging en auditing omgeving.

Java gebaseerde applicaties

Omdat er binnen de politieorganisatie grotendeels gebruik wordt gemaakt van Java gebaseerde applicaties gelden hiervoor Java aanvullende aansluitvoorwaarden.

1. Een Java Applicatie dient voor de implementatie van authenticatie en autorisatie gebruik te maken van de Java EE Security functionaliteit. Hierdoor is binnen de Java applicatie de mapping tussen de rollen in de applicatie en de rollen in de Identity Repository te configureren in een deployment descriptor (XML). In de applicatie worden de Authentication (bijv. Kerberos) en Assertion (SPNEGO token[4]) providers geconfigureerd.

W 16	[Hoog] De voorziening voldoet aan de bovengenoemde aansluitvoorwaarden en kan gekoppeld worden aan het IAM-systeem.

~~Toegang tot de voorziening is geregeld door middel van autorisaties. Hierbij moet het mogelijk zijn om autorisaties op verschillende niveaus per groep toe te kennen, waarbij een groep lid kan zijn van een bovenliggende groep. Afhankelijk van de autorisatie is bepaalde informatie voor een medewerker wel of niet zichtbaar in de voorziening of kan bepaalde informatie wel of niet worden ingevoerd of gemuteerd.~~

~~Aan gebruikers wordt toegang tot de informatievoorziening verleend op basis van noodzaak voor de uitvoering van de hen opgedragen werkzaamheden zoals beschreven in hoofdstuk 6.~~

~~Waarbij geldt:~~

- ~~Single sign-on (iedere gebruiker logt slechts één keer in);~~
- ~~Het instellen van alle autorisaties moet in de aangeboden oplossing door de beheerder kunnen worden gedaan. Zie hoofdstuk 8 Beheer;~~
- ~~Wijzigingen in de autorisatiestructuur kunnen door de beheerders van de Politie worden aangebracht;~~
- ~~Rechtstreekse toegang vanuit de toepassing tot bestanden is niet toegestaan. Toegang is mogelijk vanuit het framework in de applicatieserver;~~
- ~~Remote access door Inschrijver tot de beheeromgeving wordt niet toegestaan;~~

[1] Open standaarden zie URL: http://www.forumstandaardisatie.nl/open-standaarden
[2] http://nl.wikipedia.org/wiki/Security_Assertion_Markup_Language
[3] http://en.wikipedia.org/wiki/WS-Security
[4] http://en.wikipedia.org/wiki/SPNEGO

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

Met opmaak: Lijstalinea, Meerdere niveaus + Niveau: 7 + Nummeringstijl: 1, 2, 3, … + Beginnen bij: 1 + Uitlijning: Links + Uitgelijnd op: 0 cm + Inspringen op: 1,5 cm

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

heeft opmaak toegepast: Tekstkleur: Zwart

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

heeft opmaak toegepast: Tekstkleur: Zwart

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

Met opmaak: Lijstalinea, Meerdere niveaus + Niveau: 7 + Nummeringstijl: 1, 2, 3, … + Beginnen bij: 1 + Uitlijning: Links + Uitgelijnd op: 0 cm + Inspringen op: 1,5 cm

heeft opmaak toegepast: Lettertype: 10 pt, Tekstkleur: Zwart

- ~~De politie is gehouden aan de Wet Politie gegevens en de Wet Bescherming Persoonsgegevens. In mei 2018 wordt de AVG volledig van kracht (internationaal aangeduid als GDPR).~~

~~Identity and Access Management (IAM) wordt toegepast. Bij voorkeur wordt Role Based Access Control (RBAC) toegepast.~~

- ~~IAM maakt gebruik van Active Directory (AD) van DICT. Het is niet toegestaan een eigen IAM server toe te passen voor de applicatie. Ook de ontwikkelomgeving en de beheeromgevingen maken gebruik van een AD;~~
- ~~Autorisaties en authenticaties vinden alleen in eerste instantie plaats van de AD, dat geldt ook voor database toepassingen en voor beheer. Voor fijnmazige toegangscontrole kan een applicatie, binnen deze algemene regel, extra regelingen treffen. Dit geldt met name als toegang tot bepaalde gegevens per geval door een teamchef moet worden toegekend.~~

~~UE 181.~~	~~De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 9.1 Beveiliging zijn vermeld.~~

~~9.2.~~9.3. Protocollen

- Alle netwerkverkeer werkt op basis van IP op basis van veilige (versleutelde) protocollen;
- Er wordt gebruik gemaakt van standaard netwerk services van het rekencentrum zoals NTP, DNS en DHCP (dus niet van separate voorzieningen per toepassing);
- De toepassingen communiceren, voor zover het interactieve gebruikers betreft, via de standaard load-balancing faciliteiten van de rekencentra (F5 Big-IP), zowel voor de site selectie als voor scale-out. Communicatie verloopt standaard via web services;
- Een fileshare kan geleverd worden via NFS of via CIFS;

~~9.2.1.~~9.3.1. PaaS

Bij deze vorm van hosting levert de D-ICT behalve de hardware en de virtualisatie laag ook het besturingssysteem en de database- en applicatieserver producten. De dienst ICT van de politie levert PaaS componenten op basis van een menukaart met standaardoplossingen. Hiertoe behoren:

- Besturingssystemen Linux of Windows (andere besturingssystemen worden binnen de politie niet ondersteund);
- Databasesystemen SQL-server, PostgreSQL en Oracle;
- Java-applicatieservers: Apache, Tomcat, JBoss en Weblogic.

Virtualisatie is standaard voor deze vorm van hosting, met uitzondering van het Oracle databasesysteem.

UE 182.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragrafen 9.2 Protocollen en 9.2.1 PaaS zijn vermeld.

~~9.3.~~9.4. Koppelvlakken ABIS componenten

De aangeboden oplossing moet kunnen koppelen met andere systemen van de Politie of (inter)nationale partners om gegevens en documenten uit te kunnen wisselen. Hierin mag geen beperking zijn.
De koppelvlakken tussen onderdelen van de informatievoorziening worden ingericht, beschreven en beheerd volgens onderstaande eisen.
Hieronder ook inbegrepen, maar niet uitsluitend, het kunnen ophalen van vingerafdrukken, foto's (gelaat) en biografische gegevens.

UE 183.	De voorziening zal via REST API's kunnen communiceren met een mogelijk door de politie in te zetten workflow systeem (diagram 9.2 nummer 1). De voorziening in zijn geheel (het blauwe blok in diagram 9.1, bestaande uit applicatie, ingebouwde workflow en Specifieke Biometrische Componenten) zal separaat als service te gebruiken zijn via REST API's (diagram 9.2 nummer 2). De Specifieke Biometrische Componenten (zie woordenlijst) van de voorziening zijn separaat van het applicatiedeel van de voorziening te gebruiken via REST API's (diagram 9.2 nummer 3).

UE 184.	De interface om te communiceren met de biometrische componenten (zoals hierboven voor drie gevallen is beschreven) zal werken op basis van open marktstandaarden zoals beschreven op deze website: https://www.forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen.

UE 185.	De documentatie van de interface (API's) om te communiceren met de biometrische componenten (zoals hierboven voor drie gevallen is beschreven) worden meegeleverd. Het recht om genoemde API's te mogen gebruiken is inbegrepen in de door de aanbieder genoemde prijs.

~~9.3.1.9.4.1.~~ Koppelingen met andere toepassingen

De voorziening zal moeten functioneren in het huidige en toekomstige applicatielandschap van de Politie.
De voorziening zal daartoe de volgende reeds bestaande koppelingen kennen:

- Prüm;
- Interpol: Invoer van sporen via een NIST bestand dat via mail wordt aangeleverd;
- Interpol: Invoer vingerafdrukken via een NIST bestand dat via mail wordt aangeleverd;
- Uitvoer NIST pakketten naar NIST Archief;
- Uitvoer van NIST-pakketten naar het aangevulde NIST-archief (inclusief aanpassingen op de originelen om de werking van het systeem te verbeteren);
- Uitvoer van gegevens voor een toekomstige gegevens migratie;
- Een Workflow management oplossing, op basis van SharePoint of anderszins;
- ID-Zuil – Spelverdeler;
- SKDB – Spelverdeler;
- SIS;
- Import gelaatsafbeeldingen BVV;

Er staan ook een fors aantal nieuwe koppelingen op stapel en daarnaast zijn er wensen op koppelingen gebied. Te verwachten valt dat veel zo niet alle onderstaande koppelingen met de nieuwe voorziening gerealiseerd moeten/zullen worden.
Toekomstige koppelingen:

- PCSC;
- SISII;
- Ecris;
- Eurodac;
- BVI;
- BVV;
- EUvis;
- Eurodac;
- VVI;
- Europol;
- DJI;
- Digitaal werken in de strafrechtketen (DWS);
- Multimedia en logging servers;
- Kernregister personen (KRP);
- MEOS (Mobiel Effectief Op Straat).

Het DevOps team zal bovenstaande koppelingen realiseren en onderhouden. Uiteraard zal de Opdrachtnemer hier in het begin, met kennis en kunde, een grote rol in spelen.

UE 186.	De Inschrijver zal alle in paragraaf 9.3.1 Koppelingen genoemde koppelingen realiseren tijdens de implementatie. Om een gelijk speelveld te creëren kan hiervoor 250 uur worden opgenomen. De inschrijver garandeert dat het mogelijk is de genoemde koppelingen te realiseren via de genoemde technieken.

Met opmerkingen [RH(28]: Uitgangspunt is dat we zelf de koppelingen realiseren (DevOps).

UE 187.	Alle koppelingen met andere applicaties zullen in een Interface Communicatie Document (ICD) beschreven zijn.

UE 188.	Indien voor uw oplossing voor de gevraagde koppelingen on-premises onderdelen nodig zijn, dan dient u te allen tijde ervoor te zorgen dat bij updates de koppelingen 100% blijven werken. Indien het noodzakelijk is dat de on-premises onderdelen ook bijgewerkt dienen te worden dient u dat minimaal 12 weken van te voren kenbaar te maken.

~~9.4.~~9.5. Beheer

- De infrastructuur wordt aangesloten op het centrale beheersysteem van de dienst ICT van de politie (operations control room en security operation center). Zowel de hardware, alle systeemsoftware als de toepassingen kunnen hier 24 uur per dag worden bewaakt;
- Alle toepassingen en databases sluiten aan op het licentie asset management systeem (Flexnet manager platform). Hiermee wordt de uitnutting van het gebruiksrecht gemeten. Dit geldt bij deze toepassing alleen voor de eventueel benodigde licenties van onderliggende producten, niet voor de biometrische applicaties zelf.
- Bovengenoemde beheervoorzieningen worden bij de implementatie aangesloten door de beheerder. (zie Hoofdstuk 10).

UE 189.	De inschrijver gaat akkoord met het feit dat de infrastructuur en de toepassing op de beheersystemen worden aangesloten. Tevens levert de inschrijver voldoende informatie om de beheerder in staat te stellen deze aansluiting te realiseren.

~~9.5.~~9.6. Registratie en controle

- Logging zal op de centrale logging server geplaatst worden, waarbij de gegevens lokaal gebufferd moeten worden indien het logging systeem tijdelijk niet bereikbaar is;
- Logging gegevens worden op verzoek aan leverancier verstrekt. De Dienst ICT van de politie bepaalt per geval of de gegevens ter beschikking worden gesteld. Voor dit doel moeten ze automatisch geanonimiseerd kunnen worden;
- Logging wordt ten behoeve van techniek toegepast maar ook voor audit/compliancy. Daarom moeten beheerhandelingen tot op de persoon traceerbaar zijn. De audit logging wordt apart van andere logging opgeslagen en verwerkt;
- De voorziening legt vast welke gebruiker wanneer ingelogd is geweest en legt vast welke gebruiker op welk moment een bepaalde handeling heeft verricht en welke of wijzigingen zijn doorgevoerd;
- De logginggegevens worden ter beschikking gesteld aan operationele- en beheermedewerkers voor zover dat voor hun rol of functie nodig is;
- De voorziening logt fouten die zich in de applicatie hebben voorgedaan;
- Logging t.b.v. techniek zal aanpasbaar zijn, zodat t.b.v. probleemanalyse deze gedetailleerder kan en bij goede operationele werking op een hoger level (rekening houdend met wettelijke eisen) i.v.m. performance;
- Logging zal opschoonbaar zijn met inachtneming van wettelijke bewaartermijnen.

UE 190.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf Registratie en controle zijn vermeld.

~~9.6.~~9.7. Applicatief

- Gegevens zullen los staan van het ABIS. Als gegevens specifiek ten behoeve van één toepassing moeten worden aangepast of gemodificeerd, worden de gegevens ook zodanig opgeslagen, zodat ze ook vanuit andere applicaties kunnen worden benaderd (zie de beschrijving bij diagram 9.1).
- De toepassing zal automatisch kunnen worden uitgerold (automatic deployment and roll back);
- Toepassingen bevinden zich op dezelfde fysieke locatie als de benodigde gegevens. Op deze manier hoeven gegevens niet verplaatst of gekopieerd te worden via een lijnverbinding (WAN);
- Als de toepassing met een Web-interfaces kan worden geleverd dan heeft dat de voorkeur boven het gebruik maken van service based computing. Een client/server architectuur mag alleen worden toegepast als er geen andere oplossing voorhanden is;

- Foutmeldingen lopen altijd via de Servicedesk ICT, deze schakelt afhankelijk van de overeengekomen procedures interne teams in. De interne teams hebben afhankelijk van de afspraken de mogelijkheid een externe leverancier in te schakelen.

UE 191.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf Applicatief zijn vermeld.

~~W 14~~W 1	[Hoog] De Politie wenst gebruik te maken van een voorziening met een hoge mate van beschikbaarheid. Welke garanties biedt uw oplossing ten aanzien van beschikbaarheid? Beschrijf op welke manier hoge beschikbaarheid wordt gegarandeerd door uw oplossing. Denk hierbij aan: beschikbaarheid by design, (zie woordenlijst) active-active configuratie, scale-out, loadbalancing en andere mogelijke manieren om de beschikbaarheid te verhogen. Beoordeling vindt plaats op basis van de mate waarin uw oplossing garanties biedt voor hoge beschikbaarheid.

De Politie is bezig haar infrastructuur te gaan baseren op cloud computing volgens NIST SP 800 - 145.

~~W 15~~W 1	[Hoog] De Politie wenst gebruik te maken van een cloud infrastructuur. In hoeverre maakt uw oplossing gebruik van een cloud infrastructuur volgens NIST SP 800-145? Beschrijf daarbij in hoeverre uw oplossing een dergelijke cloud infrastructuur volgt. Beoordeling vindt plaats op basis van de mate waarin uw oplossing een cloud infrastructuur volgens NIST SP 800-145 ondersteunt.

~~9.7.~~9.8. Infrastructuur en platform

- De Dienst ICT van de politie levert en is verantwoordelijk voor de basisinfrastructuur (zoals DHCP, DNS) en het beschikbaar stellen van het platform (PaaS/IaaS);
- De applicatie is schaalbaar middels scale-out, niet via scale-up (zie woordenlijst)
- Het life-cycle-management van het IaaS of PaaS platform wordt gevolgd door leverancier. De leverancier zal op zijn beurt de onderliggende leveranciers volgen, zoals Microsoft of RedHat. Het gaat hierbij om geplande upgrades. Beveiligingspatches en bugfixes komen daar uiteraard nog bovenop;
- De applicatie zal gepackaged kunnen worden ten behoeve van Citrix.
- Voor beschikbaarheid over meerdere locaties wordt de global site selector/load balancing faciliteit toegepast.

~~W 16~~W 1	[Hoog] Beschrijf op welke manier de door de inschrijver te leveren applicatie geschaald kan worden om de benodigde extra capaciteit die mogelijk benodigd is voor een software update of voor de initiële implementatie (inlezen van gegevens en dergelijke) te kunnen leveren.

UE 192.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 9.7 Infrastructuur en platform zijn vermeld.

~~9.8.~~9.9. Compliancy checks

Jaarlijks wordt een compliancy check uitgevoerd om te controleren of de applicatie nog voldoet aan de gestelde eisen en of de afgesproken en vastgelegde procedures nog voldoen. De wijze waarop deze wordt ingericht zal worden opgenomen in het Dossier Afspraken en Procedures (DAP.).

Met opmerkingen [CR(29]: Check DAP dat dit in template genoemd wordt

UE 193.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 9.8 Compliancy checks is vermeld.

~~9.9.~~9.10. Kwaliteit dienstverlening

Zoals al eerder vermeld stelt Politie hoge eisen aan de kwaliteit van de voorziening.

UE 194.	De inschrijver zal na implementatie van de voorziening een verklaring afgeven voor het geheel van programmatuur en onderliggende infrastructuur. Uit deze verklaring zal blijken dat de onderliggende, door de beheerder geleverde infrastructuur geschikt is om de applicatie te ondersteunen zonder enige beperking.

~~9.10.~~9.11. Opgave benodigde infrastructuur

De beheerder wil in een vroeg stadium worden geïnformeerd over de benodigde infrastructuur. Doel is het tijdig kunnen reserveren van de capaciteit op de eerder beschreven platforms. De beschrijving van de capaciteit gaat over de benodigde aantallen virtuele machines volgens onderstaande tabel. De beheerorganisatie wil voldoende informatie om snel de benodigde infrastructuur te kunnen inrichten. Alle toepassingen die servers of opslagcapaciteit nodig hebben moeten in de tabel worden ingevuld.

Daarnaast is van belang om aan te geven of voor een software update of voor de initiële implementatie een andere capaciteit nodig is dan voor een normale productiefase in de daarvoor bedoelde kolom. De infrastructuur kan dan worden geschaald op de tijdstippen dat dit gewenst is. Verder zijn er kolommen voor test- en acceptatie-omgevingen.

Met software wordt bedoeld een lijst van op de Virtual Machine benodigde software met de eventueel benodigde licenties.

Doel	Productie	Import/Update Capaciteit	Testomgeving	Acceptatieomgeving
Matching (voorbeeld)	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software
Data(base) (voorbeeld)	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software
Gebruik a	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software
Gebruik b	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software	Aantal VM's Aantal cores Opslag GB. Opslag IOPS Network capaciteit Software
Etc.	Etc.	Etc.	Etc.	Etc.
Etc.				

UE 195.	Inschrijver zal bij inschrijving een overzicht opleveren in tabelvorm waarin de gewenste infrastructuur capaciteit is beschreven. Deze capaciteit zal gebaseerd zijn op de functionele eisen en wensen zoals aangegeven in Hoofdstuk 6. Dat wil zeggen dat de capaciteit voldoende moet zijn om de gegeven functionaliteit te kunnen leveren met voldoende performance voor verschillende doeleinden als aangegeven in bijgevoegde tabel.

UE 196.	Inschrijver zal bij inschrijving een plan opleveren waarin wordt aangegeven op welke wijze de biometrische systemen kunnen worden ondersteund als het gebruik van Oracle binnen de politie wordt afgebouwd binnen de contractperiode.

~~W 17~~W 2	[Hoog] Geef aan van welke PaaS producten u gebruik kunt maken. Aangezien de dienst ICT een voorkeur heeft voor het leveren van PaaS ten opzichte van het leveren van IaaS zoals aan het begin van dit hoofdstuk omschreven willen we in een vroeg stadium weten van welke PaaS producten u gebruik kunt maken.

Hoofdstuk 10. Implementatie

In dit hoofdstuk worden de voorwaarden beschreven die van toepassing zijn op het implementatietraject van de Opdracht en de initiële vulling met de aanwezige dataset.

UE 197.	De implementatie c.q. configuratie van de nieuwe voorziening vindt plaats op locatie van Politie. Waarbij medewerkers van Politie en Inschrijver op dezelfde locatie samenwerken om tot implementatie en configuratie te komen.
UE 198.	Voor elke fase van de implementatie wordt door de Inschrijver vooraf een plan van aanpak opgesteld waarin wordt vastgelegd wat het eindproduct van de fase is en welke voorwaarden van de Politie gelden voor acceptatie in deze fase.
UE 199.	Gedurende de realisatie van het product zal Inschrijver met drie consultants (1 projectleider en 2 technici) constant deelnemen in ieder van de 2 genoemde DevOps teams van de Politie. Deze 6 consultants zullen effectief door andere DevOps team leden van de Politie of die namens de Politie in het team deelnemen worden ondersteund. Ervan uitgaande dat de implementatieperiode 1,5 jaar duurt, gaat het hier om 1,5 * 6 * 1920 = 17280 consultancy uren.
UE 200.	Aansluiting op de beheervoorzieningen uit paragraaf 9.4 worden gerealiseerd bij de implementatie.
UE 201.	De acceptatietest op de voorziening zal succesvol doorlopen zijn en eventuele fouten zullen verholpen zijn in de overeengekomen herstelperiode.
~~W 18~~W 2	De implementatie c.q. configuratie van de nieuwe voorziening vindt bij voorkeur plaats op scrum/agile wijze. Waarbij medewerkers van Politie en Inschrijver nauw samenwerken om tot het beste resultaat te komen. Geef een beschrijving van de wijze waarop u hier invulling aan kunt geven. Beoordeling vindt o.a. plaats op basis van de mate waarin de gewenste werkwijze door Inschrijver ingevuld kan worden.

Met opmerkingen [LI(30]: Eeeuuuuu zie hoofdstuk DevOps voor de inzet van personeel van de leverancier en periode enz.

10.1. Plan van Aanpak (PvA) Inschrijver

Inschrijver maakt een PvA waarin Inschrijver zijn totaaloplossing voor dit project nader toelichten wat wordt opgeleverd bij de inschrijving.

Met opmerkingen [CR(31]: Is relatie met dev opps voldoende vastgelegd.

De uitgangspunten voor het PvA zijn als volgt:

- Inschrijver zal bij inschrijving een plan van aanpak (PvA) opleveren ten aanzien van de implementatie van zijn oplossing;
- De implementatie moet vanuit Inschrijver op of voor 30-11-2019 afgerond kunnen zijn. In het bij de inschrijving op te leveren PvA kan worden uitgegaan van de eigen planning zonder nog rekening te houden met de Politie;
- Het PvA is gebaseerd op de verwachtingen, eisen en randvoorwaarden van de Politie, zoals weergegeven in het aanbestedingsdocument;
- Het PvA bevat duidelijke fases en stappen die voor de implementatie nodig zijn. In deze stappen wordt ook beschreven wat de geplande doorlooptijd is;
- In het PvA wordt bij acties aangegeven wat de rol en verantwoordelijkheid is van de Politie en Inschrijver;
- De eindverantwoordelijkheid voor de werking van de geleverde Biometrie voorziening ligt bij Inschrijver. Deze is te allen tijde verantwoordelijk voor de tijdigheid en de kwaliteit van de door Inschrijver op te leveren producten en diensten en voor de inzet van zijn deskundigen.

- In het PvA wordt rekening gehouden met de inzet van een DevOps team, waarin medewerkers van de Politie inzitten. De medewerkers van de Politie komen van de biometrische afdeling bij de Dienst Forensische Opsporing en uit de IV-organisatie
- In het PVA worden de bijdragen aangegeven, die in het DevOps team geleverd moeten gaan worden door de consultants van de Inschrijver, de medewerkers van de Politie komend van de biometrische afdeling bij de Dienst Forensische Opsporing en uit de IV-organisatie. Daarbij wordt beschreven wat de afhankelijkheid inhoudt tussen de bijdragen van de bovengenoemde medewerkers binnen het DevOps Team.
- Minimaal de eerste 3 maar eventueel verder nog nader te bepalen hoeveelheid sprints zal onder verantwoordelijkheid worden uitgevoerd van de inschrijver waarna deze de verantwoordelijkheid overdraagt aan de opdrachtgever om in de resterende sprints de voorziening geheel naar de eisen van de opdrachtgever ingericht te krijgen.
- Op basis van de in dit document genoemde zaken en in overleg met de opdrachtgever, zal de inschrijver aangeven in het PvA wat eventueel een geschikt moment zal zijn voor de overdracht van verantwoordelijkheid.
- In de vervolgsprints zal de inschrijver verantwoordelijk blijven voor de functionaliteit van de initiële opgeleverde functionaliteit.
- Het PvA bevat informatie over de technische implementatie evenals de planning van zowel medewerkers van de Politie, het DevOps team als uw eigen medewerkers en de communicatieplanning met Politie;
- Het PvA bevat een hoofdstuk beheer, waarin alle beheerwerkzaamheden worden beschreven.

~~W 19~~W 2	De Inschrijver stelt een PvA op voor de hele implementatie. Het PvA moet voldoen aan de gegeven uitgangspunten voor het PvA zoals hierboven beschreven.

Het Plan van Aanpak wordt beoordeeld op wat weergegeven is in de volgende wensen. Hierbij wordt de mate van duidelijkheid, compleetheid, realisme en inhoudelijke relevantie als rode draad gehanteerd.

- De beschrijving van fases en stappen die voor de implementatie nodig zijn. Bij deze stappen wordt ook beschreven wat de geplande doorlooptijd is;
- De beschrijving van de technische implementatie evenals de planning van zowel medewerkers van de Politie, de beheerder als uw eigen medewerkers en de communicatieplanning met Politie;
- De beschrijving van het kwaliteitsregime (maatregelen om foutloze software te garanderen) van Inschrijver met betrekking tot op te leveren software.

10.2. Datamigratie

In de basis kiest de Politie voor een NIST migratie strategie. Voor deze strategie wordt alle data uit Havank en catch/Face geëxporteerd en vervolgens omgezet naar de NIST standaard in XML-formaat in een nieuw Biometrie-Migratie-Store. Bij de NIST migratie strategie wordt uitgegaan van een bijgewerkt Biometrie-Migratie-Store, waarin alle data uit Havank en catch/Face met betrekking tot vingers / handpalmen, sporen, biografische gegevens en gelaat zijn opgenomen en actueel wordt gehouden totdat alle data uit Catch en Havank en is gemigreerd naar de door u geleverde Biometrievoorziening.

De Biometrie-Migratie store gaat opgezet worden door het DevOps Migratieteam. De product owner van dit team wordt geleverd door de politie. In bijlage 1 is weergegeven hoe de opbouw van Biometrie-Migratie-Store er uit moet zien. Op advies van de Inschrijver kan de opbouw van de Biometrie-Migratie-Store worden aangepast. Vanuit de Biometrie-Migratie-Store wordt de door u geleverde biometrievoorziening gevuld. Het is de bedoeling dat de bijgewerkte Biometrie-Migratie-Store ook kan worden gebruikt om nieuwe technieken en algoritmen om met biometrische gegevens te werken te testen.

Met opmerkingen [RH(32]: Wie voert regie: Politie of leverancier?

Om de migratie voor de business uitvoerbaar te houden wordt er in fasen gemigreerd van de huidige naar de nieuwe Biometrievoorziening. De volgende 3 fasen zijn gekozen:

1. Gelaatsafbeeldingen
2. Vingerafdrukken / handafdrukken
3. Sporen

Alle bovenstaande data is opgenomen in een geactualiseerde Biometrie-Migratie-Store, zoals hierboven is beschreven. De nieuwe Biometrievoorziening kan van hieruit worden geladen met een NIST standaard in XML-formaat.
Voor de afzonderlijke fasen wordt een moment-x afgesproken dat big-bang van het huidige naar de nieuwe biometrievoorziening wordt overgegaan. De nieuwe biometrievoorziening dient in iedere fase vanaf moment x de Biometrie-Migratie-Store ook te voeden met nieuwe, gemuteerde en verwijderde zaken.

Het ontwikkelen en testen van de tooling die de migratie en het testen van de migratie mogelijk maakt wordt uitgevoerd in de ontwikkelomgeving en testomgeving. Bij tooling voor de migratie wordt gedacht aan scripts, schoning scripts om database tabellen te schonen, monitoring tools om bijvoorbeeld uitval te monitoren en test scripts om testdata te creëren en de datamigratie te testen. Om te voorkomen dat de DevOps teams Functionaliteit en Migratie elkaar in de weg zitten met hun ontwikkel- en testwerkzaamheden, wordt er gebruik gemaakt van een eigen ontwikkel- en testomgeving per DevOps team.

De acceptatietesten van de datamigratie worden uitgevoerd in de acceptatieomgeving. Tot het moment dat de productieomgeving voor productie werkzaamheden wordt gebruikt kan, indien nodig, ook de productieomgeving worden gebruikt voor acceptatietesten. Van alle productiedata moet worden vastgesteld of het succesvol kan worden gemigreerd naar de nieuwe Biometrievoorziening. Daarmee is het onvermijdelijk dat alle productiedata wordt gebruikt voor de acceptatietesten. Voor het gebruik van productiedata in de acceptatieomgeving zal toestemming gegeven moeten worden en aanvullende maatregelen genomen worden om toegang tot deze data, het risico dat het ontsloten wordt voor derden of vermengd kan raken met andere verwerkingen te minimaliseren.

De technische consultants die de Inschrijver voor het DevOps team migratie gaat leveren, heeft kennis en ervaring met:

1. Het uitvoeren van migraties met de NIST standaard in XML-formaat
2. Het actualiseren van de Biometrie-Migratie-Store met mutaties uit de nieuwe Biometrievoorziening
3. Ontwikkeling en testen van bovengenoemde tooling, die de migratie en testen van migraties mogelijk maakt.

Voorafgaand aan het in productie nemen van nieuwe type data en/of processen in de productieomgeving wordt er altijd een productie acceptatietest hierop uitgevoerd alvorens er een vrijgave wordt gegeven voor in productie name.

Inschrijver zal, t.b.v. een eventuele toekomstige aanbesteding en/of migratie (bijvoorbeeld na de beëindiging van de overeenkomst), zich bereid verklaren tot het verstrekken (aan de Politie) van alle voor het betreffende doel (migratie) relevante (aanvullende) documentatie van de gehele voorziening, incl. alle functionele ontwerpen en beschrijvingen met inbegrip van (logische) datamodellen en technische ontwerpen van alle relevante koppelingen. Daarnaast zal Inschrijver akkoord gaan met de verstrekking daarvan - onder toezegging van vertrouwelijkheid - aan eventuele belanghebbenden in dat kader (zoals potentiële deelnemers aan een dergelijke aanbesteding, partijen die diensten leveren aan de Politie op het gebied van migratie, etc.).

Van Inschrijver wordt verwacht bij inschrijving een plan van aanpak met betrekking tot datamigratie op te leveren als onderdeel van het plan van aanpak voor het totale project. In dit plan van aanpak over de datamigratie staat minimaal beschreven:

- Fasering werkzaamheden;
  - Migratie
  - Koppelingen
- Eisen/Wensen ten aanzien van de bronbestanden;
- Eisen/Wensen ten aanzien van de benodigde infrastructuur en capaciteit;
- Eisen/Wensen ten aanzien van de benodigde personele capaciteit van de Politie;
- Planning van de migratie (tijdsduur);
- Risico's;

- Omgaan met kwaliteit van de biometrische kenmerken (Wat als de bronbestanden niet kunnen worden ingelezen vanwege kwaliteitsissues);
- (Technische) Rapportages over de datamigratie. De migratie van data moet aanwijsbaar goed zijn gegaan en er moet logging zijn waarin alle handelingen, bewerkingen, enz. traceerbaar en herleidbaar zijn;
- Beveiliging van de gegevens tijdens de migratie;
- Logging moet ook de integriteit van de gegevens 'tracen'. Aantonen dat gegevens ongewijzigd zijn gebleven of dat wijzigingen puur functioneel waren.

UE 202.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf Datamigratie is vermeld.

10.3. Opleidingen

Met opmerkingen [RH(33)]: Hoe ziet het opleidingsplaatje er voor de gebruikers uit? Volgen we het train the trainer principe of laten we iedereen opleiden door de Inschrijver?

Na in productie name van de voorziening zal het genoemde centrale DevOps team het beheer en door ontwikkelen uitvoeren. Dit team blijft dus bestaan. Het migratie team zal na het uitvoeren van haar specifieke taak van data migratie worden ontbonden. Alle opleidingsinvestering zal dus gericht zijn op het centrale team.

De Politie zal in de productionele fase met eigen daarvoor aangestelde mensen de ondersteuning, beheer en veranderingen uitvoeren (DevOps). Dit betekent dat de beoogde medewerkers van de Politie, opgeleid worden door de Inschrijver zodat deze medewerkers zelfstandig:

- De voorziening in hoge mate zelf aan te passen door configuratie en/of faciliteiten om door middel van externe programmering, functionaliteit van de voorziening aan te sturen. Denk hierbij aan de aansturing van een voorziening via RPC API technologie.
- De voorziening kunnen configureren volgens de in dit document genoemde vereiste en gewenste functionaliteit;
- Door middel van openstandaarden zelf systeemkoppelingen met andere systemen kan realiseren;
- Direct maar ook via tooling, dynamisch de werking van het operationele systeem kan controleren op diverse functionaliteiten (technisch);
- Management rapportages kan samenstellen e/o ontwerpen en kan laten genereren door de voorziening;
- Het functioneren of het niet functioneren van programma onderdelen van de nieuwe voorziening kan onderzoeken;
- Correcte en bruikbare probleem analyses en probleemrapportages kan maken voor Inschrijver zodat deze problemen sneller kan oppakken;
- De dagelijks operationele functionele en technische bedieningen en beheer uit kan voeren op de nieuwe voorziening;
- Kleinere, door Inschrijver opgeleverde systeem updates zelfstandig kan uitvoeren.

Van belang is dat de DevOps teamleden kennis opdoen van alle nodige technische achtergrond, mechanismes en processen die horen bij bovengenoemde punten en specifiek van toepassing zijn voor de aangeboden voorziening.

Om dit te bereiken maakt de Inschrijver een opleidingsplan voor de medewerkers van de Politie. Hierbij gelden de volgende uitgangspunten:

- Inschrijver zal bij inschrijving een opleidingsplan opleveren waarin duidelijk wordt aangegeven waar de opleiding uit bestaat;
- De opleiding zal bestaan uit trainingen voor gebruik en beheer;
- De opleiding vindt plaats op een door de Politie en Inschrijver samen te bepalen locatie;
- Voor de opleidingslocatie en de voor de opleiding gebruikte infrastructuur en faciliteiten gelden bepaalde verplichtende voorwaarden in verband met veiligheid en geheimhouding;
- Het opleidingsplan bevat tevens de aanpak voor individuele begeleiding tijdens werkzaamheden van de door de Politie aangewezen medewerkers die een bepaalde rol invullen (functioneel beheer, technisch beheer, etc.);

- Het intellectueel eigendom van de opleiding en opleidings- en trainingsmaterialen blijft bij inschrijver;
- De inschrijver staat toe dat de Politie opleidingsmaterialen te verveelvoudigen (kopiëren) voor intern gebruik bij de Politie;
- De inschrijver staat toe dat de geleverde opleidingsmaterialen vrij gebruikt kunnen worden binnen de gehele organisatie van de Politie;
- De inschrijver staat toe dat kopieën van de geleverde opleidingsmaterialen vrij mogen worden aangepast en aangevuld door de Politie, zodat de Politie in staat is zelf trainingen voor eigen personeel te verzorgen;
- De trainingen voor beheer en ontwikkeling zijn in de Nederlandse of Engelse taal;
- De trainingen en trainingsmaterialen voor gebruikers (indien van toepassing) zijn in de Nederlandse taal;
- Opleidings- en trainingsmaterialen zijn aangepast op deze implementatie;
- De onderwerpen in de opleidingen zijn duidelijk beschreven. Hierbij wordt onderscheid gemaakt in verschillende benodigde specialisaties;
    - Technisch beheer, onder andere onderhoudsprocessen (handmatig en geautomatiseerde batch verwerkingen), database koppelingen, koppelvlakken en andere systeem koppelingen, enz.;
    - Configuratie, inrichting, koppelvlakken, systeem parameters en hun werking etc.;
    - Customizing;
    - Functioneel beheer, onder andere de tooling voor bijvoorbeeld de workflows, standaard aanwezige functionaliteit en waar deze gevonden kunnen worden in de applicatie;
    - Ontwikkeling (RPC/API);
    - Praktijk gebruik door normale gebruikers;
    - Praktijk gebruik door normale specialistische gebruikers;
    - Aanmaken en gebruik van functionele en technische procesinrichting;
    - Andere nader te bepalen items die nodig zijn voor de uitvoering van de taken van een DevOps team in een opbouw en operationele fase.
- De specialisatie onderwerpen zijn logisch gegroepeerd en gemoduleerd;
- De opleiding bestaat niet alleen uit systeem gerelateerde trainingen maar ook uit minimaal één, maar bij voorkeur meerdere trainingen, inclusief workshops, op het gebied van de logische werking van de algoritmes en zoekmethodes. In deze training en workshops zal door de Inschrijver uitgebreid aandacht worden besteed aan de meest optimale zoekmethoden die gebruikt kunnen worden, aangepast op de situaties waarin ze worden gebruikt door de Politie. Aangezien deze situaties voor de Inschrijver niet inzichtelijk zijn, zal na gunning voor dit deel van de opleiding, met medewerking van de Politie, de bedoelde situaties zo snel mogelijk worden bepaald. Alles eventueel onder geheimhouding zodat bedrijfsgeheimen van de Inschrijver beschermd zijn. De inschrijver zal duidelijk aangeven welke zaken hieronder vallen;
- De kosten van de opleiding en trainingen zitten in de fixed price zoals aangegeven bij inschrijving.

UE 203.	Inschrijver zal een opleiding bieden voor xx gebruikers van de voorziening.
UE 204.	Inschrijver zal een opleiding bieden voor maximaal 2 x 9 mensen (gebruikers en beheerders) die onderdeel zijn of gaan uitmaken van de twee DevOps teams.
UE 205.	Inschrijver levert een concept opleidingsplan conform bovengenoemde uitgangspunten bij de inschrijving. De Inschrijver gaat ermee akkoord dat het definitieve opleidingsplan na gunning wordt vastgesteld
UE 206.	Inschrijver gaat akkoord met de procedure en onderwerpen voor het opleiden na gunning zoals in bovenstaande paragraaf beschreven.

Met opmerkingen [FvL34]: Aanvullen met XX technisch applicatie beheerder, xx functioneel beheerders, xx systeembeheerders. Het zijn andere soorten opleidingen, mogelijk ook met een andere duur en dus kosten

10.4. OTAP

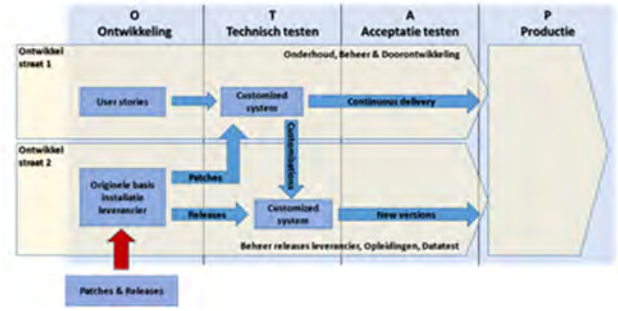
De door Inschrijver geleverde producten (standaard en eventueel maatwerk software) worden door DevOps team via het reguliere OTAP-straat principe naar productie gebracht. Dit betekent dat er op meerdere omgevingen installaties plaatsvinden. Voorlopig komen er minstens 7 omgevingen, waarbij alle omgevingen alle gespecificeerde functionaliteiten aan kunnen:

1. De O-omgeving Functionaliteit: Hierop vindt de eerste installatie plaats en wordt gekeken of de installatie en werking goed verloopt. Bovendien wordt hier eventueel software op ontwikkeld of aangepast door DevOps team.
2. De O-omgeving Migratie: Hierop worden migratiescripts ontwikkeld en/of aangepast door DevOps team.
3. De T-Omgeving Functionaliteit: Wordt gebruikt om stabiele releases te kunnen testen op functionele en non-functionele requirements. Deze omgeving kent geen performance eisen. Voor het testen van koppelingen worden stubs en drivers gebruikt.
4. De T-Omgeving Migratie: Wordt gebruikt om migratiescripts te kunnen testen op een goede werking. Deze omgeving kent performance eisen, waardoor doorlooptijden zijn extraheren naar de productie omgeving. Voor het testen van koppelingen worden stubs en drivers gebruikt.
5. De A-Omgeving: Deze productieconforme omgeving wordt gebruikt voor acceptatietesten van een release. Voor het testen van koppelingen worden indien beschikbaar acceptatietest systemen van de Politie en ketenpartijen gebruikt. De omgeving is geschikt voor performance testen.
6. De P-Omgeving: De productieomgeving.
7. De Opleidingsomgeving: Een stabiele omgeving waar opleidingen op kunnen worden gegeven.

De volgende plaatjes illustreren een mogelijke opzet:

OTAP gebruik realisatie fase

OTAP gebruik productionele fase



Voor opleidingen in de productionele fase zal de A omgeving van de ontwikkelstraat 2 worden gebruikt.

Met opmerkingen [RH(35]: Dit verwoord niet precies hoe we met dit onderwerp denken om te gaan. Zie plaatjes!

Met opmerkingen [SM(36]: Is ook afhankelijk van het release beleid (gaat er na DevOps elke sprint een release naar productie). Ik zou uitgaan van 2 versies in OTA, namelijk versie N (productie versie) waarop een productieverstoring kan worden opgelost en Versie N+1 (lopende sprint).

UE 207.	De inschrijver zal ten behoeve van het testen van de basis installatie een test dataset leveren waarmee de juiste werking van de installatie aangetoond kan worden. Deze test dataset zal onderhouden worden.

UE 208.	De inschrijver gaat akkoord met de eisen en uitgangspunten zoals in bovenstaande paragraaf 10.4 OTAP is vermeld.

Hoofdstuk 11. Dienstverlening

De dienstverlening wordt beschreven en vastgelegd in de meegeleverde Service Level Agreement (SLA) (Bijlage x.x) en sub-bijlages (x.x.*). De Inschrijver dient zich te committeren aan minimaal de in de SLA inclusief bijlages genoemde diensten.

De SLA definieert tevens het niveau (Level) van deze diensten. Op deze manier kunnen de diensten objectief worden gemeten en kunnen verslechteringen of verbeteringen in de dienstverlening gemakkelijk worden geconstateerd.
De hier beschreven dienstverlening wordt georganiseerd en ingericht volgens ITIL-richtlijnen. Wijzigingen in deze richtlijnen en daarmee in de organisatie van de werkzaamheden, zullen in gezamenlijk overleg met Opdrachtgever worden doorgevoerd.

Het strategisch, tactisch en operationele beheer van de Biometrievoorziening wordt uitgevoerd door de Dienst ICT Politie.
Alle afspraken in de SLA tussen Inschrijver en Opdrachtgever die betrekking hebben op het operationele beheer worden in praktijk uitgevoerd door Opdrachtnemer, dit wordt in de DAP, na gunning, nader uitgewerkt.

De D-ICT zal als gemandateerd Opdrachtgever optreden richting Opdrachtnemer in het kader van afhandeling van storingen met inachtneming van de gestelde prioriteiten en afgesproken oplostijden. Inschrijver vervult dus eigenlijk alleen derdelijns ondersteuning.

De meegeleverde bijlages bij de SLA (x.x), dienen op detailniveau nog nader te worden ingevuld na gunning.

UE 209.	Inschrijver committeert zich aan bovengenoemde uitgangspunten.

UE 210.	Inschrijver committeert zich (minstens) aan Bijlage x.x en Bijlage x.x, zijnde de minimale concept SLA en DAP.

UE 211.	Inschrijver werkt na gunning mee aan de completering van de SLA en de vulling van de bij de SLA meegeleverde bijlages en stelt met de Opdrachtgever een DAP op.

Hoofdstuk 12. Verklarende afkortingen- en woordenlijst

Info-object	Toelichting
TP	Tenprint, alle referentievinger categorieën
PP	Palmprint, alle referentie handpalm categorieën
LT	Latent, alle dactyloscopische sporen
FC	Face, alle referentieafbeeldingen met een gelaatsafbeelding
PR	Probe, alle 'sporen' met een gelaat t.b.v. zoeking.
DVI	Disaster Victim Identification
Persoon	De persoon kan betrekking hebben op het te identificeren subject. Bij een persoon horen biografische kenmerken (Naam, adres, woonplaats, nationaliteit, geboortedatum, geslacht e.d.) en biometrische kenmerken (afbeeldingen van vingers, iris, gelaat, etc.). De persoon kan een vreemdeling, een verdachte, getuige, slachtoffer of veroordeelde zijn.
Identificerend persoonsnummer	Ieder (fysiek) persoon heeft over het algemeen in het juridisch domein meerdere persoonsnummers. Zo kent iedere in het BRP ingeschreven persoon een Burgerservicenummer. Daarnaast worden in de strafrechtketen SKN-nummers toegekend, in het vreemdelingendomein V-nummers en bij DJI DJI-nummers.
NIST bestand	Een NIST bestand is een verzameling gegevens bestaande uit biometrisch kenmerken en metadata en is opgebouwd conform de NIST standaard. Het is een internationale standaard die van toepassing is voor elk type biometrisch kenmerk/modaliteit
Afbeelding	De afbeelding is de algemene term die gebruikt wordt voor matching. Een afbeelding kan bestaan uit: 1. Eén biometrisch kenmerk van één persoon 2. Meerdere biometrische kenmerken van dezelfde persoon 3. Meerdere biometrische kenmerken van mogelijk meerdere personen. De afbeelding kan afgenomen zijn in een beheerste omgeving, waarbij het mogelijk is afbeeldingen te maken conform gewenste kwaliteitscriteria of in een omgeving waarbij dat niet het geval is. Daarnaast is het kenmerk van een afbeelding dat deze één 'timestamp' kent, m.a.w. naar één moment is terug te leiden.
Biometrische kenmerkenset	Een verzameling biometrische kenmerken die bij één persoon genomen zijn en die bij elkaar bij één persoon horen, waarbij elk biometrisch kenmerk bij één onderdeel van persoon hoort. Meestal is één biometrische kenmerkenset in één keer opgenomen, er zijn echter uitzonderingen waarbij een set bestaat uit de beste afbeeldingen die op verschillende momenten genomen zijn. Het beste voorbeeld is de hand die bestaat uit een meerdere vingers en daarmee uit meerdere afbeeldingen.
Biometrische Template	De template is de uitkomst van een algoritme en bestaat uit een cijfer van 364 posities. Naast dat het algoritme gepatenteerd is, is het ook nog eens beveiligd met encryptie.
Codering	Een volgens een standaard afgesproken representatie van de template.
Spoor	Een spoor is een specifiek soort afbeelding met biometrische kenmerken die mogelijk kunnen leiden tot één of meerdere personen. Het kenmerkt zich door het feit dat de biometrische kenmerken in meeste gevallen niet de gewenste kwaliteit hebben.
Samengesteld/ composiet signalement	Dit is de biometrische kenmerkenset die is opgebouwd uit de beste afbeeldingen die logisch bij elkaar horen. Dit is relevant indien er van één persoon slechts één biometrische kenmerkenset in het referentiebestand beschikbaar is.
Annotatie	Het moet mogelijk zijn bij een template dan wel een biometrisch kenmerk een annotatie toe te voegen.
Proces	Het identificerend proces waar de identificatie/verificatie wordt toegepast. Voor ieder proces zijn verschillende eisen (naast kwaliteitseisen) van toepassing. Het verifiëren op deze eisen zit over het algemeen niet in de scope van de biometrie voorziening (bijv. de BVV bepaalt dat COA niet mag identificeren voor haar meldplicht proces). De ABIS heeft echter wel te maken met verschillende domeinen waar biometrie voor wordt toegepast, de gegevens van personen die met dit doel geregistreerd worden dienen gescheiden te worden (i.e. een domein vreemdelingen, strafrecht).
Metadata	Bij biometrische kenmerken worden metadata vastgelegd die de context van de opnames beschrijven. Het betreffen: - Persoonsnummer - Registrerend proces (uitputtende lijst van mogelijke processen) - Datum/tijdstip opname - Biometrisch kenmerk (beschrijving van de afbeelding), m.n. relevant als er sprake is van een set waarbij meerdere afbeeldingen zijn opgenomen (bijv. 10 vingers) - Attributen t.b.v. het maken van een selectie Eén van de doelen van metadata is tegemoet te komen aan traceerbaarheid – elke registrerende activiteit moet herleid kunnen worden.
Vergelijkingsactiviteit	De handeling die wordt uitgevoerd om een persoon te matchen (verifiëren en/of identificeren). Deze activiteit is als entiteit opgenomen omdat in een aantal gevallen verantwoording afgelegd moet kunnen worden over de handelingen die zijn uitgevoerd door medewerkers. Indien dit vanuit het proces geëist wordt moet traceerbaarheid en auditeerbaarheid ingeregeld worden.
Vergelijkingsscore	Een matchingstransactie zal een bepaalde score opleveren die antwoord geeft op de vraag of het een hit, weet niet of no hit is. Deze score is daarmee een mate van zekerheid op de matching. Elke Inschrijver kan zijn eigen score systematiek hanteren. Bij voorkeur is dit een percentage.

Gebruiker	Waar wordt gesproken over gebruiker, wordt iedere medewerker van de Politie bedoeld die deze functionaliteit ter beschikking zal krijgen. Geautoriseerde gebruiker wordt gebruikt om aan te geven dat alleen een gebruiker met specifieke rechten deze functionaliteit ter beschikking zal krijgen. Bij de inrichting van de voorziening zal de term gebruiker nader ingevuld worden met specifieke rollen.
Drempelwaarde	Drempelwaarden worden gebaseerd op het specifieke ABIS system van Inschrijver. Waarbij zaken als performance metrieken (accuratesse), data base grootte enz. een rol spelen.
Lights-out	Automatisch verrichten van handelingen zonder menselijke tussenkomst. Bijvoorbeeld het automatisch vergelijken van vingerafdrukken.
ID-Zuil	Afkorting van Identificatiezuil. Om er zeker van te zijn dat de aangehouden persoon is wie hij/zij zegt dat hij/zij is, moet door de opsporingsambtenaar de identiteit van de verdachte worden vastgesteld (art 27a / 55c WvSv) en is het noodzakelijk om op het bureau een goede identificatie te organiseren. De Wet Identiteitsvaststelling veroordeelden, verdachten en getuigen verplicht hiertoe het gebruik van de ID-zuil. Op de meeste Politiebureaus is identificatieapparatuur (ID-zuil) geplaatst
Scale-up	Het beschikbaar stellen van extra capaciteit door extra computers of virtual machines in te zetten. Hiermee wordt het mogelijk voor iedere toepassing vergelijkbare machines in te zetten . Verder zal bij uitval van een virtual machine capaciteit voor de applicatie beschikbaar blijven via de andere virtual machines. Als de werklast verandert, kan de capaciteit eenvoudig worden aangepast.
Scale-out	Het beschikbaar stellen van extra capaciteit door een zwaardere computer of virtual machine ter beschikking te stellen.
Specifieke Biometrische Component (SBC)	Een onderdeel of service van een biometrische applicatie dat is ingericht om bijvoorbeeld een vingerafdruk, iris of een gelaat te herkennen.
LMF	Landelijk Meldingsformulier Personen. Hiermee leggen politie medewerkers de signalementsgegevens van een verdachte vast.

Bijlage 1. Opbouw van Biometrie-Migratie-Store

Om de data over te krijgen van Havank3 naar Biometriematch wordt gebruik gemaakt van de Biometrie-Migratie store. De Biometrie-Migratie-Store wordt ook gebruik om wijzigingen in Biometriematch te kunnen opslaan. De Biometrie-Migratie-Store wordt gedurende de migratieperiode dus zowel door Biometriematch als Havank3 gevuld. Deze wetenschap stelt eisen aan het aantal lagen waarin mutaties moeten kunnen worden opgeslagen. De lagen die voorzien zijn worden in de onderstaande paragraven uitgewerkt in de volgende categorieën:

1. Vingers/handpalmen;
2. Sporen;
3. Gelaat;
4. Biografische gegevens.

Vingers/handpalmen

Om alle mutaties van vingers en handpalmen in Havank3 en Biometriematch te kunnen opslaan zijn de volgende lagen voorzien:

a. Origineel: het origineel afkomstig van de ID-zuil, de scan van een papieren slip of de foto van een mobiele telefoon;
b. Mimex: NIST standaard;
c. Autocodering Havank3: de automatische codering door Havank3 van het origineel;
d. Muteren origineel in Havank3: het rechtzetten van de afbeelding, spiegelen door de dactyloscopisch expert;
e. Handmatig coderen in Havank3: het aanpassen van de automatische codering van de afbeelding door de dactyloscopisch expert inclusief verwijderen van automatische punten;
f. Autocodering Biometriematch: nadat vingers/handpalmen gemigreerd zijn, vindt de autocodering van het origineel door Biometriematch plaats;
g. Muteren origineel in Biometriematch: het rechtzetten van de afbeelding, spiegelen door de dactyloscopisch expert;
h. Handmatig coderen in Biometriematch: het aanpassen van de automatische codering van de afbeelding door de dactyloscopisch expert inclusief verwijderen van automatische punten;
i. Geoptimaliseerde codering;
j. Nieuwe algoritme codering.

Sporen

Om alle mutaties van sporen in Havank3 en Biometriematch te kunnen opslaan zijn de volgende lagen voorzien:

a. Origineel: de scan van een papieren slips, af te nemen van in beslag genomen materiaal of de foto van een mobiele telefoon;
b. Autocodering Havank3: de automatische codering door Havank3 van het origineel;
c. Muteren origineel in Havank3: het rechtzetten van de afbeelding, spiegelen door de dactyloscopisch expert;
d. Handmatig coderen in Havank3: het aanpassen van de automatische codering van de afbeelding door de dactyloscopisch expert inclusief verwijderen van automatische punten;
e. Autocodering Biometriematch: nadat de sporen gemigreerd zijn, vindt de autocodering van het origineel door Biometriematch plaats;
f. Muteren origineel in Biometriematch: het rechtzetten van de afbeelding, spiegelen door de dactyloscopisch expert;
g. Handmatig coderen in Biometriematch: het aanpassen van de automatische codering van de afbeelding door de dactyloscopisch expert inclusief verwijderen van automatische punten;

h. Geoptimaliseerde codering;
i. Nieuwe algoritme codering.

Gelaat

Om alle mutaties van gelaat in Catch en Biometriematch te kunnen opslaan zijn de volgende lagen voorzien:

a. Origineel: de foto zoals deze genomen is met de ID-zuil, fotocamera of mobiele telefoon
    a. Catch1: vreemdelingen;
    b. Catch2: gelaatsafbeeldingen, gedupliceerd;
    c. FCM database.
b. Handmatige aanpassingen in Catch: het handmatig aanpassen van de afbeelding door de forensisch medewerker;
c. Autocodering Biometriematch: de automatische codering van het origineel;
d. Handmatige codering in biometriematch: het handmatig aanpassen van de afbeelding door de forensisch medewerker;
e. Geoptimaliseerde codering;
f. Nieuwe algoritme codering.

Biografische gegevens

Om alle mutaties op de biografische gegevens te kunnen opslaan zijn de volgende lagen voorzien:

a. Origineel: de biografische gegevens zoals deze bij de registratie zijn opgenomen, waaronder de:
    a. Persoonsgegevens: naam, geslacht, geboortedatum, geslacht, schoenmaat;
    b. Biometrienummer;
    c. SKDB-nummer;
    d. Geverifieerde gegevens met persoonsregister als persoon zich legitimeert met geldig legitimatiebewijs;
    e. Velden voor bijzonderheden
        i. Aan de persoon gekoppelde zaakgegevens (bijvoorbeeld PV of DAS-nummer);
        ii. Aan het spoor gekoppelde zaakgegevens;
        iii. Afdrukkenblad zonder aangegeven categorie gebruikt voor een strafrecht zaak.
    f. Zoekinggegevens;
    g. Zaakgegevens met betrekking tot gerelateerd incident;
    h. Historie.
b. Mutatie van biografische gegevens in Havank3;
c. Mutatie van biografische gegevens in Biometriematch.

Plan van aanpak – Doorontwikkeling Gelaatsherkenning

Centrum voor Biometrie (DLOS-LFSC)

5.1.2.e

Operationeel Expert Gelaatsherkenning

Definitief

Versie 1.0

Versie datum 6 september 2019

« waakzaam en dienstbaar »

Plan van aanpak

Het Centrum voor Biometrie (CvB) levert diensten op het gebied van het herkennen van personen op basis van biometrische kenmerken met behulp van forensische methoden en technieken. Sinds 2014 houdt deze afdeling zich bezig met gelaatsherkenning. In eerste instantie is de afdeling gestart met een pilotfase in samenwerking met ATOE. In deze pilotfase is gebleken dat gelaatsherkenning een wezenlijke bijdrage kan leveren binnen de opsporing. In 2017 is besloten verdere ervaring op te doen met deze nieuwe productlijn en binnen dit expertisegebied.

Op dit moment worden succesvolle producten geleverd die bewezen hebben, een bijdrage te leveren aan het oplossen en voorkomen van strafbare feiten. 5.2.1 . Gelaatsherkenning is een relatief jong expertisegebied waarop veel ontwikkelingen in de markt en de maatschappij te zien zijn. Om in de behoefte van de organisatie te voorzien en om mee te kunnen gaan in de innovatie is het nodig deze productlijn door te ontwikkelen.

Met opmerkingen [A1]: 5.2.1

In opdracht van de Programma Directeur Forensische Opsporing 5.1.2.e start er binnen het Centrum voor Biometrie het project Gelaatsherkenning. Het doel is om te komen tot een kwalitatief hoogwaardige productlijn gelaatsherkenning die kan voorzien in de behoefte/vraag van de organisatie en partners, maar ook zo is ingericht dat productlijn mee kan blijven ontwikkelen met de innovatie op de markt en in de maatschappij.

Het project ken de volgende rollen:

Opdrachtgever	Programmadirecteur FO	5.1.2.e
Eigenaar	Centrum voor Biometrie	5.1.2.e
Senior Suplier NP	Teamchef LFSC	5.1.2.e
Senior Suplier CvB	Team coördinator CvB	5.1.2.e
Senior User	OSD	John Riemen
Projectleider	Operationeel Expert CvB	5.1.2.e

Dit project zal de volgende fasen doorlopen om tot een goed eindresultaat te komen.

- Fase 1: Het in kaart brengen van de huidige situatie. Hierbij worden de sterke en zwakke punten vastgesteld.
- Fase 2: Op basis van de huidige situatie de gewenste situatie schetsen.
- Fase 3: Door middel van een prioritering, vaststellen in welke volgorde de verschillende aspecten zullen worden aangepakt.
- Fase 4: De gekozen aspecten vertalen naar concrete actiepunten.
- Fase 5: Het uitvoeren van de actiepunten.
- Fase 6: Het eindresultaat evalueren en uitdragen dan wel uitleren binnen het Centrum voor Biometrie.

Doordat dit project verschillende aspecten bevat die in fase 3 geprioriteerd worden, zullen deze niet allemaal gelijktijdig fase 4 t/m 5 doorlopen. Deze fasen zullen zich herhalen tot alle aspecten behandeld zijn.

Fase 1 tot en met fase 3 zullen in het projectplan verwerkt worden. De voortgang van de uitvoering van de actiepunten zullen door middel van voortgangrapportages gecommuniceerd worden.

Voor dit project wordt een werkgroep samengesteld die bestaat uit inhoudsdeskundigen van het CvB die zich op verschillende plekken binnen het proces bezighouden met de uitvoering van het vak gelaatsherkenning. Deze werkgroep zal om de week bij elkaar komen. Zij zullen met elkaar brainstormen over de gewenste situatie en de te ondernemen actiepunten. Vervolgens zullen de actiepunten verdeeld worden over de groep om hier de komende

twee weken aan te werken. Naast dit project zijn er ook andere projecten gaande, zoals het ontwikkelen van een nieuwe ABIS. Met deze projecten zal een nauwe aansluiting zijn.

Eens per kwartaal komt de stuurgroep bijeen. De stuurgroep bestaat uit:

Senior Suplier NP	Teamchef LFSC	5.1.2.e
Senior Suplier CvB	Team coördinator CvB	5.1.2.e
Senior User	OSD	John Riemen
Projectleider	Operationeel Expert CvB	5.1.2.e

In de stuurgroep wordt de voortgang gepresenteerd, de issues weergegeven met advies en er worden keuzemogelijkheden voorgelegd, met adviezen.

Akkoord

Rol	Functie	Naam	Handtekening
Opdrachtgever	Programmadirecteur FO	5.1.2.e	Datum: Plaats:
Opdrachtnemer	Centrum voor Biometrie	John Riemen	Datum: Plaats:

Beleid

Bewaartermijnen

GEGEVENS AUTORITEIT

VASTGESTELD
document

Inleiding

Bij het uitvoeren van de politietaak en in onze bedrijfsvoering verwerken we gegevens van collega's, verdachten en andere betrokkenen. Deze inbreuk op privacy is onvermijdelijk. Zolang het voor de politietaak of de bedrijfsvoering noodzakelijk is, mogen we deze gegevens verwerken en omgekeerd geldt dus ook; als de noodzaak er niet meer is, stopt de verwerking.

Het zorgvuldig verwijderen en vernietigen van gegevens is dus de uitkomst van een afweging tussen het kunnen uitvoeren van de politietaak en de bedrijfsvoering enerzijds en het borgen van de privacy van collega's, verdachten en andere betrokkenen anderzijds.

Het Uitvoeringskader Privacy & Security by Design (PSbD) beschrijft alle kaders voor de zorgvuldige omgang met gegevens door de politie. Zowel bij het uitvoeren van de politietaak als bij de bedrijfsvoering. Het uitvoeringskader bestaat uit twaalf principes. Principe 8 gaat specifiek over bewaartermijnen:

Gegevens worden niet langer verwerkt dan is toegestaan en worden vernietigd zodra ze niet langer noodzakelijk zijn.

In PSbD wordt toegelicht wat hiermee wordt bedoeld (de rationale);

"De termijnen voor het verwerken, verwijderen en vernietigen zijn gekoppeld aan het doel waarvoor de gegevens verzameld worden en de werkprocessen waarin de gegevens verwerkt worden. Voor de termijn waarbinnen de gegevens bewaard moeten worden, moet de informatievoorziening waarborgen treffen voor duurzame beschikbaarheid en toegankelijkheid. Deze waarborgen worden uitgewerkt in het Normenkader Duurzame Toegankelijkheid van Overheidsinformatie (DUTO). De 'spelregels' voor gegevensbeheer zijn vastgelegd in de Beheerregeling Documentaire Informatie Politie 2017 en de termijnen voor bewaren en vernietigen zijn verzameld in de Generieke Selectielijst voor de Nationale Politie (concept)."[1]

1 Zie p. 61 van het Uitvoeringskader Privacy & Security by Design, versie 2.0

Het principe voor verwijderen en vernietigen van gegevens is dus vrij eenvoudig.

Maar de uitwerking is minder eenvoudig. Zo stelt de Archiefwet 1995 eisen aan de bewaartermijn van overheidsinformatie, maar stellen de Wet politiegegevens (Wpg) en de Algemene Verordening Gegevensbescherming (AVG) eisen aan de termijn van verwijderen en vernietigen van persoonsgegevens. Ook het Wetboek van Strafvordering (Sv) stelt beperkingen bij het verwerken van specifieke politiegegevens.

Om gegevens tijdig te verwijderen en vernietigen moeten we al deze wetten in samenhang overzien. Daarbij zijn veel van de bepalingen 'open' geformuleerd, wat betekent dat we als politie zelf concrete invulling moeten geven aan de bewaartermijn. Dat geeft wat vrijheid maar ook de verantwoordelijkheid het beleid op bewaartermijnen helder op te schrijven en goed te motiveren.

Die verantwoordelijkheid houdt ook in, dat we de politieke realiteit niet uit het oog verliezen bij het daadwerkelijk uitvoeren van dit beleid. Zo heeft de minister van J&V in reactie op de motie van TK lid van Oosten[2] toegezegd cold case informatie vooralsnog niet te vernietigen[3]. Dat houdt voorlopig in dat bepaalde gegevens ook na de bewaartermijn niet worden vernietigd. Voor een analyse van dit besluit en de consequenties verwijzen we naar de Gegevensautoriteit binnen directie IV van politie.

2 kst-35000-VI-37

3 brief van de minister aan de TK in reactie op de moetie van Oosten, kst-29628-859

Doel en doelgroep

In dit beleidskader werken we principe 8 – Bewaren en vernietigen- verder uit. Bijvoorbeeld wordt concreet wanneer termijnen voor verwijderen en vernietigen voor verschillende gegevenssoorten starten en hoe lang ze zijn. We gaan ook in op de begrippen zelf; wat bedoelen we precies met verwerken, wat doen we op systeemniveau als we gegevens verwijderen en wat als we gegevens vernietigen? Door dit uit te werken, stellen we de doelgroep hopelijk in staat de relevante wetsbepalingen, bedrijfsregels, begrippen en bewaartermijnen in samenhang te bezien zodat bij de implementatie daarvan juiste keuzes worden gemaakt. Bijvoorbeeld door grenzen aan gegevensverwerking te stellen in een project of programma. Maar ook indirect, door de bepalingen te vertalen naar requirements voor ontwikkeling van een applicatie of werkproces

Waar dit mogelijk is, verwijzen we naar relevante bestaande kaders, richtlijnen, procedures en werkinstructies.

In het algemene Privacybeleid van de politie zijn wettelijke verplichtingen uitgewerkt in normen. Dit beleidskader moet worden aangemerkt als specifiek beleid ten aanzien van het bewaren van bewaren van persoonsgegevens[1].

Dit document is bedoeld voor:

- Adviseurs op het gebied van (informationele) privacy, waaronder privacyfunctionarissen.
- Programma –en projectmanagers, Senior Business-experts, Product owners en andere betrokkenen bij de ontwikkeling van processen en systemen waarin persoonsgegevens worden verwerkt.
- Functioneel beheerders en andere experts die betrokken zijn bij de inrichting van systemen.
- Lijnmanagers die sturing geven aan de inachtneming van de bewaartermijnen

Beleid

Bewaartermijnen

Inhoud

Hoofdstuk 1: Overzicht van wet- en regelgeving die kaderstellend is voor het bewaren van persoonsgegevens.

Hoofdstuk 2: Begrippen en uit de politiepraktijk waarin we uitleggen wat we met gebruikte termen bedoelen en hoe dit vertaald moet worden naar proces- en systeemontwerp.

Hoofdstuk 3: Concrete bewaartermijnen per categorie van politiegegevens, een afwegingskader voor bewaartermijnen van persoonsgegevens en enkele veelgevraagde beleidsuitspraken over bewaartermijnen.

1. Juridisch kader

In de basis mogen persoonsgegevens niet langer worden verwerkt dan noodzakelijk is voor het doel van de verwerking. De AVG en de Wpg geven echter op een verschillende manier invulling aan dit principe.

In dit hoofdstuk wordt eerst weergegeven met welke aspecten van de AVG rekening moet worden gehouden. Daarna wordt uitgebreider ingegaan op het juridisch kader met betrekking tot het verwijderen en vernietigen van politiegegevens. Dit kader wordt gevormd door verschillende wettelijke bepalingen en uitvoeringsregelingen. Deze hebben enerzijds tot doel de politie te laten beschikken over de persoonsgegevens die nodig zijn voor een goede bedrijfsvoering en uitvoering van de politietaak en anderzijds de persoonlijke levenssfeer van de burger in verband met het vastleggen en verstrekken van persoonsgegevens te beschermen.

Daar waar duiding wordt gegeven aan onderdelen van de AVG, of aan aspe cten die voor zowel de AVG als de Wpg relevant zijn, gebruiken we het begrip ‘persoonsgegeven(s)’. Als specifiek wordt ingegaan op elementen uit de Wpg dan hebben we het over ‘politiegegeven(s)’.

1.1. Algemene Verordening Gegevensbescherming

In de AVG is bepaald hoe de politie moet omgaan met persoonsgegevens. Algemene uitgangspunten daarbij zijn:

- Persoonsgegevens moeten worden bewaard zodanig dat de betrokkene niet langer is te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt
- Persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wo rden verwerkt
- De verwerkingsverantwoordelijke informeert de betrokkene over de periode gedurende welke de gegevens worden opgeslagen of (tenminste) over de criteria ter bepaling van die bewaarter mijn. Organisaties bepalen dus zelf hoe lang zij persoonsgegevens verwerken, rekening houdend met het doel van de verwerking. Daarbij kunnen bewaartermijnen uit meer specifieke wet- en regelgeving overigens leidend zijn, zoals bijvoorbeeld de belastingwetgeving
- Ook hebben betrokkenen het recht op gegevenswissing, bijvoorbeeld wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of de betrokkene zijn of haar toestemming intrekt.

Voor zover persoonsgegevens binnen de politieorganisatie worden verwerkt op grond van de AVG, vooral in de bedrijfsvoering en als het gaat om vreemdelingenzaken en de korpscheftaken, moet dus voorafgaand aan de verwerking bepaald worden binnen welke beoogde termijn de gegevens worden gewist. De verantwoordelijke bepaalt en motiveert de bewaartermijn en dit moet vervolgens zijn beslag krijgen in applicaties en werkprocessen. Daarnaast speelt het onderwerp bewaartermijnen, in het kader van transparantie en verantwoording, een belangrijk rol in het privacystatement (actieve informatieplicht), bij het verwerkingsregister en desgevraagd bij verzoeken om inzage of wissing.

1.2. Wet en Besluit politiegegevens

In de Wpg en het Besluit politiegegevens (Bpg) is bepaald hoe de politie moet omgaan met politiegegevens. Algemene uitgangspunten daarbij zijn:

- Politiegegevens worden slechts verwerkt voor zover ze noodzakelijk zijn voor in de Wpg beschreven doeleinden.
- Politiegegevens worden uitsluitend voor een ander doel verwerkt voor zover de Wpg daar uitdrukkelijk in voorziet, de verwerking niet onverenigbaar is met het doel waarvoor ze zijn verkregen en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.
- De nodige maatregelen worden getroffen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.

Ter invulling van het eerste uitgangspunt zijn in de Wpg de volgende doelen voor de verwerking van politiegegevens bepaald:

- Politiegegevens voor uitvoering van de dagelijkse politietaak (artikel 8);
- Politiegegevens voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9);
- Politiegegevens voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10);
- Politiegegevens voor controle en beheer van informanten (artikel 12), en
- Politiegegevens voor ondersteunende taken (artikel 13).

Het doel is dus bepalend voor de wijze waarop politiegegevens mogen worden gebruikt en onder welke voorwaarden en op welk moment de gegevens verwijderd of direct vernietigd moeten worden. Deze termijnen worden bepaald in de hierboven genoemde wetsartikelen en staan ook in hoofdstuk 4 (Bewaartermijnen) van dit document genoemd.

In het algemeen geldt dat gedurende de gehele verwerkingsperiode beoordeeld moet worden of de gegevens voor een andere doel verder verwerkt kunnen worden.

1.3. Wetboek van Strafrecht (Sr)

De Wpg stelt dus belangrijke voorwaarden aan het verwerken van politiegegevens, maar staat die verwerking toe zolang er een verwerkingsgrond bestaat. Om te kunnen bepalen of dit nog het geval is, moet ook naar het Wetboek van Strafrecht (Sr) gekeken worden. Politiegegevens kunnen immers nog noodzakelijk zijn totdat de onderliggende zaak onherroepelijk is geworden. Als de zaak niet is opgelost en ook niet is ingezonden naar het OM, dan wordt het onderzoek weliswaar voortgezet, maar vaak op een minder intensief niveau. De gegevens moeten beschikbaar blijven voor het geval er nieuwe aanknopingspunten zijn. Verwerking van de politiegegevens blijft dan noodzakelijk tot uiterlijk het moment dat de feiten waarop het onderzoek zich richt verjaard zijn. De verjaringstermijnen zijn beschreven in artikel 70 Sr.

1.4. Wetboek van Strafvordering (Sv)

Zoals vermeld moeten politiegegevens worden verwijderd of vernietigd zodra dit door enige wettelijke bepaling wordt vereist[2]. Dergelijke bepalingen zijn onder andere te vinden in Sv in het kader van bijzondere opsporingsbevoegdheden.

Zo worden termijnen gesteld in verband met de bewaring en vernietiging van processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door bijvoorbeeld het opnemen van vertrouwelijke communicatie (tappen) of de vordering van telecommunicatiegegevens, voor zover die niet bij de processtukken zijn gevoegd[3]. Maar ook ten aanzien van processen-verbaal of andere voorwerpen die mededelingen van geheimhouders bevatten[4] en ten aanzien van gegevens die zijn vastgelegd tijdens een doorzoeking en die van geen betekenis zijn voor het onderzoek[5].

Hier wordt dus een belangrijke beperking gesteld aan het verwerken van politiegegevens gedurende het onderzoek. Gegevens die niet (meer) nodig zijn voor dat onderzoek moeten eerder worden vernietigd.

Ook in het kader van de identiteitsvaststelling van verdachten, veroordeelden en getuigen, het bewaren van kentekengegevens en het bewaren van auditieve en audiovisuele registraties worden specifieke bewaartermijnen gesteld.

2 artikel 4, lid 2 Wpg
3 artikel 126cc en artikel 126dd Sv
4 artikel 126aa Sv
5 artikel 126nn Sv

1.4.1. Besluit bewaren en vernietigen niet-gevoegde stukken

In dit besluit worden nadere voorschriften gegeven omtrent de wijze waarop de processen-verbaal en andere voorwerpen[6] worden bewaard en vernietigd. Zo dient de officier van justitie een bevel tot vernietiging af te geven en wordt uiteengezet wat onder ‘vernietiging’ wordt verstaan.

1.4.2. Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen

Om er zeker van te zijn dat een verdachte is wie hij zegt te zijn, moet de opsporingsambtenaar de identiteit van de verdachte vaststellen[7]. De foto’s en vingerafdrukken worden weliswaar afgenomen in het kader van de uitvoering van de politietaak en vallen daarmee onder de werking van de Wpg, maar voor wat betreft de verdere verwerking van die gegevens, zoals de bewaartermijnen, is Sv[8] en het Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen leidend.

1.4.3. Besluit tot vaststelling van nadere regels voor het vastleggen en bewaren van kentekengegevens op grond van artikel 126jj van het Wetboek van Strafvordering door de politie

In dit besluit worden nadere voorschriften gegeven omtrent de wijze waarop ANPR-gegevens (hits) aangewend mogen worden voor een onderzoek. Voor het overige moeten de gegevens vier weken na vastlegging worden vernietigd.[9]

1.4.4. Aanwijzing auditief en audiovisueel registreren van verhoren van aangevers, getuigen en verdachten

In het belang van de waarheidsvinding is het wenselijk dat in bepaalde gevallen aangiften en/of verhoren auditief of audiovisueel worden opgenomen. In genoemde aanwijzing en het bijbehorende protocol wordt niet alleen voorgeschreven in welke gevallen dit nodig is, maar ook hoe lang de registraties bewaard mogen worden en op welke wijze ze vernietigd moeten worden.

6 zoals bedoeld in artikel 126cc Sv

7 artikel 27a en 55c Sv

8 artikelen 27b en 55c Sv

9 artikel 126jj, lid 2 Sv en artikel 9, lid 5 van het AN-PR-besluit

1.5. Wet en besluit justitiële en strafvorderlijke gegevens

Deze wet regelt de verwerking van justitiële gegevens, strafvorderlijke gegevens en persoonsdossiers bij onder andere de Justitiële Informatiedienst en de arrondissementsparketten. De Wet en het Besluit justitiële en strafvorderlijke gegevens (Wjsg en Bjsg) spelen in eerste instantie dan ook geen rol bij het vraagstuk van verwijderen en vernietigen van politiegegevens. Indirect zijn een paar bepalingen uit het Bjsg echter wel relevant omdat zij de grondslag vormen voor de verstrekking van zogenaamde afloopberichten.

Politiegegevens die in het kader van een (omvangrijk) strafrechtelijk onderzoek worden verwerkt[10], moeten worden verwijderd indien zij niet langer noodzakelijk zijn voor het doel van het onderzoek. Dat zal vaak het geval zijn nadat de zaak onherroepelijk is geworden. In het Bjsg is geregeld [11]dat justitiële gegevens kunnen worden verstrekt aan de politie om te kunnen voldoen aan de naleving van de verplichting uit de Wpg om politiegegevens te verwijderen/vernietigen indien deze niet meer noodzakelijk zijn voor de uitvoering van de politietaak. Deze gegevens worden verstrekt in de vorm van afloopberichten

10 artikel 9 Wpg

11 artikel 11b

1.6. Archiefwet 1995

De gegevens die politie verwerkt vallen vanaf het moment van vastlegging zowel onder de werking van de AVG of Wpg als onder die van de Archiefwet 1995 (Archiefwet). De Archiefwet verplicht overheidsorganen om overheidsinformatie in goede, geordende en toegankelijk staat te brengen en te bewaren. Met de term overheidsinformatie worden alle informatieobjecten bedoeld, dus documenten, beeld- en/of geluidsmateriaal, informatie van websites of apps, e-mails etc., die door de politie wordt opgemaakt of ontvangen.

De Archiefwet vereist dat overheidsorganen een selectielijst opstellen aan de hand waarvan wordt bepaald welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven.
De politie heeft de vernietigingstermijnen in de selectielijst in overeenstemming gebracht met de eerdergenoemde bewaartermijnen uit de Wpg en Sr.

2. Definities en bedrijfsregels

In het juridisch kader hierboven zijn wetten en bepalingen genoemd waarin de verplichting tot bewaren, verwijderen en vernietigen is vastgelegd. Om een praktische vertaling naar werkprocessen en applicaties te maken, gebruiken we bedrijfsregels. Daarvan zijn er al veel beschreven in het document Wpg Begrippen Definities Bedrijfsobjecten[12]. De regels in dit document zijn daarop een toevoeging of aanscherping.

- De bedrijfsregels over 'verwerken' (3.1 tot 3.3) zijn bedoeld om technische invulling te geven aan de verschillende verwerkingen. Met andere woorden: wat doen we op applicatieniveau en gegevensbeheerniveau als we spreken over archiveren, verwerken, of bijvoorbeeld wissen?
- Bij de bedrijfsregels voor datamanagement (3.4) gaan we in op een aantal beheerprocessen zoals logging en het maken van backups. Om de bewaartermijn van dit soort gegevens te weten moeten we eerst vaststellen onder welke bepalingen deze verwerkingen vallen;
- De bedrijfsregels over statussen van politieonderzoeken (3.5) ondersteunen die bepalingen in de wet waarin het 'doel van een verwerking' een rol speelt. Het doel van de verwerking is in veel gevallen het onderzoek, en afhankelijk van de status van dat onderzoek is het doel bereikt en gaat de termijn voor verwijderen en vernietigen lopen.

12 Zie de agorasite van de sector GGB: https://agora.portal.politie.local/sites/ggb/Termen%20en%20definities/Termen%20en%20definities.aspx

FIGUUR: VERWERKEN VAN GEGEVENS: VERDER VERWERKEN, VERWIJDEREN, HERNIEUWD VERWERKEN, VERNIETIGEN

2.1. Verwerken

De AVG en de Wpg hanteren vrijwel dezelfde definitie van het begrip verwerken. Het verwerken van gegevens omvat het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen, verwijderen of vernietigen van persoonsgegevens. Kortom alles wat je met gegevens kan doen vanaf het moment van ontstaan tot het moment van vernietiging óf – in uitzonderlijke gevallen- bij overbrenging naar een archiefbewaarplaats

2.1.1. Verder Verwerken (Wpg / AVG)

De Wpg en de AVG kennen de term **verder verwerken** voor een verwerking van persoonsgegevens voor een ander doel dan het oorspronkelijke doel.

2.1.2. Hernieuwd Verwerken (Wpg)

Het onder specifieke voorwaarden beschikbaar stellen aan de operatie van reeds verwijdere politiegegevens. Zie ook verwijderen.

2.1.3. Archiveren (Archiefwet)

Archiveren is het zorgdragen voor goed beheer van overheidsinformatie vanaf moment van ontvangst of creatie tot het moment van vernietiging of overbrenging. Wat onder overheidsinformatie valt, wordt niet bepaald door de vorm van de informatie, maar door het ontstaan en gebruik ervan. Bij overheidsinformatie gaat het niet alleen om tekstdocumenten, zoals notities en verslagen. Maar bijvoorbeeld ook om databasegegevens, ingevulde formulieren, foto's, video's, websites en Tweets.

De activiteit 'archiveren' is dus dermate breed dat we liever spreken van (informatie)beheer als parallelle activiteit ter uitvoering van de Archiefwet.

Archiveren eindigt ook, zie hiervoor § 3.3.3 ***Overdragen (Archiefwet)*** hieronder.

2.2. Beperken van de verwerking

2.2.1. Verwijderen (Wpg)

Onder **verwijderen** verstaan we het buiten de operationele verwerking plaatsen van politiegegevens. Verwijderen is dus een privacybevorderende maatregel, namelijk door het beperken van de toegang. Verwijderde gegevens zijn nog wel beschikbaar, maar alleen voor functioneel beheerders en de zogenoemde poortwachter[13] voor het doel van een artikel 9-verwerking of een artikel 10-verwerking. In dat geval spreken we van hernieuwd verwerken (§ 2.1.2 2.1.2)

2.2.2. Pseudonimiseren

Onder pseudonimiseren verstaan we het vervangen van de identificerende gegevens uit een bestand met een zogenaamd pseudoniem. De gepseudonimiseerde data worden los van de identificerende gegevens en bijbehorend pseudoniem beheerd. Pseudonimiseren is dus een privacybevorderende maatregel, namelijk door het beperken van de herleidbaarheid. Deze beperking van de herleidbaarheid is per definitie niet volledig, doordat de datasets in combinatie weer herleidbaar zijn naar personen[14]. Bovendien kunnen gepseudonimiseerde bestanden in combinatie met andere bestanden worden verwerkt, zodat de herleidbaarheid weer toeneemt.

Er zijn ook vormen van pseudonimisering, zoals cryptografische hashing, waarbij de herleidbaarheid naar persoonsgegevens nihil mag worden verondersteld. Deze hashing dient te voldoen aan specifieke voorwaarden. De Rijksoverheid heeft een meer praktische handreiking pseudonomisering beschikbaar gesteld met instructies voor pseudonimisering van persoonsgegevens.[15]

2.2.3. Verwerkingsbeperking (AVG en Wpg)

De AVG en de Wpg bieden beide de mogelijkheid van verwerkingsbeperking16, door opgeslagen gegevens te markeren met als doel de verwerking ervan in de toekomst te beperken, bijvoorbeeld omdat de juistheid daarvan door de betrokkene wordt betwist en dit geverifieerd moet worden.

In de Wpg wordt dit ook wel aangeduid met het begrip afschermen. Naast de eerder genoemde betwiste (on)juistheid moet gedacht worden aan situaties waarbij vernietiging niet aan de orde kan zijn omdat de gegevens moeten worden bewaard als bewijsmateriaal.

Het beperken van de verwerking geldt voor alle gebruikers. Als de toegang tot specifieke verwerkingen van bepaalde gegevens (inzien, wijzigen, etc.) voor bepaalde personen of groepen van personen wordt beperkt, wordt autorisatie toegepast. Hier kunnen overwegingen van bijvoorbeeld tactische aard of van veiligheid van betrokkenen aan ten grondslag liggen. Dit zijn dan echter geen beperkingen van de verwerking in de zin van de AVG of Wpg. De kaders voor het instellen van autorisaties voor het in beslotenheid verwerken van gegevens zijn uitgewerkt in het autorisatiebeleid[17].

13 De functionaris die namens de operatie beoordeelt of aan specifieke voorwaarden is voldaan om de gegevens opnieuw beschikbaar te stellen

14 Zie ook “2.2.3. Verwerkingsbeperking (AVG en Wpg)” on page 12

15 https://www.rijksoverheid.nl/documenten/richtlijnen/2018/02/15/stroomschema-pseudonimisering-avg

16 Artikel 18 van de AVG en artikel 28 van de Wpg

17 Agora, autorisatiebeleid politie 2016 – 2020 (link)

2.2.4. Rectificeren (AVG en Wpg)

Onder **rectificeren** verstaan we het aanvullen van onjuiste of onvolledige gegevens met gegevens die wel juist of volledig zijn. Het resultaat daarvan zijn de gerectificeerde gegevens. Het effect van rectificeren is dus tweeledig

- Bij het opvragen van de actuele gegevens worden de gerectificeerde gegevens getoond;
- Bij het opvragen van gegevens uit de periode vóór de rectificatie worden de oorspronkelijke gegevens getoond. Gegevens uit het verleden gaan dus niet verloren.

2.3. Beëindigen van de verwerking

2.3.1. Vernietigen (Wpg) en Wissen (AVG)

Onder vernietigen verstaan we het onherstelbaar wissen van persoonsgegevens. In de AVG wordt het begrip wissen gehanteerd, in de Wpg wordt het begrip vernietigen aangehouden. Wissen en vernietigen hebben totale werking, ook naar registraties in het verleden. (Vergelijk rectificatie hierboven).

Voor de technische invulling van vernietigen c.q. wissen wordt aangesloten bij de procedure Noodvernietiging fysieke en digitaal. Daarin wordt het begrip praktisch ingevuld als het ‘zodanig verminken van de informatiedragers (…) dat de vastgelegde content niet meer de toegankelijk en beschikbaar is. Uitgangspunt vormen daarbij de normen voor vernietiging van gerubriceerde informatie zoals vastgelegd in de DIN 66399 (2012-10).’

2.3.2. Anonimiseren

Onder anonimiseren verstaan we het vernietigen of wissen van identificerende gegevens uit een bestand. De geanonimiseerde data zijn daarmee niet meer herleidbaar tot personen en daarmee is anonimiseren een privacybevorderende maatregel. Geanonimiseerde gegevens vallen niet onder de werking van de AVG of Wpg.

De vraag is of de herleidbaarheid in praktijk is uit te sluiten. Een willekeurige geanonimiseerde dataset die tot op detailniveau van personen iets registreert, is op zichzelf anoniem maar bevat per definitie een aanknopingspunt om met andere datasets te combineren. Het in combinatie verwerken van grote op het oog willekeurige gedetailleerde data, is zelfs de kern van big data.

Met de publieke beschikbaarheid van grote hoeveelheden persoonsgegevens, krachtige big data algoritmes en rekenkracht zijn data die verondersteld waren anoniem te zijn, keer op keer toch herleidbaar tot personen gebleken.

2.3.3. Overdragen (Archiefwet)

Overheidsinformatie die blijvend bewaard moet worden als onderdeel van cultureel erfgoed moet na twintig jaar[18] worden overgedragen naar een archiefbewaarplaats. Het overdragen kan met goedkeuring van de minister van Cultuur worden opgeschort. Na het overdragen van de originele archiefbescheiden/informatie-objecten wijzigt;

- Ligt het zorgdragerschap (eigendom) voor die archieven niet meer bij Politie maar bij de minister voor Cultuur. (OCW)
- Het regime voor openbaarheid van de Wet openbaarheid bestuur (de Wob) in de Archiefwet. Overgedragen overheidsinformatie is dus niet meer op te vragen met een beroep op de Wob.

De zorgdrager kan voor een bepaalde termijn beperkingen aan de openbaarheid stellen, om redenen van privacy of veiligheid van de staat, zijn bondgenoten, of ter voorkoming van onevenredige benadeling of bevoordeling van betrokkenen of derden. Redenen die bij politiegegevens vaak aan de orde zullen zijn.

Na het overdragen moeten de duplicaten of werkkopieën van de overgebrachte archiefbescheiden worden vernietigd[19].

18 Er is een aanpassing van de Archief wet voorzien waarin deze termijn van 20 jaar wordt teruggebracht naar 10 jaar

19 Bron: https://www.nationaalarchief.nl/archiveren/kennisbank/overbrenging

2.4. Bedrijfsregels datamanagement

2.3.4. Vervreemding (Archiefwet)

Vervreemding is de overdracht van eigendom door de zorgdrager van het archief aan een andere zorgdrager of een natuurlijk of rechtspersoon van archiefbescheiden. Hiervoor is toestemming nodig van de Minister van Cultuur (OCW).[20]

Onder overdracht verstaan we de faseverandering van dynamisch archief (waarbij de lijn verantwoordelijk is voor het beheer) naar semi-statisch archief (waarin DIV het beheer overneemt).

In bepaalde gevallen is overbrenging naar het rijksarchief aan de orde, in plaats van vernietigen (Wpg) of wissen (AVG). Dat is bij informatie die van waarde is als bestanddeel van cultureel erfgoed of voor historische onderzoek.

20 Archiefwet 1995, artikel 8

2.4.1. Productiedata voor testen en opleiden

Bij het verwerken van productiedata voor testen en opleiden worden gegevens uit een geautomatiseerd systeem gedupliceerd met als doel deze in een testomgeving[21] te gebruiken voor het testen van een geautomatiseerd systeem of gebruik in een opleidingsomgeving.

De testdata en opleidingsdata zijn een ‘afslag’ (duplicaat) van productiedata en worden eventueel nabewerkt om geschikt te zijn voor specifieke toepassing. De gegevens worden van het moment van de afslag niet meer actueel gehouden; verwerkingen op het productiesysteem worden niet uitgevoerd op deze gedupliceerde gegevens. De verwerking van productiedata voor testen en opleiden valt onder de AVG, voor zover het persoonsgegevens betreffen.

Verwerken van productiedata voor testen en opleiden onder de AVG is wegens de gevoelgheid alleen mogelijk met instemming (ontheffing) van de dienst IM[22]. Het is ook mogelijk data voor testen en opleiden uit willekeurige gegevens op te bouwen, of op basis van geanonimiseerde productiedata (zie 2.3.2 2.3.2). In dat geval valt de verwerking niet onder de AVG of Wpg. De bewaartermijn dient door de verwerkingsverantwoordelijke te worden vastgesteld.

21 OTAP, omgeving voor ontwikkelen, testen, acceptatie en in productie brengen

22 Hoofd GGB namens deze, zoals besproken in afstemmingsoverleg DirIV, IM en ICT 16 oktober 2019

2.4.2. Trainingsdata voor slimme algoritmen (Wpg)

Bij het verwerken van politiegegevens voor het trainen van slimme algoritmen worden politiegegevens uit een geautomatiseerd systeem gedupliceerd met als doel de routines van een geautomatiseerd systeem (door te) ontwikkelen. Ook hier worden de gegevens vanaf het moment van dupliceren niet meer actueel gehouden. Net als bij productiedata voor testen en opleiden is het trainen van slimme algoritmes met trainingsdata een verwerking onder de AVG. De bewaartermijn dient door de verwerkingsverantwoordelijke te worden vastgesteld.

2.4.3. Gegevensbackup

Het maken van een (gegevens-) backup is het regelmatig[23] dupliceren van (persoons)gegevens, met als doel de beschikbaarheid ervan te borgen en te bevorderen. Die beschikbaarheid kan worden bedreigd door bijvoorbeeld een calamiteit (brand, water, diefstal) maar ook door onzorgvuldige of moedwillig onjuiste bewerking. De back-up is door tussenkomst van een applicatiebeheerder beschikbaar voor de eindgebruiker.

Het maken van een backup dient dus hetzelfde doel als de oorspronkelijke verwerking onder de AVG of de Wpg. De bewaartermijn van de oorspronkelijke verwerking loopt in feite door in de backup.

23 De frequentie van het maken van een back-up is doorgaans een aantal maal per dag tot elke maand, maar andere frequenties zijn niet ongewoon

2.4.4. Redundante gegevensopslag

Een redundante gegevensopslag is een duplicaat van (persoons)gegevens dat voortdurend[24] gelijk (synchroon) wordt gehouden met de oorspronkelijke gegevens. Elke verwerking van het gegeven wordt zonder tussenkomst van de gebruiker ook uitgevoerd op de duplicaten, waarmee de gebruiker ervaart dat het gegeven maar één keer in het geautomatiseerde systeem voorkomt. Bij bijvoorbeeld beperkte bandbreedte of beperkte toegang tot gegevensdragers neemt daarmee de gemiddelde beschikbaar of de betrouwbaarheid van het systeem toe.

Het doel van de redundante opslag is dus beschikbaarheid of betrouwbaarheid van de dienstverlening. De verwerking van persoonsgegevens in een configuratie met redundante opslag heeft directe werking op alle duplicaten in de opslag en is dus een verwerking voor het oorspronkelijke doel. De bewaartermijn is daarmee die van de oorspronkelijke verwerking.

24 De frequentie van synchronisatie van gegevens en redundante opslag varieert van milliseconden tot een dag, maar andere frequenties zijn niet ongewoon.

2.4.5. Logging

Logging is het registreren van verwerkingen van gegevens in een geautomatiseerd systeem.
De Wpg stelt logging verplicht voor bepaalde verwerkingen op persoonsgegevens, als één van de maatregelen;

- om de rechtmatigheid van de verwerking van persoonsgegevens te waarborgen
- voor het uitvoeren van interne controles
- ter waarborging van de integriteit en de beveiliging van de politiegegevens
- voor strafrechtelijke procedures.

De AVG stelt logging niet verplicht. De verwerking van logginggegevens heeft tot doel om de redenen voor handelingen als raadplegen, wijzigen etc. (op basis van de Wpg of AVG) te kunnen vaststellen. De loggingsgegevens zelf zijn daarmee persoonsgegevens in de zin van de AVG, indien de gegevens tot personen herleidbaar zijn. De verplichting tot logging, evenals de bewaartermijn van loggingsgegevens, is voor de politie uitgewerkt in het beleidskader logging[25].

25 Agora; Beleidskader logging (link)

2.4.6. Documentatie

Documentatie is het schriftelijk vastleggen van bepaalde gegevensverwerkingen met als doel daar verantwoording over af te kunnen leggen. De Wpg kent een documentatieplicht [26] tot vastleggen van de volgende gegevens;

- de doelen van onderzoeken bedoeld in artikel 9, lid 2 Wpg
- de verstrekking of doorgifte van politiegegevens;
- de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing op een verzoek in het kader van rechten van betrokkene;
- een inbreuk op de beveiliging van persoonsgegevens, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.

De privacyfunctionaris kan aan de hand van deze gegevens toezicht houden. Deze gegevens zijn gegevens in de zin van de Wpg en moeten bewaard blijven tot ten minste de datum waarop de laatste controle/audit heeft plaatsgevonden.[27]

26 Artikel 32 lid 1 Wpg

27 Artikel 32, lid 4 Wpg

2.5. Bedrijfsregels politieonderzoeken (artikel 9 Wpg)

Termijnen voor het verwerken van gegevens hebben een startmoment in het operationele proces. Deze momenten zijn te vinden in de bedrijfsregels rondom de start en eventuele verjaring van een delict en van het openen en sluiten van onderzoeken. In dit beleid op bewaartermijnen worden volledigheidshalve de relevante bedrijfsregels toegelicht[28].

2.5.1. Pleegdatum / datum feit

Datum waarop het vermeende feit volgens het PV is gepleegd. De termijn voor verjaring van het feit start in beginsel een dag na de pleegdatum.[29] De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval eindigt bij verjaring[30].

2.5.2. Voltooid onderzoek

Een onderzoek is voltooid als het operationele politie onderzoek is afgesloten, het onderzoeksdoel is behaald en de dossiers van alle verdachten, inclusief dat van de intellectuele dader, zijn overgedragen aan het OM. Het voortduren van de grond voor de verwerking is nader uitgewerkt in par 4.4 (Politiegegevens voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9)) op pagina 23.

28 Voor de statussen van artikel 9 onderzoeken wordt verwezen naar het document Beëindigen artikel9 onderzoeken (versie 26.06.2018) van de werkgroep Summit.

29 Let op: in artikel 71 Sr worden enkele uitzonderingen genoemd waarbij de termijn op een ander moment start.

30 Zie voor de verjaringstermijnen paragraaf 3.4.1 Verwijderen op pagina 22 e.v.

2.5.3. Gestaakt onderzoek

Beëindigd onderzoek omdat zich geen strafbaar feit heeft voorgedaan. De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval eindigt.

2.5.4. Opgeschort onderzoek

Onderzoek waarbij het onderzoeksdoel niet (volledig) is behaald. Niet alles is ingezonden en het betreft geen cold case. De grond voor verwerking voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval blijft bestaan.

2.5.5. Cold case

Een opgeschort (of lopend) onderzoek dat door het bevoegd gezag de status cold case heeft gekregen. De grond voor verwerking voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval blijft bestaan.

2.5.6. Overzicht

Schematisch zien de statussen onderzoek en de relatie met het beheerproces er als volgt uit;

Statussen onderzoek van Politie als trigger voor het privacy beheerproces (bron werkgroep SUMMIT 26.06.2018)

3. Bewaartermijnen

3.1. Overheidsinformatie (Archiefwet)

De Archiefwet verplicht de politie om overheidsinformatie in goede, geordende en toegankelijk staat te brengen en te bewaren. Dat geldt voor alle informatie, ook voor persoons- en politiegegevens. Van vernietiging[31] wordt daarom afgezien als de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden na 20 jaar overgebracht naar een archiefbewaarplaats. Daarbij worden beperkingen aan de openbaarheid gesteld en zijn de gegevens niet meer (zonder vordering) voor operationele doeleinden beschikbaar.

De politie heeft een selectielijst [32]opgesteld aan de hand waarvan wordt bepaald welke gegevens na hoeveel tijd vernietigd worden en welke gegevens bewaard blijven. De vernietigingstermijnen van politiegegevens komen in de selectielijst overeen met bewaartermijnen uit de Wpg en Sv. Daarmee is geborgd dat we met de uitvoering van het selectiebeleid zowel de Archiefwet uitvoeren, als de Wpg.

De bewaartermijnen voor overige gegevens vinden hun grondslag in van toepassing zijnde wetgeving, bijvoorbeeld fiscaal recht, of op basis van belangenafweging (belang van de bescherming van de persoonlijke levenssfeer versus belang taakuitvoering, belang voor verantwoording, belang cultureel erfgoed etc.).

De plicht tot het bewaren van persoonsgegevens op basis van de Archiefwet 1995 is een andere dan het bewaren van persoonsgegevens voor eigen verwerkingsdoeleinden. De verwerkingsverantwoordelijke komt pas aan de plichten van de Archiefwet 1995 toe, wanneer de gegevens reeds in overeenstemming met de AVG worden verwerkt (zie onder IV. en de uitspraak van de Raad van State 23 augustus 2017 onder V).

31 Artikel 14, lid 1 Wpg.

32 De selectielijst staat op agora (link)

3.2. Bedrijfsvoeringsgegevens (AVG)

De AVG verplicht de verwerkingsverantwoordelijken na te gaan of ze gehouden zijn aan wettelijke vastgestelde termijnen. Wanneer er geen wettelijk vastgestelde termijn is, dient de verwerkingsverantwoordelijke de termijn zelf vast te stellen. Daarbij bieden de vragen die gesteld worden bij een GEB goede aanknopingspunten voor een zorgvuldige motivering van de bewaartermijnen. Daarnaast is door het ministerie van J&V een stappenplan voor het beschrijven van bewaartermijnen opgesteld. [33]

3.2.1. **Bewaartermijn bij wet voorgeschreven**

Bekijk welke wetgeving op de gegevensverwerking van toepassing is, en of er bij of krachtens die betreffende wet een bewaartermijn is vastgesteld.

Voor fiscale gegevens is de bewaarplicht bijvoorbeeld op 7 jaar vastgesteld[34] en voor medische gegevens in principe 15 jaar[35].

3.2.2. Verwerkingsverantwoordelijke bepaalt bewaartermijn

Indien er geen wettelijke bewaartermijn voor de gegevensverwerking is vastgesteld, dan moet de verwerkingsverantwoordelijke de bewaartermijn bepalen. Dit kan aan de hand van de vragen in het schema op de volgende pagina.

33 2 november 2018 | Bewaartermijn persoonsgegevens in de AVG, F. Makhloufi V.D.W. van Dijk, Justid (voorbeelden aangepast)

34 artikel 52, lid 4, Awr

35 artikel 7:454 BW

Wat zijn de doeleinden van de gegevensverwerking?	Aan de hand van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden bepaalt de verwerkingsverantwoordelijke hoe lang het noodzakelijk is de persoonsgegevens te bewaren[1].
Wanneer is dit doel bereikt?	Bepaal wanneer het niet meer nodig is de gegevens langer te bewaren. Bijvoorbeeld bij de beëindiging van een dienstverband of de afhandeling van een klacht.
Wat is de aard van de gegevens?	Bij het bepalen van de bewaartermijn houdt de verwerkingsverantwoordelijke rekening met de aard van de gegevens; hoe gevoeliger de gegevens, hoe minder snel een lange bewaartermijn te rechtvaardigen is. Houd er rekening mee dat voor het bewaren van bijzondere persoonsgegevens en strafrechtelijke gegevens er hogere eisen gelden voor de beveiliging, bijvoorbeeld door middel van versleuteling of beperking van de toegang[2].
Welke gegevens zijn noodzakelijk om te verwerken[3]?	Alleen gegevens die strikt noodzakelijk zijn voor het doel mogen worden verwerkt. Na verloop van tijd moet gekeken worden of (alle) vastgelegde gegevens nog wel nodig zijn voor de doeleinden van de gegevensverwerking.
Wat is een redelijke (gepaste) bewaartermijn?	Ga na, gelet op het doel van de verwerking en de aard van de gegevens, wat een redelijke termijn is en let er daarbij op dat de gegevens door tijdsverloop hun relevantie of geldigheid kunnen verliezen.

1 artikel 5 lid 1 onderdeel b AVG

2 Zie verder artikel 32 AVG

3 artikel 5 lid 1 sub c AVG: minimale gegevensverwerking

BRON: Justid- Bewaartermijn persoonsgegevens in de AVG [35]

3.3. Politiegegevens voor uitvoering van de dagelijkse politietaak (artikel 8)

Voor politiegegevens die worden verwerkt bij de uitvoering van de dagelijkse politietaak zijn termijnen voor verwijdering en vernietiging in artikel 8 van de Wpg bepaald. Het gaat om gegevens die worden verwerkt in het kader van de basispolitiezorg. De werkzaamheden bestaan uit surveillance, afhandeling van verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels. Onder eenvoudige recherchewerkzaamheden wordt verstaan het onderzoeken van diefstallen en inbraken, het veilig stellen van sporen en het opnemen van een aangifte van een inbraak (VVC-zaken). Eerste hulp wordt bijvoorbeeld verleend als een persoon met een psychose op straat rondzwerft. In het kader van het handhaven van wetten en regels wordt bijvoorbeeld de algemene plaatselijke verordening gehandhaafd en de Wet op de economische delicten, waarin overtreding van bepalingen uit onder meer milieuwetten strafbaar zijn gesteld.

In geval van VVC-zaken bepaalt de politie (al dan niet in afstemming met OM) of een zaak wordt opgepakt en beslist (al dan niet in afstemming met OM) over vroegtijdig beëindigen van een zaak zonder geïdentificeerde verdachte. Het OM geeft een kader voor het oppakken en beëindigen en beslist over vervolging en sepot (bij zaak met geïdentificeerde verdachte).[36]

Uitgangspunt is dat gegevens voor elke geautoriseerde vijf jaar beschikbaar zijn. De toegang beperken tot gegevens ouder dan ***één*** jaar wordt alleen rol-gebaseerd gedaan voor landelijk vastgestelde gebruikersgroepen. Vooralsnog zijn er geen groepen geselecteerd.**Verwijderen**

In ieder geval vijf jaar na de datum van de eerste verwerking (artikel 8, lid 6 Wpg).

3.3.1. Vernietigen

- Zodra ze niet meer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak (artikel 8, lid 6 Wpg).
- Verwijderde gegevens worden gedurende vijf jaar bewaard en vervolgens vernietigd (artikel 14, lid 1 Wpg).
- Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats (artikel 14, lid 4 Wpg).
- Gegevens die zijn verkregen op grond van gemeentelijk cameratoezicht[37] worden na ten hoogste vier weken vernietigd, tenzij er concrete aanleiding bestaat te vermoeden dat die gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit en daartoe verder worden verwerkt.
- Gegevens die zijn verkregen met behulp van ANPR-camera's worden uiterlijk na vier weken vernietigd, tenzij de gegevens overeenkomstig art. 126jj Sv verder mogen worden verwerkt.

36 Aanwijzing voor de opsporing

37 Artikel 151c, lid 9 Gemeentewet

3.4. Politiegegevens voor onderzoek in verband met de handhaving van de rechtsor de in een bepaald geval (artikel 9)

Voor politiegegevens die worden verwerkt voor onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval zijn termijnen voor verwijdering en vernietiging in artikel 9 van de Wpg bepaald.

Dat is het geval wanneer extra inspanningen worden geleverd om gericht omvangrijke hoeveelheden gegevens te vergaren ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval. De term 'gericht' heeft betrekking op de verwerking van grote hoeveelheden gegevens met betrekking tot bepaalde personen. Behalve in geval van opsporingsonderzoeken zal dit ook het geval zijn bij gegevens die worden verwerkt in het kader van een veelplegerdossier of een Staf Grootschalig Bijzonder Optreden (SGBO), zoals grote demonstraties, ontruimingen, Koningsdag, de Sinterklaasintocht en andere grootschalige evenementen. Er is in elk geval sprake van gerichte verwerking in de zin van artikel 9 zodra een rechercheonderzoek is aangemeld, een verkennend onderzoek wordt gestart en zodra bijzondere opsporingsmethoden worden ingezet, zoals stelselmatige observatie en het afluisteren van telecommunicatie. In zulke gevallen gaat het immers om een omvangrijke gegevensverwerking over personen, ten aanzien van wie de precieze betrokkenheid bij de te onderzoeken strafbare feiten nog niet vast staat.

3.4.1. Verwijderen

- Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van het onderzoek;
- Of na verloop van een periode van maximaal een half jaar waarin ze verwerkt worden teneinde te bezien of ze aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 (artikel 9, lid 4 Wpg).

In geval van HIC/ondermijnende criminaliteit gaat de politie over tot een opsporingsonderzoek. Het OM heeft het gezag over de opsporing. Het OM beslist over duur en wijze van de opsporing en (mogelijke) beëindiging van de opsporing, in samenspraak met de politie. Tevens beslist het OM over al dan niet vervolging van de geïdentificeerde verdachte.[38]

De Justitiële Informatiedienst (JustID) verstrekt aan de politie gegevens over door het OM genomen vervolgingsbeslissingen, uitspraken door de strafrechter en gegevens over de tenuitvoerlegging van straffen en maatregelen (ook wel afloopberichten). Deze gegevens worden verstrekt zodat beoordeeld kan worden of gegevens op grond van artikel 9, lid 4 Wpg verwijderd moeten worden[39]. In dat kader worden de volgende gegevens verstrekt:

- het parketnummer;

en indien het feit is geseponeerd:

- de datum van de beslissing;
- de sepotcode en de bijkomende sepotgrond of sepotgronden;
- de bij de beslissing tot voorwaardelijk seponeren gestelde voorwaarden;
- de datum waarop aan alle gestelde voorwaarden is voldaan;

indien over het feit bij strafbeschikking is beslist;

- de datum waarop de strafbeschikking volledig ten uitvoer is gelegd[42];

indien een voorlopige maatregel op grond van de Wet op de economische delicten is opgelegd:

- de aanduiding van de voorlopige maatregel;
- de beëindiging, verlenging, wijziging, intrekking of opheffing;
- indien over het feit bij rechterlijke uitspraak is beslist; de inhoud van de uitspraak, waaronder de kwalificatie van het feit en de daarbij betrokken strafbepalingen[40];

indien de rechterlijke beslissing ten uitvoer is gelegd;

- de datum en de wijze waarop de tenuitvoerlegging is beëindigd;
- de datum en de wijze waarop de taakstraf of vrijheidsstraf is aangevangen en beëindigd;

indien de volledige tenuitvoerlegging niet is gerealiseerd, de datum van tenuitvoerlegging van de vervangende straf.

Doorgaans is het doel van het onderzoek gerealiseerd wanneer alle daders van het strafbare feit zijn opgespoord en vervolgd en de door de rechter opgelegde straf of maatregel daadwerkelijk geheel ten uitvoer is gelegd. Zodra voor alle ingezonden verdachten één van de afloopberichten is ontvangen, bepaalt de bevoegd functionaris of het doel is bereikt. Daarnaast zijn er ook andere omstandigheden die leiden tot verwijdering:

- verdachte-veroordeelde is overleden;
- het dossier wordt in overleg met OvJ/hopper opgelegd en de verjaringstermijn is verstreken.

38 Aanwijzing voor de opsporing

39 Artikel 11b Besluit justitiële en strafvorderlijke gegevens

40 Aanvullend aan de gegevensleveringen die in het besluit zijn bepaald, zijn er afspraken met Justid en OM over het ontvangen van afloopberichten met de datum waarop de uitspraak onherroepelijk is geworden.

Verjaringstermijnen conform artikel 70 Sr zijn gedefinieerd op basis van de voorziene straf.

De termijn van verjaring begint op de dag nadat het strafbare feit is gepleegd, of in sommige gevallen later[41]. Zo begint de termijn bij een zedendelict met een minderjarig slachtoffer bij het meerderjarig worden van het slachtoffer. (tabel)

Artikel 9-verwerkingen waarover geen evident contact met het OM bestaat zoals voorbereidende onderzoeken, veelplegerdossiers, SGBO's en preweegdocumenten moeten aan de hand van een expiratiedatum worden bewaakt door de bevoegd functionaris.

41 Artikel 71 Sr

Straf	Verjaringstermijn Art 70
Overtreding	3 jaar
Misdrijf met geldboete, hechtenis of gevangenisstraf van drie jaar of minder	6 jaar
Misdrijf met gevangenisstraf van meer dan drie jaar	12 jaar
Misdrijf met gevangenisstraf van acht jaar of meer	20 jaar
Misdrijf met gevangenisstraf van twaalf jaar of meer	Geen verjaring

3.4.2. Beoordelen

Zolang het doel van het onderzoek nog niet is bereikt, beoordeelt de bevoegd functionaris voortdurend of gegevens aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking als bedoeld in artikel 10 Wpg.

Nadat de bevoegd functionaris heeft geconstateerd dat het doel van het onderzoek is bereikt, heeft hij maximaal een half jaar de tijd om dit een laatste keer te beoordelen. Pas daarna moet tot verwijdering worden overgegaan.

3.4.3. Vernietigen

- Verwijderde gegevens worden gedurende 5 jaar bewaard en vervolgens vernietigd (artikel 14, lid 1 Wpg).
- Voor auditieve en audiovisuele registraties geldt dat de instantie waar de registratie is opgeslagen de OvJ moet verzoeken om een opdracht tot vernietiging van de registratie. De opdracht tot vernietiging wordt binnen 30 dagen uitgevoerd.[42]
- Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats (artikel 14, lid 4 Wpg).
- Gegevens die na een doorzoeking niet van belang zijn gebleken (artikel 125n Sv), gegevens die mededelingen van geheimhouders bevatten (artikel 126aa Sv) en gegevens die o.a. zijn verkregen door het opnemen van vertrouwelijke communicatie of telecommunicatie (artikel 126cc Sv) moeten eerder worden vernietigd, tenzij de Officier van Justitie anders heeft bepaald.

42 Zie voor de volledige procedure de Aanwijzing auditief en audiovisueel registreren van verhoren van aangevers, getuigen en verdachten (2018A008)

3.5. Politiegegevens voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10)

Voor politiegegevens die worden verwerkt voor inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde zijn termijnen voor verwijdering en vernietiging in artikel 10 van de Wpg bepaald. Het gaat hier om gegevensverwerking om inzicht te verwerven in de betrokkenheid van bepaalde personen bij bepaalde ernstige strafbare feiten of bij handelingen die kunnen wijzen op het beramen of plegen van bepaalde categorieën van misdrijven die ernstige bedreigingen voor de rechtsorde opleveren of bij handelingen die een ernstige schending van de openbare orde vormen. Dit artikel ziet op de meer permanente vormen van gegevensverwerking. Deze meer permanente verwerking van gegevens is nodig in verband met de aard van de misdrijven of handelingen die in het geding zijn, zoals hierna bij de toelichting op het eerste lid aan de orde komt.

3.5.1. Verwijderen

Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van de verwerking worden ze verwijderd. Daartoe worden de gegevens periodiek gecontroleerd.

Uiterlijk 5 jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de politiegegevens van betrokkene op grond van het doel, worden de gegevens verwijderd (artikel 10, lid 6 Wpg).

3.5.2. Vernietigen

- Verwijderde gegevens worden gedurende 5 jaar bewaard en vervolgens vernietigd (artikel 14, lid 1 Wpg).
- Van de vernietiging wordt afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. De betreffende gegevens worden zo spoedig mogelijk overgebracht naar een archiefbewaarplaats (artikel 14, lid 4 Wpg).

3.6. Politiegegevens voor controle en beheer van informanten (artikel 12)

Voor politiegegevens die worden verwerkt voor controle en beheer van informanten zijn termijnen voor verwijdering en vernietiging in artikel 12 van de Wpg bepaald. Het gaat hier om gegevens omtrent informanten en om integrale verslagen van de met de informanten gevoerde gesprekken. De gegevens moeten worden afgeschermd en dienen niet voor operationeel gebruik. De informatie die wordt verwerkt op grond van artikel 12, kan slechts tot maximaal vier maanden na de start van de verwerking ter beschikking worden gesteld voor verdere verwerking met het oog op de uitvoering van de dagelijkse politietaak, een onderzoek als bedoeld in artikel 9 of een analyse van artikel 10.

3.6.1. Verwijderen

Gegevens moeten direct worden vernietigd en worden niet voorafgaand verwijderd.

3.6.2. Vernietigen

- Zodra de politiegegevens niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens elk half jaar gecontroleerd.
- Uiterlijk 10 jaar na de datum van laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van politiegegevens van betrokkene voor dit doel (artikel 12, lid 6 Wpg).

3.7. Politiegegevens voor ondersteunende taken (artikel 13)

Voor politiegegevens die verder worden verwerkt ter ondersteuning van de geldt dat de termijn door de verwerkingsverantwoordelijke zelf moet worden bepaald. In een protocol moet onder andere worden vastgelegd voor welk doel de gegevens verder worden verwerkt, om welke categorieën van personen en gegevens het gaat en wanneer de verwerking wordt beëindigd[43].

Bij doelen kan worden gedacht aan

- het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten (afgerond procesdossier);
- het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte (bijvoorbeeld VVC-zaken);
- identificatie van personen of zaken (HAVANK, FCM);
- het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen (OPS, NSIS, BVH);
- het verkrijgen van landelijk inzicht in specialistische onderwerpen (overvallen, kinderporno, voetbalvandalisme etc.) .

3.7.1. Verwijderen

Gegevens moeten direct worden vernietigd en worden niet voorafgaand verwijderd.

3.7.2. Vernietigen

Uit een artikel 13-protocol moet blijken binnen welke termijn of in welke gevallen het verder verwerken van de betreffende gegevens wordt beëindigd. Deze termijn moet door de verwerkingsverantwoordelijke bepaald en gemotiveerd worden en verschilt dus per artikel 13-verwerking. De termijnen voor specifieke artikel13-verwerkingen zijn dan ook terug te vinden in de betreffende protocollen en in het verwerkingsregister.

In afwijking van het voorgaande volgt de termijn voor het bewaren van vingerafdrukken die worden verwerkt in HAVANK uit artikel 9 van het Besluit identiteitsvaststelling verdachten, veroordeelden en getuigen. In dit geval is het dus niet aan de verwerkingsverantwoordelijke om deze termijn te bepalen.

3.8. Verwijderde politiegegevens (artikel 14)

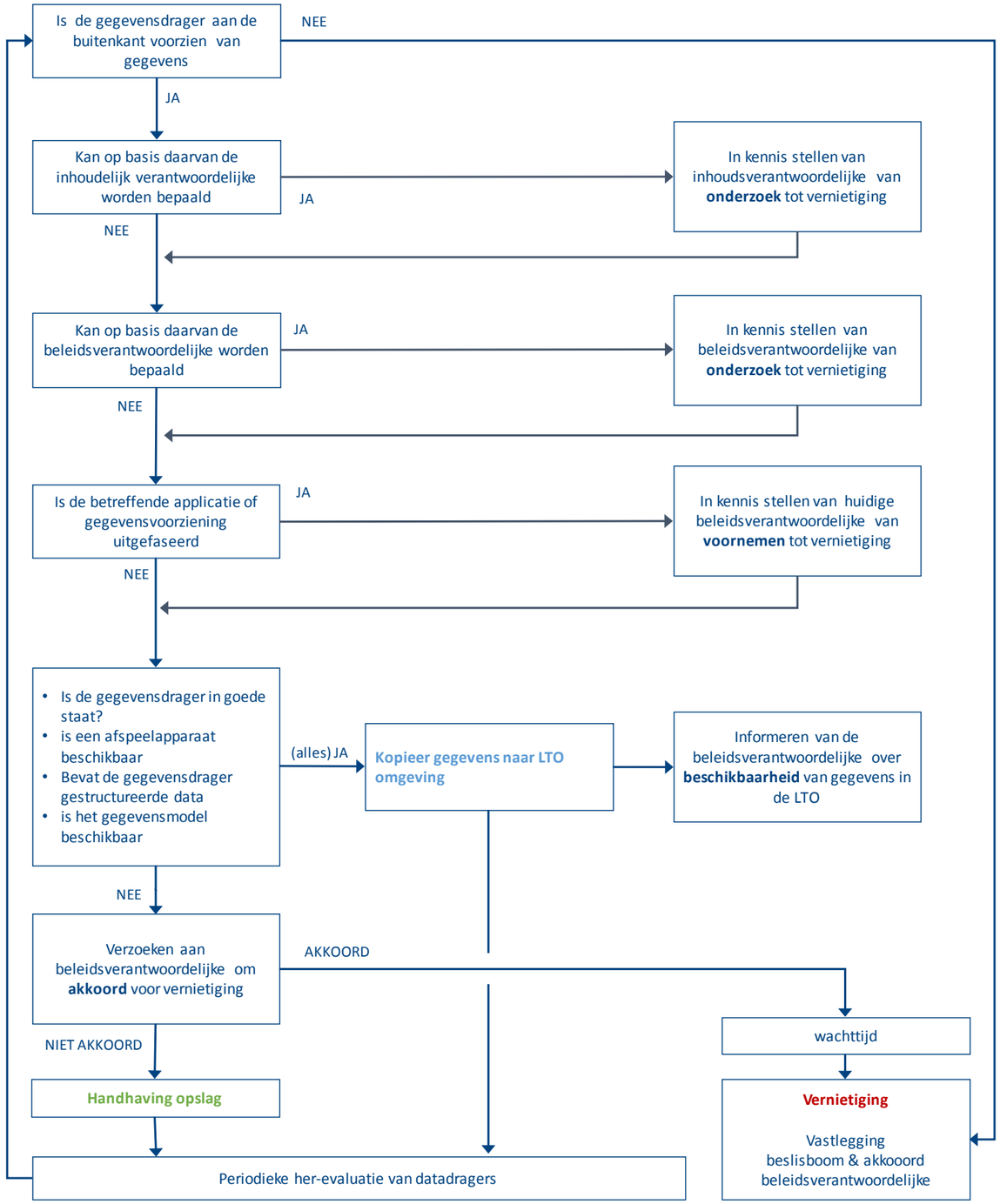
Voor politiegegevens die zijn verwijderd op grond van eerder genoemde artikelen is de termijn voor vernietiging in artikel 14 van de Wpg bepaald. Deze gegevens worden gedurende vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen. Voor het overige geldt dat deze gegevens in bijzondere gevallen en voor zover dat noodzakelijk is voor een doel als bedoeld in artikel 9 of 10 ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Dit kan alleen in opdracht van het bevoegd gezag. Deze gegevens komen ook in aanmerking voor verwerking ten behoeve van wetenschappelijk onderzoek en statistiek[44].

43 artikel 13, lid 4 Wpg j artikel 6:2, lid 1 Bpg

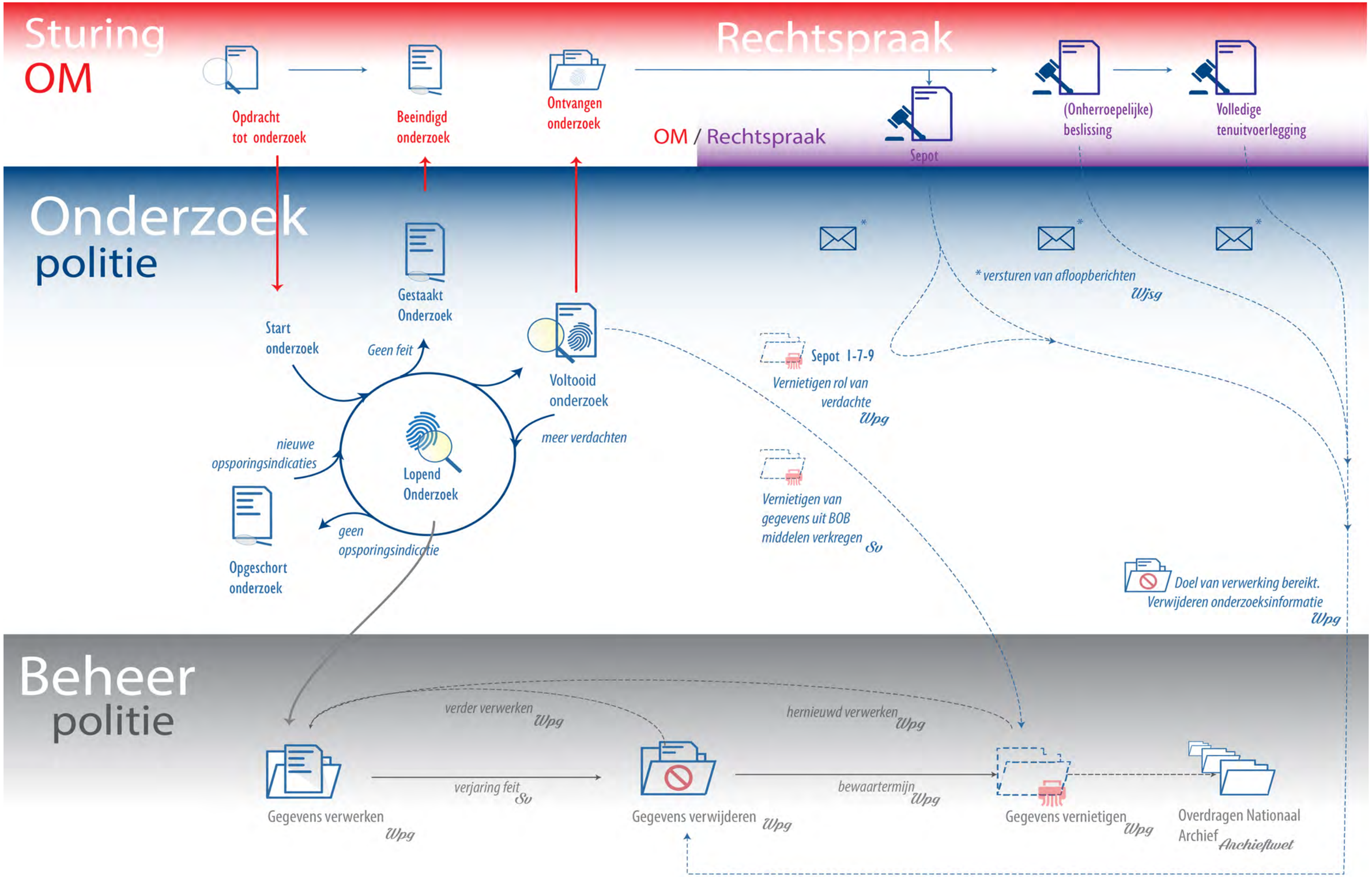
44 artikel 22 Wpg

Bijlagen

Bijlage 1. Referentieproces vernietigen van gegevensdragers



Bijlage 2. Status van onderzoeken in relatie tot archiveren en verwerken



Bijlage 3. Procedure noodvernietiging

(Oorspronkelijk
Kaderrichtlijn Noodvernietiging Politieinformatie)
Directie FM / Strategisch Beleid Services
Directie IV / Gegevensautoriteit
2018

Context

Vernietiging van politieinformatie geschiedt op basis van de Wet politiegegevens (Wpg), de Algemene Verordening Gegevensbescherming (AVG) en de vastgestelde selectielijst voor de politie (Archiefwet). De procedures die daarbij worden gehanteerd zijn vastgelegd in protocollen en het handboek DIV Politie.

Er kunnen zich echter situaties voordoen waarbij van de gestandaardiseerde werkwijzen en de bewaartermijnen Wpg, AVG en selectielijst wordt afgeweken.

Dit betreft de noodvernietiging ex artikel 9, lid 2 van de Archiefwet 1995. In bijzondere omstandigheden kan deze noodvernietiging in werking treden. De maatregel wordt genomen wanneer er sprake is van bijzondere omstandigheden waarbij informatie (papier of digitaal) met gerubriceerde of vertrouwelijke informatie gecompromitteerd dreigt te raken.

Bijzondere informatie

Onder bijzondere informatie wordt de informatie verstaan waarvan de kennisneming door niet geautoriseerde personen nadelige gevolgen kan hebben voor de belangen van de staat en/of zijn bondgenoten en/of één of meer ministeries en daaronder ressorterende diensten, bedrijven en instellingen. Dit is binnen de politie die informatie die valt onder de rubriceringen' politie zeer geheim' en 'politie geheim'.

Onder compromittering wordt verstaan de kennisname dan wel de mogelijkheid tot kennisname van bijzondere informatie door niet-geautoriseerde personen.

Bijzondere omstandigheden

De bijzondere omstandigheden waaronder tot noodvernietiging van documenten kan worden overgegaan zijn:

- Bij zware (natuur)rampen;
- In geval van (dreigende) oorlogsomstandigheden;
- Bij terroristische aanslagen en oproeren.

Scope

Deze kaderrichtlijn richt zich op zowel de papieren – als de digitale informatiedragers binnen de politie en betreft

zowel de gerubriceerde informatie die is vastgelegd in het dynamische proces (die dagelijks wordt gebruikt binnen het operationele- en bedrijfsvoeringproces) als de gerubriceerde informatie die langdurig is vastgelegd in archiefruimten en archiefsystemen met het oog op het belang van verantwoording, bedrijfsvoering of het cultuur-historisch belang.

Opdracht

Een noodvernietiging van gerubriceerde politie-informatie, en dus de informatiedragers waarop de documenten zijn vastgelegd, vindt plaats op aanwijzing van de minister-president, de minister van Veiligheid en Justitie of de korpschef van politie.

Vernietiging

Vernietiging houdt in dat de informatiedragers een dusdanige bewerking ondergaan, dat de informatie die daarop is vastgelegd niet meer te lezen en niet meer herleidbaar is. De noodvernietiging gebeurt door het zodanig verminken van de informatiedragers (zoals papier, Cd's/Dvd's, harde schijven, geluidsbanden, usb-sticks, microfilms, data-tapes, en dergelijke) dat de vastgelegde content niet meer de toegankelijk en beschikbaar is. Uitgangspunt vormen daarbij de normen voor vernietiging van gerubriceerde informatie zoals vastgelegd in de DIN 66399 (2012-10).

Aangezien het hier gerubriceerde informatie betreft zal de vernietiging van de informatiedragers vallen binnen de veiligheidsklassen 4 tot en met 7. Zie bijlage DIN 66399 (2012-10).

Bestanden

In ieder van de regionale eenheden en de landelijke eenheid maakt de teamleider DIV, in samenwerking met de proceseigenaren van de informatie en Functioneel Beheer, een overzicht in welke informatiebestanden en taakapplicaties gerubriceerde informatie is opgenomen, waar die documentbestanden zijn geplaatst en door wie deze worden beheerd.

De landelijke teamchef DIV draagt, in overleg met het hoofd IM, zorg voor een landelijk uitvoeringsprotocol, zorgt dat in iedere eenheid de middelen aanwezig zijn om tot noodvernietiging over te kunnen gaan en dat deze middelen in werkzame staat verkeren.

Verklaring

Indien de omstandigheden dit toelaten, wordt van de noodvernietiging een verklaring opgesteld die een globaal overzicht bevat van de vernietigde bestanden en de wijze waarop de vernietiging heeft plaatsgevonden.

Procedure noodvernietiging (toelichting normen en standaarden)

(Oorspronkelijk
Bijlage bij Kaderrichtlijn Noodvernietiging
Politieinformatie)

Inleiding

Er zijn verschillende normen te onderscheiden die zich richten op het vernietigen van informatiedragers met vertrouwelijke informatie. Te noemen zijn de NEN 15713 of de DIN 66399. Voor de vernietiging van confidentiële van de politie hebben we er voor gekozen om als uitgangspunt de DIN 66399 te hanteren. Reden hiervoor is dat, in tegenstelling tot in de NEN 15713, in de DIN 66399 ook de classificatieniveau 's worden benoemd met een daar aan gekoppelde norm voor vernietiging per soort informatiedrager.

DIN 66399

De DIN 66399 is een norm die is uitgegeven door het Deutschen Institut für Normung. Het betreft hier een (industrie)norm voor het vernietigen van informatiedragers en de daarop vastgelegde informatie conform vastgestelde richtlijnen Binnen de norm wordt een risicoanalyse gemaakt op grond van de op de drager vastgelegde informatie (classificatieniveau 's). Daarnaast benoemd de norm verschillende groepen van informatiedragers en daarmee de manier waarop de vastgelegde informatie wordt gepresenteerd (materiaalklassen). Het classificatieniveau en, de materiaalklasse en de veiligheidsklasse bepalen in deze norm de wijze waarop vernietiging van de vastgelegde informatie plaats heeft (veiligheidsklassen).

Classificatieniveaus

De volgende classificatieniveau 's worden onderscheiden:

Classificatieniveau 1

Standaard gevoeligheid van de informatie.
Het betreft hier informatie bedoeld voor grote groepen mensen. Kennisname van de informatie door onbedoelde openbaarheid heeft minimale schade voor de organisatie of personen tot gevolg.

Classificatieniveau 2

Hoge gevoeligheid. De vastgelegde informatie is van confidentiële aard. De informatie is bedoeld voor een kleine groep personen. Kennisname door niet geautoriseerde personen kan ernstige schade voor de organisatie of personen tot gevolg hebben.

Classificatieniveau 3

Zeer hoge gevoeligheid. De vastgelegde informatie is van zeer confidentiële of geheime aard. De informatie is bedoeld voor een zeer kleine groep geautoriseerde personen. Ongeautoriseerde kennisname kan zeer ernstige voor de organisatie of personen tot gevolg hebben.

Materiaalklassen

Op grond van de huidige stand van de techniek worden de volgende materiaalklassen onderscheiden:

Materiaalklasse P

Informatie in zijn 'originele' fysieke vorm. Denk hierbij aan papier, films, negatieven, foto's. Deze worden ook wel aan gegeven als veiligheidsklasse.

Materiaalklasse F

Informatie in verkleinde vorm. Denk hierbij aan microfilms of folies

Materiaalklasse O

Informatie op optische informatiedragers. Denk hierbij aan Cd's DVD, Blu-ray

Materiaalklasse T

Informatie op magnetische informatiedragers. Denk hierbij aan diskettes, magneetbandcassettes en ID-kaarten.

Materiaalklasse H

Informatie op harddisk met magnetische onderdelen.

Materiaalklasse E

Informatie op elektronische informatiedragers. Denk hierbij aan USB-flashdrives, SSD harddisks, chipkaarten.

Veiligheidsklassen

In de norm worden zeven veiligheidsklassen geformuleerd die mede zijn gebaseerd op de mogelijkheid tot reproductie van de vastgelegde informatie

1. Aanbevolen voor informatiedragers met openbare informatie die onleesbaar gemaakt moet worden: Reproductie met enige inspanning
2. Aanbevolen voor informatiedragers met organisatie interne informatie die onleesbaar gemaakt moet worden: Reproductie met bijzondere inspanning
3. Aanbevolen voor informatiedragers met enkele voor de organisatie gevoelige en confidentiële informatie die onleesbaar gemaakt moet worden:Reproductie met aanzienlijke inspanning
4. Aanbevolen voor informatiedragers met een hoog aantal voor de organisatie een gevoelige en confidentiële informatie dat onleesbaar gemaakt moet worden: Reproductie met buitengewone inspanning
5. Aanbevolen voor informatiedragers met geheime informatie die onleesbaar gemaakt moet worden: Reproductie met dubieuze (technische) methoden
6. Aanbevolen voor informatiedragers met geheime informatie waarvoor ongewoon hoge veiligheidstandaarden gehandhaafd worden: Reproductie technisch niet mogelijk
7. Aanbevolen voor informatiedragers met geheime informatie waarvoor de strikte veiligheidstandaarden gehandhaafd worden: Reproductie uitgesloten

Normen voor vernietiging

Door het classificatieniveau te koppelen aan het gewenste veiligheidsniveau ontslaat de volgende toepassingstabel voor het vernietigen: (zie tabel hieronder)

Per materiaalklasse vloeien daaruit de volgende normen voor vernietiging voort:

Materiaalklasse P

Informatie in zijn ‘originele’ fysieke vorm.

- P-1 Deeltjes maximaal 2000 mm² of stroken van maximaal 12 mm. Lengte van de stroken onbeperkt
- P-2 Deeltjes maximaal 800 mm² of stroken van maximaal 6 mm. Lengte van de stroken onbeperkt
- P-3 Deeltjes maximaal 320 mm² of stroken van maximaal 2 mm. Lengte van de stroken onbeperkt
- P-4 Deeltjes maximaal 160 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 6 mm
- P-5 Deeltjes maximaal 30 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 2 mm
- P-6 Deeltjes maximaal 10 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 1 mm
- P-7 Deeltjes maximaal 5 mm² en voor gelijkvormige delen een breedte van de stroken van maximaal 1 mm

	Veiligheids-klasse 1	Veiligheids-klasse 2	Veiligheids-klasse 3	Veiligheids-klasse 4	Veiligheids-klasse 5	Veiligheids-klasse 6	Veiligheids-klasse 7
Classificatie niveau 1	•[1]	•[1]	•				
Classificatie niveau 2			•	•	•		
Classificatie niveau 3				•	•	•	•

[1] Deze combinatie kan niet gebruikt worden voor persoonlijke informatie.

Materiaalklasse F

Informatie in verkleinde vorm.

- F-1 Deeltjes maximaal 160 mm^2
- F-2 Deeltjes maximaal 30 mm²
- F-3 Deeltjes maximaal 10 mm²
- F-4 Deeltjes maximaal 2,5 mm²
- F-5 Deeltjes maximaal1,0 mm²
- F-6 Deeltjes maximaal 0,5 mm²
- F-7 Deeltjes maximaal 0,2 mm²

Materiaalklasse O

Informatie op optische informatiedragers

- O-1 Deeltjes maximaal 2000 mm²
- O-2 Deeltjes maximaal 800 mm²
- O-3 Deeltjes maximaal 160 mm²
- O-4 Deeltjes maximaal 30 mm²
- O-5 Deeltjes maximaal10 mm²
- O-6 Deeltjes maximaal 5 mm²
- O-7 Deeltjes maximaal 0,2 mm²

Materiaalklasse T

Informatie op magnetische informatiedragers

- T-1 Medium niet meer functionerend
- T-2 Medium in meerdere onderdelen en deeltjes maximaal 2000 mm²
- T-3 Deeltjes maximaal 320 mm²
- T-4 Deeltjes maximaal 160 mm²
- T-5 Deeltjes maximaal30 mm²
- T-6 Deeltjes maximaal 10 mm²
- T-7 Deeltjes maximaal 2,5 mm²

Materiaalklasse H

Informatie op harddisk met magnetische onderdelen

- H-1 Schijf niet meer functionerend
- H-2 Gegevensdrager beschadigd
- H-3 Gegevensdrager vervormd
- H-4 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 2000 mm²
- H-5 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 320 mm²
- H-6 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 10 mm²
- H-7 Gegevensdrager in meerdere onderdelen en vervormt en deeltjes maximaal 5 mm²

Materiaalklasse E

Informatie op elektronische informatiedragers

- E-1 Medium niet meer functionerend.
- E-2 Medium in onderdelen
- E-3 Medium in onderdelen en deeltjes maximaal160 mm²
- E-4 Gegevensdrager in onderdelen en deeltjes maximaal 30 mm²
- E-5 Gegevensdrager in onderdelen en deeltjes maximaal 10 mm²
- E-6 Gegevensdrager in meerdere onderdelen en deeltjes maximaal 1 mm²
- E-7 Gegevensdrager in meerdere onderdelen en deeltjes maximaal 0,5 mm²

Vastgesteld Document	
Versie	1.0
Datum	13/02/2020
Vastgesteld door	BBVO (Lid Korpsleiding)
Is dit de laatste versie? Controleer dat hier of scan de QR code	

v

Van: 5.1.2.e
Aan: Riemen, John (J.A.J.M.); 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e ; 5.1.2.e
Onderwerp: GEB versie 0.9 HAVANK 4
Datum: woensdag 6 mei 2020 16:24:12
Bijlagen: GEB WPG Biometrievoorziening v0.9.docx

Beste mensen,

Hierbij stuur ik jullie de versie 0.9 van het GEB voor HAVANK 4. Vorig jaar heb ik jullie 0.1 versie van de GEB HAVANK gestuurd. Hierbij heb ik van jullie opmerkingen doorgekregen en ook zijn we nu anderhalf jaar verder met de implementatie van HAVANK en dit is in het GEB verwerkt.

Graag nog jullie reacties, ik ben benieuwd of CATCH verwerkingen goed beschreven zijn.

De GEB versie 1.0 zal voor aanvang van de productie met HAVANK 4 gereed moeten zijn. Deze staat gepland voor 1 september dit jaar.

Alvast bedankt voor een snelle reactie.

Met vriendelijke groet,

5.1.2.e
Adviseur informatiebeveiliging /risicomanagement

Politie | Politie Dienstencentrum | Kwartier Informatiebeveiliging
Ringbaan West 232, 5038 KE Tilburg
Postbus 8050, 5004 GB Tilburg
M +31 (0)6 5.1.2.e
E 5.1.2.i @politie.nl (loket informatiebeveiliging)
I http://intranet.politie.local/categorie/ondersteuning/onderwerpen/i/informatiebeveiliging/overzicht (intranetpagina)

Werkdagen: maandag, dinsdag, woensdag, donderdag tot 15 uur, vrijdagochtend

5.1.2.e

Van: Riemen, John (J.A.J.M.)
Verzonden: dinsdag 6 oktober 2020 12:39
Aan: 5.1.2.e
Onderwerp: FW: input backlog Netwerk Datakwaliteit strafrechtketen

Kan jij hier wat mee of wat voor het project?

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e (Justid) [mailto:5.1.2.e@justid.nl]
Verzonden: vrijdag 2 oktober 2020 13:37
Aan: Riemen, John (J.A.J.M.) 5.1.2.e@politie.nl>
Onderwerp: RE: input backlog Netwerk Datakwaliteit strafrechtketen

John,

Was goed je even te hebben gesproken.
Kun je aangeven op welke manier je een verwijderingsopdracht het beste zou kunnen ontvangen? Heb je randvoorwaarden hiervoor, moet het in een architectuurkader passen, etc?
Kunnen we ook over sparren als je dat beter uitkomt of je mag me doorverwijzen naar iemand waarmee ik dat kan bespreken.
Hoor graag komende week van je.

Groeten,
5.1.2.e

Van: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Verzonden: donderdag 1 oktober 2020 15:35
Aan: 5.1.2.e (Justid) 5.1.2.e @justid.nl>
Onderwerp: RE: input backlog Netwerk Datakwaliteit strafrechtketen

Hoi 5.1.2.e

Ik ben vanaf nu bereikbaar

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e . (Justid) [mailto:5.1.2.e @justid.nl]
Verzonden: donderdag 1 oktober 2020 13:46
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: RE: input backlog Netwerk Datakwaliteit strafrechtketen

John,

Kan ik je vanmiddag ergens na 15:00 uur bellen hierover?

Groeten,
5.1.2.e

Van: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Verzonden: woensdag 30 september 2020 11:20
Aan: 5.1.2.e (Justid) 5.1.2.e @justid.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e

5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: input backlog Netwerk Datakwaliteit strafrechtketen

Hallo 5.1.2.e

Ik heb nog geen issue aangeleverd maar heb er wel 1;

- Schoningsopdrachten biometrie data vanuit JUSTID en OM

Conform de wet hebben we wettelijke bewaartermijnen, JUSTID en OM moeten de politie kennisgeven wanneer data vernietigd moet worden.
Geconstateerd is dat dit waarschijnlijk onvoldoende gebeurd.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.i

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e (Justid) [mailto:5.1.2.e @justid.nl]
Verzonden: woensdag 12 augustus 2020 12:29
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>
Onderwerp: RE: input backlog Netwerk Datakwaliteit strafrechtketen

Allen,

Zoals eerder aangekondigd verzamel ik de issues mbt datakwaliteit in de strafrechtketen. Omdat de planning voor 2021 in september wordt besproken bepreek ik graag de issues, zodat ik ze mee kan nemen. Ik heb al een aantal

issues ontvangen en een aantal gehoord (en ga ik ontvangen). Graag maak ik een afspraak met een ieder van jullie om de punten helder te krijgen. Ik neem apart contact met jullie op. Als je een voorkeurstijd hebt, laat me gerust weten, dan kan ik daar rekening mee houden. Mocht je al een lijstje hebben en me die nog niet hebben gestuurd, dan houd ik me alvast aanbevolen.

Tot gauw en alvast dank voor jullie input.

Groeten,
5.1.2.e

Van: 5.1.2.e (Justid)
Verzonden: vrijdag 17 juli 2020 15:45
Aan: 5.1.2.i @politie.nl' 5.1.2.i @politie.nl>; '5.1.2.e @politie.nl'
5.1.2.e @politie.nl>; '5.1.2.e @politie.nl' <5.1.2.e @politie.nl>;
'5.1.2.e @politie.nl' 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>;
5.1.2.e @politie.nl' 5.1.2.e @politie.nl>; '5.1.2.e
5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: '5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: input backlog Netwerk Datakwaliteit strafrechtketen

Allen,

Ik verzamel de issues die jullie hebben voor de keten, zodat we die mee kunnen nemen vanuit de politie naar het Netwerk Datakwaliteit (NDK) in de strafrechtketen. Namens de politie zit 5.1.2.e in de stuurgroep. Ik rapporteer aan 5.1.2.e
Hierbij vraag ik om jullie input. Dit biedt jullie een kans om issues in de keten geagendeerd/opgelost te krijgen.

Toelichting:
Het NDK lost al enige jaren issues in de datakwaliteit in de strafrechtketen op. Voor 2021 komen er naar verwachting nieuwe middelen vrij om de issues met de keten op te pakken. Te denken valt aan koppelingen tussen ketensystemen die niet goed lopen, afloopberichten die op de verkeerde plekken aankomen, gegevens die niet aankomen, etc, etc.
De backlog wordt op 2 september besproken met alle partners. Tot die tijd heeft elke partner tijd om de issues te verzamelen die zij willen oplossen in de keten. Hierbij moet het minimaal 2 partners betreffen. De partners die nu meedoen zijn: Politie, OM, CJIB, Justid. Ik verzamel de issues voor de politie.

Medio augustus ben ik terug van vakantie en zal ik contact met jullie zoeken, of met jullie vervangers als je op vakantie bent. Ik zal dan ook checken hoe we op 2 september het ketenoverleg gaan voeren en wie daarbij aanwezig kan zijn. En op 30 september bepalen we samen met de ketenpartners de prioriteiten. Ook daarvoor gaan we nog kijken naar een vertegenwoordiging vanuit de politie.
Om jullie een beeld te geven van de huidige backlog en het detailniveau daarvan stuur ik jullie de huidige backlog mee. Graag niet verder verspreiden (tenzij naar jullie vervangers). Zouden jullie je issues willen beschrijven in een soortgelijk format en mij willen mailen? Denk dan alleen aan de kolommen a, I en J. De rest volgt later wel. Ik bespreek ze graag met jullie vanaf 10 augustus, evenals de vertegenwoordiging vanuit de politie bij de overleggen over prioriteiten.

Ik hoor graag met wie ik contact kan zoeken bij jullie afwezigheid. Ook hoor ik graag nog als ik iemand mis in jullie gezelschap, die nog belangrijke issues in de keten heeft en die daar een bijdrage aan wil leveren.

Bij voorbaat dank voor jullie aandacht en jullie input.

Met vriendelijke groet,

5.1.2.e

.....

Justitiële Informatiedienst
Burgemeester Raveslootsingel 2 | 7607 GK |Almelo
Postbus 337 | 7600 AH | Almelo
.....
M 06 5.1.2.e
5.1.2.e @justid.nl
http://www.justid.nl
.....

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit

bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
Ministerie van Justitie en Veiligheid
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
Ministry of Justice and Security
---------- Disclaimer ----------
De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen.
Kennisneming door anderen is niet toegestaan.
De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen.
Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen.
Conform het beveiligingsbeleid van de Politie wordt e-mail van en naar de politie gecontroleerd op virussen, spam en phishing en moet deze e-mail voldoen aan de voor de overheid verplichte mailbeveiligingsstandaarden die zijn vastgesteld door het Forum Standaardisatie.
Mail die niet voldoet aan het beveiligingsbeleid kan worden geblokkeerd waardoor deze de geadresseerde niet bereikt. De geadresseerde wordt hiervan niet in kennis gesteld.

The information sent in this E-mail message (including any attachments) is exclusively intended for the individual(s) to whom it is addressed and for the individual(s) who has/have had permission from the recipient(s) to read this message.
Access by others is not permitted.
The information in this E-mail message (including any attachments) may be of a confidential nature and may form part of the duty of confidentiality and/or the right of non-disclosure.
If you have received this E-mail message in error, please notify the sender without delay and delete the E-mail message (including any attachments).
In conformity with the security policy of the Police, E-mails from and to the Police are checked for viruses, spam and phishing and this E-mail must meet the standards of the government-imposed E-mail security as set by the Standardization Forum.
Any E-mail failing to meet said security policy may be blocked as a result of which it will not reach the intended recipient. The recipient concerned will not be notified.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
Ministerie van Justitie en Veiligheid
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
Ministry of Justice and Security

Van: Riemen, John (J.A.J.M.)
Aan: 5.1.2.e
Cc: 5.1.2.e
Onderwerp: RE: CATCH rapportage december 2020`
Datum: woensdag 20 januari 2021 10:45:00
Bijlagen: image001.png

Dat zou mooi zijn.
Belangrijk is voor nieuwe foto's dat het SKN wordt meegenomen.
Wettelijk gezien heeft dan JUSTID de taak om aan te geven of geschoond moet worden.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e
Verzonden: woensdag 20 januari 2021 10:11
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: CATCH rapportage december 2020`

Ik kijk bij de koppeling tevens naar de opties om te schonen en eventueel afvangen van foto's die niet in BVH geregistreerd zijn. Voor de huidige situatie moeten we ons maar een beraden wat te doen. Ik denk dat we dat in een actie om te verrijken en samenvoegen kunnen mee nemen.

Met vriendelijke groet,

5.1.2.e

Operationeel Specialist

Politie | Landelijke Eenheid | DSO|LFSC|Centrum voor Biometrie
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e
Werkdagen ma – do van 7-14.30 uur
vr van 7-11 uur

Van: Riemen, John (J.A.J.M.)
Verzonden: woensdag 20 januari 2021 09:51
Aan: 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: CATCH rapportage december 2020`

Hoi 5.1.2.e

Dank voor je uitleg.

Ik vraag dit met name omdat een journalist van NU.nl dit in zijn vizier heeft.
Dus het is goed dat we deze actie toen hebben uitgevoerd.

@ 5.1.2.e, misschien helpt het om aan te geven dat de journalist aan het graven is en werkt aan een artikel.
Het zou mooi zijn als we kunnen zeggen dat we niet alleen eenmalig dit hebben gedaan maar ook een proces aan het inrichten zijn om dit periodiek te doen.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e
Verzonden: woensdag 20 januari 2021 09:43
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: CATCH rapportage december 2020`

Hi 5.1.2.e
Het betreft hier een eenmalige schoning op basis van de verschillenlijst FCM-BVI/BVH. Deze is in feb 2020 uitgevoerd. Ik heb 5.1.2.e (FB) nog even gebeld wat de uitkomst van zijn onderzoek naar schoningsbeleid FCM is. In feite is er niets geregeld en wordt er niet of slecht geschoond. Hij krijgt ook geen gehoor bij mensen binnen privacy en security om dit op te lossen.

Met vriendelijke groet,

5.1.2.e
Operationeel Specialist

Politie | Landelijke Eenheid | DSO|LFSC|Centrum voor Biometrie
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e
Werkdagen ma – do van 7-14.30 uur
vr van 7-11 uur

Van: Riemen, John (J.A.J.M.)
Verzonden: dinsdag 19 januari 2021 17:06
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: FW: CATCH rapportage december 2020`

5.1.2.e

Was dit naar aanleiding van de FCM schoning waar jij toen naar hebt gekeken op mijn verzoek?

Zo ja is dat nu permanent geregeld dat we die periodiek krijgen?

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e
Verzonden: dinsdag 19 januari 2021 17:01
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: RE: CATCH rapportage december 2020`

Goedemiddag John,

In februari 2020 zijn er inderdaad 218.434 face (FCM) verwijderd.

Best regards/met vriendelijke groet,

Met vr. groet / best regards,

5.1.2.e
System Engineer

P. +31 (0) 5.1.2.e
M. +31 (0) 5.1.2.e
E. 5.1.2.e @politie.nl

Odijkerweg 25
3972NE Driebergen

IDEMIA

Join us on

www.idemia.com

OT-MORPHO is now IDEMIA

Van: Riemen, John (J.A.J.M.)
Verzonden: dinsdag 19 januari 2021 16:37
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: CATCH rapportage december 2020`

Hoi 5.1.2.e

Dank weer voor de cijfers

	Afgelopen maand		Sinds begin
Geïmporteerd	0		1.442.818
Duplicaten*	0		66.086
Errors	0		372
Deleted	0		218.434

Zijn dit delete acties op basis van schoning in FCM die wij ook doorgevoerd hebben?

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Centrum voor Biometrie

Van: 5.1.2.e
Verzonden: maandag 4 januari 2021 09:44
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: CATCH rapportage december 2020`

Goedemorgen John,

Allereerst de beste wensen voor het huidige jaar.

Hierbij de maandrapportage van de beide Catch systemen van afgelopen maand.

Best regards/met vriendelijke groet,

Met vr. groet / best regards,

5.1.2.e
System Engineer

P. +31 (0) 5.1.2.e
M. +31 (0) 5.1.2.e
E. 5.1.2.e @politie.nl

Odijkerweg 25
3972NE Driebergen

IDEMIA

Join us on

www.idemia.com

OT-MORPHO is now IDEMIA

Van: Riemen, John (J.A.J.M.)
Aan: 5.1.2.e ; 5.1.2.e 5.1.2.e
Onderwerp: RE: schoning of niet in CATCH
Datum: maandag 1 maart 2021 10:46:54

Allen

Zoals 5.1.2.e al aangeeft het probleem is groter, het is een keten probleem, 5.1.2.e en 5.1.2.e trekken dit politie breed.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: maandag 1 maart 2021 10:44
Aan: 5.1.2.e , 5.1.2.e 5.1.2.e @politie.nl>; Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: schoning of niet in CATCH

5.1.2.e

Je hebt gelijk, dit probleem is veel groter. Ik sprak John al. Die weet precies hoe het zit.

5.1.2.e belde. Ik heb 5.1.2.e geadviseerd een gedegen informatie analyse te laten maken.

5.2.1

5.2.1 [redacted]

5.2.1 [redacted]

5.1.2.e [redacted]

Van: 5.1.2.e [redacted]
Verzonden: maandag 1 maart 2021 09:12
Aan: 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>; 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>; 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>
Onderwerp: RE: schoning of niet in CATCH

Beste allemaal,

Is er al contact geweest met I&S? Zij doen iets soortgelijks, zijn er misschien methodieken die binnen CATCH kunnen worden overgenomen?

Groeten,

5.1.2.e [redacted]

Van: Riemen, John (J.A.J.M.)
Verzonden: donderdag 25 februari 2021 17:47
Aan: 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>; 5.1.2.e [redacted] 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>; 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>
Onderwerp: schoning of niet in CATCH

5.1.2.e [redacted] /5.1.2.e [redacted] /5.1.2.e [redacted]

Naar aanleiding van de discussie omtrent het schonen in CATCH denk ik dat de notitie van J&V die jullie al eerder van 5.1.2.e [redacted] hebben gehad al een aardige opsomming is van de achtergrond.
Wat daar echter niet genoemd wordt is dat er destijds (ik meen in 2009) door ons al is geadviseerd dat de bewaartermijnen systematiek dermate complex werd gemaakt dat het voor ons on-uitvoerbaar is.
Dit is in een formeel advies van de toenmalige RvHC overgenomen.

Waar gaat het om?
We mogen de vingerafdrukken en foto van een VH verdachte bewaren zolang hij verdachte is of als hij veroordeeld is voor dat feit.
Geen vervolging of veroordeling, dan moeten de gegevens vernietigd worden.
Uitzondering is als deze verdachte al veroordeeld is voor een ander feit dan wel nog verdachte is in een ander onderzoek.
Ook als herziening in de toekomst nog opportuun is mogen de gegevens niet weg. Dit is zeer complex om te overzien.

Wij, als politie, hebben hier natuurlijk geen zicht op en dat in het voorgenoemde advies benoemd, vandaar dat JUSTID de taak heeft gekregen, zie onderstaand geel stukje uit het besluit.

Besluit WIVVg

Artikel 9, tweede lid, voorziet erin dat het Korps landelijke politiediensten als beheerder van HAVANK de vingerafdrukken van de persoon die niet langer als verdachte van een strafbaar feit kan worden aangemerkt, uit HAVANK verwijdert en vernietigt, tenzij – zoals neergelegd is in artikel 9, tweede lid, juncto artikel 5, vierde lid – betrokkene verdacht wordt van een ander strafbaar feit of daarvoor veroordeeld is. Verder regelt artikel 9, tweede lid, dat het Korps landelijke politiediensten de vingerafdrukken vernietigt van de minderjarige die de afspraken over de Halt-afdoening volledig is nagekomen. Het spreekt voor zich dat deze organisatie alleen maar aan deze verplichting kan voldoen, indien zij in kennis is gesteld van het feit dat een van deze situaties zich voordoet. Dat geldt ook ten aanzien van de verplichting die in artikel 9, derde lid, voor het Korps landelijke politiediensten is neergelegd om de vingerafdrukken van verdachten en veroordeelden na ommekomst van de in dat artikellid gestelde termijnen te vernietigen. Artikel 9, achtste lid, voorziet er dan ook in dat de Justitiële Informatiedienst de daarvoor benodigde informatie die deze dienst op grond van artikel 8 van het openbaar ministerie verkregen heeft, bundelt, op volledigheid en juistheid controleert en daarna doorverstrekt aan het Korps landelijke politiediensten. Deze intermediaire rol past bij de functie van de Justitiële Informatiedienst van centrale voorziening voor het verwerken van persoonsgebonden strafrechtelijke informatie ten behoeve van alle partners in de strafrechtsketen.

Als wij dus een opdracht krijgen vernietigen bij, dus mijn standpunt blijft dat wij aan de Wet en het besluit voldoen.
Dat we weinig opdrachten van JUSTID krijgen klopt.
Daarbij kan het dan ook nog zijn dat wij wel een eerdere registratie hebben (HAVANK heeft meer data als de SKDB (vanaf 2010)) of een HIT op een spoor.
Dit maakt het uiterst complex.

Dat is overigens ook al geconstateerd door een Inspectierapport uit 2015;

Inspectie Veiligheid en Justitie, onderzoek naar de toepassing van de WIVVg
Bijzondere aandacht vraagt de schoning van registraties die op basis van wet en protocol zijn aangelegd, wanneer de rechtsgrond voor de registratie is vervallen. Als uitvoerder met bijzondere verantwoordelijkheden moet het OM worden genoemd. Niet alleen heeft het OM eigen verifiërende taken te vervullen, alsmede een rol in de schoningsprocessen, ook is het OM als eindverantwoordelijke voor de opsporing een belangrijke partij in de controle op een zorgvuldig verloop van de identificatietaken.

Er is al een tijd een groep vanuit J&V mee bezig, soms is die weer stilgevallen en dan werd er weer nieuw leven in geblazen, ik heb daar soms in gezeten maar wij zijn slechts de achterkant die wat met de data doet.
Het heeft nog niet tot verbetering geleid.
Men probeert nu de bal bij de politie te leggen door te zeggen dat het bij de BVID niet goed geregistreerd wordt.
Niet alle feiten waarvoor iemand is aangehouden worden daar vastgelegd.

Doordat nu een NU/nl journalist zich ermee bezighoudt begint iedereen zenuwachtig te worden.
Deze heeft zich gefocust op CATCH maar het gaat op voor alle registraties in het kader van deze wet, dus de gegevens in de SKDB, HAVANK, CATCH en volgens mij speelt bij DNA hetzelfde.
Wel is het natuurlijk zo dat de privacy en politiek (D66) al een tijd zorgen uit over Automatische Gelaatsherkenning dus daar ligt de gevoeligheid.
In CATCH heb ik in 2020 overigens een schoning van 200 K bestanden laten uitvoeren. Dit op FCM data die niet meer te linken was aan een registratie in de politie.

Afbreukrisico is dat door NU.nl gesteld zal worden dat er onterecht personen in CATCH zitten met hun foto.
Hoe erg is dat?

1. Je komt alleen naar voren als wij een mogelijke MATCH hebben met een foto vanuit een opsporingsonderzoek
2. Alle kandidaat lijsten uit CATCH worden door menselijke experts vergeleken en die trekken een conclusie
3. De uitkomst uit CATCH is slechts een indicatie voor de opsporing, er zal meer bewijs moeten worden verzameld
4. De OvJ bepaalt of hij voldoende heeft om te vervolgen, dat moet dus meer zijn als alleen een rapport Gezicht Vergelijkend onderzoek.
5. De rechter beoordeelt uiteindelijk of het rechtmatig is wat de opsporing heeft gedaan
6. De HR heeft al eerder uitspraak gedaan dat data die niet verwijderd is terwijl dit wel had gemoeten niet automatisch leidt tot onrechtmatig bewijs

Mochten jullie meer vragen hebben dan hoor ik het graag?

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 20:09
Aan: Riemen, John (J.A.J.M.) <5.1.2.I @politie.nl>
Onderwerp: RE: JustID

Top!!
Dank je en spreek je morgen

Met vriendelijke groet,

5.1.2.e
Teamchef

06 - 5.1.2.e

Politie | Landelijke Eenheid | DSO| LFSC

Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC Driebergen

Van: Riemen, John (J.A.J.M.)
Verzonden: woensdag 24 februari 2021 20:07
Aan: 5.1.2.e @politie.nl>
Onderwerp: RE: JustID

Ik maak wel even een stukje.

Vrijdag ben ik gevraagd deel te nemen aan de werkgroep 5.1.2.e, directie IV staf Korpsleiding en ook doet me 5.1.2.e van de Gegevens Autoriteit Politie.
Er wordt dus al op hoog niveau aan gewerkt…

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: woensdag 24 februari 2021 19:25
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: JustID

Hoi John,

Naar aanleiding van een opmerking van 5.1.2.e kort even met 5.1.2.e gesproken mbt de problematiek dat eventuele informatie die wij gebruiken voor oa het proces face (gebruik foto's uit systemen die er eigenlijk niet meer behoren te zitten) besproken. Zie jij kans om dit heel kort te mailen en de eventuele risico's voor onze dienst kunnen benoemen (dit omdat wij mogelijk weten dat er foto's inzitten die niet meer gebruikt mogen worden)

Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

Teamchef

06 - 5.1.2.e

Politie | Landelijke Eenheid | DSO| LFSC
Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC Driebergen

POLITIE

Biometrievoorziening

Cybersecurityanalyse
Versie 1.0

4 maart 2021

« waakzaam en dienstbaar »

Managementsamenvatting

Als onderdeel van het Cyber Security Programma (CSP) heeft een team van cyber security professionals een security analyse uitgevoerd op de omgevingen van de Biometrievoorziening. Deze analyse bestond uit het uitvoeren van interviews met betrokken stakeholders en technische securitytesten op de omgeving. Voor deze interviews zijn van te voren een aantal aanvalsscenario's gekozen, waarvan de geïmplementeerde mitigerende maatregelen getoetst zijn. Tijdens deze analyse zijn acht observaties vastgesteld met een hoog risico, twaalf met een medium risico en zestien met een laag risico. Deze kwetsbaarheden kunnen leiden tot het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van data binnen de Biometrievoorziening applicaties. De belangrijkste observaties en conclusies van deze analyse staan hieronder samengevat.

⚠️ Scenario A: Onbedoeld datalek

De Biometrievoorziening bevat veel gevoelige gegevens, zoals vinger- en gelaatsafdrukken, waar geen centraal overzicht en/of dataclassificatieschema van is. Deze gegevens zijn onversleuteld opgeslagen, en er is geen inzicht in het gebruik van clouddiensten en externe opslagapparatuur door gebruikers. Omdat de applicatie daarnaast nauwelijks wordt gemonitord op security, is het realistisch dat er onbedoeld een datalek plaatsvindt en dit niet tijdig gedetecteerd wordt.

🔒 Scenario B: Risico van derde/externe partij

Externe toegang tot de Biometrievoorziening is opgezet zodat dit alleen mogelijk is via een API of een VPN via de Externe Politie Broker (EPB). Toegang is verleend aan geselecteerde partijen en tot een selectieve hoeveelheid data. Wanneer een kwaadwillende vanuit een derde/externe partij zich in het politie netwerk bevindt, is het wel mogelijk om door het netwerk te propageren door het gebrek aan netwerksegmentatie, maar zal deze op de systemen waarschijnlijk worden opgemerkt door monitoring op de firewalls. Om deze redenen zijn de belangrijkste risico's van dit scenario gemitigeerd.

⚠️ Scenario C: Interne dreiging

Toegang tot de Biometrievoorziening wordt alleen verleend wanneer dit noodzakelijk is voor de werkzaamheden, en betreft ongeveer 150 accounts met een gecontroleerde verdeling van rechten die periodiek gecontroleerd worden. Uit technische testen is echter gebleken dat zelfs gebruikers zonder een Biometrieaccount toegang kunnen krijgen tot veel gevoelige data. In combinatie met het beperkte beheer van toegangsrechten van het DevOps account en de mogelijkheid tot exfiltratie van gegevens via cloudopslag of externe gegevensdragers, maakt dit het aanvalsscenario realistisch.

⚠️ Technische test

Er zijn tijdens de technische test verschillende ernstige kwetsbaarheden gevonden in de Biometrievoorziening:

- De infrastructuur bevat gedeelde mappen, waar iedereen on het interne netwerk zonder authenticatie gevoelige gegevens kan inzien en aanpassen. Dit omvat foto's van verdachten, configuraties en logbestanden.
- De Havank applicatie mist toegangscontrole voor belangrijke functies, zoals het inzien en downloaden van gevoelige data en het opslaan van gebruikersacties in het audit log. Dit maakt het om eenvoudig alle vinger-afdrukken te downloaden vanuit het interne netwerk, ook voor politiemedewerkers zonder toegang tot Havank.
- Binnen de Catch applicatie kunnen gebruikers toegang krijgen tot gegevens van zaken waartoe zij niet zijn geautoriseerd, waaronder wachtwoorden van serviceaccounts. De eerder genoemde gedeelde mappen bevatten o.a. Catch applicatielogs waarin plaintext wachtwoorden van politieaccounts staan opgeslagen.

🔒 **Risico gemitigeerd**
⚠️ **Risico niet gemitigeerd**

Status scenario's

Voor het interview zijn drie relevante scenario's geselecteerd: het onbedoeld lekken van gevoelige data door een medewerker, een aanval door toegang via een derde of externe partij, en een interne aanvaller. Onderstaande tabellen representeren de scenario's die zijn doorlopen, met de randvoorwaarden waaraan moet worden voldaan voor een succesvolle aanval. Per randvoorwaarde is ingeschat of deze voldoende gemitigeerd is (🔒) of dat het risico onvoldoende gemitigeerd is (⚠). De nummers in de observaties verwijzen naar de waarnemingen uit het interview, die in hoofdstuk 2 nader worden toegelicht.

⚠ Scenario A: Onbedoeld datalek

Randvoorwaarden	Observatie	Status
• Gevoelige data beschikbaar	2.4, 2.5, 2.6*	⚠
• Gebrek aan een veilig (extern) apparaatbeleid	2.7	⚠
• Mogelijkheid om data te exfiltreren	2.9, 2.11	⚠
• Gebrek aan monitoring	2.8	⚠
• Onvoldoende incident responseplannen		🔒

🔒 Scenario B: Risico van derde/externe partij

Randvoorwaarden	Observatie	Status
• Externe toegang		🔒
• Gebrek aan netwerksegmentatie	2.1, 2.10	⚠
• Mogelijkheid tot scannen zonder te worden opgemerkt		🔒
• Toegang tot gevoelige data of onveilige configuraties	2.4, 2.5, 2.6*	⚠
• Mogelijkheid om data te exfiltreren	2.9, 2.11	⚠

⚠ Scenario C: Interne dreiging

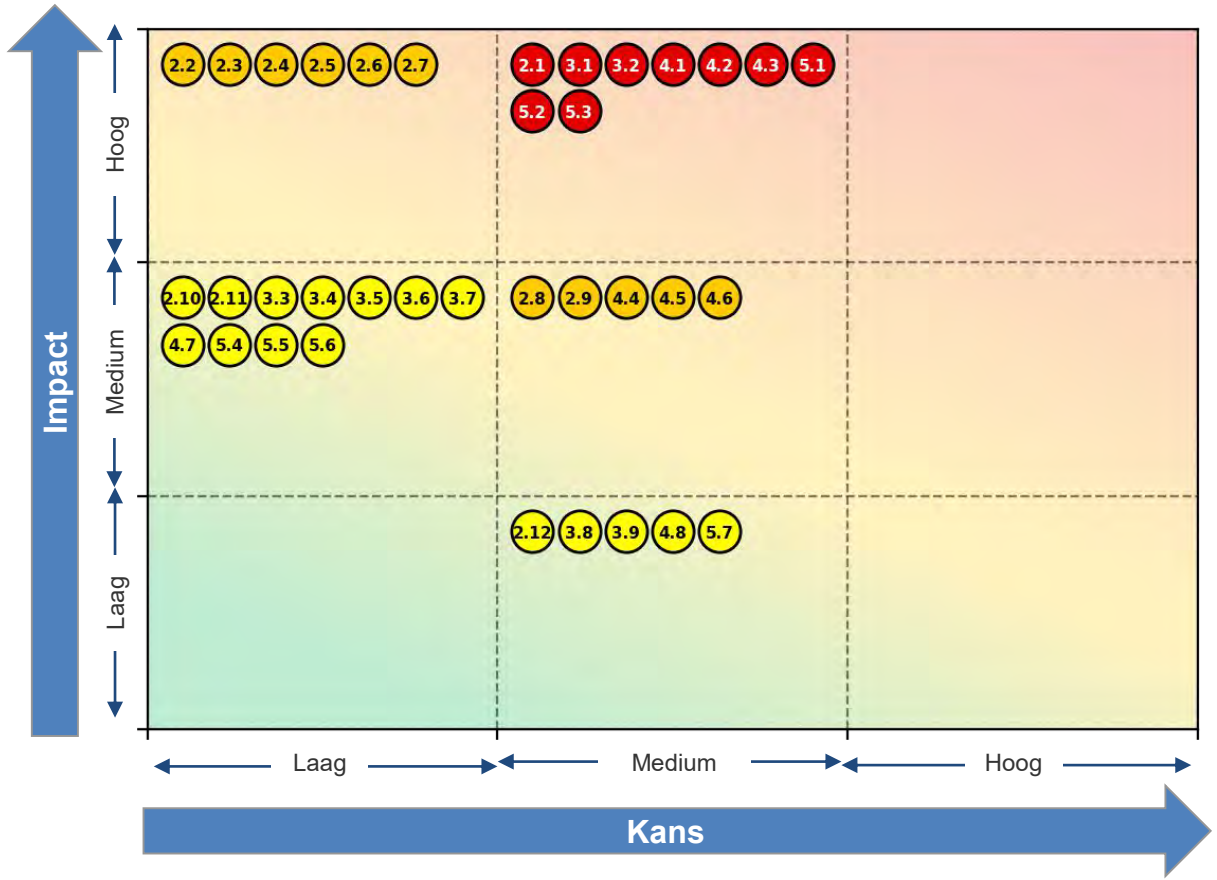
Randvoorwaarden	Observatie	Status
• Geldig gebruikersaccount		🔒
• (Optioneel: verhogen privilege/rechten)	2.2	⚠
• Toegang tot gevoelige data of onveilige configuraties	2.4, 2.5, 2.6*	⚠
• Mogelijkheid om data te exfiltreren	2.9, 2.11	⚠

** Naast deze observaties in het interviewdeel, is er tijdens de technische testen geconstateerd dat een aanvaller ongeautoriseerde toegang kan krijgen tot een grote hoeveelheid gevoelige data (zie onder andere 3.1, 4.1-4.3, 5.1-5.3).*

🔒 **Risico gemitigeerd**
⚠ **Risico niet gemitigeerd**

Risico heatmap

Onderstaande heatmap toont een grafisch overzicht van alle geïdentificeerde risico's:



Overzicht van observaties

Interview

- **2.1** Gebrek aan segmentatie binnen het netwerk
- **2.2** Beperkt beheer toegangsrechten DevOps account
- **2.3** Ontoereikend back-upbeleid
- **2.4** Patches worden niet snel genoeg geïnstalleerd
- **2.5** Onveilige dataoverdracht via de EPB
- **2.6** Onversleutelde dataopslag
- **2.7** Geen beleid voor versleutelen van mobiele gegevensdragers
- **2.8** Gebrek aan monitoring
- **2.9** Geen blokkade voor cloudopslag
- **2.10** Mogelijk onveilige configuratie poorten/protocollen
- **2.11** Geen restricties op ongebruikelijke data-activiteit
- **2.12** Onvolledig dataclassificatiemodel

Interne infrastructuurtest

- **3.1** Openbare NFS shares beschikbaar op het interne netwerk
- **3.2** Beheerinterfaces beschikbaar op het interne netwerk
- **3.3** Onveilige SMB configuratie
- **3.4** Gevoelige data onversleuteld verstuurd
- **3.5** Onveilige TLS configuratie
- **3.6** Zwakheden in TLS certificaten
- **3.7** Verouderde en kwetsbare software geïdentificeerd
- **3.8** Versie informatie geïdentificeerd
- **3.9** Overbodige bestanden aangetroffen

Applicatietest Havank

- **4.1** Ongeautoriseerde toegang tot gevoelige data
- **4.2** Local file inclusion via API
- **4.3** Ongeauthentiseerde audit logging vanuit fatclient
- **4.4** Zwakheden in wachtwoordbeleid
- **4.5** Gebruikerscertificaten worden geaccepteerd
- **4.6** Beperkte inputfiltering
- **4.7** Verouderde en kwetsbare software geïdentificeerd
- **4.8** Technische informatie in foutmeldingen

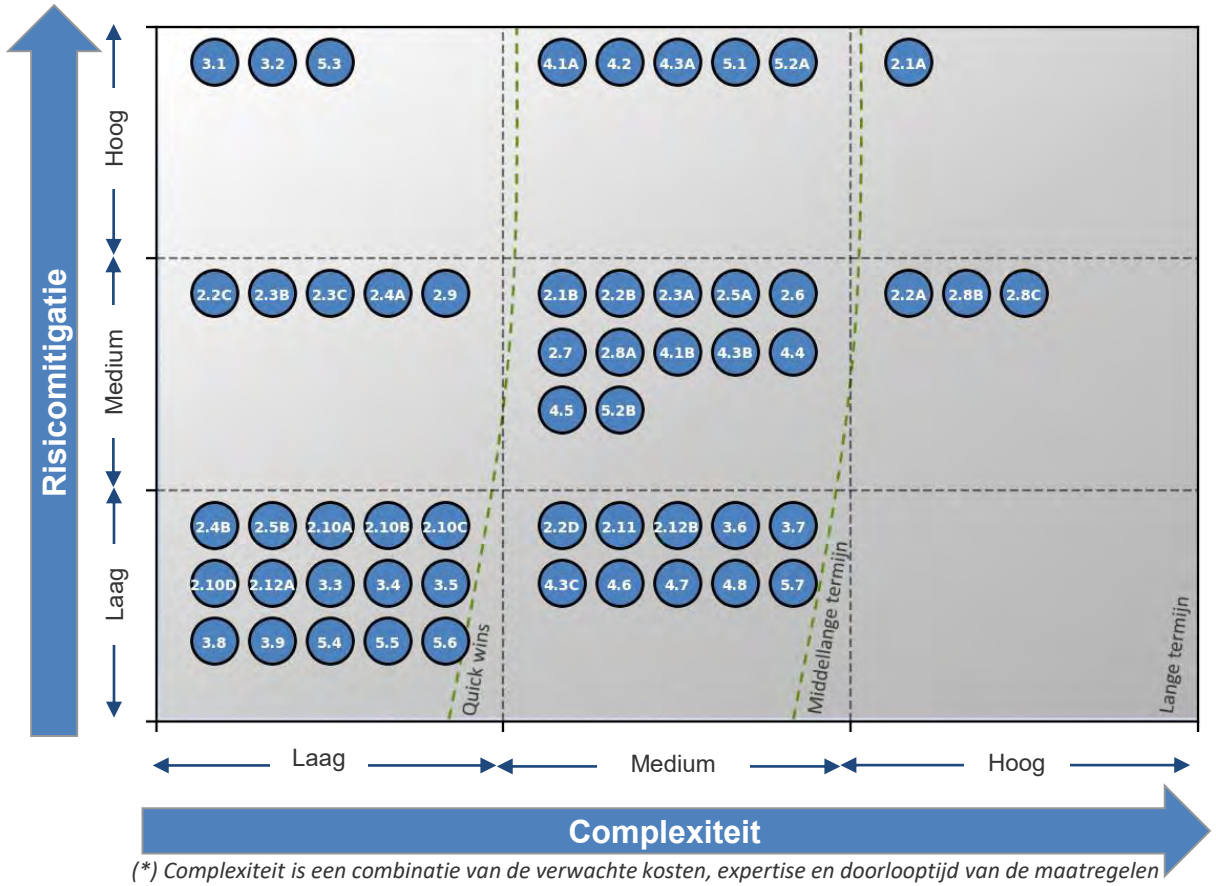
Webapplicatietest Catch

- **5.1** Ongeautoriseerde toegang tot gevoelige data
- **5.2** Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd
- **5.3** Gevoelige data in applicatielogs
- **5.4** Onveilige bestand upload functie
- **5.5** Onveilige HTTP response header configuratie
- **5.6** Onveilig gebruik van cookie parameters
- **5.7** Technische informatie in foutmeldingen

Laag	Medium	Hoog
L	M	H

Aanbevelingen heatmap

Onderstaande heatmap toont een grafisch overzicht van alle aanbevelingen:



(*) Complexiteit is een combinatie van de verwachte kosten, expertise en doorlooptijd van de maatregelen

Geschatte implementatietermijnen

Quick wins (te realiseren binnen twee maanden):

- **2.2C** Periodieke KeePass wachtwoordwijziging
- **2.4A** Verhoog de reguliere patchfrequentie
- **2.4B** Formaliseer een spoed patchprocedure
- **2.5B** Beperk EPB-communicatie d.m.v. een allow-list
- **2.9** Blokkeer of monitor clouddiensten
- **2.10A** Houd een overzicht van protocollen bij in de firewall sheets
- **2.10B** Herzie periodiek firewall regels
- **2.10C** Voer periodiek port scans uit
- **2.10D** Implementeer logging op poortniveau
- **2.12A** Inventariseer alle gevoelige data binnen de omgeving
- **3.1** Beperk toegang tot de NFS shares
- **3.2** Beperk toegang tot de beheerinterfaces
- **3.3** Verbeter de SMB configuratie
- **3.4** Schakel cleartext authenticatie uit
- **3.5** Verbeter de SSL/TLS configuratie
- **3.6** Verwijder overbodige bestanden van webservers
- **3.9** Verwijder overbodige bestanden van webservers
- **5.3** Beveilig de uploadfunctie
- **5.4** Log geen plaintext wachtwoorden
- **5.5** Verbeter de HTTP response header configuratie
- **5.6** Maak gebruik van de ‘Secure Flag’ parameter

Lange termijn (onderdeel van cyber security programma):

- **2.1A** Richt microsegmentatie in
- **2.2A** Implementeer een PAM tool
- **2.8B** Deel logs met het SOC
- **2.8C** Monitor gebruikersgedrag en afwijkingen

Middellange termijn (te realiseren binnen zes maanden):

- **2.1B** Controleer netwerkpaden periodiek
- **2.2B** Personaliseer het DevOps account
- **2.2D** Monitor de KeePass file
- **2.3A** Gebruik een ‘offline’ locatie voor back-up opslag
- **2.3B** Verifieer de back-ups
- **2.5A** Implementeer authenticatie bij communicatie met de EPB
- **2.6** Versleutel de data
- **2.7** Versleutel mobiele gegevensdragers
- **2.8A** Centraliseer loganalyse en opslag
- **2.11** Stel restricties in op data-activiteit
- **2.12B** Stel een dataclassificatiemodel op
- **3.7** Vraag nieuwe SSL/TLS certificaten aan
- **3.8** Verbeter het update proces
- **4.1A** Dwing toegangscontrole af op de Havank backendsystemen
- **4.1B** Geef bijlages in Havank moeilijk te raden identifiers
- **4.2** Limiteer de bestandstoegang
- **4.3A** Voer audit logging uit op backend systemen
- **4.3B** Voer audit trail logging uit op basis van sessies
- **4.3C** Beveilig audit logging met authenticatie
- **4.4** Dwing het gebruik van sterke wachtwoorden af
- **4.5** Maak gebruik van ‘certificate pinning’
- **4.6** Pas filtering toe op de invoer
- **4.7** Verbeter het update proces
- **4.8** Toon geen technische details in foutmeldingen
- **5.1** Dwing toegangscontrole af op de Catch backendsystemen
- **5.2A** Verwijder de RabbitMQ inloggegevens uit het configuratiebestand
- **5.2B** Gebruik sterke wachtwoorden voor serviceaccounts
- **5.7** Gebruik standaard foutmeldingen

Inhoudsopgave

Toelichting op de hoofdstukken

De managementsamenvatting beschrijft de achtergrond en context van de analyse. De huidige status en belangrijkste risico's van het kroonjuweel op het gebied van cyber security worden benoemd, inclusief een overzicht van de observaties en aanbevelingen hieromtrent.

In de introductie beschrijven we gedetailleerd:

- Het projectoverzicht met daarin achtergrondinformatie over de analyse en het kroonjuweel;
- De aanpak van de analyse;
- De aanvalsscenario's en systemen die in scope waren voor deze analyse.

In de daaropvolgende hoofdstukken worden alle observaties met de bijbehorende risico-inschatting en aanbevelingen gedetailleerd beschreven.

1

Introductie

Projectoverzicht

Als onderdeel van het Cyber Security Programma (CSP) is een team van cyber security professionals opdracht gegeven om security analyses uit te voeren op meerdere kritieke IT-omgevingen binnen de Nationale Politie (hierna ook: politie). Deze kritieke IT-omgevingen zijn aangewezen als 'kroonjuwelen' van de politie. Het is van uiterst belang dat deze IT-omgevingen voldoen aan hedendaagse best-practices, zodat de politie op een veilige manier haar kerntaken in de Nederlandse maatschappij kan vervullen.

Aanpak: Critical Security Controls (CSC)[1] aan de hand van aanvalsscenario's

De analyse is uitgevoerd door middel van interviews en technische testen. In de interviews worden met technisch beheerders drie relevante en realistische aanvalsscenario's doorlopen om te identificeren welke beveiligingsmaatregelen zijn geïmplementeerd om tegen zulke scenario's bescherming te bieden. Tijdens de technische analyse zijn drie testen uitgevoerd; één op de interne infrastructuur van de Biometrievoorziening, één op de verzameling (Java) applicaties van Havank en één op de Catch webapplicatie, om daarin de meest urgente en kritische kwetsbaarheden te identificeren. Alle observaties worden gecategoriseerd op basis van de Critical Security Controls (CSC) van het Center for Internet Security (CIS) [1]. Als resultaat van de analyse, met observaties uit zowel het interview als de technische testen, ontstaat een overzicht van de meest kritieke kwetsbaarheden in de omgeving en de beveiligingsmaatregelen die geïmplementeerd zouden moeten worden om de risico's van realistische aanvalsscenario's te beperken.

Omgeving

Het doel van de Biometrievoorziening is om forensische sporen effectief te kunnen gebruiken in opsporingsonderzoeken, en bestaat hoofdzakelijk uit twee onderdelen: Havank en Catch. De Biometrievoorziening heeft in totaal ongeveer 150 gebruikers, voornamelijk bestaand uit forensisch specialisten. Zowel Havank als Catch is ontwikkeld door IDEMIA, en beiden maken grotendeels gebruik van dezelfde achterliggende systemen.

Havank (Het Automatisch VingerAfdrukkensysteem Nederlandse Kollektie) is gericht op de dactyloscopische component van forensisch onderzoek, wat gebaseerd is op sporen op huidlijnen aan de binnenzijde van de handen en vingers, en afdrukken en sporen van handpalmen, voeten en tenen (in de praktijk wordt hier vaak naar gerefereerd als vingerafdrukken en vingersporen). In Havank worden deze sporen met elkaar vergeleken door experts om te bepalen of ze afkomstig zijn van een en dezelfde bron.

Catch (Centrale Automatische TeChnologie voor Herkenning van personen) is gericht op de morfologische component van forensisch onderzoek, wat betrekking heeft op de vorm en structuur van een gelaat. In Catch worden twee gelaatsafbeeldingen met elkaar vergeleken door experts op basis van onder andere de vorm van de neus, lippen, oren en oogkassen. Catch wordt ook de 'Face Expert' applicatie genoemd.

De technische test zoals beschreven in dit rapport vond plaats in december 2020 en januari 2021, kort voor de ingebruikname van de nieuwe Havank en Catch applicaties.

De product owner van de biometrievoorziening is John Riemen, en de business owner is Ruud Staaijen.

1: CIS Critical Security Controls: https://www.cisecurity.org/controls/cis-controls-list/

Aanpak

De resultaten in deze memo zijn gebaseerd op interviews en technische testen en zijn gekoppeld aan de Center for Internet Security Critical Security Controls (CIS CSC).

Het doel van de ***interviews*** is om te evalueren of het uitvoeren van de drie geselecteerde aanvalsscenario's binnen het kroonjuweel kan worden beperkt of voorkomen. Om dit te bewerkstelligen, worden voor elke aanwezige randvoorwaarde binnen dit kroonjuweel beveiligingsmaatregelen aanbevolen die geïmplementeerd zouden moeten worden om de risico's van deze aanvalsscenario's te beperken, gebaseerd op de volgende CIS CSC domeinen die geprioriteerd zijn vanuit het Cyber Security Programma:

- CSC01: Inventory and control of hardware assets
- CSC02: Inventory and control of software assets
- CSC03: Continuous vulnerability management
- CSC04: Controlled use of administrative privileges
- CSC09: Limit, and control of network ports, protocols & services
- CSC10: Data recovery capabilities
- CSC13: Data protection
- CSC14: Controlled access, based on the need to know
- CSC19: Incident response and management

De gekozen aanvalsscenario's worden aan de hand van deze geprioriteerde CIS CSC domeinen opgedeeld, en waar nodig aangevuld met tussenstappen uit andere CSC domeinen. De scenario's worden verder toegelicht op de volgende pagina.

Het doel van de ***technische testen*** is om technische kwetsbaarheden te identificeren, welke gemitigeerd zouden moeten worden om het risico op en van een potentieel incident te beperken.

Onderstaande tabellen geven weer met wie er gesproken is voor de interviews en welke technische testen er zijn uitgevoerd.

Interviews
Technisch Beheerders Biometrie, 26 november 2020 • Rob Piederiet, Martin Storm, Ahmet Mentes, Nicolo Giacomello, Marco Haenraets
Database beheerder Oracle PaaS, 1 december 2020 • Jan van Golen
Functioneel Beheerder Biometrie, 12 januari 2021 • Jasper de Veth
Architect Generieke Infrastructuur, 19 januari 2020 • Pieter Horsting

Technische tests
Interne infrastructuurtest Biometrievoorziening, 7 december 2020 en 13 januari 2021 • 'Black box' test op een aantal geselecteerde systemen die via het interne netwerk benaderbaar zijn. Deze test is gericht op het identificeren van kwetsbaarheden in beveiligingsmaatregelen op het niveau van het netwerk en besturingssysteem van deze systemen.
Windows Java-applicaties ('fatclients') Havank, 2 t/m 18 december 2020 en 4 t/m 7 januari 2021 • 'Grey box' applicatietesten vanuit het perspectief van zowel een niet-geautoriseerde als een geautoriseerde gebruiker van de applicaties. Hierbij testten we op veelvoorkomende kwetsbaarheden, zoals gebrek aan inputvalidatie, aanwezigheid van gevoelige gegevens, en autorisatiecontroles van backend systemen.
Webapplicatie Catch (Face expert), 11 t/m 15 januari 2021 • 'Grey box' webapplicatietest vanuit het perspectief van zowel een niet-geautoriseerde als een geautoriseerde gebruiker van de webapplicatie. Hierbij testten we op veelvoorkomende kwetsbaarheden, zoals SQL-injectie, Cross-Site Scripting (XSS), gebrek aan inputvalidatie en kwetsbare managementinterfaces.

Scenario's in scope voor het interview

De onderstaande drie scenario's zijn geselecteerd voor evaluatie in het interview. Deze scenario's zijn in overleg met stakeholders van het kroonjuweel gekozen omdat voor de Biometrievoorziening vertrouwelijkheid belangrijker wordt geacht dan integriteit en beschikbaarheid, gezien de Biometrievoorziening een grote hoeveelheid gevoelige informatie bevat zoals gelaats- en vingerafdrukken. Er is voor scenario B gekozen omdat een groot deel van zowel Catch als Havank wordt geleverd door een derde partij (de leverancier IDEMIA), en er veel koppelingen zijn naar andere partijen. De randvoorwaarden geven aan welke omstandigheden nodig zijn voor een succesvolle aanval, met de bijhorende CIS Critical Security Control(s).

Scenario A: Onbedoeld datalek	Randvoorwaarden die een aanvaller nodig heeft voor dit scenario	CIS CSC[1]
Een gebruiker wil gevoelige informatie verplaatsen naar een ander systeem of een andere gebruiker. Door ontbrekend beleid of proces, kan de gebruiker de data op een onveilige manier verplaatsen, waardoor deze kan worden onderschept. Voorbeelden van onbedoelde datalekken zijn het sturen van bestanden over persoonlijke mail of het kwijtraken van een onversleutelde USB-stick met gevoelige informatie in de openbare ruimte.	• Gevoelige data beschikbaar • Gebrek aan een veilig (extern) apparaatbeleid • Onveilig apparaat • Gebrek aan monitoring • Gebrek aan een incident response plan	13 13 13 06 19

Scenario B: Risico van derde/externe partij	Randvoorwaarden die een aanvaller nodig heeft voor dit scenario	CIS CSC[1]
Een derde partij of een aanvaller heeft toegang tot een systeem dat zich buiten de kroonjuweelomgeving bevindt, maar er wel een koppeling mee heeft. Als de actor het externe systeem gecompromitteerd heeft, kan dit systeem gebruikt worden voor verdere verplaatsing binnen het netwerk zoals naar dit kroonjuweel. Daarmee kan de actor toegang krijgen tot gevoelige informatie en/of beschikbaarheidsproblemen veroorzaken. Voorbeeld: een medewerker van een leverancier die door een gebrekkige API toegang kan verkrijgen tot gevoelige data.	• Externe toegang • Gebrek aan segmentatie • Mogelijkheid om netwerk te scannen zonder detectie • Toegang tot gevoelige data of onveilige services • Mogelijkheid om data te exfiltreren	12 09, 12, 14 06, 09, 14 03, 05, 14 13

Scenario C: Interne dreiging	Randvoorwaarden die een aanvaller nodig heeft voor dit scenario	CIS CSC[1]
Een gebruiker met een geldig account gebruikt zijn/haar account en kennis van het kroonjuweel om schade aan de organisatie toe te brengen door het lekken van informatie of beschikbaarheidsproblemen te veroorzaken. Dit kan ook zonder medeweten gebeuren doordat een aanvaller via een phishing-aanval toegang krijgt tot een geldig gebruikersaccount. Voorbeeld: een ontslagen medewerker of een medewerker die gechanteerd wordt en daardoor zijn geldige account misbruikt.	• Geldig gebruikersaccount • Optioneel: verhogen privilege/rechten • Toegang tot gevoelige data of onveilige configuraties • Mogelijkheid om data te exfiltreren	16 04 03, 04, 15 13

N.B. In de analyses worden drie uit vijf scenario's gekozen, in overleg met stakeholders van het kroonjuweel. Voor deze analyse zijn de scenario's "ransomware uitbraak" en "ongeautoriseerde gast met fysieke toegang" buiten beschouwing gelaten.

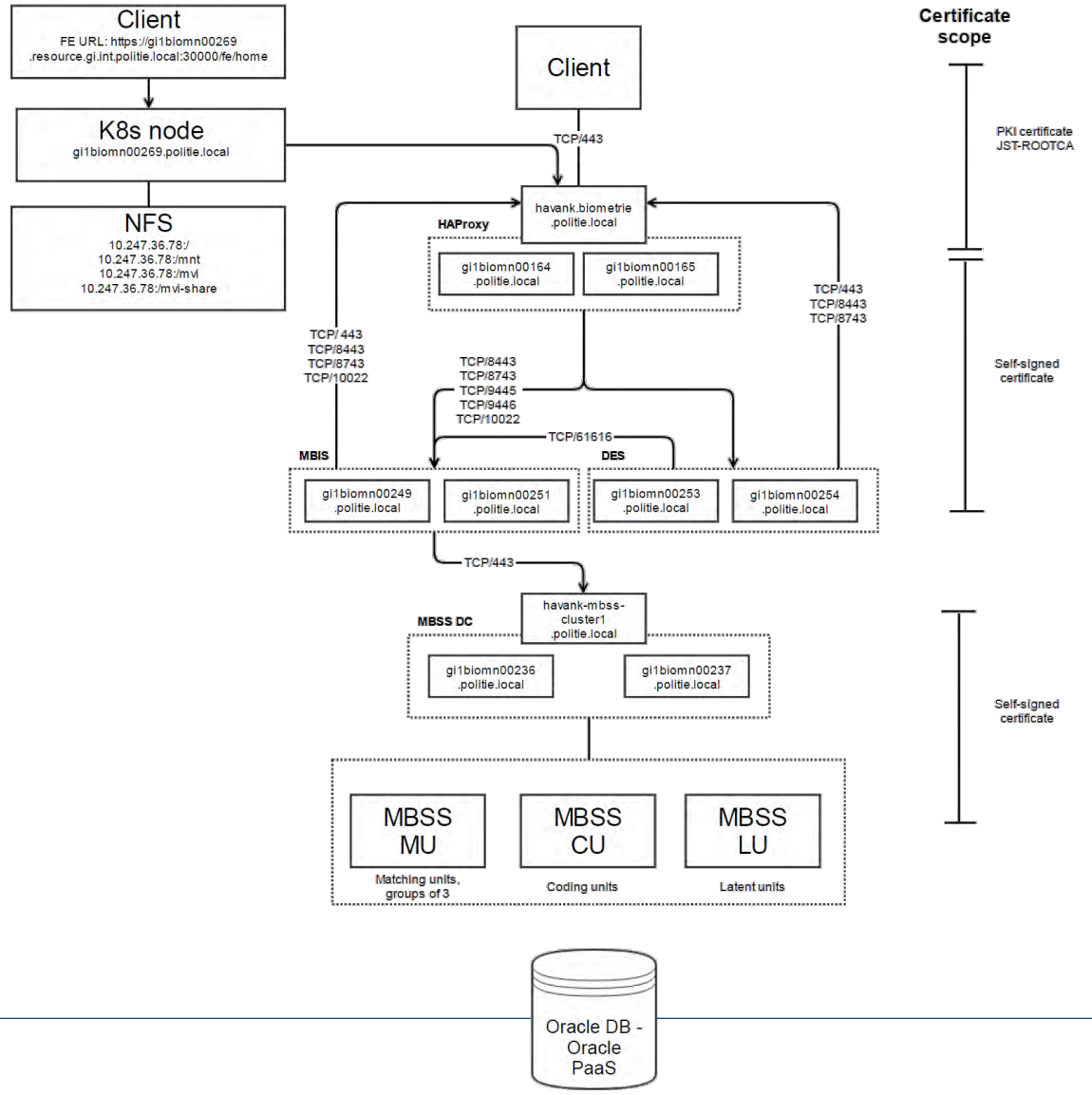
1: CIS Critical Security Controls: https://www.cisecurity.org/controls/cis-controls-list/

Architectuur- / netwerktekening

De infrastructuur van de Biometrievoorziening bevindt zich op de Generieke Infrastructuur (GI) van de politie. Alle hosts zijn virtuele (VMWare) machines en bevinden zich in het politie.local domein. Daarnaast wordt gebruik gemaakt van een Oracle PaaS database.

De gebruiker logt in op een VM waarop de Havank applicaties zijn geïnstalleerd, en kan Catch in de browser openen. Beiden applicaties communiceren door middel van een HTTPS verbinding met de frontend server, welke via de HAProxy verbonden is met achterliggende systemen.

MBSS staat voor Multi-Biometric Search Services, dat door leverancier IDEMIA wordt aangeleverd als backend voor het opslaan, verwerken en vergelijken van biometrische gegevens.



Beperkingen test en geplande wijzigingen

De tekening toont de omgeving ten tijde van de test; op dat moment was de applicatie nog niet gelanceerd voor gebruik. Er zijn een aantal factoren die bij livegang zullen veranderen aan de omgeving, ten opzichte van de omgeving tijdens de test:

- De fatclients van Havank zijn getest in een Virtual Machine (VM) in het politienetwerk. Voor normale gebruikers zullen deze applicaties via het Software Center als package worden geïnstalleerd in hun KA-omgeving;
- Een deel van de gebruikersinterface, waaronder de workflow overzichten, wordt in de toekomst in een Sharepoint webapplicatie aangeboden.
- Er zijn nog geen koppelingen naar andere omgevingen. Voor de livegang wordt een Data Exchange Server (DES) ingericht om te communiceren met externe partijen via de Externe Politie Broker (EPB), mail (Exchange server) en Sharepoint.
- Voor het inloggen op de applicaties wordt gebruik gemaakt van losse gebruikersaccounts voor de Biometrievoorziening; in de toekomst zal een SSO-oplossing worden gebruikt met een koppeling naar de Active Directory met alle politieaccounts.

Systemen in scope voor de technische tests

Onderstaande tabellen geven weer welke systemen in scope waren voor de technische tests.

Interne infrastructuurtest

Systeem	Omschrijving
gi1biomn00164.politie.local gi1biomn00165.politie.local	HAProxy
10.247.32.81	HAProxy (vanuit cluster)
gi1biomn00249.politie.local gi1biomn00251.politie.local gi1biomn00253.politie.local gi1biomn00254.politie.local	Morphobis
giapolis02.kdpol.gi.int.politie	Morphobis shares
pdcpsx7010-p-scan.politie.local	Database
gi1biomn00236.politie.local gi1biomn00237.politie.local	MBSS Zookeeper
10.247.32.182	MBSS VIP
gi1biomn00183.politie.local gi1biomn00184.politie.local gi1biomn00185.politie.local gi1biomn00186.politie.local gi1biomn00187.politie.local gi1biomn00188.politie.local	MBSS

Interne infrastructuurtest (vervolg)

Systeem	Omschrijving
gi1biomn00189.politie.local gi1biomn00190.politie.local gi1biomn00191.politie.local gi1biomn00192.politie.local gi1biomn00193.politie.local gi1biomn00194.politie.local gi1biomn00195.politie.local gi1biomn00196.politie.local gi1biomn00197.politie.local gi1biomn00198.politie.local gi1biomn00199.politie.local gi1biomn00200.politie.local gi1biomn00201.politie.local gi1biomn00202.politie.local gi1biomn00203.politie.local gi1biomn00206.politie.local gi1biomn00211.politie.local gi1biomn00207.politie.local gi1biomn00214.politie.local gi1biomn00215.politie.local gi1biomn00216.politie.local gi1biomn00217.politie.local	MBSS (vervolg)

Havank 'fatclient' applicatie

Modules en onderdelen	
MBISS AppBar	Descriptors Entry
Latent Expert	Person Management
Compare (Reviewer)	Central Viewer
User preferences	List Manager
Card Capture	Known Print
Print Screen	Coordinator

Catch (Face Expert) webapplicatie

URL
gi1biomn00269.resource.gi.int.politie

N.B.: De systemen in scope omvatten de "productie"-omgeving van de nieuwe Biometrievoorziening. Deze waren nog niet in live gebruik ten tijde van de test.
De vorige pagina bevat een overzicht van de geplande wijzigingen in de omgeving.

2

Observaties interviews

Observatieoverzicht

Onderstaande tabel bevat de observaties die zijn geïdentificeerd tijdens het interview en de inschatting van de kans, impact en het bijbehorende risico (laag, medium of hoog) per observatie. De details per observatie zijn opgenomen op de volgende pagina's van deze sectie.

#	Domein	Observatie	Kans	Impact	Risico
2.1	CSC12	Gebrek aan segmentatie binnen het netwerk	M	H	H
2.2	CSC04	Beperkt beheer toegangsrechten DevOps account	L	H	M
2.3	CSC10	Ontoereikend back-upbeleid	L	H	M
2.4	CSC03	Patches worden niet snel genoeg geïnstalleerd	L	H	M
2.5	CSC12	Onveilige dataoverdracht via de EPB	L	H	M
2.6	CSC13	Onversleutelde dataopslag	L	H	M
2.7	CSC13	Geen beleid voor versleutelen van mobiele gegevensdragers	L	H	M
2.8	CSC06	Gebrek aan monitoring	M	M	M
2.9	CSC13	Geen blokkade voor cloudopslag	M	M	M
2.10	CSC09	Mogelijk onveilige configuratie poorten/protocollen	L	M	L
2.11	CSC16	Geen restricties op ongebruikelijke data-activiteit	L	M	L
2.12	CSC13	Onvolledig dataclassificatiemodel	M	L	L

Laag	Medium	Hoog
L	M	H

2.1 Gebrek aan segmentatie binnen het netwerk

Domein	Kans	Impact	Risico
CSC12	M	H	H

Observatie

De backend van de Biometrievoorziening is geplaatst in een netwerksegment waarin verschillende politieapplicaties en het ‘portaal’ aan elkaar gekoppeld zijn. In het verleden waren de segmenten gesplitst op basis van domain, VLAN en hosts. Om doelmatigheidsredenen is ervoor gekozen om segmentatie op basis van VLANs uit te schakelen, gegeven het feit dat alle hosts al voldoende beschermd zouden zijn door gebruik van host-based firewalls.

Naar het nu blijkt zijn op veel systemen de host-based firewalls echter uitgeschakeld. Door samenval van deze 2 keuzes kunnen alle systemen in hetzelfde domein (politie.local) vrij communiceren met ieder systeem zonder host-based firewalls. Hiermee wordt in feite één grote zone gecreëerd, wat ook geldt voor systemen van de Biometrievoorziening.

Er wordt niet gecontroleerd of netwerksegmentatie ook daadwerkelijk wordt afgedwongen (bijvoorbeeld of de databaseserver niet direct kan verbinden met gewone werkstations).

N.B. Het gebrek aan strikte regels in de host-based firewalls verhoogt de kans op misbruik van kwetsbaarheden en configuratiefouten, zie ook observaties 3.1 en 3.2.

Kans: Om dit risico te verwezenlijken dient een aanvaller (of malware) zich te bevinden op een van de systemen in het ‘politie’ netwerk van het datacenter.

Impact: Indien een aanvaller onbevoegd toegang heeft verkregen tot het ‘politie’ netwerk, kan deze door het gebrek aan netwerksegmentatie vrij routeren binnen dit netwerk en vanuit geïnfecteerde machines andere systemen benaderen. Ook kan malware hierdoor in het geval van een malware uitbraak in één van de politie applicaties met een kwetsbaarheid andere kwetsbare applicaties (inclusief kroonjuwelen) in dit netwerk infecteren.

Aanbevelingen	C	R
A **Richt microsegmentatie in** • Inventariseer voor welke machines host-based firewalls zijn ingeschakeld, en welke poorten en protocollen hierdoor geblokkeerd worden. Open hierbij alleen poorten die noodzakelijk zijn voor het functioneren van de dienst(en). • Bij voorkeur: migreer van het ‘politie.local’ naar het ‘prd.int.politie’ domein. Binnen deze nieuwe omgeving is netwerksegmentatie architecturaal strakker ingericht door gebruik van NSX firewalls, en is het toepassen van host-based firewalling minder noodzakelijk.	H	H
B **Controleer netwerkpaden periodiek** • Voer periodiek netwerkscans uit om netwerkpaden te verifiëren, zodat gecontroleerd kan worden of netwerksegmentatie daadwerkelijk wordt afgedwongen.	M	M

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met het GI/Netwerken Team, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.2 Beperkt beheer toegangsrechten DevOps account

Domein	Kans	Impact	Risico
CSC04	L	H	M

Observatie

Het DevOps team van de Biometrievoorziening maakt (tijdelijk) gebruik van een enkele KeePass file waar alle wachtwoorden van onder andere service- en databaseaccounts voor beide omgevingen instaan. Deze file wordt op dit moment door ongeveer 12 beheerders gebruikt, en operaties hierop worden niet gemonitord. Het wachtwoord van deze KeePass file wordt nauwelijks gewijzigd: de laatste keer was in ieder geval meer dan een jaar geleden.

Kans: Om de aanval uit te kunnen voeren dient een aanvaller toegang te hebben tot een account van een van de beheerders. Daarnaast dient een aanvaller het wachtwoord te weten van de KeePass file. Het feit dat dit wachtwoord een tijd lang niet is veranderd, vergroot deze kans.

Impact: In het geval van een succesvolle aanval zou een aanvaller volledige toegang krijgen tot het DevOps 'root' account, wat beheertoegang verschaft tot onder andere de test- en ontwikkelomgevingen van Catch en Havank. Dit kan leiden tot ernstige confidentialiteitsproblemen (door het lekken van informatie), integriteitsproblemen (doordat data op de test- en ontwikkelomgevingen en zonder sporen aangepast kan worden, en dit mogelijk ook op de productieomgeving doorgevoerd kan worden), en beschikbaarheidsproblemen (doordat systemen met beheerrechten naar vrije wil aangepast en uitgeschakeld kunnen worden).

Aanbevelingen		C	R
A	**Implementeer een PAM tool** • Bij voorkeur: implementeer een Privileged Account Management (PAM) oplossing waarbij de inloggegevens van het beheeraccount na ieder gebruik worden vervangen.	H	M
B	**Personaliseer het DevOps account** • Zorg dat het DevOps account niet voor elke beheerder toegankelijk is, en dat inloggen alleen kan via een persoonlijk beheerderaccount voor elke beheerder. Gebruik bij voorkeur een tweede authenticatie factor (2FA).	M	M
C	**Periodieke KeePass wachtwoordwijziging** • Wijzig het KeePass wachtwoord periodiek, bij voorkeur jaarlijks.	L	M
D	**Monitor de KeePass file** • Monitor wie operaties uitvoert op de Keepass files (.kdbx en config.xml) om misbruik te kunnen detecteren, bijvoorbeeld door gebruik van SIEM tooling.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.3 Ontoereikend back-upbeleid

Domein	Kans	Impact	Risico
CSC10	L	H	M

Observatie

Gegevens in de Biometrievoorziening worden dagelijks geback-upt en op drie locaties (geografisch) redundant opgeslagen. Veranderingen aan back-ups op de primaire locatie worden direct op de andere locaties doorgevoerd. Er worden echter geen back-ups 'offline' opgeslagen, waardoor de omgevingen gevoelig zijn voor aanvallen die data onherstelbaar maken (zoals bijvoorbeeld ransomware-aanvallen) gezien de data op de andere back-up locaties ook direct wordt versleuteld.

Er vinden incidenteel tests op back-ups plaats. Back-ups worden echter niet structureel getest, wat zou kunnen betekenen dat het herstellen van grotere hoeveelheden data van deze back-ups niet (goed) werkt.

Back-ups op de database (Oracle PaaS) worden gemaakt op niveau van het hele platform, en niet op individueel niveau. Mochten er door een aanvaller specifieke bestanden gemanipuleerd worden, is er geen manier om dit te herstellen behalve door het hele platform terug te zetten. Data op fileshares (NFS) kan ook individueel tot 28 dagen terug gehaald worden. Alle systemen naast de database en fileshares worden beheerd door het Generieke Infrastructuur (GI) team, en hierbij kunnen individuele bestanden uit de geback-upte VMs op verzoek wel tot 28 dagen terug hersteld worden. Dit is echter in de praktijk tot op heden nog nooit aangevraagd.

Kans: Dit risico kan zich alleen manifesteren na het kwijtraken van data, bijvoorbeeld door een corrupt bestand, een gebruikersfout of een ransomware-infectie. De kans dat de back-ups in een dergelijk geval niet toereikend zijn is moeilijk in te schatten gezien back-ups niet worden getest, maar waarschijnlijk klein. De kans dat data onherstelbaar wordt gemanipuleerd is ook klein, gezien een aanvaller hiervoor zowel de data op de database als de back-ups moet manipuleren en dus schrijftoegang tot beide dient te hebben. Dit is echter wel mogelijk in het geval van bijvoorbeeld ransomware, wanneer deze zich eerst over het netwerk verspreidt en daarna de aanwezige data op zowel de database als de back-up servers versleutelt.

Impact: In geval van een incident waarbij data niet hersteld kan worden, zou in het ergste geval alle data van de Biometrievoorziening onherstelbaar verloren kunnen gaan.

Aanbevelingen		C	R
A	**Gebruik een 'offline' locatie voor back-up opslag** • Gebruik naast de huidige opslagwijzen voor back-ups een back-up locatie die niet aan hetzelfde netwerk aangesloten zit, en welke aanpassingen aan de primaire back-up locatie niet direct doorvoert. Hierdoor blijft data herstelbaar in geval van bijvoorbeeld een ransomware incident.	M	M
B	**Implementeer herstelmogelijkheden voor individuele bestanden op de database** • Implementeer een methode waarbij niet alleen het hele platform maar ook individuele bestanden hersteld kunnen worden na een mogelijke gebruikersfout of aanval op de database.	L	M
C	**Verifieer de back-ups** • Laat de back-up software de integriteit van de back-up verifiëren en voer periodiek controles uit om de herstelfunctie van de back-ups te kunnen garanderen.	L	M

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met het GI team, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.4 Patches worden niet snel genoeg geïnstalleerd

Domein	Kans	Impact	Risico
CSC03	L	H	M

Observatie

Nieuwe patches op de database en besturingssystemen worden volgens een vaste procedure semi-automatisch door het bijbehorende infra team uitgevoerd. Patches op applicaties die op deze systemen draaien worden echter ad hoc geïnstalleerd, en veel applicatieversies zijn daarom waarschijnlijk verouderd en mogelijk kwetsbaar. Voor leveranciers staat wel in een SLA hoe snel patches op dit soort applicaties zouden moeten worden geïmplementeerd, maar in de praktijk gebeurt dit niet altijd. Er is geen centraal overzicht (bijvoorbeeld een CMDB) van softwareversies voor gebruikte applicaties.

Het doorvoeren van kritische patches, wat nodig is bij situaties zoals een nieuwe ontdekte kritische kwetsbaarheid aangekondigd door een High-High Security (HHS) melding vanuit het NCSC, gebeurt vaak binnen een dag. Hier is één beheerder voor verantwoordelijk, die controleert of de melding van toepassing is. Wanneer dit zo is, zet deze beheerder de kwetsbaarheid door naar de juiste persoon. Hier is echter geen formele procedure voor ingericht, wat de kans vergroot dat kritische kwetsbaarheden niet volledig opgelost of over het hoofd gezien worden, waardoor het patchproces niet wordt gestart.

Kans: Wanneer nieuwe kwetsbaarheden gepubliceerd worden die de applicatieomgeving raken, kunnen deze worden misbruikt door een aanvaller met toegang tot het KA netwerk. Afhankelijk van de bekendheid van de kwetsbaarheid zijn er publiekelijk exploits beschikbaar die deze kwetsbaarheid automatisch uitbuiten, waardoor er weinig of geen technische kennis vereist is voor een aanvaller. Wel dient de aanvaller naast toegang tot het KA netwerk het IP adres en de juiste poort van deze systemen te kennen om de aanval uit te voeren, waardoor deze kans laag is.

Impact: In het geval van een succesvolle aanval zou een aanvaller in het ergste geval via de kwetsbare systemen volledige toegang kunnen krijgen tot alle (ook niet-kwetsbare) systemen. Dit kan leiden tot ernstige vertrouwelijkheidsproblemen door het lekken van informatie, integriteitsproblemen doordat data op het systeem ongewild en zonder sporen aangepast kan worden, en beschikbaarheidsproblemen doordat het systeem met beheerrechten naar vrije wil aangepast en uitgeschakeld kan worden.

Aanbevelingen		C	R
A	**Verhoog de reguliere patchfrequentie** • Update de applicaties vaker met de nieuwste stabiele versies die de security updates omvatten, met name bij onopgeloste NCSC High-High security kwetsbaarheden die van toepassing zijn op de applicaties. De aangeraden patchfrequentie en de richtlijn vanuit het patchproces binnen de Nationale Politie is één keer per vier weken. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd. • Houd versie-informatie van software bij, idealiter in een CMDB.	L	M
B	**Formaliseer een spoed patchprocedure** • Formaliseer een spoed patchprocedure, zodat gegarandeerd wordt dat kritische kwetsbaarheden worden gedicht met een snellere doorlooptijd dan in het reguliere patchproces. De richtlijn voor de maximale doorlooptijd hiervan vanuit het proces binnen de Nationale Politie is 72 uur. • Zorg ervoor dat de rol die de beheerder verantwoordelijk voor HHS patches inneemt goed wordt overgedragen als deze beheerder het team verlaat.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.5 Onveilige dataoverdracht via de EPB

Domein	Kans	Impact	Risico
CSC12	L	H	M

Observatie

Communicatie tussen de omgevingen en een aantal derde partijen vindt hoofdzakelijk via de Externe Politie Broker (EPB) plaats. De dataoverdracht tussen de Biometrievoorziening servers en de communicerende server van de EPB (het EEP) maakt gebruik van een HTTPS verbinding. Er vind echter geen authenticatie plaats voor berichten van en naar de EPB. Daardoor kan een aanvaller namens de Biometrievoorziening gegevens sturen naar (en ontvangen van) de EPB.

Kans: Een aanvaller heeft toegang nodig tot het politienetwerk om de EPB en de Biometrievoorziening te kunnen bereiken; binnen politie.local is er geen filtering op IP-adressen voor dit communicatiekanaal. Verder dient een aanvaller te weten in welke vorm de EPB berichten verwacht om deze kwetsbaarheid effectief te kunnen exploiteren.

Impact: Wanneer een aanvaller weet in welke vorm de EPB berichten verwacht, stelt het de aanvaller in staat malware te verspreiden naar de omgeving en derde partijen. Daarnaast kan een aanvaller vervalste gegevens over zaken uploaden, zowel naar de Biometrievoorziening namens een derde partij, als naar een derde partij namens de Biometrievoorziening (via de EPB).

Aanbevelingen		C	R
A	**Implementeer authenticatie bij communicatie met de EPB** • Zorg dat er authenticatie plaatsvindt bij communicatie met de EPB en dat deze communicatie versleuteld verstuurd wordt. Dit kan door middel van het meesturen van een key, of een meer geavanceerde authenticatie zoals OAuth2.1.	M	M
B	**Beperk EPB-communicatie d.m.v. een allow-list** • Sta op de Biometrievoorziening alleen communicatie toe van en naar IP-adressen van de communicerende servers van de EPB (het EEP). Dit kan bijvoorbeeld met host-based firewalls worden afgedwongen. • Sta op EEP servers alleen communicatie toe van en naar IP-adressen van diensten die via de EPB informatie dienen uit te wisselen.	L	L

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met de EPB, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.6 Onversleutelde dataopslag

Domein	Kans	Impact	Risico
CSC13	L	H	M

Observatie

Alle data in de database van de Biometrievoorziening is onversleuteld opgeslagen. Deze database bevat een grote hoeveelheid zeer gevoelige data waaronder vinger- en gelaatsafdrukken.

De back-ups van deze data zijn tevens onversleuteld opgeslagen.

Kans: Om toegang te krijgen tot de onversleutelde bestanden dient een aanvaller toegang te krijgen tot de Biometrievoorziening server, de database zelf, of de back-ups. Hiervoor zou deze aanvaller fysiek bij deze machines moeten komen, of een manier moeten vinden om via politie.local met een van deze databases te verbinden.

Impact: Een succesvolle aanval op de database of de back-up server kan ertoe leiden dat deze aanvaller de onversleutelde bestanden (waaronder vinger- en gelaatsafdrukken) kan inzien, uitlezen en downloaden.

Aanbevelingen	C	R
A **Versleutel de data** • We raden aan om de data op de database te versleutelen (encrypten), zodat een aanvaller, wanneer hij toegang heeft tot het systeem, niet direct alles kan uitlezen. • Daarnaast raden we aan om data op de back-uplocatie te versleutelen. Uit gesprekken met het Oracle PaaS team is gebleken dat er al een product zo goed als klaar ligt om in gebruik te worden genomen, maar dit is nog niet is gebeurd. *N.B.: we raden bij het implementeren van deze aanbeveling aan om samen te werken met het Oracle PaaS team, gezien hun expertise in dit gebied.*	M	M

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.7 Geen beleid voor versleutelen van mobiele gegevensdragers

Domein	Kans	Impact	Risico
CSC13	L	H	M

Observatie

Het gebruik van versleuteling op mobiele gegevensdragers, zoals USB-sticks, wordt niet afgedwongen of gemonitord. Hierdoor kan iedereen met toegang tot de KA vrij data van dit systeem naar zijn of haar eigen USB-stick verplaatsen.

Het team gaf aan dat voor de Biometrie-gebruikers aparte, geïsoleerde VMs gaan worden ingeregeld, waarin de applicaties worden uitgevoerd. Hierdoor is het lastiger om applicatiedata direct van en/of naar een USB-stick te verplaatsen.

Kans: Door het gebruik van de geïsoleerde VMs is de kans klein dat een gebruiker in staat is om gegevens uit de Biometrievoorziening naar een mobiele gegevensdrager te verplaatsen. Bij verlies van een onversleutelde mobiele gegevensdrager bestaat de kans dat een onbevoegde deze in handen krijgt.

Impact: Het verliezen van onversleutelde mobiele gegevensdragers kan ertoe leiden dat gevoelige gegevens uitlekken, zoals vingerafdrukken en foto's van verdachten, zonder te kunnen achterhalen waar de data oorspronkelijk vandaan kwam en wie de veroorzaker van dit datalek was.

Aanbevelingen	C	R
A **Versleutel mobiele gegevensdragers** • Dwing versleuteling af bij het gebruiken van mobiele gegevensdragers. • Blokkeer mobiele gegevensdragers volledig (op de VMs) wanneer deze niet nodig zijn voor de werkzaamheden. *N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met de Dienst ICT, gezien hun expertise in dit gebied.*	M	M

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.8 Gebrek aan monitoring

Domein	Kans	Impact	Risico
CSC06	M	M	M

Observatie

Alle acties die in de applicatie worden ondernomen (zoals views, edits, en deletes) worden op applicatieniveau gelogd. Gebruikers kunnen alle werkprocessen zien; het is via de applicatie makkelijk om in te zien welke zoekopdrachten andere gebruikers open hebben staan. Daarnaast worden op de servers acties zoals inlogpogingen en draaiende services ook gelogd met een focus op performance.

Logs worden naast deze incidentele checks echter in de praktijk nauwelijks actief gebruikt, behalve op ad hoc verzoek voor rechtszaken of vanuit het VIK. Logs worden verder ook niet gemonitord of verzonden naar een centrale log-oplossing voor opslag of analyse: het traject om dit te implementeren is wel gaande.

Kans: De kans op het detecteren van een 'ongoing' aanval is aanwezig gezien logs wel regelmatig worden bekeken, maar niet proactief en niet buiten kantoortijd. Het vervolgrisico, dat logs worden aangepast zodra een kwaadwillende zich op het systeem begeeft, neemt hierdoor toe. Verder is de kans dat een aanval achteraf wordt gedetecteerd nagenoeg nihil, doordat de logs niet structureel worden geanalyseerd.

Impact: Doordat de logs niet worden geanalyseerd kan een aanvaller ongemerkt zijn gang gaan zodra het systeem gecompromitteerd is, waardoor vrijwel iedere aanval ongemerkt doorgang zal kunnen vinden áls deze zich manifesteert.

Aanbevelingen		C	R
A	**Centraliseer loganalyse en opslag** • Centraliseer de opslag en analyse van (audit) logs.	M	M
B	**Deel logs met het SOC** • Deel (audit) logs met het SOC van de Nationale Politie om mogelijke security incidenten te kunnen detecteren.	H	M
C	**Monitor gebruikersgedrag en afwijkingen** • Monitor het gedrag van gebruikers, en de afwijkingen hierin van normaal gebruik, om misbruik van de omgeving te kunnen detecteren.	H	M

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met het SOC, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.9 Geen blokkade voor cloudopslag

Domein	Kans	Impact	Risico
CSC13	M	M	M

Observatie

Het gebruik van publieke diensten voor cloudopslag (zoals Box, Dropbox of Google Drive) is verboden volgens het beleid van de Nationale Politie, maar wordt niet geblokkeerd. Hoewel bij het openen van sommige diensten, zoals Dropbox, op het intranet wel eerst een waarschuwing wordt getoond, kan de gebruiker door op een link te klikken alsnog doorgaan naar de website.

Het gebruik van clouddiensten wordt niet gemonitord op mogelijke datalekken.

Kans: Om dit risico te verwezenlijken moet een gebruiker per ongeluk gevoelige data naar een onveilige cloudomgeving kopiëren, of wordt deze bewust gebruikt als data-exfiltratiekanaal door een aanvaller wanneer deze binnen is.

Impact: Het kopiëren van data naar een onveilige cloudomgeving kan ertoe leiden dat (gevoelige) gegevens zoals vingerafdrukken uitlekken, zonder te kunnen achterhalen waar de data oorspronkelijk vandaan kwam en wie de veroorzaker van dit datalek was.

Aanbevelingen	C	R
A **Blokkeer of monitor clouddiensten** • Blokkeer het gebruik van cloudopslag diensten zoveel mogelijk, en monitor het netwerkverkeer op mogelijke data-exfiltratie waar blokkade niet mogelijk is.	L	M

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met de Dienst ICT, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.10 Mogelijk onveilige configuratie poorten/protocollen

Domein	Kans	Impact	Risico
CSC09	L	M	L

Observatie

Standaard worden op de firewalls binnen het netwerk vrijwel alle poorten en protocollen geblokkeerd. Via een verzoek naar het GI Team kunnen specifieke poorten worden opengezet. Resulterende wijzigingen aan openstaande poorten worden direct opgeslagen in firewall (Excel) sheets, waarop wordt gemonitord wie toegang heeft en wie er mutaties doorvoert. In deze sheets worden gebruikte protocollen en de bijbehorende versies echter niet bijgehouden, waardoor de kans bestaat dat er mogelijk kwetsbare protocollen worden gebruikt (bijvoorbeeld een verouderde SMB versie). Wel is dit risico laag gezien er periodiek (Tripwire) vulnerability scans plaatsvinden op protocollen en de bijbehorende versies, en resultaten hiervan worden gedeeld met het politie SOC.

Reviews op de configuratie van de firewalls en benodigdheid van open poorten worden niet periodiek uitgevoerd. Ook vinden er geen (automatische) port scans plaats. Dit verhoogt het risico van onnodig openstaande poorten en netwerkroutes, waardoor er mogelijke aanvalsroutes voor een aanvaller toegankelijk zijn.

Netwerkverkeer wordt op firewallniveau gelogd, wat kan helpen in het geval van potentiele dreigingen op het netwerk. Op poortniveau wordt echter niet gelogd, waardoor niet bevestigd kan worden of (openstaande) poorten alleen gebruikt worden waar ze voor bedoeld zijn. Zo kunnen bijvoorbeeld andere protocollen dan bedoeld over deze poorten worden getransporteerd (zoals SSH over HTTP).

Kans: Door de bovengenoemde punten bestaat de kans dat netwerkverkeer, poorten of protocollen gebruikt kunnen worden door aanvallers. Daarmee zijn gedeeltes van het netwerk bereikbaar voor malafide programma's of aanvallers in het netwerk terwijl deze afgeschermd zouden moeten zijn.

Impact: Het openstaan van netwerkverkeer, poorten of protocollen geeft een mogelijkheid voor malafide programma's of aanvallers om op het netwerk te komen, wat kan leiden tot beschikbaarheids-, integriteits- en vertrouwelijkheidsproblemen.

Aanbevelingen		C	R
A	**Houd een overzicht van protocollen bij in de firewall sheets** • Houd in de firewall sheets, naast een overzicht van poorten, ook een overzicht van protocollen bij.	L	L
B	**Herzie periodiek firewall regels** • Herzie de firewall regels periodiek om er zeker van te zijn dat geen onbedoelde netwerkpaden beschikbaar zijn.	L	L
C	**Voer periodiek port scans uit** • Voer periodiek (bij voorkeur maandelijks) scans op poorten uit, zodat mogelijk onnodige dan wel kwetsbare poorten worden gedecteerd en kunnen worden uitgeschakeld.	L	L
D	**Implementeer logging op poortniveau** • Zorg dat de logging op firewalls ook op poortniveau wordt geïmplementeerd, zodat potentiele kwaadwillenden vroegtijdig kunnen worden gedetecteerd.	L	L

N.B.: we raden bij het implementeren van deze aanbevelingen aan om samen te werken met het GI Team, gezien hun expertise in dit gebied.

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.11 Geen restricties op ongebruikelijke data-activiteit

Domein	Kans	Impact	Risico
CSC16	L	M	L

Observatie

Op de Biometrievoorziening omgevingen zijn er geen restricties ingesteld op ongebruikelijke handelingen op data. Wanneer pieken in data-activiteit (frequentie en/of grootte) niet op een dergelijke manier gedetecteerd of geblokkeerd worden, is het mogelijk voor een aanvaller om in een hoog tempo ongewenste activiteiten met deze data uit te voeren.

Kans: Om deze kwetsbaarheid te misbruiken is toegang tot de Biometrie-applicatie nodig, welke authenticatie door een geldige gebruikersnaam en wachtwoord vereist. Een aanvaller kan deze credentials bijvoorbeeld verkrijgen door het uitvoeren van een phishing aanval op het gebruikersaccount van een medewerker.

Impact: In het geval van een succesvolle aanval zou een aanvaller met een geldig gebruikersaccount alle bestanden waar deze toegang toe heeft, bijvoorbeeld de vinger- of gelaatsafdrukken, in een snel tempo kunnen downloaden en/of bewerken.

Aanbevelingen		C	R
A	**Stel restricties in op data-activiteit** • Stel restricties in op ongebruikelijke data-activiteit zoals bijvoorbeeld het overmatig openen, bewerken, verwijderen, downloaden en uploaden van data zoals vinger- en gelaatsafdrukken, alvorens het account (tijdelijk) te blokkeren. Bekijk hierbij vanuit functioneel beheer of er uitzonderingen nodig zijn zodat essentiële processen niet onnodig worden belemmerd.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

2.12 Onvolledig dataclassificatiemodel

Domein	Kans	Impact	Risico
CSC13	M	L	L

Observatie

Er is geen centraal overzicht van de data in de Biometrievoorziening, en data wordt daarnaast niet geclassificeerd op gevoeligheid en waarde voor de organisatie bij aanpassing, diefstal en vernietiging. Hierdoor kunnen maatregelen m.b.t. de behandeling van gevoelige data of wettelijke eisen (zoals versleuteling van de data bij opslag en/of overdracht) niet overzichtelijk worden afgedwongen.

Wel wordt er aan data zoals gelaats- en vingerafdrukken een bewaartermijn gekoppeld – in lijn met de wetgeving - afhankelijk van het type misdrijf wat de bijbehorende persoon heeft gepleegd. Zo worden DNA en dactyloscopische sporen voor de volgende termijnen bewaard:

- 12 jaar voor feiten met een strafbedreiging van minder dan 6 jaar;
- 20 jaar voor feiten met een strafbedreigingen tussen de 6 en 12 jaar;
- 80 jaar voor feiten met een strafbedreigingen van meer dan 12 jaar.

Kans: De processen en bijhorende data zijn niet op gevoeligheidsniveau geclassificeerd, waardoor de kans bestaat dat data niet adequaat wordt beschermd en/of niet aan regelgeving voldoet.

Impact: Mocht een incident optreden, kan het niet adequaat beschermen van data de afhandeling van dit incident vermoeilijken. Daarnaast kan het (mogelijk) niet voldoen aan regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), de Wet politiegegevens (Wpg), en de Wet justitiële en strafvorderlijke gegevens (Wjsg) leiden tot boetes van de Autoriteit Persoonsgegevens.

Aanbevelingen		C	R
A	**Inventariseer alle gevoelige data binnen de omgeving** • Inventariseer waar alle data zich bevindt binnen de omgeving van de Biometrievoorziening en zorg dat er een overzicht gedocumenteerd is.	L	L
B	**Stel een dataclassificatiemodel op** • Breidt de classificatie op geïnventariseerde data op gevoeligheid uit, gebaseerd op de wettelijke eisen en geschatte impact bij aanpassing, diefstal of vernietiging, en documenteer deze. • Zorg dat gepaste beveiligingsmaatregelen worden toegepast per gevoeligheidsniveau. • Zorg door middel van processen dat het data classificatiemodel up to date blijft, bijvoorbeeld door middel van jaarlijkse evaluaties of bij het toevoegen van nieuwe processen aan de Biometrievoorziening omgeving.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3

Observaties interne infrastructuurtest

Observatieoverzicht

Onderstaande tabel bevat de observaties die zijn geïdentificeerd tijdens de interne infrastructuurtest en de inschatting van de kans, impact en het bijbehorende risico (laag, medium of hoog) per observatie. De details per observatie zijn opgenomen op de volgende pagina's van deze sectie.

#	Domein	Observatie	Kans	Impact	Risico
3.1	CSC14	Openbare NFS shares beschikbaar op het interne netwerk	M	H	H
3.2	CSC14	Beheerinterfaces beschikbaar op het interne netwerk	L	H	M
3.3	CSC05	Onveilige SMB configuratie	L	M	L
3.4	CSC14	Gevoelige data onversleuteld verstuurd	L	M	L
3.5	CSC05	Onveilige TLS configuratie	L	M	L
3.6	CSC05	Zwakheden in TLS certificaten	L	M	L
3.7	CSC03	Verouderde en kwetsbare software geïdentificeerd	L	M	L
3.8	CSC05	Versie informatie geïdentificeerd	M	L	L
3.9	CSC05	Overbodige bestanden aangetroffen	M	L	L

Laag	Medium	Hoog
L	M	H

3.1 Openbare NFS shares beschikbaar op het interne netwerk

Domein	Kans	Impact	Risico
CSC14	M	H	H

Observatie

We hebben vastgesteld dat er meerdere zogenaamde Network File Systems (NFS) op het interne netwerk aanwezig zijn die benaderd kunnen worden zonder authenticatie.

De volgende NFS mounts zijn aangetroffen:

- 10.247.36.78:/mvi;
- 10.247.36.78:/mvi-share.

De aangetroffen mounts bevatten gevoelige informatie zoals foto's van verdachten en technische informatie zoals configuratie en logbestanden.

N.B.: Zie ook observatie 2.1 'Gebrek aan segmentatie binnen het netwerk'.

Kans: Om misbruik te kunnen maken van deze kwetsbaarheid moet een aanvaller zich op het interne 'politie.local' netwerk bevinden. Beschikbare NFS shares kunnen worden gevonden met tools die vrij beschikbaar zijn.

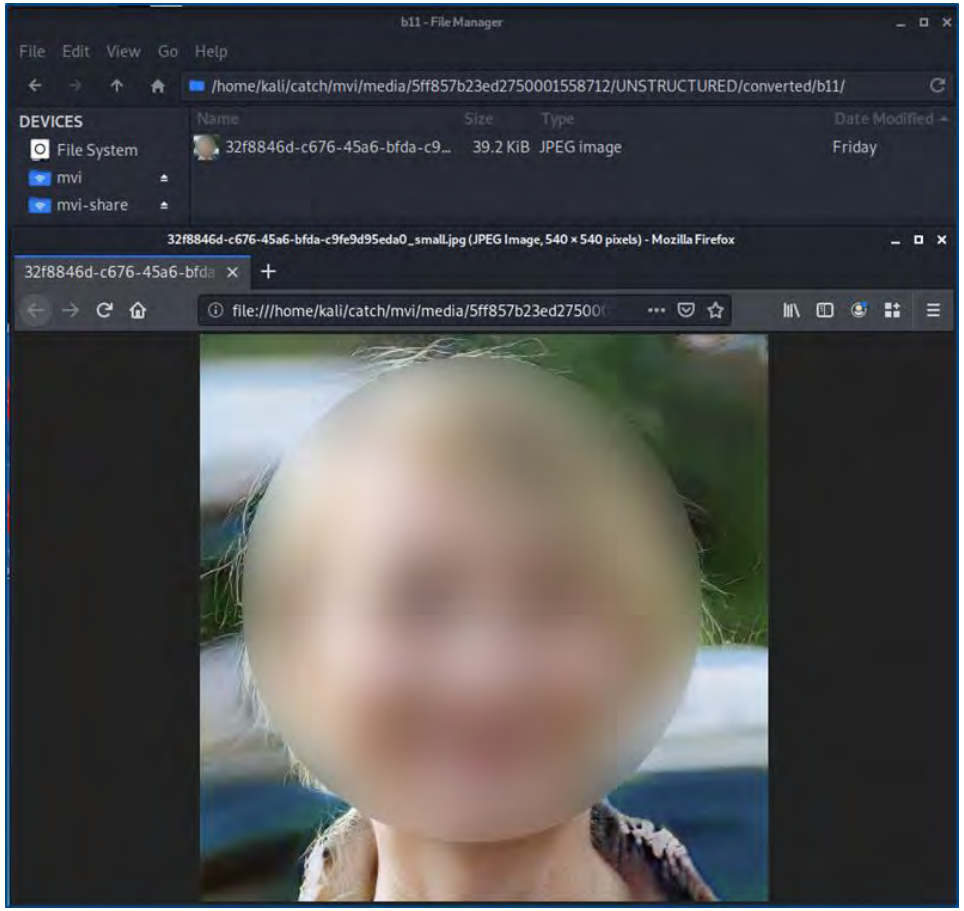
Impact: De NFS shares bevatten gevoelige persoonlijke data zoals foto's en technische informatie zoals configuratie en logbestanden. Een succesvolle aanval kan leiden tot toegang tot deze gevoelige data. Daarnaast kan de inhoud van de aangetroffen bestanden ook worden gebruikt door een aanvaller als een platform voor verdere aanvallen. Ook kan de aanvaller de inhoud van de bestanden aanpassen of zelf bestanden uploaden.

Aanbevelingen	C	R
A **Beperk toegang tot de NFS shares** • We adviseren om de configuratie van de NFS mounts aan te passen, zodat ze alleen bereikbaar zijn voor geautoriseerde gebruikers.	L	H

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – Openbare NFS shares beschikbaar op het interne netwerk



Screenshot 1 – Het was mogelijk om deze foto op de openbare NFS share te openen.

3.2 Beheerinterfaces beschikbaar op het interne netwerk

Domein	Kans	Impact	Risico
CSC14	L	H	M

Observatie

We hebben vastgesteld dat beheerinterfaces bereikbaar zijn voor iedereen vanaf het interne netwerk. Dit betekent dat iedereen vanaf politie.local kan proberen een gebruikersnaam en wachtwoord te verkrijgen om ongeautoriseerde toegang te verkrijgen tot de beheerinterface(s). De volgende beheerinterfaces zijn aangetroffen:

- 85 SSH beheerinterfaces*;
- Meerdere OneFS beheerinterfaces*;
- Meerdere RabbitMQ beheerinterface*;
- Een Pacemaker/Corosync beheerinterface op 10.247.32.182, 10.247.32.168 en 10.247.32.166 via TCP poort 2224;
- Een Jetty beheerinterface op 10.149.103.75:7879.

** N.B: het overzicht van alle SSH, OneFS en RabbitMQ interfaces is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage van dit rapport*.

Kans: De beheerinterfaces vereisen authenticatie om toegang te krijgen tot de services. Omdat verkeer naar de RabbitMQ, Pacemaker/Corosync en Jetty interfaces onversleuteld wordt verzonden, kunnen inloggegevens ook worden verkregen door het onderscheppen van netwerkverkeer. De aanvaller moet zich op specifieke netwerken bevinden om de gegevens te onderscheppen (bijvoorbeeld in het netwerkpad tussen de gebruiker en de server). Geavanceerde technische vaardigheden zijn benodigd om dit verkeer te onderscheppen.

Impact: In geval van een succesvolle aanval zou een aanvaller volledige toegang krijgen tot de onderliggende systemen, de OneFS storage en de beheerpagina's van services. Dit kan leiden tot het ongeautoriseerd lezen, aanpassen en/of verwijderen van inloggegevens, persoonsgegevens, verstuurde berichten en andere gevoelige data, zoals biometrische gegevens.

Aanbevelingen

		C	R
A	**Beperk toegang tot de beheerinterfaces** • We raden aan beheerwerkzaamheden uit te voeren via een ander kanaal dan die van normale gebruikers naar de servers. Het is mogelijk om IP filtering te gebruiken om toegang tot de beheerinterface te limiteren tot specifieke locaties of systemen, maar in het geval van de Politie zouden beheerservices alleen beschikbaar moeten zijn vanaf het iscbeheer.local netwerk via de beheer netwerkinterface op de systemen; • Daarnaast raden we aan om HTTP te vervangen door de veiligere variant HTTPS die over een versleutelde verbinding communiceert; • Tot slot raden we aan om authenticatie af te dwingen op iedere beheerinterface met een tweede authenticatie-factor (MFA/2FA). Kies bij het implementeren van MFA/2FA voor een 'two-factor' authenticatie oplossing welke gebaseerd is op 'standards-based' algoritmen en authenticatie protocollen (zoals de Google Authenticator of het U2F-protocol).	L	M

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3.3 Onveilige SMB configuratie

Domein	Kans	Impact	Risico
CSC05	L	M	L

Observatie

Server Message Block (SMB) is een netwerkprotocol dat gebruikt wordt om bestandsuitwisseling tussen meerdere systemen in een domein of werkgroep mogelijk te maken. SMB wordt voornamelijk gebruikt voor beheerdoeleinden van servers.

We hebben vastgesteld dat “SMB Signing” niet wordt afgedwongen op een groot aantal systemen op het interne netwerk. Dit stelt een aanvaller in staat om een zogenaamde “man-in-the-middle” aanval uit te voeren waardoor de integriteit van de opgevraagde bestanden mogelijk gecompromitteerd wordt.

N.B.: op de volgende pagina hebben wij een overzicht toegevoegd van alle systemen in scope waarop SMB Signing uitgeschakeld staat.

Kans: Het uitvoeren van een “man-in-the-middle” aanval vereist geavanceerde technische kennis. Bovendien moet de aanvaller zich op het interne pad tussen de server en de gebruiker bevinden.

Impact: Door het uitvoeren van een “man-in-the-middle” aanval kan een aanvaller bestanden onderscheppen maar ook de integriteit en authenticiteit van een bestand compromitteren. Dit stelt een aanvaller in staat om malafide bestanden te verspreiden op het netwerk, zoals virussen of malware, of specifieke wijzigingen te maken aan bestanden die bedoeld zijn voor een getroffen server. De kwetsbaarheid heeft echter alleen invloed op de gebruikers bij wie de aanvaller een “man-in-the-middle” aanval kan uitvoeren.

Aanbevelingen		C	R
A	**Verbeter de SMB configuratie** • Wij raden aan om gebruik te maken van “SMB Signing”. Door deze optie te gebruiken worden de SMB pakketten op netwerk niveau beveiligd met een digitale handtekening. Hierdoor kan de ontvanger van het bestand altijd de authenticiteit en integriteit van het bestand valideren.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Overzicht van kwetsbare SMB services

Onderstaande tabel toont de SMB services die zijn geïdentificeerd op het interne politie.local netwerk en waarop “SMB Signing” niet wordt afgedwongen:

Systemen waarop SMB Signing niet wordt afgedwongen via TCP poort 445				
10.247.193.134	10.247.193.124	10.247.193.114	10.247.193.104	10.247.193.94
10.247.193.133	10.247.193.123	10.247.193.113	10.247.193.103	10.247.193.93
10.247.193.132	10.247.193.122	10.247.193.112	10.247.193.102	10.247.193.92
10.247.193.131	10.247.193.121	10.247.193.111	10.247.193.101	10.247.193.91
10.247.193.130	10.247.193.120	10.247.193.110	10.247.193.100	10.247.193.90
10.247.193.129	10.247.193.119	10.247.193.109	10.247.193.99	10.247.193.89
10.247.193.128	10.247.193.118	10.247.193.108	10.247.193.98	
10.247.193.127	10.247.193.117	10.247.193.107	10.247.193.97	
10.247.193.126	10.247.193.116	10.247.193.106	10.247.193.96	
10.247.193.125	10.247.193.115	10.247.193.105	10.247.193.95	
10.247.193.134	10.247.193.124	10.247.193.114	10.247.193.104	

3.4 Gevoelige data onversleuteld verstuurd

Domein	Kans	Impact	Risico
CSC14	L	M	L

Observatie

We hebben vastgesteld dat er Advanced Message Queuing Protocol (AMQP) services zijn die inloggegevens onversleuteld versturen. Dit stelt een aanvaller in staat om gevoelige data te onderscheppen.

N.B.: op de volgende pagina hebben wij een overzicht toegevoegd van alle systemen waarop de beheerinterfaces beschikbaar zijn.

Kans: Geavanceerde technische kennis is vereist om netwerkverkeer te onderscheppen. De aanvaller moet zich op specifieke netwerken bevinden om de gegevens te onderscheppen (bijvoorbeeld het netwerkpad tussen de gebruiker en de webserver).

Impact: Een succesvolle aanval kan ertoe leiden dat een aanvaller inloggegevens kan onderscheppen. Hierdoor kan een aanvaller toegang krijgen tot de AMQP service en de informatie die hierover verstuurd wordt. Dit kan gebruikt worden als een platform voor verdere aanvallen.

Aanbevelingen		C	R
A	**Schakel cleartext authenticatie uit** • Schakel cleartext authenticatie uit in de configuratie van de AMQP services.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Overzicht van AMQP services op het interne netwerk

Onderstaande tabel toont de AMQP services die zijn geïdentificeerd op het interne politie.local netwerk:

Systemen met een AMQP interface via TCP poort 5672		
10.247.32.182	10.247.32.106	10.247.32.96
10.247.32.166	10.247.32.105	10.247.32.95
10.247.32.115	10.247.32.104	10.247.32.94
10.247.32.114	10.247.32.103	10.247.32.93
10.247.32.113	10.247.32.102	10.247.32.92
10.247.32.111	10.247.32.101	10.247.32.91
10.247.32.110	10.247.32.100	10.247.32.90
10.247.32.109	10.247.32.99	10.247.32.89
10.247.32.108	10.247.32.98	10.247.32.85
10.247.32.107	10.247.32.97	10.247.32.84
10.247.32.182	10.247.32.106	10.247.32.96

3.5 Onveilige SSL/TLS configuratie

Domein	Kans	Impact	Risico
CSC05	L	M	L

Observatie

We hebben de volgende zwakheden vastgesteld in de gebruikte TLS configuraties op verschillende systemen:

- Zwakke Diffie-Hellman-Keys, kwetsbaar voor de cryptografische kwetsbaarheid Logjam;
- Ondersteuning van RC4, kwetsbaar voor de cryptografische kwetsbaarheden;
- Ondersteuning voor het gebruik van een block cipher met 64-bit blokken in één of meerdere cipher suites, welke de "SWEET32" kwetsbaarheid bevat. Hierdoor is het mogelijk om bepaalde man-in-the-middle (MITM) aanvallen uit te voeren;
- Ondersteuning voor TLS 1.0 en TLS 1.1, welke de POODLE kwetsbaarheid bevatten. Verder omvatten deze protocollen cryptografische zwakheden, zoals de BEAST-aanval. Deze aanvallen kunnen leiden tot MITM.

N.B.: het overzicht van alle zwakheden in de TLS configuraties per systeem is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage.

Kans: Om deze TLS kwetsbaarheden te misbruiken moet de aanvaller zich op specifieke netwerken bevinden (bijvoorbeeld het netwerkpad tussen de gebruiker en de server). Geavanceerde technische kennis is benodigd om TLS verkeer te onderscheppen en het versleutelde verkeer te ontcijferen. Ook moet de browser van de gebruiker achterlopen op recente security updates of fout geconfigureerd zijn om te kunnen misbruiken voor zwakke ciphers.

Impact: Een succesvolle aanval kan ertoe leiden dat een aanvaller inzicht verkrijgt in gevoelige informatie, zoals foto's of vingerafdrukken van verdachten. De zwakheid treft echter alleen gebruikers van wie de aanvaller het TLS verkeer kan onderscheppen.

Aanbevelingen	C	R

A **Verbeter de SSL/TLS configuratie**
• We raden aan de TLS configuratie op de kwetsbare systemen te verbeteren. Dit kan gedaan worden door:
  • Een unieke 2048-bit of sterkere Diffie-Hellman Group te gebruiken;
  • TLS 1.2/1.3 met GCM te ondersteunen;
  • Alleen ondersteuning te bieden voor sterke cipher algoritmen met een minimale sleutellengte van 128 bits en die geen gebruik maken van het MD5 algoritme;
  • Te onderzoeken of TLS 1.0 en TLS 1.1 nodig zijn voor de huidige gebruikers van de applicatie. Indien mogelijk raden wij aan TLS 1.0 en 1.1 uit te schakelen.
• Zie ook: https://www.ssllabs.com/projects/best-practices/index.html voor een gedetailleerde aanpak om TLS op een veilige manier te configureren.
	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3.6 Zwakheden in SSL/TLS certificaten

Domein	Kans	Impact	Risico
CSC05	L	M	L

Observatie

We hebben de volgende zwakheden vastgesteld in de gebruikte TLS certificaten:

- Verschillende systemen gebruiken een TLS certificaat dat niet is afgegeven door een vertrouwde derde partij, maar dat “self-signed” is;
- Verschillende systemen gebruiken RSA keys met minder dan 2048 bits in de ‘certificate chain’.

N.B.: het overzicht van alle zwakheden in de TLS certificaten per systeem is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage.

Kans: Gebruikers worden gewaarschuwd voor self-signed certificaten in de browser, aangezien dit kan wijzen op een man-in-the-middle aanval. Als de applicatie geen gebruik maakt van een certificaat van een vertrouwde partij, wordt deze waarschuwing bij ieder gebruik getoond, en kan de gebruiker gewend raken aan de beveiligingswaarschuwingen en een aanval niet meer herkennen. Hierdoor wordt de kans verhoogd dat een aanvaller een succesvolle man-in-the-middle aanval kan uitvoeren. De aanvaller moet zich op specifieke netwerken bevinden om de gegevens te onderscheppen (bijvoorbeeld het netwerkpad tussen de gebruiker en de server). Geavanceerde technische kennis is vereist om een man-in-the-middle aanval uit te voeren.

Impact: Een succesvolle aanval kan ertoe leiden dat een aanvaller inzicht verkrijgt in gevoelige informatie, zoals foto’s of vingerafdrukken van verdachten. De kwetsbaarheid heeft echter alleen invloed op de gebruikers waarvoor de aanvaller een man-in-the-middle aanval kan uitvoeren.

Aanbevelingen	C	R

A **Vraag nieuwe SSL/TLS certificaten aan**
• We raden aan nieuwe TLS certificaten aan te vragen waarin de volgende problemen zijn verholpen:
  • De certificaten moeten verstrekt worden door een vertrouwde derde partij die door alle grote browsers ook wordt vertrouwd. Op het interne netwerk betekent dit dat een interne certificaatautoriteit gebruikt moet worden waarvan het root-certificaat op de endpoints geïnstalleerd wordt;
  • Zorg ervoor dat TLS certificaten in de “certificate chain” gebruik maken van RSA keys van minstens 2048 bits en vernieuw alle certificaten die zijn gesigned door de oude certificaten.
• Zie ook https://www.ssllabs.com/projects/best-practices/index.html voor een gedetailleerde aanpak om SSL op een veilige manier te configureren.
	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3.7 Verouderde en kwetsbare software geïdentificeerd

Domein	Kans	Impact	Risico
CSC03	L	M	L

Observatie

We hebben vastgesteld dat een verouderde library in gebruik is binnen de Catch en Havank omgeving. Onderstaande verouderde library is geconstateerd:

- jQuery versie 1.12.4, uitgebracht in mei 2016, terwijl jQuery versie 3.5 is uitgebracht in april 2020. jQuery 1.12.4 is kwetsbaar voor Cross-Site Scripting (XSS) aanvallen.

N.B.: het overzicht van alle systemen waarop de library gevonden is, is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage.

Kans: Deze kwetsbaarheid kan worden misbruikt door iedereen op het interne netwerk. Geavanceerde technische kennis is vereist voor een aanvaller om een exploit voor de aangetroffen kwetsbaarheid te ontwikkelen. Daarnaast is het vereist dat er daadwerkelijk gebruik gemaakt word van de specifieke kwetsbare functie uit de library.

Impact: Als een aanvaller de software kan compromitteren, is het mogelijk om XSS aanvallen uit te voeren op gebruikers van de applicatie. Een succesvolle aanval kan ertoe leiden dat een aanvaller inzicht verkrijgt in gevoelige informatie, zoals foto's of vingerafdrukken van verdachten.

Aanbevelingen	C	R
A **Verbeter het update proces** • We raden aan de systemen te voorzien van de laatste security updates. • Verder raden we aan om het update proces aan te scherpen om kwetsbare software tijdig te identificeren. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3.8 Versie informatie geïdentificeerd

Domein	Kans	Impact	Risico
CSC05	M	L	L

Observatie

We hebben vastgesteld dat gedetailleerde versie informatie getoond wordt in de zogenaamde HTTP response headers, via foutmeldingen, ‘welcome banners’ of op webpagina’s van de betreffende software.

Deze informatie omvat bijvoorbeeld:

- 10.149.103.75:7879, toont de Jetty versie;
- 10.247.32.91:8008, toont de Apache versie.

Deze informatie kan worden gebruikt in verdere aanvallen.

N.B.: het complete overzicht van versies die getoond worden is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage.

Kans: Deze versie informatie is toegankelijk voor iedereen vanaf het interne politie.local netwerk. De versies staan op de homepage of in de response headers van de webservers.

Impact: De versie informatie kan door een aanvaller gebruikt worden als een platform voor verdere aanvallen.

Aanbevelingen	C	R
A **Verwijder overbodige bestanden van webservers** • We raden aan geen technische informatie en gedetailleerde versie informatie te tonen. Om dit te bewerkstelligen moet de achterliggende software ingesteld worden om geen versie informatie te tonen in HTTP response headers, via foutmeldingen of op webpagina’s.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

3.9 Overbodige bestanden aangetroffen

Domein	Kans	Impact	Risico
CSC05	M	L	L

Observatie

We hebben vastgesteld dat een groot aantal overbodige bestanden aanwezig zijn op de verschillende webservers.

Onderstaande systemen tonen overbodige bestanden:

- Een Apache “default installation” pagina op:
  - 10.247.32.182;
  - 10.247.32.166
- 10.247.32.182:8008/icons, toont overbodige “default” Apache bestanden;
- 10.247.32.113:9100/metrics, toont “metric” informatie die overbodig is voor gebruikers.

N.B.: het complete overzicht van overbodige bestanden per systeem is te zien in het Nessus kwetsbaarhedenscanrapport dat is toegevoegd als bijlage.

Kans: Deze bestanden zijn toegankelijk voor iedereen vanaf het interne politie.local netwerk. De overbodige bestanden staan vaak op de homepage van de webserver.

Impact: De overbodige bestanden bevatten technische informatie die gebruikt kan worden om verdere aanvallen op te baseren.

Aanbevelingen	C	R
A **Verwijder overbodige bestanden van webservers** • We raden aan alle overbodige bestanden te verwijderen van de webserver. • Daarnaast bevelen we aan om een proces te implementeren dat periodiek de overbodige bestanden van de server verwijdert.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

4

Observaties fatclient applicatietest Havank

Observatieoverzicht

Onderstaande tabel bevat de observaties die zijn geïdentificeerd tijdens de ‘fatclient’ testen op de Havank applicaties en de inschatting van de kans, impact en het bijbehorende risico (laag, medium of hoog) per observatie. De details per observatie zijn opgenomen op de volgende pagina’s van deze sectie.

#	Domein	Observatie	Kans	Impact	Risico
4.1	CSC14	Ongeautoriseerde toegang tot gevoelige data	M	H	H
4.2	CSC18	Local file inclusion via API	M	H	H
4.3	CSC18	Ongeauthentiseerde audit logging vanuit fatclient	M	H	H
4.4	CSC16	Zwakheden in wachtwoordbeleid	M	M	M
4.5	CSC05	Gebruikerscertificaten worden geaccepteerd	M	M	M
4.6	CSC18	Beperkte inputfiltering	M	M	M
4.7	CSC03	Verouderde en kwetsbare software geïdentificeerd	L	M	L
4.8	CSC05	Technische informatie in foutmeldingen	M	L	L

Laag	Medium	Hoog
L	M	H

4.1 Ongeautoriseerde toegang tot gevoelige data

Domein	Kans	Impact	Risico
CSC14	M	H	H

Observatie

De Havank applicatie geeft gebruikers de mogelijkheid om te communiceren met diverse API's op havank.biometrie.politie.local/api/ en havank.biometrie.politie.local/MorphoREST/. We hebben vastgesteld dat er geen toegangscontrole plaatsvindt op al deze API's, en dat er zonder gebruikersauthenticatie applicatiegegevens worden teruggestuurd.

Voorbeelden van verzoeken waarmee gevoelige data kan worden ingezien:

- https://havank.biometrie.politie.local/api/v2/ads/elements/4863/document, documenten die zijn geüpload in de applicatie, zoals afbeeldingen van vingerafdrukken;
  - De documenten zijn oplopend genummerd: door te beginnen bij 0 en te eindigen bij 4863, kan een aanvaller snel alle bijlages downloaden.
- https://havank.biometrie.politie.local/MorphoREST/dataAccess/getCasesByQuery, gegevens omtrent zaken op basis van een zoekquery.

N.B. Alle endpoints in /api en /MorphoREST zijn ongeauthenticeerd.

Kans: Om deze kwetsbaarheid te misbruiken is alleen toegang tot het politie.local netwerk nodig, en de URL moet bekend zijn. De aanvaller heeft geen Havank-account nodig, omdat de URL zonder authenticatie kan worden bereikt.

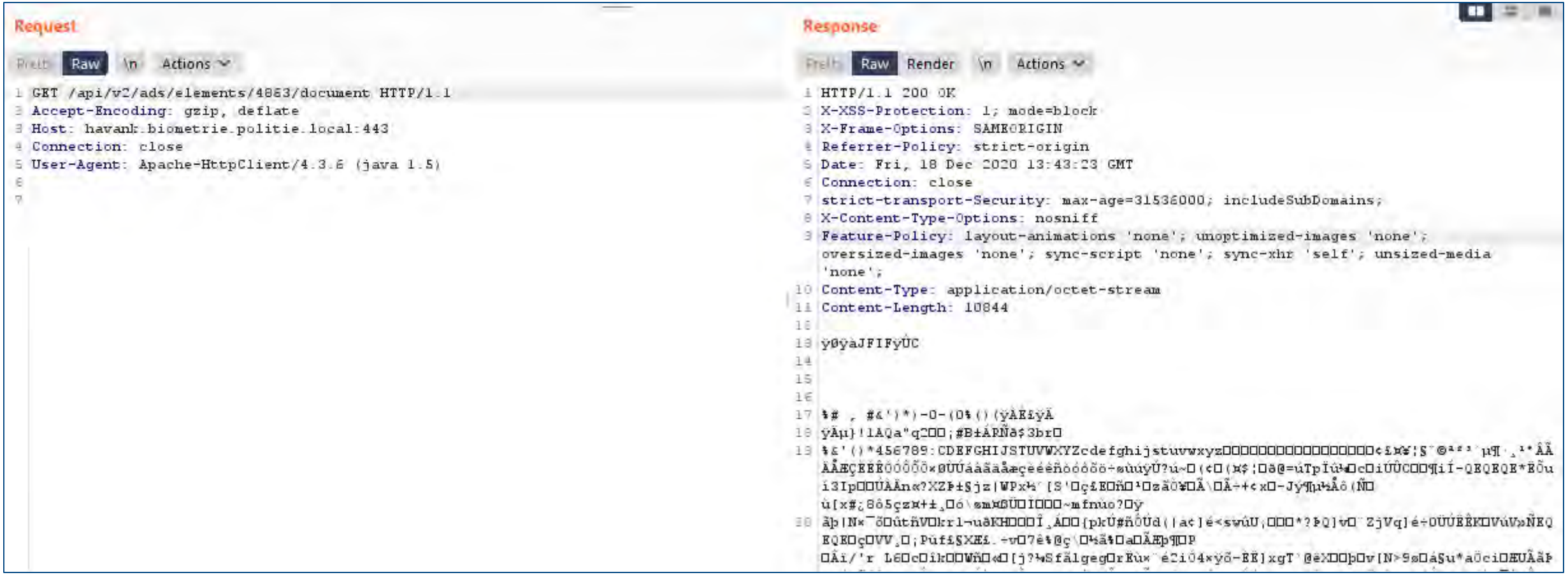
Impact: Een aanvaller kan toegang verkrijgen tot gevoelige gegevens, zoals dossierinformatie en geüploade documenten. Omdat de bijlages zijn genummerd, kan een aanvaller snel alle vingerafdrukken uit de database downloaden. Dit is zeer gevoelige informatie en kan leiden rechtszaken, reputatieschade en boetes vanuit de Autoriteit Persoonsgegevens. Het ongeautoriseerd aanpassen van gegevens leidt tot integriteitsproblemen van de omgeving en kan lopende onderzoeken ernstig hinderen.

Aanbevelingen		C	R
A	**Dwing toegangscontrole af op de Havank backendsystemen** • We raden aan logische toegangscontrole af te dwingen voor alle toegang tot gevoelige data. In een ideale situatie wordt dit afgedwongen vanuit een centrale component die gebruikt wordt om enerzijds toegangscontrole af te dwingen en anderzijds weer te geven welke data toegankelijk is voor iedere gebruiker.	M	H
B	**Geef bijlages in Havank moeilijk te raden identifiers** • We adviseren bijlages niet oplopend te nummeren, maar in plaats daarvan willekeurig gegenereerde en moeilijk te raden identifiers te geven, zoals GUID's, waarmee zij kunnen worden opgevraagd door de gebruikersinterface.	M	M

C: Complexiteit
R: Risico mitigatie

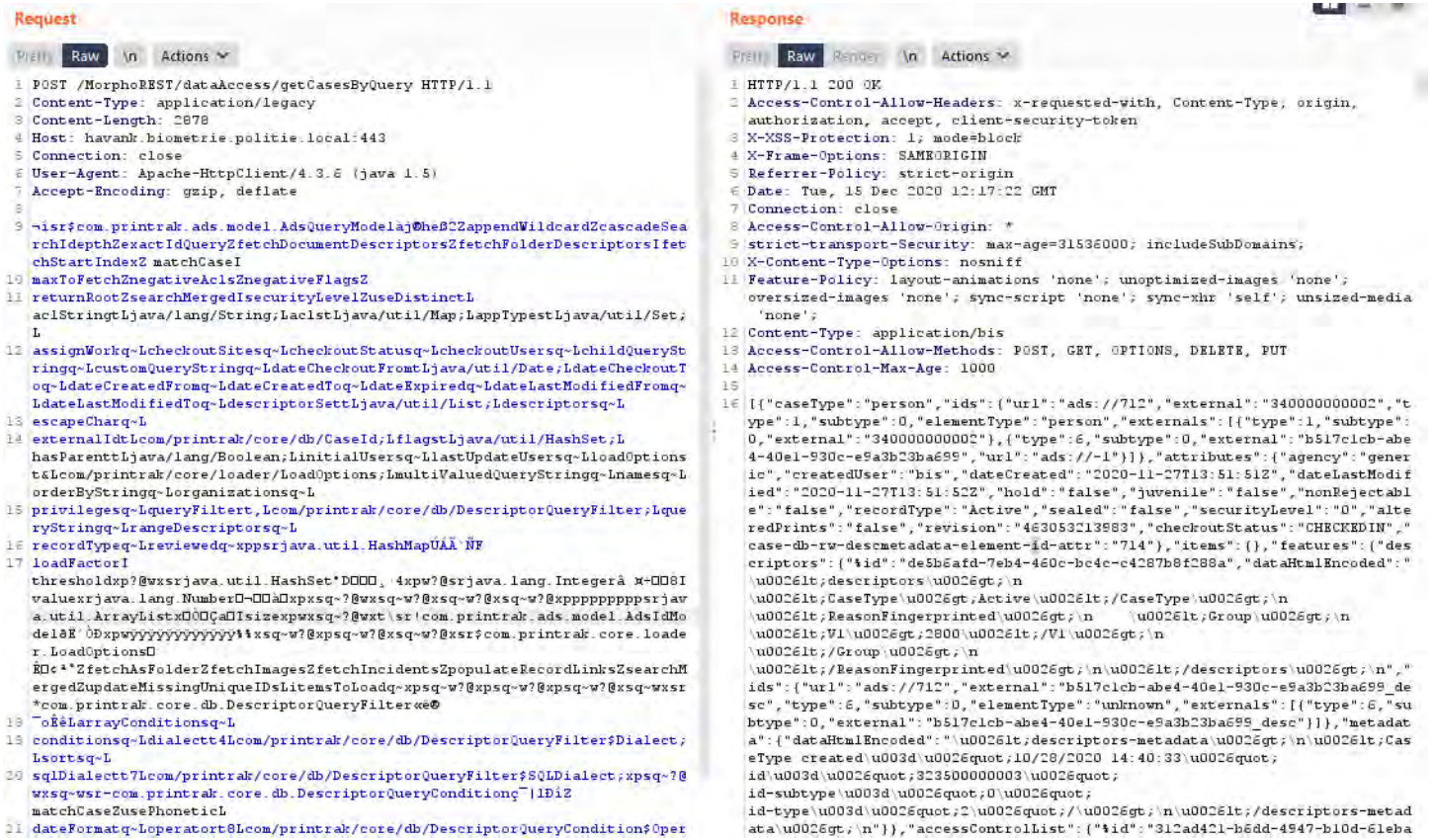
	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – ongeautoriseerde toegang tot gevoelige data (1/2)



Screenshot 1 – Het downloaden van een bijlage in de applicatie (afbeelding vingerafdruk).

Screenshot – ongeautoriseerde toegang tot gevoelige data (2/2)



Screenshot 2 – Dossierinformatie op basis van een query.

4.2 Local file inclusion via API

Domein	Kans	Impact	Risico
CSC18	M	H	H

Observatie

Voor het downloaden van bestanden met configuratie-instellingen, maakt de Havank applicatie gebruik van een API endpoint die bestanden van de server naar de applicatie terug stuurt. Daarbij worden echter geen beperkingen opgelegd over welke bestanden worden ingelezen. Zo kunnen bijvoorbeeld het /etc/passwd bestand, waarin de gebruikers van de Linux-machine staan vermeldt, worden gedownload.

Deze service kan worden bereikt op https://havank.biometrie.politie.local/MorphoREST/configurationAccess/getFile;directory=**[map]**;file=**[bestand]**

Kans: Om deze kwetsbaarheid te misbruiken is alleen toegang tot het politie.local netwerk nodig, en de URL moet bekend zijn. De aanvaller heeft geen gebruikersaccount nodig met toegang tot Havank, omdat de URL zonder authenticatie kan worden bereikt.

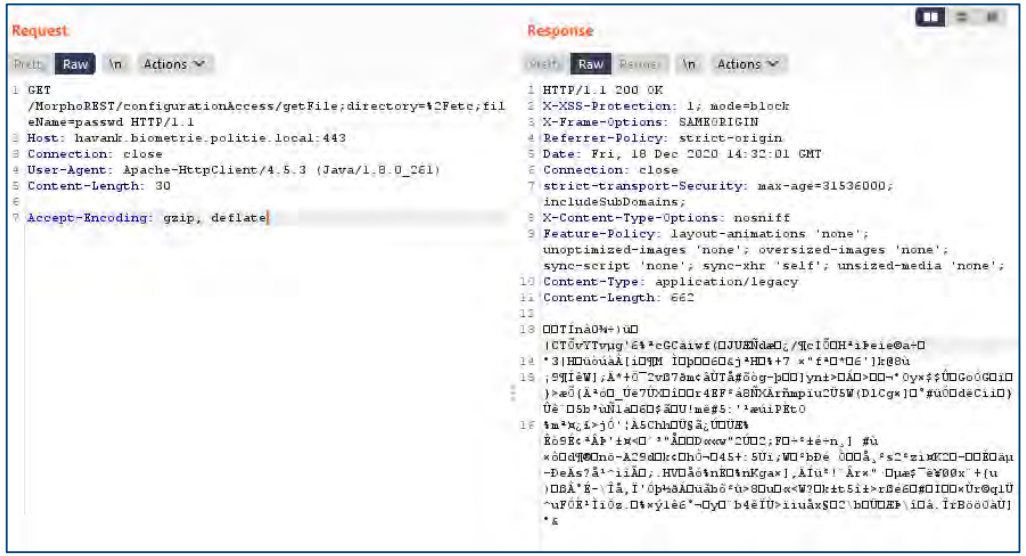
Impact: Een aanvaller kan alle bestanden uitlezen waar het serviceaccount van de Java applicatie bij kan. Dit kan leiden tot het lekken van gevoelige data die op de server aanwezig is, waaronder applicatiedata. Daarnaast wordt de aanvaller door het inzien van alle (systeem)bestanden, geholpen in het vinden van gebruikersaccounts en (kwetsbare) software. Dit maakt het aannemelijk dat een aanvaller het systeem zou kunnen overnemen en zich vanaf deze machines verder kan verspreiden over het netwerk.

Aanbevelingen	C	R
A **Limiteer de bestandstoegang** • De MorphoREST API hoeft alleen configuratiebestanden aan te bieden voor de werking van de applicatie. Het downloaden zou alleen uit de map met configuratiebestanden moeten worden toegestaan. • Waar mogelijk moet aan bestanden worden gerefereerd met een identifier waarin het absolute pad naar het bestand niet voorkomt. In plaats daarvan, moet indirect gerefereerd worden aan de bestanden (bijvoorbeeld “het 5e bestand dat kan worden gedownload”).	M	H

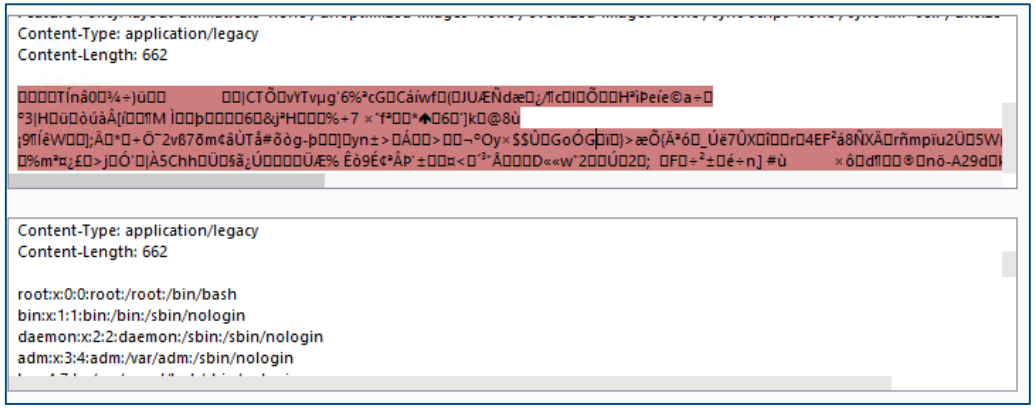
C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – local file inclusion via API



Screenshot 1 – Het downloaden van het /etc/passwd bestand.



Screenshot 2 – Decoding van de verstuurde gzip laat het oorspronkelijke bestand zien.

4.3 Ongeauthentiseerde audit logging vanuit fatclient

Domein	Kans	Impact	Risico
CSC18	M	H	H

Observatie

Het audit log van de Havank applicatie wordt (deels) gevuld met gegevens die door de fatclient direct naar de audit endpoint op https://10.247.32.81MorphoREST/auditAccess/post wordt verstuurd, zonder dat daarvoor authenticatie plaatsvindt. Hierdoor kan een aanvaller de informatie richting het backend log beïnvloeden, en de audit logs vervuilen met onzinnige of incorrecte informatie.

Daarnaast wordt er bijgehouden welke gebruiker wijzigingen maakt in bijvoorbeeld de “Person Management” module. Door de gebruikersnaam parameter in het verzoek naar de backend aan te passen naar een andere gebruiker, kan een aanvaller acties uitvoeren en het laten lijken dat een andere gebruiker dit gedaan heeft.

Kans: Om deze kwetsbaarheid te misbruiken is alleen toegang tot het interne ‘politie.local’ netwerk nodig, en de URL moet bekend zijn. De aanvaller heeft geen gebruikersaccount nodig met toegang tot Havank om onjuiste gegevens naar het log te versturen; om logging te blokkeren is echter wel technische kennis vereist.

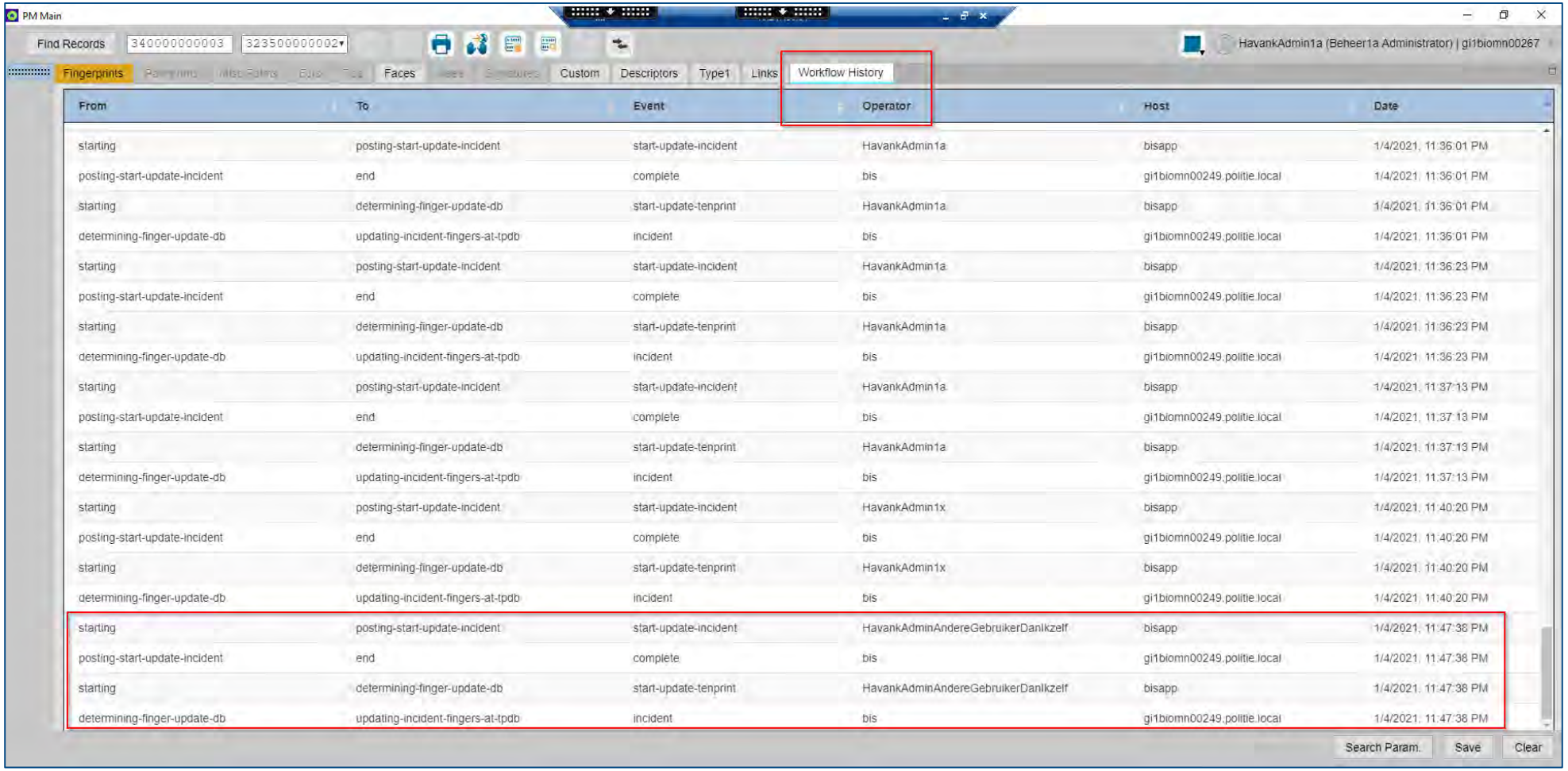
Impact: Het audit log van de applicatie is niet volledig betrouwbaar omdat iedereen in de fatclient namens een willekeurige gebruiker acties kan registreren. Daarnaast bestaat het risico dat het audit log niet compleet is, wanneer acties niet vanuit de backend systemen worden gelogd.

	Aanbevelingen	C	R
A	**Voer audit logging uit op backend systemen** • Omdat een (interne) aanvaller een zekere controle heeft over de fatclient en het systeem waarop deze draait, kan het audit log het beste worden gevuld vanuit de backend systemen.	M	H
B	**Voer audit trail logging uit op basis van sessies** • We raden aan om de audit trail met betrekking tot het wijzigen van informatie binnen de applicatie niet op basis van POST parameters te doen, maar op basis van sessies.	M	M
C	**Beveilig audit logging met authenticatie** • Om te voorkomen dat een aanvaller het audit log kan vervuilen met onjuiste gegevens over andere gebruikers, zou deze functie moeten worden afgeschermd door een authenticatiecontrole toe te voegen.	M	L

C: Complexiteit
R: Risico mitigatie

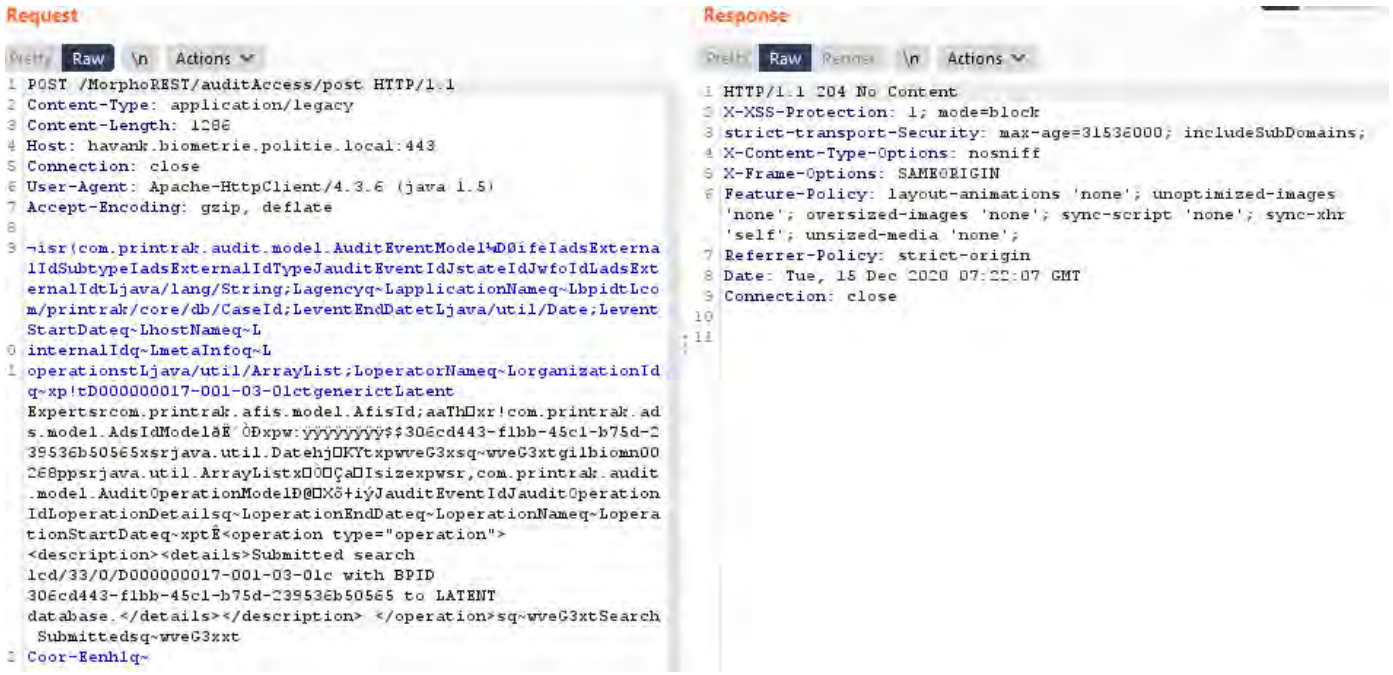
	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – Ongeauthentiseerde audit logging vanuit fatclient (1/2)



Screenshot 1 – Door POST parameters in het verzoek naar de backend aan te passen, kunnen acties worden uitgevoerd namens andere gebruikers.

Screenshot – Ongeauthentiseerde audit logging vanuit fatclient (2/2)



Screenshot 2 – Het audit log wordt aangevuld met acties in de applicatie vanuit de fatclient, zonder dat er authenticatie plaatsvindt.

4.4 Zwakheden in wachtwoordbeleid

Domein	Kans	Impact	Risico
CSC16	M	M	M

Observatie

We hebben vastgesteld dat het wachtwoordbeleid van de Havank applicatie niet in lijn is met “best practices”.

Zo worden er geen complexiteitseisen gesteld aan wachtwoorden (een combinatie van kleine letters, hoofdletters, cijfers en speciale karakters wordt aangeraden);

N.B. Voor de livegang van de nieuwe Havank applicatie staat inloggen d.m.v. Single Sign On (SSO) op de planning. Daar zou gebruik worden gemaakt van het politie AD waar het wachtwoordbeleid al wordt afgedwongen. Wanneer deze koppeling geïmplementeerd is, komt deze observatie te vervallen.

Kans: Door het ontbreken van een sterk wachtwoordbeleid zijn wachtwoorden makkelijker te raden door aanvallers. Aangezien het wachtwoord uiteindelijk door de gebruiker gekozen wordt, betekent dit niet noodzakelijk dat alle wachtwoorden zwak zijn. Account lock-out is ingeschakeld, waardoor een aanvaller slechts een gelimiteerd aantal pogingen kan ondernemen om het wachtwoord te raden. Om deze kwetsbaarheid te misbruiken moet een aanvaller toegang hebben tot het interne netwerk.

Impact: Het succesvol misbruiken van deze kwetsbaarheid kan leiden tot ongeautoriseerde toegang tot individuele gebruikersaccounts. Hierdoor ontstaat de mogelijkheid dat een aanvaller acties uitvoert namens legitieme gebruikers, zoals toegang verkrijgen, wijzigen of verwijderen van gevoelige dossierinformatie en geüploade documenten.

Aanbevelingen	C	R
A **Dwing het gebruik van sterke wachtwoorden af** • We raden aan een strikt wachtwoordbeleid in te voeren en deze te standaardiseren over alle systemen en applicaties. In lijn met het wachtwoordbeleid van de Nationale Politie 2020 raden wij onderstaande beveiligingseisen aan ten aanzien van het wachtwoord: 1. Het wachtwoord bestaat uit ofwel minimaal 20 karakters, ofwel 8 karakters + een tweede authenticatiemiddel; 2. Wachtwoorden die op een blacklist staan mogen niet worden gebruikt; 3. Het wachtwoord mag niet de inlognaam (accountnaam), roepnaam en/of achternaam bevatten; 4. Het wachtwoord bevat karakters uit ten minste 3 van de onderstaande 4 categorieën: a) Hoofdletters (A t/m Z) b) Kleine letters (a t/m z) c) Cijfers (0 t/m 9) d) Leestekens (bijvoorbeeld: -, !, $, #, %)	M	M

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

4.5 Gebruikerscertificaten worden geaccepteerd

Domein	Kans	Impact	Risico
CSC05	M	M	M

Observatie

De Havank fatclients maken gebruik van versleutelde TLS-verbindingen naar de backend. Daarbij wordt gebruik gemaakt van de certificate store van Windows, om te controleren of de ondertekening van het havank.biometrie.politie.local domein van een vertrouwde partij afkomstig is. Het vertrouwen van de Windows certificate store wordt meegegeven als parameter bij het opstarten van de java-client.

Gebruikers kunnen echter hun eigen gebruikerscertificaten installeren in hun Citrixomgeving; deze worden door de applicatie geaccepteerd. Hierdoor kan het verkeer worden onderschept en geanalyseerd.

Kans: Om deze kwetsbaarheid te misbruiken moet de aanvaller toegang hebben tot de Havank applicatie en een Windows omgeving (zoals de standaard Telewerken omgeving) waarbij hij certificaten kan installeren. Daarnaast moet de aanvaller software kunnen installeren om het netwerkverkeer tussen de fatclient en server te kunnen afluisteren.

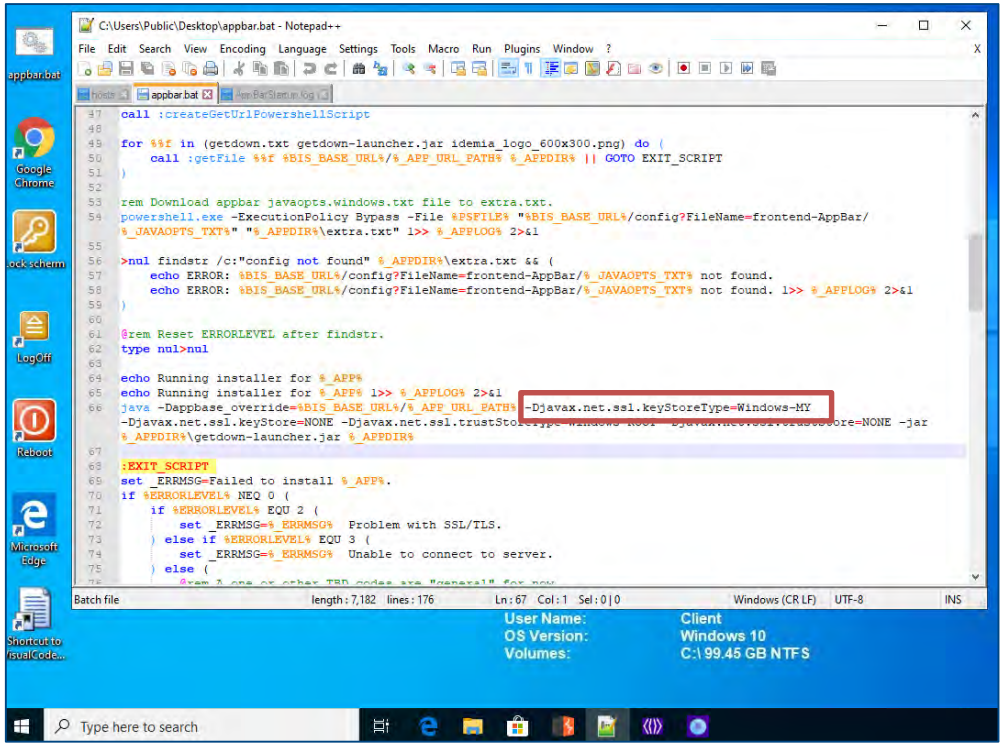
Impact: Wanneer een aanvaller het verkeer tussen de Havank applicatie en de backend servers kan afluisteren, wordt het makkelijker om naar kwetsbaarheden in de software te zoeken, zoals beschreven in de andere observaties in dit rapport.

Aanbevelingen		C	R
A	**Maak gebruik van 'certificate pinning'** • Wijs een exclusieve certificaatautoriteit aan, welke aan de basis moet staan van het havank.biometrie.politie.local domein. Dit kan bijvoorbeeld het POL-TLSCA zijn die nu de certificaten ondertekend. Andere certificaatautoriteiten moeten door de applicatie worden afgewezen, zelfs als deze in de Windows certificaten store zijn aangemerkt als vertrouwd. • Om het moeilijker te maken voor aanvallers om de javax-instellingen aan te passen, zou deze niet als parameter moeten worden meegegeven, maar in de applicatie ingebouwd moeten zijn.	M	M

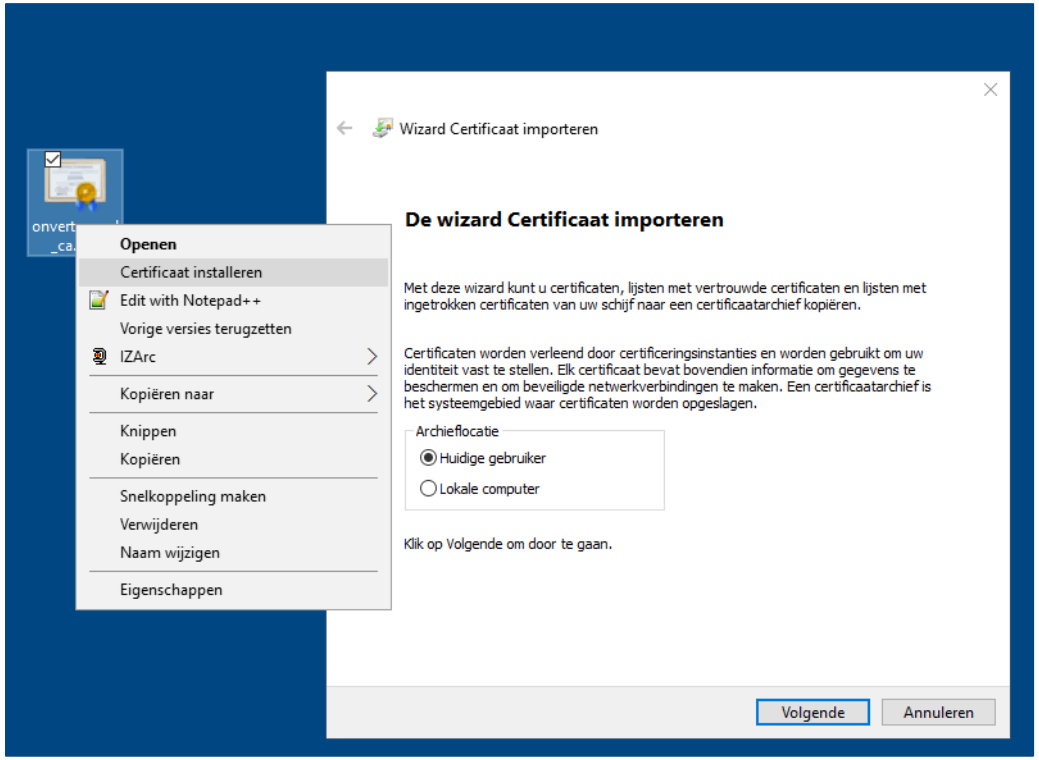
C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – gebruikerscertificaten worden geaccepteerd



Screenshot 1 – Certificaatautoriteiten uit het Windows certificate store worden standaard vertrouwd, en deze instelling wordt meegegeven bij het starten van de applicatie.



Screenshot 2 – Gebruikers kunnen een certificaat installeren in hun standaard Telewerken-omgeving.

4.6 Beperkte inputfiltering

Domein	Kans	Impact	Risico
CSC18	M	M	M

Observatie

We hebben vastgesteld dat de Havank applicatie invoervelden bevat waarop beperkte invoercontrole wordt uitgevoerd. Gedurende onze tests was het mogelijk om data op te slaan met speciale karakters in velden waar dit niet noodzakelijk is. Speciale karakters kunnen worden gebruikt in zogenaamde injectie-aanvallen. Daarnaast hield de applicatie een maximum aantal tekens per invoerveld aan, maar deze controle werd niet uitgevoerd op de server.

Een voorbeeld van een locatie waar beperkte controle van de invoer wordt gedaan is de “Descriptors” pagina in de “Person Management” module. Hier was het ook mogelijk om een groot aantal tekens in te voeren, door het request na validatie aan de client zijde aan te passen. Dit werd door de backend geaccepteerd, waarna de “Descriptors” pagina niet meer laadde.

N.B. Beperkte inputvalidatie biedt een platform voor het uitvoeren van injectieaanvallen, zoals SQL-injectie. In de beperkte tijd die beschikbaar was voor deze test hebben we niet vast kunnen stellen dat een dergelijke aanval mogelijk is.

Kans: Om deze kwetsbaarheid te kunnen misbruiken, is toegang tot de Havank fatclient applicatie en een gebruikersaccount met toegang tot de applicatie nodig. Het uitvoeren van deze aanval vereist geen technische kennis; iedereen met toegang tot de betreffende invoervelden kan speciale karakters invoeren.

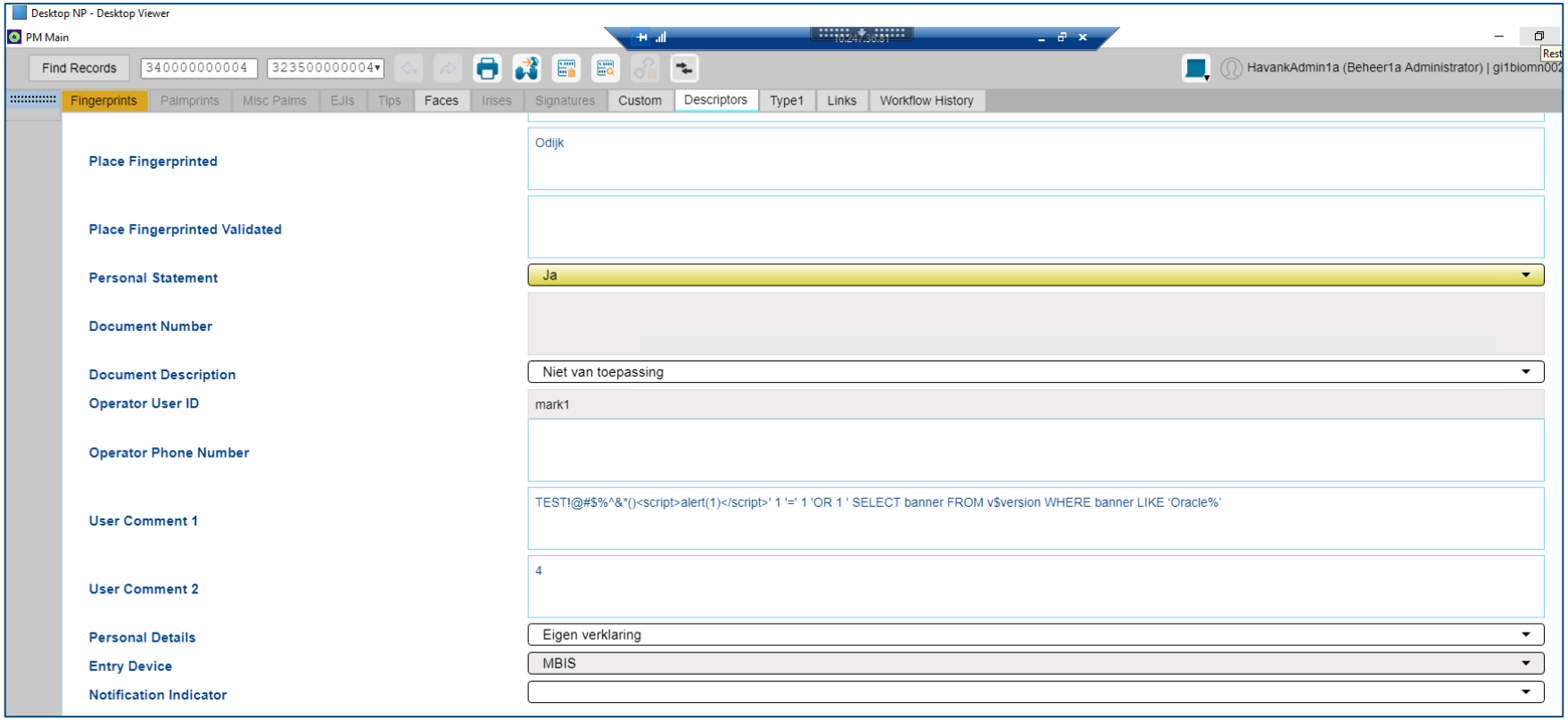
Impact: In het geval van een succesvolle SQL-injectie kan een aanvaller (gevoelige) gegevens in de database inzien en aanpassen, waar hij niet toe geautoriseerd is. Daarnaast kan dit gebruikt worden als een platform voor andere aanvallen, zoals Denial-of-Service aanvallen, die kunnen leiden tot beschikbaarheidsproblemen binnen de Havank omgeving.

Aanbevelingen	C	R
A **Pas filtering toe op de invoer** • We raden aan filtering toe te passen op alle invoervelden in de applicatie, om te verzekeren dat slechts geldige invoer wordt verwerkt. In het geval dat een invoerveld bijvoorbeeld alleen cijfers mag bevatten zou de filter alle andere typen invoer moeten weigeren zonder deze invoer door te zenden naar de database. In het geval dat speciale karakters toegestaan moeten worden in een invoerveld, zou de applicatie een standaard functie moeten gebruiken om de speciale karakters te “escapen”.	M	L

C: Complexiteit
R: Risico mitigatie

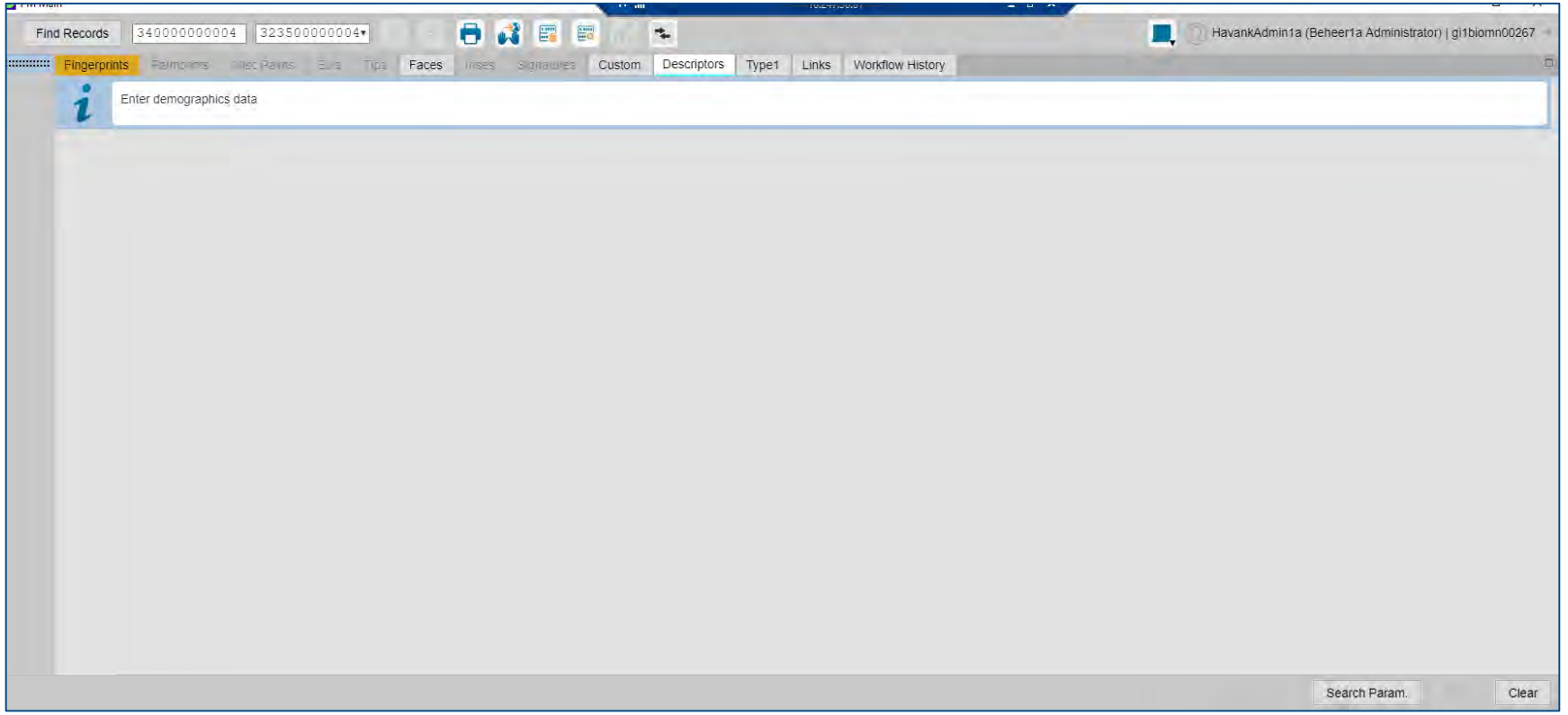
	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – Beperkte inputfiltering (1/2)



Screenshot 1 – Het is mogelijk op een groot aantal speciale tekens op te slaan in de applicatie.

Screenshot – Beperkte inputfiltering (1/2)



Screenshot 2 – Dezelfde pagina wordt niet meer geladen wanneer een zeer groot aantal tekens in een invoerveld worden opgeslagen.

4.7 Verouderde en kwetsbare software geïdentificeerd

Domein	Kans	Impact	Risico
CSC03	L	M	L

Observatie

We hebben vastgesteld dat een verouderde JDK versie gebruikt is in de Havank omgeving. Onderstaande verouderde JDK versie is geconstateerd:

- Build JDK versie 1.8.0-144, uitgebracht in juli 2017, terwijl JDK versie 1.8.0-281 is uitgebracht in januari 2021. JDK versie 1.8.0-144 is kwetsbaar voor verschillende Denial-of-Service (DoS) aanvallen.

Kans: Om deze kwetsbaarheid te kunnen misbruiken is toegang tot de applicatie vereist. Geavanceerde technische kennis is vereist voor een aanvaller om een succesvolle exploit voor de aangetroffen kwetsbaarheid te ontwikkelen.

Impact: Als een aanvaller de software kan compromitteren, is het mogelijk om DoS aanvallen uit te voeren op de applicatie. Een succesvolle aanval kan leiden tot beschikbaarheidsproblemen.

Aanbevelingen	C	R
A **Verbeter het update proces** • We raden aan de systemen te voorzien van de laatste security updates. • Verder raden we aan om het update proces aan te scherpen om kwetsbare software tijdig te identificeren. In dit proces moet ook worden geverifieerd dat de relevante updates en patches succesvol zijn geïnstalleerd.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

4.8 Technische informatie in foutmeldingen

Domein	Kans	Impact	Risico
CSC05	M	L	L

Observatie

We hebben vastgesteld dat de Havank applicatie technische informatie weergeeft in foutmeldingen.

We hebben bijvoorbeeld foutmeldingen met technische details aangetroffen wanneer een gebruiker te veel tekens invoert als wachtwoord of als er speciale tekens worden ingevoerd in parameters.

Deze informatie kan worden gebruikt in verdere aanvallen.

Kans: Deze foutmeldingen kunnen alleen worden gegenereerd door ingelogde gebruikers. Voor het succesvol uitvoeren van deze aanval is weinig technische kennis vereist.

Impact: In geval van een succesvolle aanval zou een aanvaller informatie kunnen vergaren over de software die wordt gebruikt. Deze informatie kan gebruikt worden om te bepalen of relevante kwetsbaarheden of exploits voorhanden zijn om te gebruiken in een vervolgaanval.

Aanbevelingen		C	R
A	**Toon geen technische details in foutmeldingen** • We raden aan foutmeldingen weer te geven zonder technische informatie over de applicatie of over achterliggende software.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

5

Observaties webapplicatietest Catch

Observatieoverzicht

Onderstaande tabel bevat de observaties die zijn geïdentificeerd tijdens de webapplicatietest op Catch (Face Expert) en de inschatting van de kans, impact en het bijbehorende risico (laag, medium of hoog) per observatie. De details per observatie zijn opgenomen op de volgende pagina's van deze sectie.

#	Domein	Observatie	Kans	Impact	Risico
5.1	CSC14	Ongeautoriseerde toegang tot gevoelige data	M	H	H
5.2	CSC14	Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd	M	H	H
5.3	CSC14	Gevoelige data in applicatielogs	M	H	H
5.4	CSC18	Onveilige bestand upload functie	L	M	L
5.5	CSC05	Onveilige HTTP response header configuratie	L	M	L
5.6	CSC05	Onveilig gebruik van cookie parameters	L	M	L
5.7	CSC05	Technische informatie in foutmeldingen	M	L	L

Laag	Medium	Hoog
L	M	H

5.1 Ongeautoriseerde toegang tot gevoelige data

Domein	Kans	Impact	Risico
CSC14	M	H	H

Observatie

De Catch webapplicatie geeft gebruikers de mogelijkheid om zaken in te zien waartoe zij gerechtigd zijn, en in deze zaken bijlages te uploaden en te bekijken.

We hebben vastgesteld dat gebruikers toegang kunnen krijgen tot gegevens van zaken waartoe zij niet zijn geautoriseerd. Toegang tot de data is gebaseerd op de sessiecookie in het verzoek van client naar webapplicatie. Echter wordt deze niet (volledig) afgedwongen en kan een gebruiker details over bijlages van andere zaken inzien, wanneer hij over de URL met identifier van deze zaak beschikt. Dit endpoint bevindt zich op: https://gi1biomn00269.resource.gi.int.politie:30000/i5/vdpm/camera/**<id>**/state

Daarnaast worden bij het inloggen de gebruikersrechten opgehaald, zodat de applicatie de toegestane functies aan de gebruiker kan tonen. Door het aanpassen van de POST-request kunnen de rechten van andere gebruikers worden gevraagd: https://gi1biomn00269.resource.gi.int.politie:30000/i5/authorization/privileges/requestedprivileges

Kans: Een geldig gebruikersaccount is vereist om deze kwetsbaarheid te misbruiken. Beperkte technische vaardigheden zijn nodig om applicatieverkeer aan te passen, maar de aanvaller moet wel de URL weten of raden waarop informatie over de zaak kan worden opgevraagd.

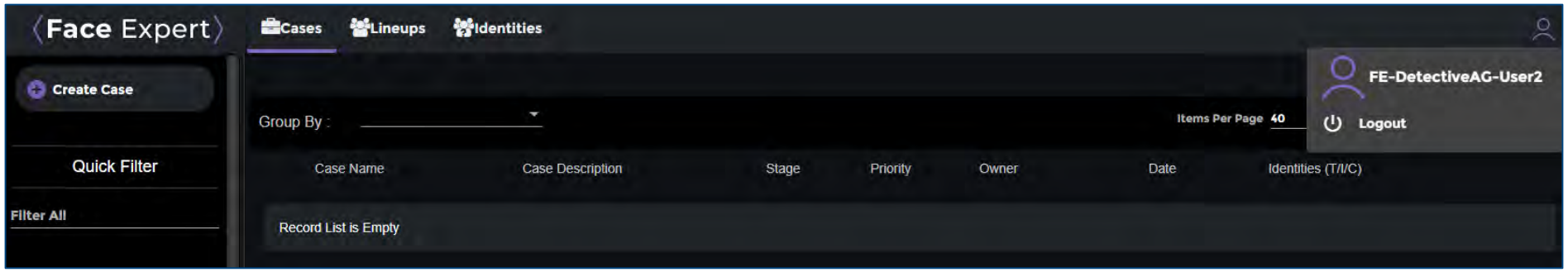
Impact: Bij een succesvolle aanval, verkrijgt een aanvaller toegang tot de gevoelige informatie rondom een zaak, waaronder gegevens over de bijlages. Daarnaast kan een aanvaller de rechten van andere accounts inzien, en dit gebruiken bij verdere aanvallen van (administratieve) gebruikers om meer acties te kunnen uitvoeren.

Aanbevelingen		C	R
A	**Dwing toegangscontrole af op de Catch backendsystemen** • We raden aan logische toegangscontrole af te dwingen voor alle toegang tot gevoelige data. In een ideale situatie wordt dit afgedwongen vanuit een centrale component die gebruikt wordt om enerzijds toegangscontrole af te dwingen en anderzijds weer te geven welke data toegankelijk is voor iedere gebruiker.	M	H

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

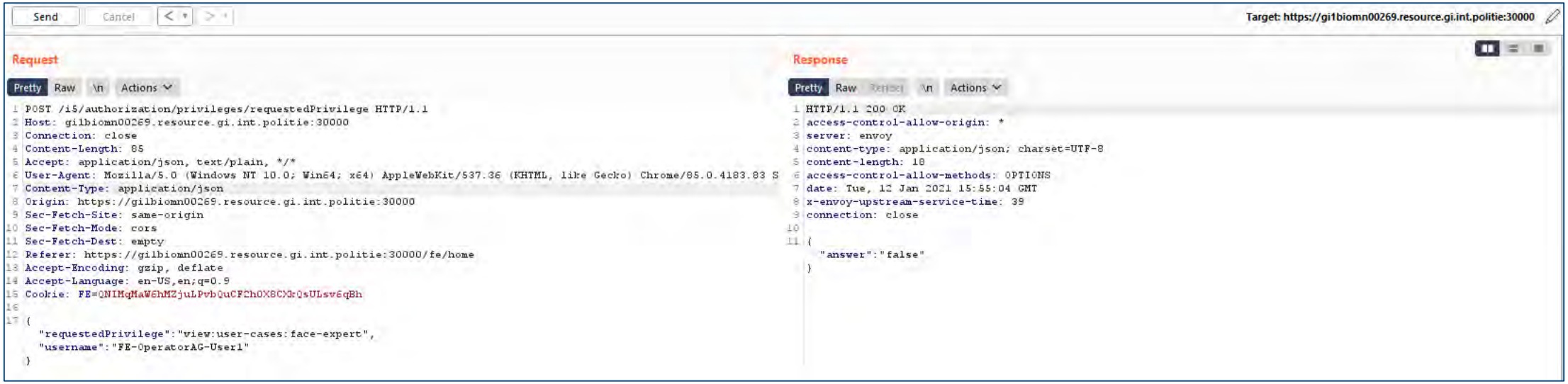
Screenshot – Ongeautoriseerde toegang tot gevoelige data (1/2)



Screenshot 1 – Gebruiker ‘Detective-User2’ heeft geen toegang tot zaken in de Face Expert applicatie.

Screenshot 2 – Wanneer de ‘Detective-User2’ de juiste URL kan achterhalen of raden, kan hij/zij de bijlages inzien.

Screenshot – Ongeautoriseerde toegang tot gevoelige data (2/2)



Screenshot 3 – Een gebruiker (in dit geval ‘FE-DetectiveAG-User1’) kan opvragen welke toegangsrechten andere users (in dit geval ‘FE-OperatorAG-User1’) hebben.

5.2 Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd

Domein	Kans	Impact	Risico
CSC14	M	H	H

Observatie

De applicatie maakt gebruik van JSON om instellingen en applicatiedata uit te wisselen tussen de browser van de gebruiker en de applicatieserver. In één van deze configuratiebestanden staat een gebruikersnaam en wachtwoord van een serviceaccount van de RabbitMQ share.

Kans: Deze inloggegevens worden door de browser van alle ingelogde gebruikers verstuurd, met daarbij ook de naam van de MBSS-instantie (geen IP-adres) en de bijhorende poort. De inloggegevens worden echter niet getoond naar de gebruiker, tenzij deze het webverkeer inspecteert. Daarnaast is er beperkte technische kennis over RabbitMQ vereist om deze kwetsbaarheid te misbruiken.

Impact: RabbitMQ wordt gebruikt om berichten tussen applicaties uit te wisselen via zogenaamde ‘queues’. Een aanvaller kan met deze inloggegevens alle berichten zien waar de ‘mbss’ gebruiker toegang toe heeft, inclusief (gevoelige) applicatiedata. Omdat het serviceaccount geen administratieve rechten heeft, kan er niet mee worden ingelogd op de administratieve interface van de RabbitMQ servers. Desalniettemin kan de aanvaller proberen door middel van het serviceaccount verdere informatie te verzamelen over de backend en/of via de queues zich verder te verspreiden over het netwerk.

Aanbevelingen		C	R
A	**Verwijder de RabbitMQ inloggegevens uit het configuratiebestand** • Verwijder de inloggegevens uit het configuratiebestand ‘mvi-config.json’, of scherm deze af en gebruik een ander configuratiebestand om naar gebruikers te sturen.	M	H
B	**Gebruik sterke wachtwoorden voor serviceaccounts** • Het wachtwoord van het ‘mbss’ account bestaat slechts uit enkele letters en is daardoor zwak. Volgens het politiebeleid (januari 2020) wordt het wachtwoord van een serviceaccount willekeurig gegenereerd en is deze “minimaal 30 posities lang, alfanumeriek met vreemde tekens”. • Verander het wachtwoord van het ‘mbss’ serviceaccount, aangezien deze mogelijk door gebruikers is ingezien.	M	M

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – Inloggegevens RabbitMQ serviceaccount wordt naar gebruikers verstuurd

Screenshot 1 – De webapplicatie laadt configuraties uit ‘mvi-config.json’, waarin de inloggegevens van het ‘mbss’ RabbitMQ serviceaccount staan vermeld.

5.3 Gevoelige data in applicatielogs

Domein	Kans	Impact	Risico
CSC14	M	H	H

Observatie

We hebben vastgesteld dat de wachtwoorden van gebruikers in plaintext aanwezig zijn in logbestanden van de Catch (Face Expert) applicatie op de 10.247.36.78 server.

Locatie van de log met daarin de aangetroffen wachtwoorden:

- 10.247.36.78:/mvi-share/fe-logs/i5authentication.log.2021-01-12.2.

Kans: Om het wachtwoord te verkrijgen is toegang tot de NFS share en/of het logbestand vereist. Er is beperkte technische kennis vereist om de log te vinden en te openen.

N.B.: zie ook observatie 3.1: Openbare NFS shares beschikbaar op het interne netwerk.

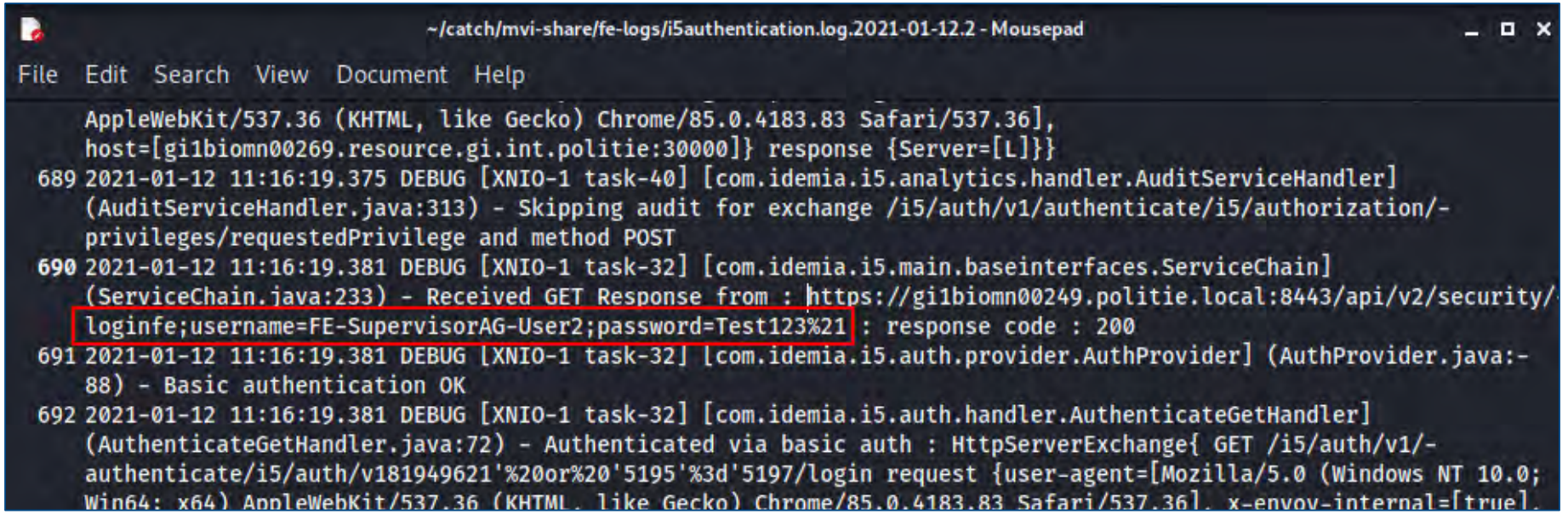
Impact: In geval van een succesvolle aanval bieden de geïdentificeerde wachtwoorden in de logs mogelijkheden voor de aanvaller om in de Face Expert applicatie in te loggen namens (andere) gebruikers. Hiermee zou een aanvaller gevoelige data, zoals foto's van verdachten, kunnen inzien en aanpassen. Daarnaast bestaat het risico dat gebruikers hetzelfde wachtwoord gebruiken voor verschillende applicaties en systemen, en dat een aanvaller de inloggegevens ook kan gebruiken om zich verder te verspreiden over het politienetwerk. Het is daardoor extra belangrijk dat wanneer politiemedewerkers op Face Expert kunnen gaan inloggen door middel van SSO of AD-inloggegevens van de politie, deze gegevens niet in plaintext worden gelogd.

Aanbevelingen		C	R
A	**Log geen plaintext wachtwoorden** • We raden aan om geen plaintext wachtwoorden in logs op te slaan.	L	H

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Screenshot – Gevoelige data in applicatielogs



Screenshot 1 – Het was mogelijk om plaintext wachtwoorden in te zien via een logbestand van de applicatie.

5.4 Onveilige bestand upload functie

Domein	Kans	Impact	Risico
CSC18	L	M	L

Observatie

De Catch webapplicatie biedt gebruikers de mogelijkheid om documenten in de applicatie te uploaden. Deze upload functie controleert op bestandstypes en alleen beeldmateriaal (afbeeldingen en video's) kunnen worden geüpload. Echter, zolang de bestandsextensie en MIME-type een mediabestand aangeeft, kunnen andere bestanden, zoals malware, worden geüpload.

Daarnaast hebben we opgemerkt dat het mogelijk is om malware (het 'EICAR' testbestand) naar de applicatie te uploaden. Dit is een indicatie van het ontbreken van antivirus software op de webserver.

N.B. We hebben alleen de uploadfunctie voor media kunnen testen. De Catch webapplicatie biedt (rechtsboven) ook een optie om direct bijlages te uploaden. Deze functie was nog niet functioneel ten tijde van de test.

Kans: Naast een geldig gebruikersaccount zijn beperkte technische vaardigheden vereist om kwaadaardige bestanden te uploaden. Als alternatief zou een aanvaller slachtoffers kunnen verleiden via mail of een URL om een kwaadaardig bestand te uploaden. Een geüpload bestand zal wel een media-bestandsextensie hebben, en zal daarom door Windows niet worden uitgevoerd totdat de extensie weer wordt veranderd.

Impact: Een aanvaller kan bestanden zoals malware uploaden, welke zich na tussenkomst (zoals het terugzetten van de extensie) verder kunnen verspreiden naar gebruikers en de ondersteunende infrastructuur van de Biometrievoorziening. Dit kan leiden tot downtime van de systemen en het verspreiden van malware naar een groot aantal politiewerknemers.

Aanbevelingen		C	R

A	**Beveilig de uploadfunctie**
	• We raden aan de volgende elementen te implementeren voor alle functies voor het uploaden van bestanden in de toepassing:
	  • Toepassen van filtering op basis van bestandsextensie op alle uploadfuncties in de gehele toepassing. Alleen extensies van de vooraf bepaalde 'whitelist' mogen worden toegestaan;
	  • Het uitvoeren van bestandstype-detectie en het weigeren van bestanden die niet het juiste formaat van een verwacht bestand hebben;
	  • Bestanden laten scannen door een antivirus oplossing.
		M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

5.5 Onveilige HTTP response header configuratie

Domein	Kans	Impact	Risico
CSC05	L	M	L

Observatie

We hebben zwakheden in de response headers van de Catch applicatie vastgesteld die een aanvaller de mogelijkheid kan geven gevoelige gegevens te onderscheppen of ongeautoriseerde acties uit te voeren. De volgende headers worden niet ingesteld door de applicatie:

- HTTP Strict Transport Security (HSTS);
- Content Security Policy (CSP);
- Cache headers;
- X-Frame-Options.

Kans: Deze kwetsbaarheden kunnen worden misbruikt door iedereen op het interne netwerk. Beperkte technische vaardigheden zijn nodig om een succesvolle clickjacking aanval uit te voeren. Het uitvoeren van een succesvolle aanval kan alleen als een gebruiker misleidt wordt om op een kwaadaardige link te klikken met een geldige ingelogde sessie. Verder kan het nodig zijn om fysieke toegang tot een computer te hebben of op een netwerk tussen de gebruiker en de server te zitten.

Impact: Een succesvolle aanval kan ervoor zorgen dat een aanvaller met een sessie van het slachtoffer kan browsen door de verzoeken door de browser van het slachtoffer te tunnelen en verzoeken door te sturen naar de webserver en mogelijkerwijs ook acties kunnen uitvoeren namens de gebruiker, zoals het opvragen, inzien, aanpassen en downloaden van gegevens in zaken. Verder kan een aanvaller ongeautoriseerde toegang krijgen tot gevoelige gegevens die zijn opgeslagen in de cache, zoals sessie-informatie en inloggegevens. Ook kan dit leiden tot succesvolle XSS- en Man-In-The-Middle (MITM) aanvallen.

Aanbevelingen	C	R

A **Verbeter de HTTP response header configuratie**
• We raden aan de HTTP header configuratie te verbeteren door:
  • De HTTP Strict Transport Security header aan te zetten om het gebruik van SSL/TLS af te dwingen in moderne browsers;
  • Een “allow list” te definiëren in het “Content Security Policy” header veld om in moderne browsers te beschermen tegen potentieel gevaarlijk gebruik van scripts en stylesheets;
  • De cache-control headers (cache-control: private, max-age=0, no-cache) en de pragma header (pragma: no-cache) voor oudere browsers aan te zetten;
  • Anti-clickjacking maatregelen te implementeren, zoals de “X-Frame-Options” header.
	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

5.6 Onveilig gebruik van cookie parameters

Domein	Kans	Impact	Risico
CSC05	L	M	L

Observatie
De Catch webapplicatie maakt geen gebruik van de ‘Secure Flag’ parameter. Wanneer de ‘Secure Flag’ parameter ontbreekt, kan de inhoud van de cookie over een onbeveiligde verbinding worden verzonden als een gebruiker de applicatie probeert te openen via HTTP in plaats van HTTPS. ***Kans:*** Om misbruik te maken van de ontbrekende ‘Secure Flag’ parameter, is geavanceerde technische kennis vereist om netwerk verkeer af te luisteren. De aanvaller moet zich op specifieke netwerken bevinden om de gegevens te onderscheppen (bijvoorbeeld het netwerkpad tussen de gebruiker en de webserver). ***Impact:*** Een succesvolle aanval kan de aanvaller in staat stellen om een beperkt aantal gebruikerssessies over te nemen en acties uit te voeren namens deze gebruikers, zoals het opvragen, inzien, aanpassen en downloaden van gegevens in zaken.

	Aanbevelingen	C	R
A	**Maak gebruik van de ‘Secure Flag’ parameter** • We raden aan het gebruik van cookie instellingen te evalueren en de ‘Secure Flag’ parameter te gebruiken waar mogelijk. De cookie flags kunnen per cookie worden gezet in de programmacode.	L	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

5.7 Technische informatie in foutmeldingen

Domein	Kans	Impact	Risico
CSC05	M	L	L

Observatie

We hebben vastgesteld dat de Catch webapplicatie technische informatie weergeeft in foutmeldingen, welke normale gebruikers niet nodig hebben.

Deze informatie wordt getoond wanneer een zoekopdracht een interne foutmelding oplevert. Deze ‘exception’ wordt ongefilterd doorgestuurd naar de gebruiker. Een voorbeeld hiervan is de volgende zoekopdracht:

- https://gi1biomn00269.resource.gi.int.politie:30000/i5/io/q?index=users&limit=0&offset=0

Kans: Deze foutmeldingen kunnen alleen worden gegenereerd door ingelogde gebruikers. Voor het succesvol uitvoeren van deze aanval is weinig technische kennis vereist.

Impact: In geval van een succesvolle aanval zou een aanvaller informatie kunnen vergaren over de software die wordt gebruikt, en hoe de achterliggende database is ingericht. Deze informatie kan gebruikt worden om te bepalen of relevante kwetsbaarheden of exploits voorhanden zijn om te gebruiken in een vervolgaanval.

Aanbevelingen	C	R
A **Gebruik standaard foutmeldingen** • We raden aan om generieke foutmeldingen weer te geven zonder technische informatie over de applicatie of achterliggende software.	M	L

C: Complexiteit
R: Risico mitigatie

	Laag	Medium	Hoog
Risico en complexiteit:	L	M	H
Risico mitigatie:	L	M	H

Van: Riemen, John (J.A.J.M.)
Aan: 5.1.2.e
Cc: 5.1.2.e
Onderwerp: RE: CATCH
Datum: donderdag 4 maart 2021 12:59:35
Bijlagen: image006.png

Hoi 5.1.2.e

Klopt dat FCM foto's ook deel uitmaken van CATCH.

We hebben daar vorig jaar wel een schoningsactie van 200K foto's uitgevoerd.
Dit waren foto's waar geen verbinding meer te vinden was in de politiesystemen.
We hebben daar dus de aanname gedaan dat deze al geschoond zijn.

5.1.2.e geeft wel aan dat systematische schoning van de FCM data nu niet is ingericht.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: maandag 22 februari 2021 08:27
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: RE: CATCH

Hoi John,

Ik heb nog een vraag. Het probleem is idd groter. Catch wordt nu gevuld door FCM (foto's uit DPS). Mijn logische redenatie zegt dat de foto's in FCM dus ook niet worden geschoond. Immers daarvoor moet hetzelfde traject worden doorlopen, wat nu hapert. Klopt deze zienswijze?

Ik stel de vraag, omdat IV collega's bezig zijn met een vooronderzoek FCM.

Met vriendelijke groet,

5.1.2.e
Politie | Politiedienstencentrum | Dienst IM | IM Advies
Ringbaan West 232, 5038 KE Tilburg

Ringwade 51, 3439 LM Nieuwegein
Postbus 8050, 5004 GB Tilburg
M +316 5.1.2.e
Werkdagen: maandag t/m donderdag
Teams 5.1.2.e @blauwonline.onmicrosoft.com

Klik hier voor de landelijke FO site op Agora

Van: Riemen, John (J.A.J.M.)
Verzonden: vrijdag 19 februari 2021 10:31
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: CATCH

Allen

Weet dat ik, in afstemming met voorlichting, aan dit vraagstuk bijdrage heb geleverd onder andere door mail en gesprekken met de journalist.
Ik heb overigens deze notitie nooit gehad…

Weet dat bij de totstandkoming van de Wet Identiteitsvaststelling Verdachten Veroordeelden en getuige (WIVVg)door de politie (toenmalige RvHC) op mijn aangeven al is geadviseerd dat deze bewaarsystematiek tot problemen zou leiden.
Daarop is, bij besluit, JUSTID aangewezen als het orgaan dat ons steeds moet kennisgegeven wanneer vernietiging aan de orde is.

In de notitie wordt de term " opsporingstraject" gebruikt, hiermee wordt bedoeld dat moet worden beoordeelt of de betreffende verdachte geen verdachte meer is in een *ander* opsporings- of vervolgingstraject, inclusief hoger beroep en cassatie. Dit maakt het zeer complex en was een van de redenen dat wij als politie hebben aangegeven hier geen zicht op te hebben.
Ook heb ik aangegeven dat ik de onderbouwing van de aantallen ***niet*** steun, het zijn aannames die de journalist in een gesprek met mij niet heeft kunnen hardmaken.

De focus wordt nu gelegd op CATCH maar het probleem is dus veel breder en begint bij de SKDB en BVID en raakt vanuit daar HAVANK, CATCH en wellicht ook de DNA databank.

Als er nog vragen zijn hoor ik het graag?

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Van: 5.1.2.e

Verzonden: vrijdag 19 februari 2021 08:39

Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>

CC: 5.1.2.e 5.1.2.e @politie.nl>

Onderwerp: FW: CATCH

Voor degene die dit nog niet wisten.

- Dit staat inmiddels goed op de agenda van 5.1.2.e en Henk Geveke begreep ik.

Met vriendelijke groet,

5.1.2.e

06 - 5.1.2.e

Van: 5.1.2.e

Verzonden: woensdag 17 februari 2021 17:20

Aan: 5.1.2.e @politie.nl>

Onderwerp: CATCH

5.2.1 . Bel je straks!

Hartelijke groet,

5.1.2.e

5.1.2.e

5.1.2.e

06 5.1.2.e

Werkdagen ma t/m don

Politie I Politiedienstencentrum I Dienst IM
Marten Meesweg 35, 3068 AV Rotterdam
Postbus 70023, 3000 LD Rotterdam

Agendabeheer: 5.1.2.e / 06 5.1.2.e

5.1.2.e @politie.nl

Bereikbaar: ma t/m do

Meer informatie? Kijk op politie.nl


Denk aan het milieu voordat u deze e-mail print

Van: 5.1.2.e
Aan: Riemen, John (J.A.J.M.); 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e
Onderwerp: RE: GEB Havank / Catch versie 0.94
Datum: woensdag 21 april 2021 15:19:00
Bijlagen: GEB WPG Biometrievoorziening v0.941.docx

Beste collega's,

Het document was nog niet opgeslagen en bevat daardoor niet de laatste wijzigingen. Ik heb in deze versie 0.941j wel alle wijzigingen opgeslagen.

Met vriendelijke groet,

5.1.2.e
Adviseur informatiebeveiliging / risicomanagement

Politie | Politie Dienstencentrum | Sector Informatiebeveiliging i.o. | Risicomanagement
Ringbaan West 232, 5038 KE Tilburg
Postbus 8050, 5004 GB Tilburg
M +31 (0)6 5.1.2.e
E 5.1.2.i @politie.nl (loket informatiebeveiliging)
I http://intranet.politie.local/categorie/ondersteuning/onderwerpen/i/informatiebeveiliging/overzicht (intranetpagina)

Werkdagen: maandag, dinsdag, woensdag, donderdag tot 15 uur, vrijdagochtend

Van: 5.1.2.e
Verzonden: woensdag 21 april 2021 15:16
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: GEB Havank / Catch versie 0.94

Beste mensen,

De aanpassingen op de GEB zijn groter dan in de laatste 0.9 versie zijn besproken. Ik zou jullie daarom willen vragen nog eens goed naar de GEB te kijken. Hierbij versie 0.94.

In grote lijnen zijn de volgende zaken aangepast:

1) Catch Vreemdelingen is een aparte verwerking waarvoor DGM verantwoordelijk is en de Politie (LE) de beheerder.
2) Biometriedossier wordt in Havank opgeslagen, alleen proces informatie in Nintext. Biometrische-, biografische en zaakgegevens komen en worden direct in het MBIS opgeslagen.
3) De LE (Zoetermeer) is bevoegd om identiteit van personen vast te leggen in de databank.

Met vriendelijke groet,

5.1.2.e
Adviseur informatiebeveiliging / risicomanagement

Politie | Politie Dienstencentrum | Sector Informatiebeveiliging i.o. | Risicomanagement

Ringbaan West 232, 5038 KE Tilburg
Postbus 8050, 5004 GB Tilburg
M +31 (0)6 5.1.2.e
E 5.1.2.i @politie.nl (loket informatiebeveiliging)
I http://intranet.politie.local/categorie/ondersteuning/onderwerpen/i/informatiebeveiliging/overzicht (intranetpagina)

Werkdagen: maandag, dinsdag, woensdag, donderdag tot 15 uur, vrijdagochtend

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Plan van Aanpak Bewaartermijnen Zaak-Zuil

3 mei 2021

Bewaartermijnen Zaak-Zuil: plan van aanpak

1. Doel en beslispunten
2. De opdracht
    1. Aanleiding
    2. Context
    3. Huidige fase
    4. Deelproducten fase 3
    5. Afbakening
    6. Projectresultaat
3. Project Aanpak
    1. Fasering en mijlpalen
    2. Fase 2 – Plan van Aanpak
    3. Fase 3 - Keuzes
    4. Fase 4 - Implementatie
4. Organisatie
    1. Stuurgroep
    2. Werkgroep
    3. Overleggen
5. Kwaliteitsborging
6. Beheersing en control
7. Risico’s, randvoorwaarden en kritische succesfactoren

1. Doel PPT

Onderhavige is het Plan van Aanpak, waarin onder meer de fasen, de aanpak en organisatie wordt beschreven. De oplossingsrichtingen worden op dit moment nader uitgewerkt en op een later moment ter besluitvorming voorgelegd.

In dit document wordt de stuurgroep meegenomen in:

- De aanpak
- De afbakening
- De oplossingsrichtingen
- De organisatiestructuur
- De beheersing
- De kwaliteitsborging

Dit document bevat nog niet de gedetailleerde uitvoeringsimpact per organisatie. Het is pas mogelijk de impact op resources en planning te geven nadat de keuzes voor de oplossing zijn gemaakt.

1. Gevraagde besluiten

De stuurgroep wordt gevraagd

1) In te stemmen met dit Plan van Aanpak, met de fasering:
    1) Uitwerking van brede oplossingsrichtingen en hoog over impact, waarna Stuurgroep keuzes maakt welke zaken zij uitgewerkt wil zien in de Impact Analyse
    2) Impact Analyse op de nadere uitwerking (impact op resources, tijd, impact) van de oplossingen zoals geprioriteerd door de Stuurgroep, waarna de Stuurgroep keuzes maakt en prioriteert voor realisatie
    3) Realisatie

2) In te stemmen met het feit dat in de eerste fase (brede oplossingsrichtingen) een brede context beschrijving wordt meegenomen, waarin mogelijk zaken worden geraakt die geen onderdeel zijn van de scope, maar welke voortkomen uit rechtmatige registraties welke invloed hebben op de rechten van burgers en betrouwbaarheid van de overheid. De stuurgroep kan hier over besluiten of en hoe ze dit wil adresseren.

3) Of de Kmar onderdeel moet zijn van de stuur- en werkgroep gegeven haar rol in dit vraagstuk

2. De opdracht: context (1/2)

- Van alle verdachten die zijn aangehouden voor een misdrijf waarvoor voorlopige hechtenis mogelijk is of bij twijfel over de identiteit van verdachten die zijn aangehouden voor een overtreding, worden personalia genoteerd, frontale gelaatsfoto's en vingerafdrukken genomen.

- De foto's worden opgeslagen in de SKDB en parallel in CATCH (de fotodatabank van de Nationale Politie), de vingerafdrukken in de SKDB en HAVANK (het vingerafdrukkenbestand van de Nationale Politie)

- Het verwijderen van gegevens zou moeten gebeuren conform artikel 5 van de BIVV, dat gebeurd nu onvoldoende. Bijv.
  - Als de strafzaak eindigt met een sepot (zie memo 'sepots') of bij vrijspraak of ontslag van rechtsvervolging en de persoon ook niet veroordeeld of verdacht is in andere zaken, moeten de desbetreffende biometrische gegevens direct worden vernietigd (w.o foto's en vingerafdrukken, maar ook kopie-ID bewijs).
  - De overige geregistreerde personalia moeten overeenkomstig met de bewaartermijnen worden vernietigd. Zie BIVV artikel 5.
  - Er zijn nog meer categorieën waarvoor eigen bewaartermijnen gelden welke overigens niet alleen via de politie binnenkomen, maar ook via andere opsporingsinstanties, zoals de KMar)

2. De opdracht: context (2/2)

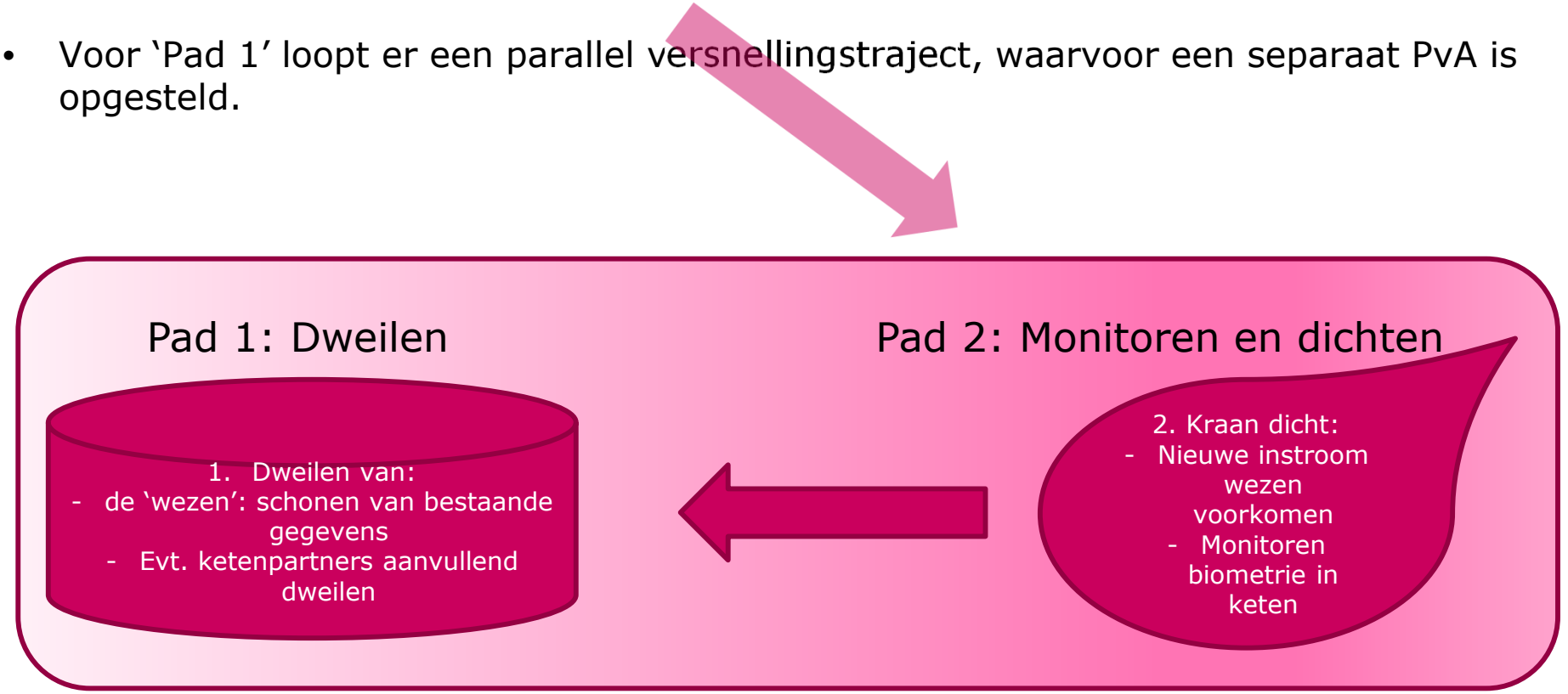
Medio 2020 is vanuit het MinJenV de opdracht gegeven aan Justid om te onderzoeken:

> *'Hoe zaak en identiteitsvaststelling eenduidig gekoppeld kunnen worden en de Justitiële Informatiedienst haar rol als centrale bewaker van de bewaartermijnen binnen de strafrechtsketen kan invullen en aan haar verplichtingen op grond van artikel 5 Bivv kan voldoen'*

2. De opdracht: huidige fase

2. De opdracht: afbakening

- Dit plan van aanpak richt zich sec op ‘Pad 2’ (zie onder)
- Voor ‘Pad 1’ loopt er een parallel versnellingstraject, waarvoor een separaat PvA is opgesteld.



2. De opdracht: afbakening

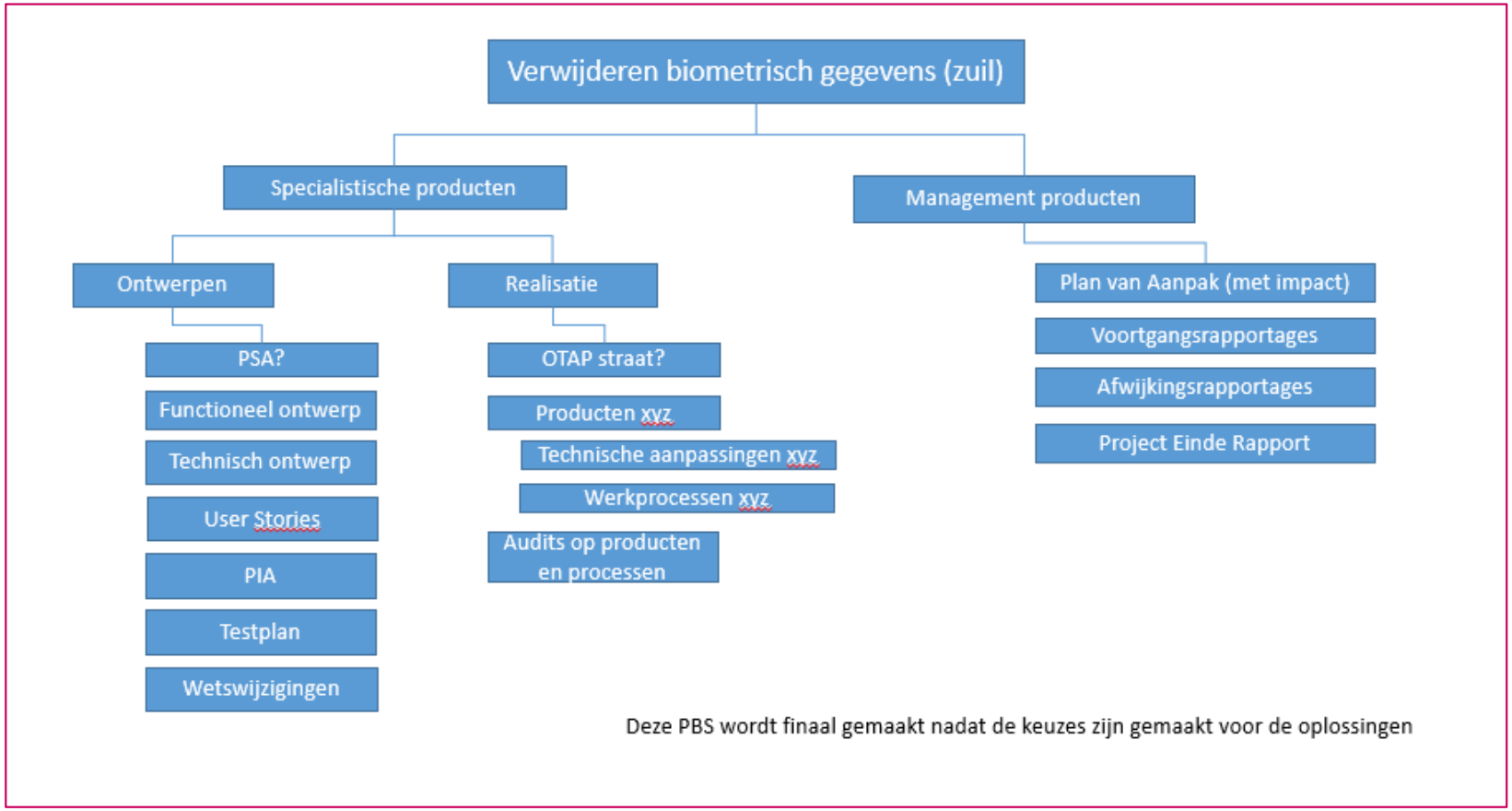
De scope van de gegeven opdracht voor de ***eerste fase*** betreft:

> *Het kunnen verwijderen van biometrische gegevens wanneer nodig, ingegeven door de regelgeving rond bewaartermijnen. We richten ons op de processen die starten bij 'de zuil'.*

Indien er punten buiten deze scope vallen, maar we ze wel tegenkomen in de analyse, wordt per punt geadviseerd of en wanneer ze in de oplossende trajecten kunnen worden meegenomen in de huidige fase, of wat een vervolgfase kan worden. De stuurgroep kan op dat moment ook besluiten of en wanneer analyses moeten worden toegevoegd t.b.v. eventuele vervolgfasen.

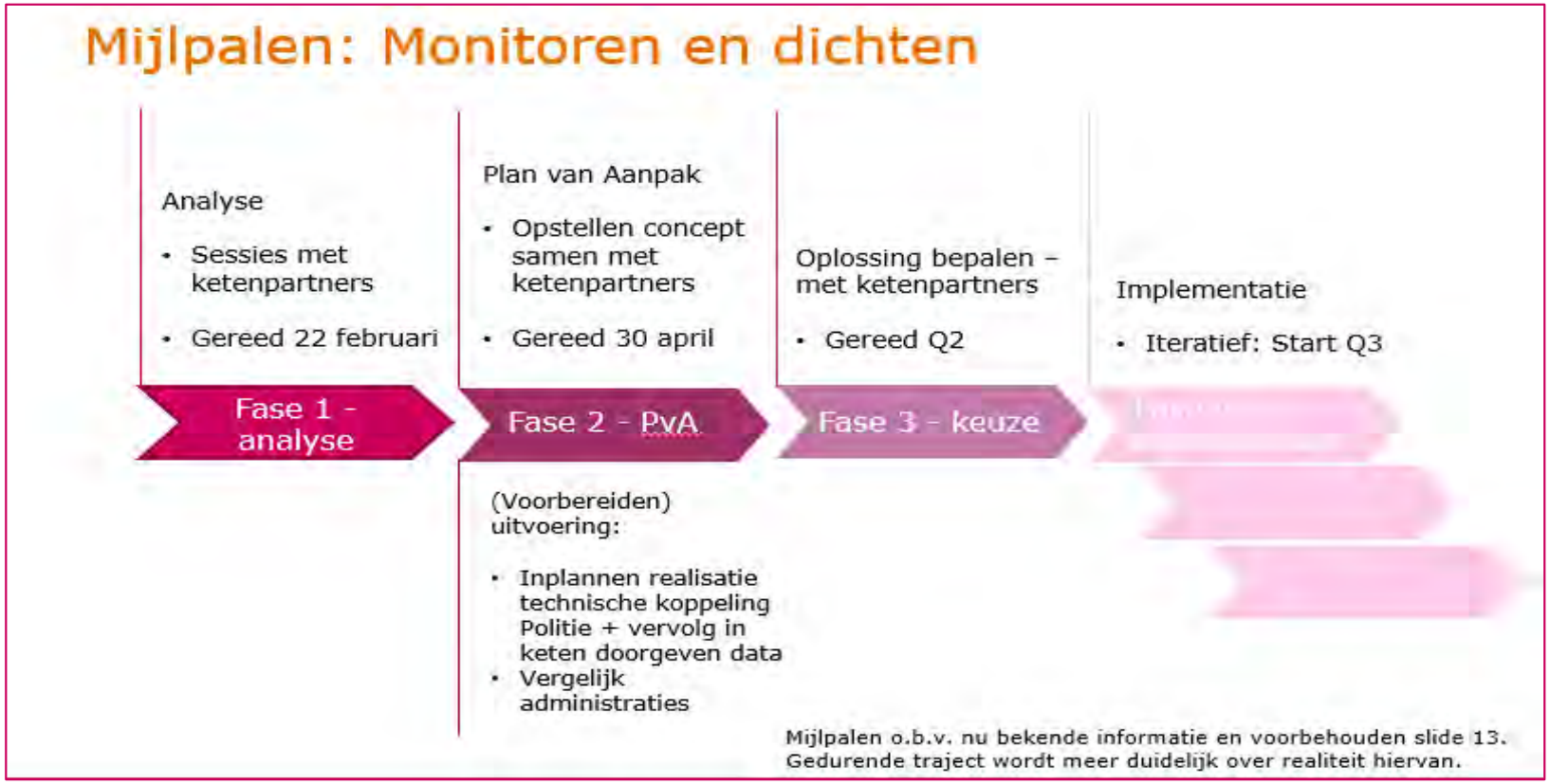
Na de keuze voor de oplossingen zal de finale scope worden vastgesteld. Hier zal tevens in worden meegenomen of ook de mogelijke wijzigingen in werkprocessen, communicatie hierover en opleidingen onderdeel uitmaken.

2. Projectresultaat



3. De aanpak: Fasering

Onderstaande fasering is geaccordeerd door de stuurgroep



3. Deelproducten Fase 3

Onderhavige PPT bevat het Plan van Aanpak voor het vervolg, zonder de uitgewerkte oplossingsrichtingen. Dat is de eerstvolgende stap. In dit PvA wordt onderscheid gemaakt in de volgende drie stappen:

1) Uitwerking van brede oplossingsrichtingen en hoog over impact, waarna Stuurgroep keuzes maakt welke zaken zij uitgewerkt wil zien in de Impact Analyse
2) Impact Analyse op de nadere uitwerking (impact op resources, tijd, impact) van de oplossingen zoals geprioriteerd door de Stuurgroep, waarna de Stuurgroep keuzes maakt en prioriteert voor realisatie
3) Realisatie

Het eerstvolgende product dat wordt opgeleverd is de uitwerking van de brede oplossingsrichtingen. Hiervoor wordt in dit document al een aanzet gegeven. De werkgroep werkt deze verder uit in Q2, waarna deze ter besluitvorming wordt voorgelegd aan de stuurgroep.

Na het besluit van de stuurgroep worden de oplossingsrichtingen die de stuurgroep prioriteert de impact verder uitgewerkt. Er is bewust voor gekozen dit in 2 fasen te doen om te voorkomen dat er veel tijd en aandacht in het bepalen van impact zit op zaken die niet worden geprioriteerd. Dit zal in Q3 plaatsvinden.

3. De aanpak: Fase 2 – Plan van Aanpak

In deze tweede fase wordt het PvA opgesteld. Onderhavige PPT dit PvA, waarbij de oplossingsrichtingen volgen.

- Werkgroep (Politie, OM, CJIB, Justid) bespreekt o.b.v. de Business Analyse de verschillende issues, ook Kmar is hierbij nodig.
- Per issue zijn of worden 1 of meerdere oplossingsrichtingen uitgewerkt
- Voor elk van deze oplossingen wordt gekeken naar een 'hoog over' impact (resources, beoogd effect, samenhang)

Huidige status

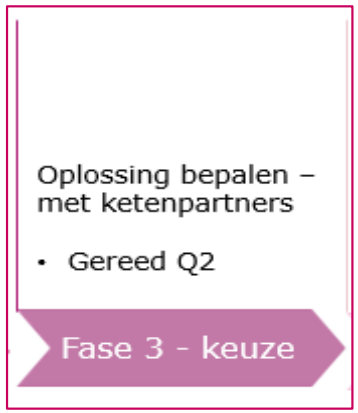
Het PvA ontbreken dus de uitgewerkte oplossingsrichtingen. Het bepalen van de oplossingsrichtingen vraagt meer tijd van de verschillende ketenpartners. Bovendien is/was capaciteit nog niet (volledig) geregeld.

3. De aanpak: Fase 3 - Keuze

In deze derde fase worden de oplossingen besproken (zie slide 12).

Het is aan de stuurgroep in deze fase om 2 keuzes te maken over hetgeen er wordt opgepakt:

- in de Impact Analyse (tweede stap fase 3)
- in de Realisatie (fase 4)



3. De aanpak: Fase 3 - Keuze

Wat?

- Er volgt een lijst met brede oplossingsrichtingen en hoog over impact
- De stuurgroep beslist obv het advies van de werkgroep
- De werkgroep gaat op basis van de keuze van de stuurgroep de geprioriteerde oplossingsrichtingen nder uitwerken op impact
- De stuurgroep beslist obv het advies van de werkgroep
- Dan worden de oplossingen in de diverse werkpaketten uitgevoerd door specialisten van de verschillende organisaties

Hoe?

Ingrediënten voor deze keuze:

- Geprioriteerde actielijst met advies
- Beschikbare middelen (DGRR)
- Maatschappelijke impact
- Absorptievermogen ketenpartners

3. Fase 3a – een inkijkje in de oplossingsrichtingen

Er zijn 2 kern-aspecten in de aanpak:

1. Ontstaan/registratie van de biometrische gegevens
2. Vernietigen van de biometrische gegevens

Diverse input/insteken:

i. De analyse is ingestoken via de processen en knelpunten. Issues weergegeven in een matrix tbv voortgang

ii. De analyse van de wezen geven inzicht in categorieen van processen/gegevensstromen waar het fout is gegaan en waar nog iets structureels moet gebeurden om herhaling te voorkomen

iii. Praatplaten rond de IV-stromen structureren de discussies

3. Fase 3a – een inkijkje in de oplossingsrichtingen

Er zijn meerdere categorieen, waaronder verdachten van overtredingen die voor de zuil zijn gezet. Deze worden geidentificeerd in de dweilllijst en per categorie opgelost.
Verdachten van overtredingen die voor de zuil zijn gezet worden mogelijk wezen Indien Politie een verdachte voor de zuil zet bij een overtreding, zijn de gegevens wel in de SKDB geregistraard maar komen ze niet in JDS en volgt er dus geen signaal naar de SKDB en Havank (en Catch) voor vernietiging. Denk hier ook aan de MEOS-stroom richting CJIB. Zie ook punt 19, hoewel die gaat over zaak-zuil-koppeling in het geval van MEOS.
Vanuit de BVH kan een persoon worden opgevraagd en kan er dus een link worden gelegd. Dit wordt door het systeem niet afgedwongen en gebeurt ook niet altijd. Daardoor is er geen link tussen zaakregistratie en ID-vaststelling, met gevolgen voor de SKDB, HAVANK, Catch en mogelijk meer systemen.
De verdachte wordt bij de Politie ontkoppeld van de rol van verdachte. De biometrische gegevens blijven echter in de SKDB ('wezen'). Er is geen terugmelding naar de SKDB of Havank of Catch.
Wezen ontstaan
Persoon gaat HALT traject in en valt dus niet langer onder strafrecht. Mag niet naar JDS en mag niet in de SKDB. Deze terugkoppeling loopt niet goed en vanuit JDS kan dan geen signaal over deze personen de keten in worden gestuurd.
Met name bij sepots: een verdachte is niet langer aangemerkt als verdachte, maar is wel gehoord. Zijn rol wijzigt bijvoorbeeld naar betrokkene, slachtoffer of getuige.
Bij een handmatige verwerking vanuit BOSZ is er geen automatische overdracht van gegevens (heen en terug) tussen politie en OM en dat heeft invloed op de rest van de keten-informatievoorziening: geen automatische uitschrijving uit SKDB en geen volledige afloopberichten). Verder gaat er ook geen conversation-ID mee in de keten zodra de gegevens niet automatisch zijn uitgewisseld.
Als een verdachte asiel wil aanvragen, wordt deze procedure eerst afgehandeld. Zodra dat is voltooid wordt een eventuele strafzaak verder afgehandeld.
DNA
Handpalmen
Foutgevoelige overgang van Politie naar OM: Koppeling BVH met Compas is handmatig (in scope? Of bij Thorbecke?)
Handmatige (na-)invoer in GPS is foutgevoelig: veroorzaakt geen geautomatiseerde vervolg-berichten (BOSZ GPS)
Vrijspraak en sepots moeten leiden tot vernietiging van biometrische gegevens: is nog niet gebeurd
In principe stuurt het CJIB een signaal tenuitvoerlegging naar GPS (datum afgehandeld). Vanuit GPS gaat dan automatisch een uitschrijvingsbericht naar de SKDB, maar niet altijd naar JDS.
Feitgecodeerde zaken met biometrie
De MEOS-stroom wordt bij de politie niet naar de BVH gemeld. Dat zou dubbel zijn. Maar dit heeft als consequentie dat als de zuil met BVH zou zijn gekoppeld, de 'MEOS-stroom' daar niet van profiteert. Deze stroom is niet in de wet voorzien en er zijn nog geen afspraken voor gemaakt. Justid kan zijn taak als centrale bewaker van de bewaartermijnen dus niet invullen voor deze stroom tot die afspraken zijn gemaakt en doorwerken in de keten.
Niet documentabele zaken (al of niet met biometrie) gaan/kunnen niet naar Justid
Koppeling SKDB-JDS is verouderd
Doorgeven verwijdersignaal aan Havank en Catch

Oplossing bepalen – met ketenpartners

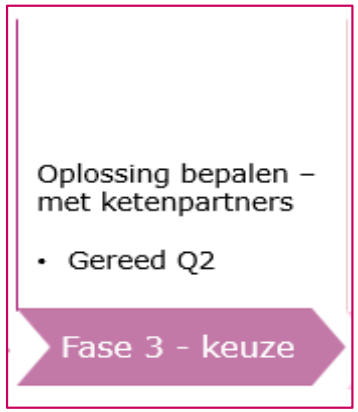
- Gereed Q2

Fase 3 - keuze

3. Fase 3a – een inkijkje in de oplossingsrichtingen

Ad 1: Ontstaan/registratie van de biometrische gegevens

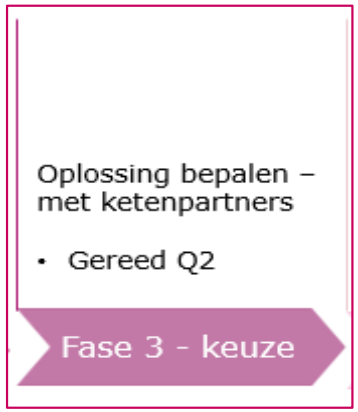
- Zaak-zuil koppeling door de hele keten (IV)
- Sluitende communicatie tot en met de documentatie in JDS (procedures en IV)
- Heldere afspraken en inrichten nog niet (goed/helder) geregelde processen (zoals HALT en asiel en omhangen verdachte, etc) (procedures en IV)
- Opzetten monitoring van verdachten of zaken die ergens tussen de systemen blijven hangen of uitvallen (IV en procedures tbv snelle reactie)



3. Fase 3a – een inkijkje in de oplossingsrichtingen

Ad 2: Vernietigen van de biometrische gegevens

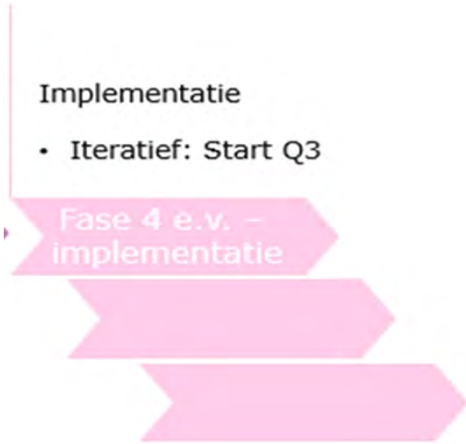
- Sluitend maken afloop OM -> Justid, waar de gegevens via het OM lopen
- Regelen afloop waar de gegevens niet via het OM lopen
- Signalering van de vernietiging Justid -> LE Politie inrichten
- Afspreken hoe om te gaan met de gegevens die Justid niet registreert ihkv documentatie (JDS), maar wel ontvangt ihkv identiteitsvaststelling (SKDB)
- Afspreken hoe de signalering en monitoring met andere partners in de strafrechtketen verloopt (KMar en andere opsporingsdiensten bijvoorbeeld)



3. De aanpak: Fase 4 – Implementatie (1/2)

Deze vierde fase beslaat de implementatie.

- De implementatie wordt iteratief en via een agile manier van werken opgepakt, hier dient nog nadere afstemming over plaats te vinden
- De keuzes van de stuurgroep in fase 3 bepalen de volgorde van de User Stories op de Product Backlog (PBL)
- De verschillende ketenpartners pakken delen van de PBL op, waar nodig in samenhang en met ketentest
- Voor aanvang van de ontwikkeling wordt door de verschillende projectleiders van ketenpartners besproken waar afhankelijkheden en risico's liggen
- Overall coördinatie ligt bij projectleider Justid, die ook rapporteert richting stuurgroep
- De User Stories bevatten acceptatiecriteria die bij de demo worden getoetst
- Er zal een overall scrummaster nodig zijn die zorgt voor rapportages over de sprints

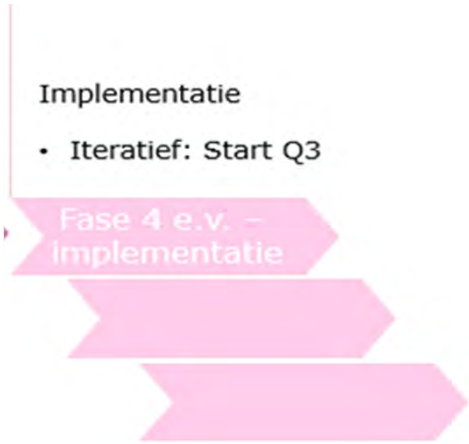


3. De aanpak: Fase 4 – Implementatie (1/2)

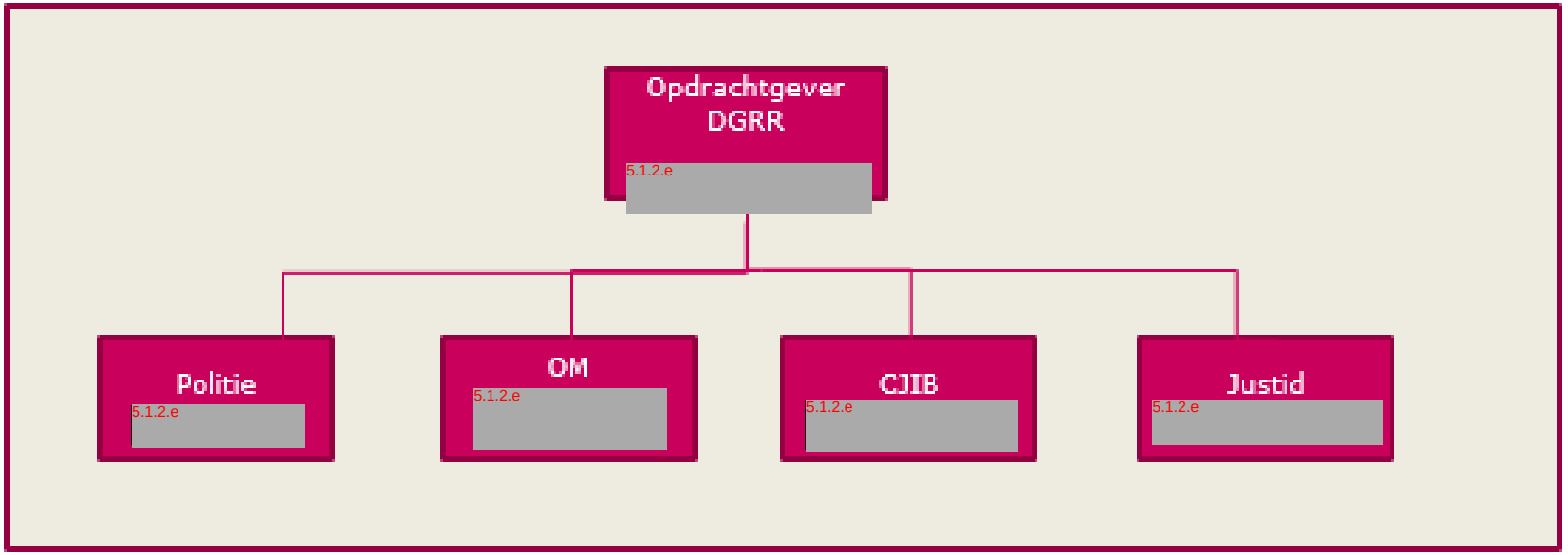
In deze vierde fase is ook aandacht voor:

- Mogelijke wijzigingen in werkprocessen en hoe dit wordt doorgevoerd (opleidingen, communicatie)
- De manier waarop zaken worden doorgevoerd
  - Het live brengen van ontwikkelde zaken
  - De overdracht naar beheer
  - Het doorvoeren van wijzigingen in werkprocessen (pilots?)

Dit zal deels afhankelijk zijn van de gemaakte keuzes in fase 3



4. De organisatie: stuurgroep (1)



Ook aanwezig bij stuurgroepvergadering:
- 5.1.2.e (KIV/DGRR): business owner
- Projectleiders ketenpartners
- 5.1.2.e (Justid) overall projectondersteuner.

4. De organisatie: stuurgroep (2)

Er is een stuurgroep ingericht, waarbinnen iedere deelnemer verantwoordelijk is voor:

- Informeren eigen bestuurlijke organisatie
- Borgen uitvoeringskeuzen PvA in eigen portfolio
- Aanjagen uitvoering in organisatie

Organisatie	Naam	Functie
DGRR	5.1.2.e	Opdrachtgever – bewaker departementale lijn
Justid	5.1.2.e	Opdrachtnemer en intern opdrachtgever Justid voor Plan van Aanpak en realisatie Penvoerder voor analyse en PvA
Politie	5.1.2.e	Opdrachtnemer en intern opdrachtgever Politie voor Plan van Aanpak en realisatie
OM	5.1.2.e	Opdrachtnemer en intern opdrachtgever OM voor Plan van Aanpak en realisatie
CJIB	5.1.2.e	Opdrachtnemer en intern opdrachtgever CJIB voor Plan van Aanpak en realisatie

4. De organisatie: werkgroep

Er is een werkgroep ingericht met als taken:

- *Problematieken analyseren en reviewen*
- *inhoudelijke expertise vanuit de partners inbrengen*
- *Adviezen opstellen tbv besluitvorming over bewaartermijnenbeleid en vernietigen van gegevens*

Randvoorwaarde: werkgroep voldoende kwantitatieve en kwalitatieve resources van ketenpartners

Organisatie	Naam	Functie
DGRR	5.1.2.e	Business Owner
Justid	5.1.2.e	Projectmanager Projectondersteuner (overall) Business consultant Productspecialist SKDB Productspecialist SKDB Productspecialist JDS
Politie	5.1.2.e	Projectmanager Product Owner, Expert BVID Expert BOSZ Gegevensexpert
OM	N.t.b. 5.1.2.e	Projectmanager Adviseur Bedrijfsvoering
CJIB	N.t.b.	
Kmar	N.t.b .	

4. De organisatie: overleggen

Naam overleg	Frequentie	Deelnemers
Stuurgroep	Maandelijks	Opdrachtgever, opdrachtnemers, projectleiders
Projectoverleg	Wekelijks	Projectleiders ketenpartners
Sprint refinement	3-wekelijks	Devopps + projectleider org.
Sprint review	3-wekelijks	Devopps + projectleider org.
Voortgangsoverleg – t.b.v. rapportage	Maandelijks	Projectleiders ketenpartners
Voortgangsoverleg – Kwartaal	Elk kwartaal	Stuurgroepleden

5. Kwaliteitsborging (1/2)

Binnen het project wordt actief georganiseerd dat er ruime is voor een kritische blik. De projectleiders van de ketenpartners spreken elkaar erop aan en in de sprint reviews is er aandacht voor.

Wat	Hoe
Beveiliging	Per organisatie zal deze intern uitgezet worden bij de betrokken CISO (chief information security officer). Overall projectleider zal deze borging monitoren en rapporteren op de voortgang.
Privacy	De Privacy Officers van de betrokken ketenpartners zijn betrokken bij het opstellen van de oplossingsrichtingen. Daarbij is tevens een indicatie aangegeven van de consequenties op het gebied van Privacy.
Product Review en Audit	Productreviews toetsen dat het product voldoet aan de eisen van de klant en aan de geldende kwaliteitseisen. In de User Stories wordt geformuleerd wat de acceptatiecriteria van het product zijn. Deze worden getoetst tijdens de sprint demo.
Proces Review en Audit	Procesreviews toetsen of de afgesproken processen gevolgd worden waarmee de kwaliteit geborgd kan worden. De PMO zal dit van tijd tot tijd toetsen. Het sprintproces wordt getoetst door een agile coach, die ook zal kijken of en hoe de onderlinge afhankelijkheid goed/beter georganiseerd kan worden.

5. Kwaliteitsborging (2/2)

Wat	Hoe
Project decharge	Tijdens elke sprint demo worden de acceptatiecriteria getoetst. Bij een akkoord vindt formeel vrijgave van de User Story plaats. Deze criteria zijn van te voren opgesteld en geaccordeerd door de gebruikers. De projectleiders zullen per kwartaal rapporteren over de uitkomsten en de stuurgroepleden middels een overall demo meenemen in hetgeen gerealiseerd en geaccepteerd. De opdrachtgever zal decharge verlenen op het moment dat die items van de Product Backlog zijn opgepakt die zij wenselijk acht en deze zijn geaccepteerd door de gebruikers. Het is daarbij relevant dat niet alle items IV items zijn. Mogelijk – maar dat is afhankelijk van de keuzes voor de oplossingen – zijn ook items uit het werkproces (opleidingen bijv) onderdeel van het project. Ook daarbij zal decharge gevraagd worden aan de opdrachtgever na implementatie van nieuwe werkwijze. Toetsing van nieuw op te leveren producten vindt bij Justid plaats op basis van door IT beheer opgestelde "Acceptatiecriteria IT inbeheername 1.0. Bij doorontwikkeling op bestaande systemen zal deze vooraf getoetst worden door Architectuur.

6. Beheersing

Rapportages

- Voortgangsrapport naar stuurgroep: maandelijks
- Voortgangsrapporten van ketenpartners naar overall projectmanager: maandelijks
- Sprintrapportages: 3-wekelijks
- Afwijkingsrapportages: bij noodzaak

Toleranties

Er is een projecttolerantie van 10%. Binnen deze kan de projectleider Justid wijzigingen in tijd, geld of scope zonder afwijkingsrapportage mag doorvoeren. Indien er binnen de verschillende organisaties sprake is van een risico op overschrijding wordt aan de projectleider Justid gerapporteerd door de projectleider van de ketenpartner.

De stuurgroep wordt op de hoogte gebracht als;

- Financiële gevolgen heeft van meer dan het met de opdrachtgever afgesproken percentage op het projectbudget en/of
- Gevolgen heeft voor het bereiken van een of meerdere mijlpalen op de geplande datum;
- Gevolgen heeft voor de inzet van resources zodat die boven de geplande aanvraag komt en deze inzet niet geleverd kan worden;
- Gevolgen heeft voor de scope van het project;
- Gevolgen heeft voor de kwaliteit van de opgeleverde producten.

7. Risico’s, randvoorwaarden en succesfactoren

Risico’s:

Voor de start van de implementatie zal er door de projectleiders van de ketenpartners een risico-inventarisatie sessie worden georganiseerd. Op basis van deze wordt een risico log gemaakt, welke bij het PMO van Justid in beheer wordt genomen.

De Risico Log wordt besproken in de stuurgroep.

Kritische succesfactoren zijn:

- Commitment van alle ketenpartners op de uitvoering van de gekozen oplossingen
- Beschikbaarheid van resources bij alle ketenpartners
- Een gezamenlijke en gelijk op lopende heartbeat

Randvoorwaarden

- Duidelijkheid over technische oplossing Politie
- Het vernieuwen van de huidige koppeling JDS-SKDB is randvoorwaardelijk om de problematiek beschreven in het onderhavige document aan te pakken
- Er wordt gestreefd te werken binnen de architectuur in de strafrechtketen

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Plan van Aanpak Dweilen

Als onderdeel Ketenissue Bewaartermijnen

17 mei 2021

Dweilen: plan van aanpak

1. De opdracht
    1. Aanleiding
    2. Context
    3. Afbakening
    4. Randvoorwaarden uitgangspunten
2. Project Aanpak
    1. Mijlpalen
    2. Werkwijze
3. Organisatie
    1. Stuurgroep
    2. Werkgroep
4. Kwaliteitsborging
    1. (Beleids)keuzes
    2. Privacy
5. Beheersing en control
    1. Rapportages, wijzigingen, toleranties
6. Risico’s

1.1 De opdracht: context (1/2)

- Van alle verdachten die zijn aangehouden voor een misdrijf waarvoor voorlopige hechtenis mogelijk is of bij twijfel over de identiteit van verdachten (ook bij overtreding), worden o.a. personalia genoteerd, frontale gelaatsfoto's en vingerafdrukken genomen.

- De foto's worden opgeslagen in de SKDB en parallel in CATCH (de fotodatabank van de Nationale Politie), de vingerafdrukken in de SKDB en HAVANK (het vingerafdrukkenbestand van de Nationale Politie)

- Het verwijderen van gegevens zou moeten gebeuren conform artikel 5 van de BIVV, dat gebeurd nu onvoldoende. Bijv.
  - Als de strafzaak eindigt met een sepot (zie memo 'sepots') of bij onherroepelijk vrijspraak of ontslag van rechtsvervolging en de persoon ook niet veroordeeld of verdacht is in andere zaken, moeten de desbetreffende biometrische gegevens direct worden vernietigd (w.o foto's en vingerafdrukken, maar ook kopie-ID bewijs).
  - De overige geregistreerde personalia moeten overeenkomstig met de bewaartermijnen worden vernietigd. Zie BIVV artikel 5.
  - Zodra een verdachte met goed gevolg een project zoals bedoeld in art 77^{e}, eerste lid van het WvS heeft afgerond (HALT) moeten zijn gegevens worden vernietigd.

1.1 De opdracht: context (2/2)

Medio 2020 is vanuit het MinJenV de opdracht gegeven aan Justid om te onderzoeken:

> *'Hoe zaak en identiteitsvaststelling eenduidig gekoppeld kunnen worden en de Justitiële Informatiedienst haar rol als centrale bewaker van de bewaartermijnen binnen de strafrechtsketen kan invullen en aan haar verplichtingen op grond van artikel 5 Bivv kan voldoen'*

1.2 De opdracht: aanleiding

Vraag Minister (n.a.v. nota bewaartermijnproblematiek en vragen Nu.nl):

- Hoe kunnen we laten zien wat we concreet binnen een overzichtelijke termijn gereed hebben?

Antwoord ketenpartners:

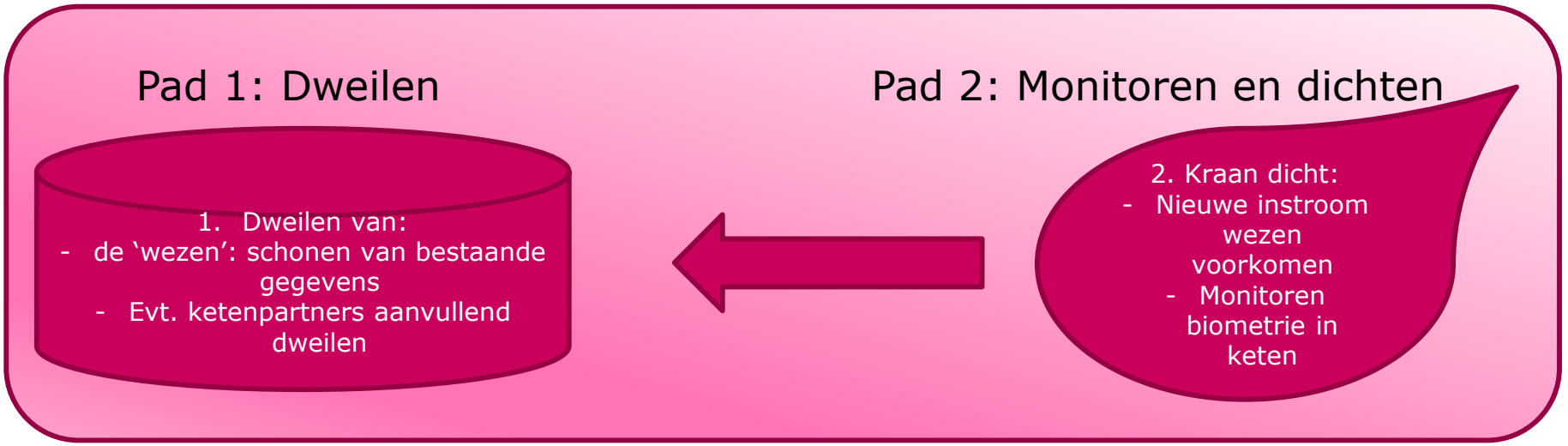
- Mijlpalenplanning opgeleverd, met daarin als 1e stap:
  - Dweilen van de wezen*
    - 80.000 bestaande *wezen beoordelen en mogelijk biometrie vernietigen*
    - Eventuele aanvullende dweil acties door ketenpartners zelf
      - Nb. Indien deze er zijn, vraagt dit om separate acties

** Wezen gedefinieerd: Identiteitsvaststelling in SKDB (w.o. biometrie) waarbij na onderzoek door de ketenpartners geen zaaksgegevens aan te koppelen zijn*

1.3 De opdracht: afbakening

- Dit plan van aanpak richt zich sec op ‘Pad 1’ (zie onder)
  - **Nb:** voor het dweilen specifiek is door DGRR besloten dat ook de persoons gegevens (onderdeel van de 80.000 wezen) onderdeel van de scope zijn.

- Voor ‘Pad 2’ loopt er een parallel traject, met separate opdracht vanuit het MinJenV aan Justid als penvoerder (in dit plan buiten scope)



1.3 De opdracht: Randvoorwaarden

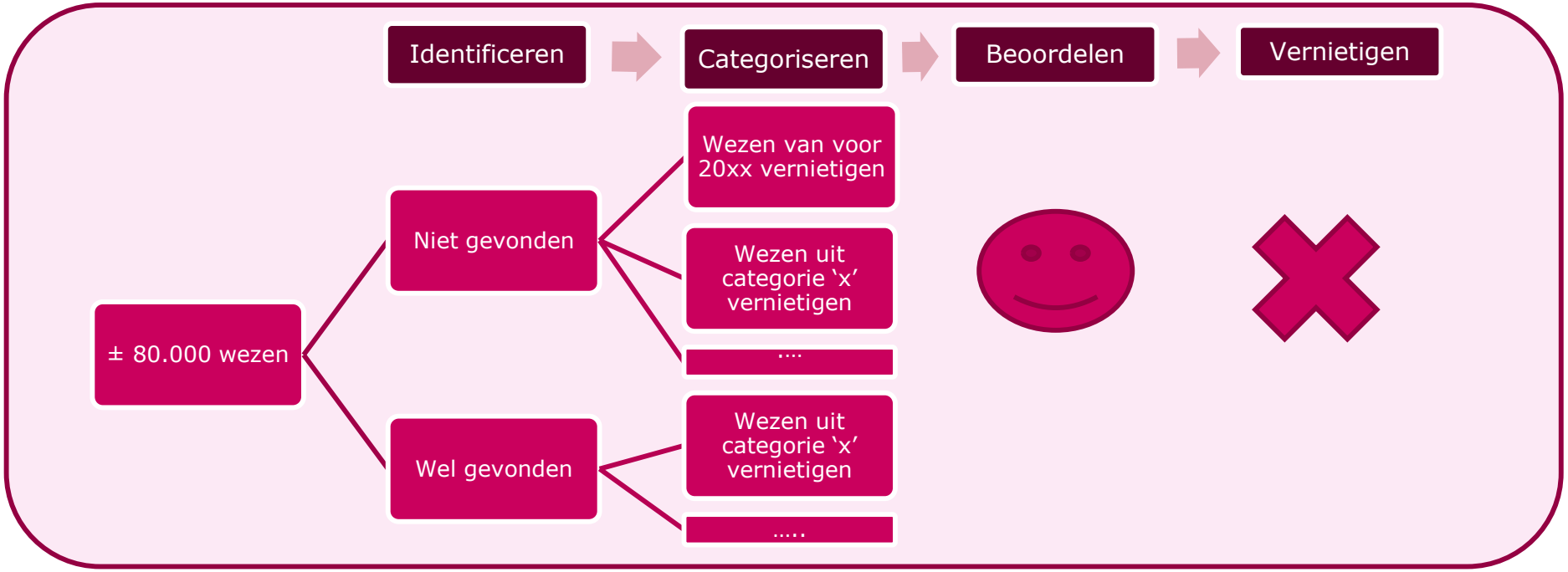
Randvoorwaarden

- Commitment van alle ketenpartners: partners zijn intern opdrachtgever en lopen gelijk op
- Besluitvorming over bijv. het categoriseren en vernietigen wordt tijdig genomen door organisaties met verantwoordelijkheid en mensen met mandaat
- De vernietiging vindt plaats cf. de BIVV

2.1 De aanpak: Werkwijze (1)

- Er zijn op dit moment ongeveer 80.000 wezen
- Elke maand komen er gemiddeld ongeveer 1.000 wezen bij

- Voorstel aanpak: identificeren, categoriseren, beoordelen en vernietigen van biometrische- en persoonsgegevens



2.1 De aanpak: Werkwijze (2)

Er is een werkgroep ingericht, in deze wordt inhoudelijke expertise van de ketenpartners (Politie, OM, CJIB, Justid en DGRR) samengebracht en vindt voorbereiding van de besluitvorming plaats. Ook de Kmar en NFI worden betrokken voor hun zaken specifiek.

Stap 1 - Identificeren:

Doel: vaststellen welke 'wezen' niet voorkomen in systemen van ketenpartners
Randvoorwaarde: schriftelijke vastlegging dat lijsten worden gedeeld en beoordeeld

1. Vanuit Justid is een lijst met namen van personen waar geen opvolging aan is gegeven (vanuit de SKDB) aangeleverd aan de Politie en Kmar.
2. Ketenpartners (Politie, OM, Kmar, NFI) deze lijst vergeleken met haar systemen, waaruit blijkt welke wel/niet herkend zijn in haar systemen.

Gepland gereed: Q1 2021 (Status: Onderhanden, gereed voor BVH (Bluespotmonitor), matching loopt nog tegen MEOS (Politie) en bij KMar)

2.1 De aanpak: Werkwijze (3)

Stap 2 - Categoriseren:

Doel: Onderscheid maken naar categorieën, zodat inzicht ontstaat in de aantallen en een advies kan worden gegeven over de mogelijk oplossingen/vervolgstappen: bijv. vernietigen.

1. De door Politie verrijkte wezenlijst uit de SKDB van mogelijke categorieën en aantallen voorzien en evt. check door andere ketenpartners op systemen
2. Bespreken en evt. wijzigen van dit voorstel in de werkgroep, zodat gedeeld beeld ontstaat
3. Categorieën voorzien van advies en grondslag, waaronder bijv.:
    1. Starten met de eenvoudige zaken of grote aantallen
    2. Rekening houdende met Sepots (zie memo sepots)
    3. Voorstel op verwijderen na bijv. ‘x’ aantal jaren
    4. Risico’s worden meegenomen
4. Interne en ketenbrede afstemming waar nodig om tot gedragen advies te komen

Gepland: Start Q1, doorloop Q2 (status: onderhanden)

2.1 De aanpak: Werkwijze (4)

Stap 3 - Beoordelen:

Doel: Beoordelen en besluit op de voorgestelde categorieën t.b.v. het vernietigen
Randvoorwaarde: overeenstemming over volgen BIVV v.w.b. vernietiging (art 8)

1. Het advies van de werkgroep over de categorieën en de aanpak van beoordelen per categorie en de daaruit voortvloeiende acties worden ter beoordeling voorgelegd aan DGRR
2. Het door DGRR beoordeelde advies wat te doen met welke categorie wordt ter besluitvorming op proces voorgelegd aan de stuurgroep
    1. Dit gebeurt mogelijk stapsgewijs: de kans is aanwezig dat niet voor elke categorie op hetzelfde moment een advies gereed is
3. Besluit Stuurgroep

Gepland: Start Q2 - stapsgewijs

2.1 De aanpak: Werkwijze (5)

Stap 4 - Vernietigen:

Doel: Vernietigen van de gegevens uit de systemen

Randvoorwaarde:

- Vernietiging vindt plaats o.b.v. overeengekomen wijze
  - (Nb. er zit een verkeerd uitgangspunt in de Bivv. Namelijk dat het Openbaar Ministerie de Justitiële Informatiedienst de informatie verstrekt die nodig is om te kunnen voldoen aan de artikelen 5 tot en met 7') Dit kan het OM niet waarmaken, aangezien zij geen totaaloverzicht heeft. Een deel van de oplossing is dus een lijn vanuit politie naar Justid en keten).
- Duidelijkheid over wijze van logging

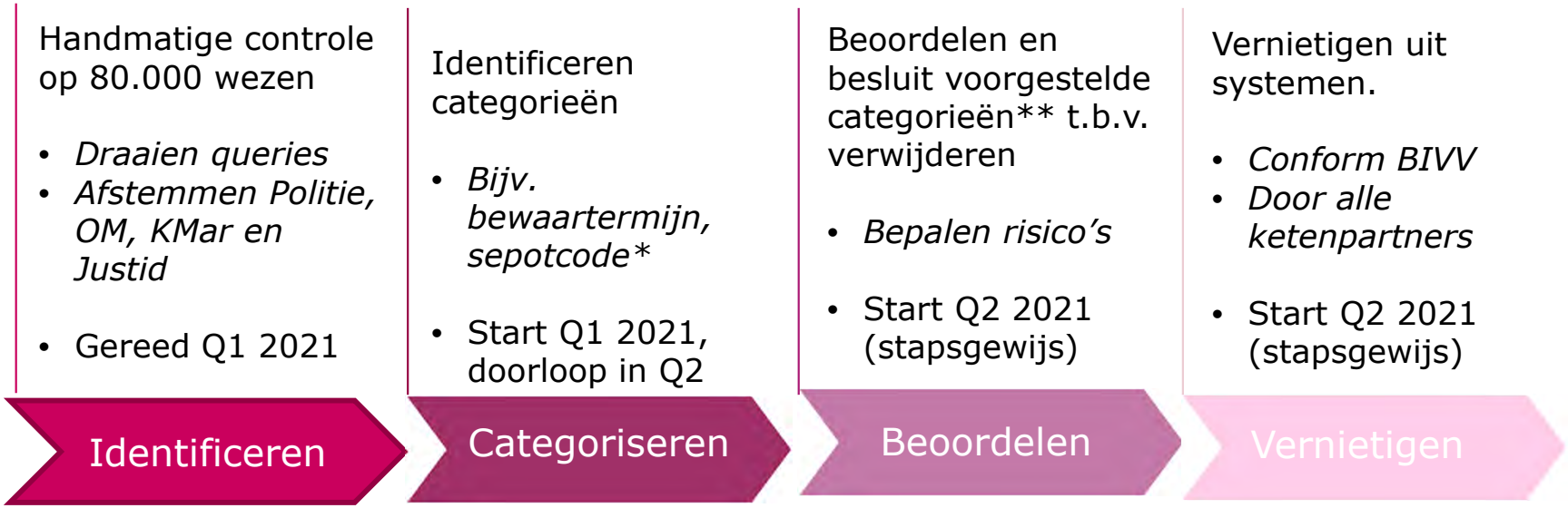
1. Akkoord op aanpak wijze van vernietigen door stuurgroep
2. Vernietigen van gegevens uit de systemen conform de overeengekomen wijze van vernietigen

   > Dit gebeurt mogelijk stapsgewijs: de kans is aanwezig dat niet voor elke categorie op hetzelfde moment een besluit wordt genomen.

   > Er vindt logging plaats van hetgeen vernietigd

Gepland: Start Q2 - stapsgewijs

2.2 De aanpak: Mijlpalen

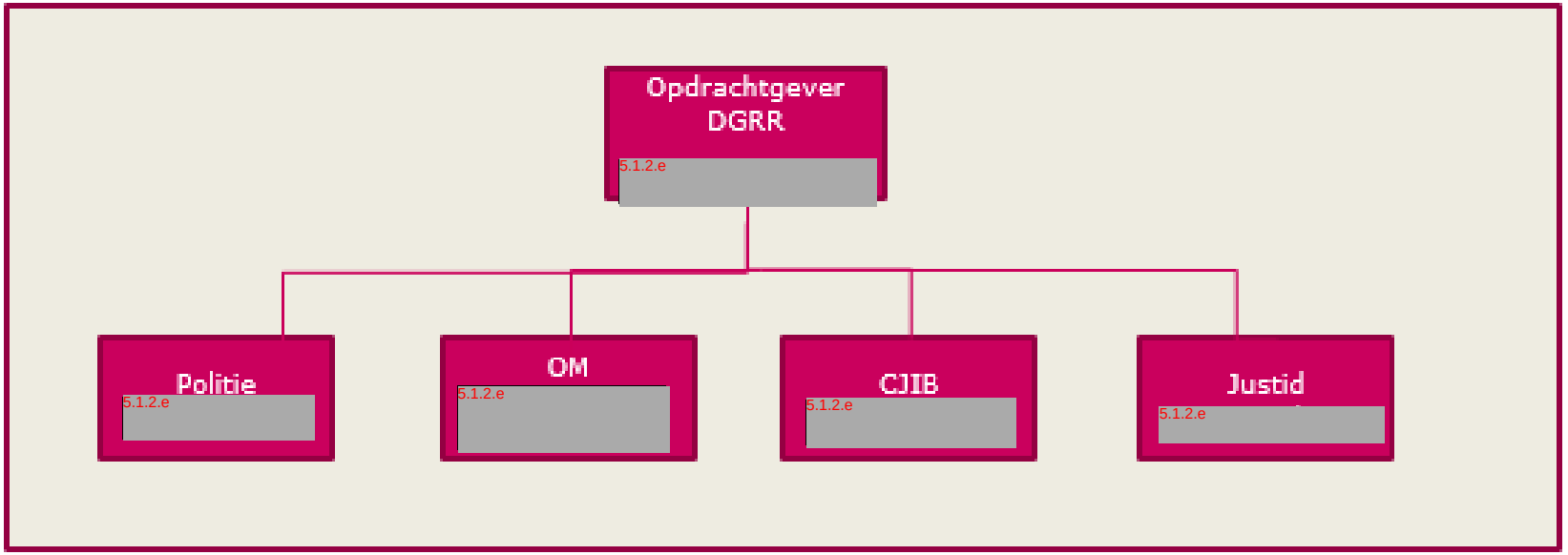


*Juridische check DGRR op o.m. sepotcodes die vernietigd kunnen worden
** Beleidsbeslissing op categorieën w.o. verwijderen na 'xx' jaar

Afhankelijk van de risico's blijft er mogelijk een restcategorie over welke nader beoordeeld of niet verwijderd kunnen worden of welke bij recente matching bij ketenpartners wel een zaaksverwijzing is aangetroffen. Deze categorie zal ook kenbaar worden gemaakt aan de stuurgroep, voorzien van advies.

Mijlpalen o.b.v. nu bekende informatie en voorbehouden. Gedurende traject wordt meer duidelijk over realiteit hiervan

3.1 De organisatie: stuurgroep (1)



Ook aanwezig bij stuurgroepvergadering:
- 5.1.2.e (KIV/DGRR): business owner
- 5.1.2.e (Justid) overall projectmanager
- 5.1.2.e (Justid) overall projectondersteuner.

3.1 De organisatie: stuurgroep (2)

Er is een stuurgroep ingericht, waarbinnen iedere deelnemer verantwoordelijk is voor:

- Informeren eigen bestuurlijke organisatie
- Borgen uitvoeringskeuzen PvA in eigen portfolio
- Aanjagen uitvoering in organisatie

Organisatie	Naam	Functie
DGRR	5.1.2.e	Opdrachtgever – bewaker departementale lijn
Justid	5.1.2.e	Opdrachtnemer en intern opdrachtgever Justid voor Plan van Aanpak en realisatie Penvoerder voor analyse en PvA
Politie	5.1.2.e	Opdrachtnemer en intern opdrachtgever Politie voor Plan van Aanpak en realisatie
OM	5.1.2.e	Opdrachtnemer en intern opdrachtgever OM voor Plan van Aanpak en realisatie
CJIB	5.1.2.e	Opdrachtnemer en intern opdrachtgever CJIB voor Plan van Aanpak en realisatie

3.2 De organisatie: werkgroep

Er is een werkgroep ingericht met als taken:

- *Problematieken analyseren en reviewen*
- *inhoudelijke expertise vanuit de partners inbrengen*
- *Adviezen opstellen tbv besluitvorming over bewaartermijnenbeleid en vernietigen van gegevens*

Randvoorwaarde: werkgroep voldoende kwantitatieve en kwalitatieve resources van ketenpartners

Organisatie	Naam	Functie
DGRR	5.1.2.e	Business Owner
Justid	5.1.2.e	Projectmanager (overall) Projectondersteuner (overall) Business consultant Productspecialist SKDB Productspecialist SKDB Productspecialist JDS
Politie	5.1.2.e	Projectmanager Product Owner, Expert BVID Expert BOSZ Gegevensexpert
OM	N.t.b. 5.1.2.e	Projectmanager Adviseur Bedrijfsvoering
CJIB	N.t.b.	

4. Kwaliteitsborging

(Beleids)keuzes:

In het project zullen een aantal keuzes moeten worden gemaakt. Hieronder keuzes die gevolg kunnen hebben tot het definitief verwijderen van gegevens. In de werkwijze zijn deze keuzemomenten (voor zover op dit moment voorzien) gedefinieerd.

Gedurende de uitvoering zullen deze keuzes expliciet worden voorgelegd aan de stuurgroep. Indien er aanvullend advies is gewenst voor een besluit, zal het project hiervoor zorgdragen.

Privacy:

Voor de uitwisseling van gegevens zullen afspraken worden gemaakt waarbij de privacy afdelingen van de verschillende organisaties worden betrokken.

5. Beheersing

Rapportages

- De voortgang van het project Bewaartermijnen wordt maandelijks via het voortgangsrapport met de stuurgroep gedeeld. In deze wordt tevens specifiek aandacht besteed aan het dweilen van de wezen. Mocht er aanleiding zijn om tussentijds te rapporteren (over wijzigingen) dan zal dat gebeuren.
- Vanuit de ketenpartners zal maandelijks via de projectleiders richting Justid (overall projectleider) worden gerapporteerd over de voortgang inclusief risico's en maatregelen. Dit gebeurd uiterlijk de 5e werkdag van de maand, via een voortgangsrapport, zodat dit meegenomen kan worden in de overall rapportage.

Toleranties

- Er is in de offerte Bewaartermijnen (opdracht aan Justid) afgesproken dat de werkelijk bestede uren worden gefactureerd. Indien het aantal uren meer dan 25% naar boven afwijkt, zal hiervoor een nadere offerte worden uitgebracht.
- Voor het dweilen van de wezen is 25.000 separaat beschikbaar gesteld aan Justid. In lijn met hetgeen voor de bredere offerte is afgesproken zal worden geacteerd.
- De stuurgroep wordt op de hoogte gehouden van de voortgang in tijd. Bij vertraging wordt afgesproken hoe hiermee om te gaan.

Nb. Nog spreken over budget partners?

6. Risico’s

- Onvoldoende of niet de juiste capaciteit bij de ketenpartners om o.a.:
  - *Te participeren in voorbereiding besluiten*
  - *Uitvoering te geven aan genomen besluiten*
  - *Nb. 1 aanspreekpunt (projectleider) is nodig voor de Overall Projectleider bij elke organisatie*

- Geen tijdige besluitvorming over o.a.:
  - *Categorieën t.b.v. verwijderen (denk aan bewaartermijn en sepotcodes)*
  - *Het daadwerkelijk vernietigen*

- Mijlpalen zijn o.b.v. nu bekende informatie. Gedurende het traject wordt meer duidelijk over realiteit hiervan.

- Er blijft een grote restcategorie over, waarover geen besluit genomen kan worden

- Vernietigen van informatie = echt vernietigen van informatie (voorbeeld Groot-Brittannië)

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

ONGERUBRICEERD - CONCEPT
Stuurgroep Issues Strafrechtketen

Justitiële Informatiedienst
Burg. Raveslootsingel 2
7607 GK Almelo
Postbus 337
7600 AH Almelo
www.justid.nl

Contactpersoon
5.1.2.e

T 5.1.2.i
5.1. @justid.nl
2.i

Datum
27 mei 2021

Projectnaam
Issues Strafrechtketen

memo

Issue bewaartermijnen: sepots

Geachte heer/mevrouw,

Graag vraag ik uw aandacht voor het volgende punt, naar aanleiding van een vraagstuk rond bewaartermijnen van geseponeerde zaken in het concept analyserapport 'Issues bewaartermijnen'. Dit vraagstuk speelt mede naar aanleiding van de wezenproblematiek[1] en het oplossen van de bestaande gevallen (dweilactie). Zie voetnoot 1 over definitie en details over de wezen. De focus van deze memo ligt echter op de vernietiging van persoonsgegevens van zaken na een sepot (zie BIVV art 5 lid 1 voor het onderscheid in biometrische gegevens en andere persoons- en zaaksgegevens). Een memo met focus specifiek op de wezen (en niet uitsluitend betreffende sepots), volgt later.

De lijn die hieronder is beschreven is afgestemd met 5.1.2.e , de Senior wetenschappelijk medewerker van het parket generaal van het openbaar ministerie en het ministerie van J&V/KIV.

Een zaak kan om diverse redenen worden geseponeerd. Voor elke reden om te seponeren is een code afgegeven door het OM. De verschillende sepotcodes worden in de keten gebruikt in de communicatie over de (afloop van) zaken. De omgang met sepots en de codes zijn vastgelegd in de 'Aanwijzing gebruik sepotgronden OM'.

Op basis van artikel 5 lid 1 en 3 Bivv moeten Justid en de Politie de biometrische gegevens van verdachten vernietigen bij een sepotbeslissing. Uitzondering hierop

[1] Wezen zijn persoonsgegevens zonder zaaksverwijzing. Hiervan zijn twee hoofdgroepen te onderscheiden:

- een (grote) groep identiteitsvaststellingen die niet 'gelinkt' kan worden aan een mutatie/proces-verbaal of een zaak, ook niet via de politieadministratie (bijvoorbeeld de identiteiten uit BVID met de processen verbaal uit de BVH). Het gaat hier dus om los zwevende identiteitsgegevens (al of niet met biometrische gegevens).
- een groep identiteitsvaststellingen die wel is te achterhalen met allerlei statussen en dus verschillende (eind)beslissingen, parketnummers etc.

Onderhavige memo is (mede) van toepassing op de tweede groep wezen, omdat deze na uitlopen in de diverse administraties in de keten in veel gevallen nog wel te achterhalen zijn.

zijn beschreven in artikel 5 lid 4[2], van vernietiging wordt afgezien als iemand in een andere zaak als verdachte van een strafbaar feit is aangemerkt of in een andere zaak is veroordeeld, en artikel 5 lid 5[3].
Bij een sepot is iemand 'niet langer verdachte'. Voor het bepalen van de bewaartermijn is de reden van het sepot niet relevant. De bewaartermijn van de biometrische gegevens is dus 0 voor elk sepot.

Hierop is toch één nuance aan te brengen: het voorwaardelijk sepot. Dit sepot is (tot 01-03-2021, zie verder) vergelijkbaar met een transactie. Daarbij kan het voorwaardelijk sepot zo worden benaderd: de officier van justitie zegt toe om af te zien van de vervolging wanneer de verdachte zich houdt aan de voorwaarden. Zolang de voorwaarden nog niet zijn vervuld, heeft de officier van justitie nog niet definitief besloten (Corstens/Borgers & Kooijmans 2018, p. 632 noemen het een uitstel van de beslissing). Zolang de officier van justitie nog niet definitief heeft besloten mogen de biometrische gegevens van de verdachte nog niet te worden vernietigd. De bewaartermijn van de biometrische gegevens van dit sepot is dus ook 0, maar gaat pas in na de proefperiode als de voorwaarde is vervuld.

De 'Aanwijzing gebruik sepotgronden OM' is heel recentelijk gewijzigd per 01-03-2021[4] en beperkt sindsdien het gebruik van het voorwaardelijk sepot: 'In beginsel wordt bij een beslissing tot sepot slechts de algemene voorwaarde gesteld dat de verdachte geen strafbare feiten begaat binnen een proeftijd van ten hoogste een jaar. Een sepot met bijzondere voorwaarden wordt in beginsel niet meer ingezet'.

Op basis van artikel 8 Bivv is het openbaar ministerie verantwoordelijk voor het verstrekken van de informatie over de afdoening van de zaak aan Justid, zodat Justid de beslissing over de vernietiging van de biometrische persoonsgegevens kan nemen (artikel 5 Bivv) en tevens de Politie (HAVANK) kan informeren over deze afloop van de zaak (artikel 9a, lid 8, Bivv). In het geval van een voorwaardelijk sepot of een transactie is dat dus inclusief de informatie of de verdachte zich heeft gehouden aan de voorwaarden.

De stuurgroepleden wordt gevraagd om deze lijn ook te implementeren in de eigen organisatie voor de wezenproblematiek. Dat betekent dat de biometrische gegevens van alle wezen met geseponeerde zaken worden vernietigd (tenzij na onderzoek in het kader van wezen de persoon nog verdachte of veroordeelde blijkt te zijn van een ander strafbaar feit). In het geval van de voorwaardelijke

---

[2] In afwijking van het eerste en tweede lid wordt van het vernietigen van de in deze leden bedoelde gegevens afgezien indien degene wiens gegevens het betreft, in een andere zaak als verdachte van een strafbaar feit is aangemerkt of in een andere zaak is veroordeeld.

[3] In afwijking van het eerste en tweede lid wordt van het vernietigen van de in deze leden bedoelde gegevens afgezien indien degene wiens gegevens het betreft, een gewezen verdachte is die niet eerder voor hetzelfde feit in een herzieningsprocedure als bedoeld in Titel VIII van het Derde Boek van de wet is vrijgesproken of ontslagen van alle rechtsvervolging. De gegevens kunnen in dat geval uitsluitend worden geraadpleegd:
a.met het oog op een herziening ten nadele op de in artikel 482a, eerste lid, onder a, van de wet bedoelde grond en na toestemming van de rechter-commissaris, of
b.ingeval van een vergelijking als bedoeld in artikel 9, zesde lid, of als bedoeld in artikel 14, zevende lid, van het Besluit DNA-onderzoek in strafzaken.

[4] Aanwijzing gebruik sepot en sepotgronden, https://wetten.overheid.nl/BWBR0044670/2021-03-01

sepots moet dus ook de proefperiode in acht worden genomen en moet zijn vastgesteld dat aan de voorwaarde is voldaan.

Met vriendelijke groet,
5.1.2.e (Justid)
5.1.2.e (ministerie van JenV)

Bijlage: De volgende personen zijn betrokken geweest bij onderliggende memo:

Naam	**Functie**	**Organisatie**
5.1.2.e	Ged. Opdrachtgever	J&V
5.1.2.e	Business Consultant	Justid
5.1.2.e	5.1.2.e	Justid
5.1.2.e	Adviseur Bedrijfsvoering	OM
5.1.2.e		Politie
5.1.2.e		Politie
5.1.2.e	Jurist	J&V
5.1.2.e	Jurist	J&V
5.1.2.e	projectleider	Justid
5.1.2.e	Hoofd Matching	Justid
5.1.2.e	Productspecialist Matching	Justid
5.1.2.e	Productspecialist Matching	Justid
5.1.2.e	Productspecialist Matching	Justid
5.1.2.e	Productspecialist JDS	Justid

Van: 5.1.2.e
Aan: Riemen, John (J.A.J.M.)
Onderwerp: RE: Concept memo bewaartermijnen sepots 0.991.docx
Datum: maandag 7 juni 2021 15:59:30

Ja zo zie je maar.. 5.2.1

Even nog iets anders.. Niet onder reikwijdte

Hoor het graag!

Van: Riemen, John (J.A.J.M.)
Verzonden: maandag 7 juni 2021 15:52
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: Concept memo bewaartermijnen sepots 0.991.docx

Kijk hier word ik vrolijk van… ;-)

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: maandag 7 juni 2021 12:36
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: RE: Concept memo bewaartermijnen sepots 0.991.docx

Hi John,

Dank en terechte punten ☺. De beoordeling van de memo heb ik inderdaad al door 5.1.2.e en 5.1.2.e laten doen. Met name 5.1.2.e heeft vanuit het oogpunt van Wb v Sv nog wel wat opmerkingen. Zie hieronder.

Hoi 5.1.2.e

Ik heb de memo bekeken. De kernzin, waarop de hele memo en het daarin geformuleerde advies is gebaseerd, is: ¨Bij een sepot is iemand 'niet langer verdachte"¨. Dat lijkt mij alleen zo te zijn bij sepotcodes 01 en 05. Bij de rest van de sepotcodes/gronden is iemand nog wel degelijk verdachte, alleen is er onvoldoende ´wettig en overtuigend´ bewijs voor een succesvolle vervolging, of dat bewijs is er wel, maar vervolging/berechting wordt door de OvJ niet opportuun geacht. Een verdachte is iemand tegen wie een ´redelijk vermoeden van schuld´ bestaat. Dat is een behoorlijk tandje minder dan ´wettig en overtuigend bewijs´.

Het Besluit identiteitsvaststelling verdachten en veroordeelden waar deze memo zich op baseert, zegt in artikel 5 lid 1 dat de biometrische gegevens vernietigd moeten worden als iemand ´niet langer als verdachte van een strafbaar feit kan worden aangemerkt´. In het derde lid worden voorbeelden gegeven van situaties waarin daarvan sprake is. Zo wordt genoemd een beslissing tot niet-vervolging en een door de rechter uitgesproken ontslag van alle rechtsgevolgen. In de toelichting (Staatsblad 2009, 352) op dat derde lid staat het volgende:

´De omstandigheden die meebrengen dat een persoon wiens gegevens in de strafrechtsketendatabank zijn verwerkt, niet langer als verdachte van een strafbaar feit kan worden aangemerkt, zijn in artikel 5, derde lid, van dit besluit opgesomd. Deze omstandigheden zijn dezelfde als die in artikel 16, tweede lid, van het Besluit DNA-onderzoek in strafzaken zijn genoemd. Van zo'n omstandigheid is bijvoorbeeld sprake in geval van een verdachte die een kennisgeving van niet verdere vervolging heeft gekregen of een rechterlijke verklaring heeft ontvangen dat de zaak geëindigd is. In die situaties, waarin niet alleen de schuld van de verdachte niet in rechte is vastgesteld 5.2.1 , verdient deze (mede gelet op de onschuldpresumptie van artikel 6, tweede lid, van het van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)) dezelfde behandeling als een onschuldige.´

Kort en goed: alleen bij een sepotcode 01 (ten onrechte als verdachte aangemerkt) en sepotcode 05 (feit niet strafbaar) is sprake van een situatie waarin de verdenking is vervallen. Bij alle overige sepotgronden kan dit niet gezegd worden, en is de vernietigingsplicht van artikel 5 BIVV dus niet aan de orde.

Tot zover de puur juridische duiding. Iets anders is natuurlijk de vraag of je niet meer zou moeten schonen dan wettelijk verplicht is, waarom dan en wat de (lange termijn) effecten daarvan zijn voor de politie. Ik sprak je voicemail al even in om wat nadere context bij dit vraagstuk te krijgen.

Groet,

5.1.2.e
Juridisch adviseur

Ook de aanleiding van de memo hebben wij nagevraagd. Deze blijkt echter niet helemaal meer duidelijk. Justid gaat dit na. Wordt vervolgd..

Groet,

5.1.2.e

Van: Riemen, John (J.A.J.M.)
Verzonden: maandag 7 juni 2021 09:54
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: Concept memo bewaartermijnen sepots 0.991.docx

Hoi 5.1.2.e

Zoals beloofd een reactie.
Ik heb het met belangstelling gelezen en hoop dat dit duidelijkheid gaat scheppen.
Fijn dat ook zij moeten constateren dat de politie geïnformeerd moet worden door JUSTID ;-).

Opmerkingen van mijn kant;

1. In algemene zin mijn eerdere opmerking, hoe gaat JUSTID bepalen of de persoon geen

verdachte meer is in politie onderzoeken? Als dat bij ons wordt neergelegd is dat een aanzienlijke administratieve belasting waar wij nu geen capaciteit voor hebben. JUSTID heeft nu (denk ik) geen toegang.

2. “Bewaartermijn sepot is 0 “ suggereert dat je dan direct kan vernietigen, dit is natuurlijk niet waar en schept een verkeerd verwachtingsmanagement. Er zal een verwerking door OM en vervolgens een beoordeling door JUSTID aan vooraf gaan. Daarna moeten wij geïnformeerd worden. Afhankelijk van de mate van automatisering en wie de beoordeling gaat doen van “verdachte in een andere zaak” politie kan dat best even duren.
3. Het zou goed zijn als JUSTID ook nog een check doet/laat doen op HAVANK aangezien HAVANK ook historische registraties van voor 2010 bevat.

Daarnaast zou mijn advies zijn om dit ook door onze eigen juristen zoals 5.1.2.e te laten beoordelen (maar misschien heb je dat al gedaan).

Kortom mooie eerste stap!

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK en CATCH

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Let op: Met ingang van 2 april 2020 is **DSO, Dienst Specialistische Operaties**, de nieuwe naam van de dienst DLOS.

Van: 5.1.2.e
Verzonden: dinsdag 1 juni 2021 13:47
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: Concept memo bewaartermijnen sepots 0.991.docx

Hi John,

Hierbij de memo waarover ik je net gesproken heb. Ben benieuwd naar jouw review!

Met vriendelijke groet,

5.1.2.e

Van: Riemen, John (J.A.J.M.)
Aan: 5.1.2.e
Onderwerp: RE: Jaarcijfers Catch
Datum: donderdag 22 juli 2021 12:50:34

Tuurlijk

De schoning hebben wij gedaan op de zogenaamde Foto Confrontatie Module foto's.
Dit op basis van de schoningssystematiek van deze foto's.
Niet bekend over hoeveel unieke personen dit gaat, er is op foto niveau geschoond.

De aantallen

In 2019 ook nog 8 internationale matches dus ik het totaal was 98.

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK, CATCH en DNA Eliminatie DataBank

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 22 juli 2021 11:34
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: FW: Jaarcijfers Catch

Hi John,

Zoals verwacht ;-) Zie hieronder de vragen van Stan.
Kun jij toelichten?

Groet,
5.1.2.e

Van: 5.1.2.e [mailto:5.1.2.e @nu.nl]
Verzonden: donderdag 22 juli 2021 11:28
Aan: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: Re: Jaarcijfers Catch

Hee 5.1.2.e ,

Dank! Ik ben wel benieuwd naar de 218.000 opgeschoonde foto's in 2020. Wat is hier de achtergrond van? En is bekend om hoeveel unieke personen het hierbij gaat?

Ter dubbelcheck: bij het bezoek aan het Centrum voor Biometrie in januari 2020 zei John Riemen dat er 98 matches waren in 2019. In dit overzicht staat nu 90. Is hier een correctie toegepast?

Hoor het graag!

Met vriendelijke groet,
5.1.2.e

Op do 22 jul. 2021 om 10:35 schreef Ariaans, Therese (T.T.P.) <5.1.2.i @politie.nl>:

> Hi 5.1.2.e
>
> Zoals net afgesproken, de jaarcijfers zijn gepubliceerd op politie.nl:
> https://www.politie.nl/binaries/content/assets/politie/onderwerpen/forensische-opsporing/catch-jaarcijfers-2020-hr-online.pdf
> Mocht je nog vragen hebben, dan hoor ik het graag.
>
> Groet,
> Thérèse
>
> **Thérèse Ariaans**
> Senior adviseur / woordvoerder
>
> 06 – 5.1.2.e
> Werkdagen: ma, di, do, vrij
>
> Politie | Landelijke Eenheid | Communicatie
> Hoofdstraat 54, 3972 LB, Driebergen
> Postbus 100, 3970 AC Driebergen
>
> Meer informatie? Kijk op politie.nl
>
>

Van: Riemen, John (J.A.J.M.)
Aan: Ariaans, Therese (T.T.P.)
Onderwerp: RE: Vragen NRC m.b.t. CATCH
Datum: vrijdag 23 juli 2021 12:45:44

En hierbij de antwoorden.

Voor NRC wat uitgebreider gedaan met verwijzing naar het Kamerdebat en de antwoorden van de Minister

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK, CATCH en DNA Eliminatie DataBank

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Van: Ariaans, Therese (T.T.P.)
Verzonden: vrijdag 23 juli 2021 11:16
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
Onderwerp: FW: Vragen NRC m.b.t. CATCH

En hierbij de vragen van NRC.
Kun jij beantwoorden?

Thanks!
Thérèse

Van: 5.1.2.e [mailto:5.1.2.e @nrc.nl]
Verzonden: vrijdag 23 juli 2021 11:10
Aan: LEE - Staf - Team Media en Publiciteit - Mediadesk <mediadesk.media-en-publiciteit.landelijke-eenheid@politie.nl>
Onderwerp: Vragen NRC m.b.t. CATCH

Ha Therese Ariaans,

N.a.v. ons telefoongesprek over de jaarcijfers omtrent CATCH, hierbij de vragen:

1. Op welke dag zijn deze cijfers gepubliceerd? 21-07-2021

2. Welke foto's vallen onder die 2,6 miljoen die in de cijfers genoemd staan? Dit getal lijkt namelijk zo gigantisch voor het aantal veroordeelden/verdachten in Nederland. Je zei al even dat telkens als iemand verdacht wordt, nieuwe foto's worden gemaakt. Is dit dan inderdaad drie foto's (links, rechts voor) per keer? En gaat dat dan om alle aanhoudingen of wanneer komt het tot een foto/foto's? Om hoeveel individuen gaat dit?

Elke keer dat een verdachte wordt aangehouden voor een VH feit wordt opnieuw de foto gemaakt. Elke foto is van belang omdat er verschillen in het gezicht kunnen zijn, bijv leeftijdsverschillen, ziektes, drugsgebruik of andere zaken die invloed hebben op het gezicht. Van belang is dus om diverse foto's van dezelfde persoon te hebben voor herkenning. Daarnaast mogen de foto's, conform de wettelijke regels, langjarig bewaard worden. De aantallen van aangehouden verdachten liggen per jaar rond boven de 200.000 zie https://opendata.cbs.nl/#/CBS/nl/dataset/82315NED/table. De database bestaat uit een mix van de foto's van de BVID zuilen/SKDB en de 2 luik verdachte foto's.

In het Besluit identiteitsvaststelling verdachten en veroordeelden (Bivv) zijn de bewaartermijnen voor foto's die worden bewaard in de SKDB vastgelegd. De termijn varieert van 20 tot 80 jaar. De termijn voor het bewaren van politiegegevens is geregeld in de Wet politiegegevens (Wpg) dit geldt voor de zogenaamde 2-luik verdachte foto's van voor 2010

Zie ook antwoorden van de Minister van Justitie en Veiligheid

3932
Vragen van het lid Verhoeven (D66) aan de Minister van Justitie en Veiligheid over het bericht «Gezichtendatabase van politie bevat foto's van 1,3 miljoen mensen» (ingezonden 25 juli 2019).
Antwoord van Minister Grapperhaus (Justitie en Veiligheid), mede namens de Minister voor Rechtsbescherming (ontvangen 11 september 2019) Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3606.

3. De belangrijkste vraag: die 218.000 foto's, om welke reden(en) zijn die opgeschoond? Kunt u hier wat uitgebreider op in gaan? Dus graag alle redenen noemen.
Bij een bestandsvergelijking tussen het bronsysteem en CATCH is geconstateerd bewaartermijnen van deze specifieke WPG foto's waren verstreken. Hierop zijn ze uit CATCH verwijderd.

4. Heeft deze opschoning te maken met de eerdere kritische berichtgeving hierover van NU.nl. Zo ja/nee, op welke manier wel/niet?
Nee de bewaartermijn gaven aanleiding voor deze schoning.

5. Wat is het reguliere beleid voor het opschonen van foto's? Wanneer worden die

weggehaald?
Zie antwoord 2

6. Hoeveel foto's werden de afgelopen vijf jaar jaarlijks weggehaald? (Als dit jaar daarvan afwijkt: waarom wijkt dit jaar daar van af?)
In 2020 is de schoningsactie uitgevoerd voor deze categorie WPG foto's. Dit op initiatief door de beheerder.

Veel dank!

Hartelijke groet,

5.1.2.e
T: 06-5.1.2.e

5.1.2.e

Van: Riemen, John (J.A.J.M.)
Verzonden: vrijdag 16 juli 2021 13:48
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: schonen FCM foto's - advies
Bijlagen: Beleid+bewaartermijnen.pdf

Hoi 5.1.2.e

Hierbij wat input voor foto's uit FCM

Met vriendelijke groeten/kind regards

John A.J.M. Riemen
Leidend Specialist Biometrie
Beheerder HAVANK, CATCH en DNA Eliminatie DataBank

Politie | Landelijke Eenheid | DSO | LFSC | Centrum voor Biometrie (CvB)

Bezoekadres: Europaweg 45, 2711 EM Zoetermeer
Postadres: Postbus 100, 3970 AC Driebergen
Mobiel: +31 6 5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 24 maart 2021 07:44
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: schonen FCM foto's - advies

John,
In aanvulling op de mail hieronder. Zie hoofdstuk 3.7 uit de bijlage van deze mail. We zouden voor schoning van Catch onderzoeken mogelijk een protocol moeten opstellen. Er is een protocol voor FO zaken, maar ik kan mij voorstellen dat de Catch zaken niet gezien worden als FO onderzoek. Met een protocol zouden we ons zeker stellen van bewaartermijnen zonder afhankelijk te zijn van de systemen waarin deze onderzoeken zijn geregistreerd.
Graag je feed back

Met vriendelijke groet,

5.1.2.e
Operationeel Specialist

Politie | Landelijke Eenheid | DSO|LFSC|Centrum voor Biometrie
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e
Werkdagen ma – do van 7-14.30 uur

vr van 7-11 uur

Van: 5.1.2.e
Verzonden: dinsdag 23 maart 2021 11:02
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: schonen FCM foto's - advies

Hi 5.1.2.e
Onderstaand mijn advies hoe om te gaan met de FCM foto's in Catch2 op basis van de bijlage. Dit in afwachting van verbeteringen. Ik weet niet of je bijgaand stuk al eens hebt gelezen, maar dan alsnog ter info. Op dit moment is er nog niets geregeld voor het schonen van FCM foto's of informatie die daar bij hoort in enig systeem zo lijkt het. Ik lees in de laatste paragrafen een paar dingen;
–4.2.4 De verwijderingstermijn hangt onder meer af van het strafmaximum dat voor dat feit in de wet staat. Onderaan de mail de tekst van artikel 6. Ik lees hier een minimale bewaartermijn van 20 jaar voor feiten waar maximaal 6 jaar op staat.
-4.2.6.1 Alleen het OM is bevoegd te seponeren. Dit gebeurt via BOSZ. De sepots die het OM via BOSZ verwerkt komen automatisch in de BVH terecht en er wordt een actie I24 aan het incident gekoppeld. Bij het toepassen van sepotgrond 01 (ten onrechte als verdachte aangemerkt) verdwijnt automatisch de rol van verdachte in het bovenliggende incident.
Er moet dus een signaal worden afgegeven naar de systemen met deze biometrische gegevens, maar hier is momenteel geen sprake van.

4.2.6.2 Vanuit het OM wordt een afloopbericht naar de politie gestuurd. Vervolgens dient handmatig een I24 te worden opgemaakt.11
Er moet dus een signaal worden afgegeven naar de systemen met deze biometrische gegevens, maar hier is momenteel geen sprake van.

4.2.8 Zie BIVV, artikel 6. De termijnen zijn 20 of 30 jaar (afhankelijk van strafbaar feit). Ook hier moet er bij het aflopen van een bewaartermijn een signaal worden afgegeven naar alle systemen die gegevens bewaren. Momenteel nog geen sprake van gezien BVH er sinds 2008 is en de minimale bewaartermijn 20 jaar is, maar er is bij ons niet bekend dat hier iets voor afgesproken is.

Conclusie en advies
FCM bevat foto's vanaf 1994. Deze foto's zijn geregistreerd in HKS tot circa 2016 en vanaf dat moment in BVH.
De foto's mag je minimaal 20 jaar bewaren, tenzij er sepots of afloopberichten worden ontvangen. Ook bij overlijden is er een uitzondering, dan moeten de gegevens na 12 of 20 jaar worden verwijderd. De verantwoordelijkheid voor het doorgeven ligt bij het OM. Ons kan als ontvanger en gebruiker van de foto's niets worden aangerekend. We zouden hooguit kunnen onderzoeken of we de sepotberichten via een I24 kunnen achterhalen en verwijderingen doorvoeren.

5.2.1

Graag je feed back.

Artikel 6

- 4

- 1De gegevens, bedoeld in artikel 2, van verdachten en veroordeelden wegens misdrijven worden vernietigd:
    - **a.**twintig jaar nadat een einduitspraak als bedoeld in de artikelen 351 en 352, tweede lid, van het Wetboek van Strafvordering is gedaan in verband met een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van minder dan zes jaar is gesteld, en in het kader van het misdrijf de gegevens zijn verwerkt of nadat een strafbeschikking wegens het misdrijf volledig ten uitvoer is gelegd, dan wel twaalf jaar na het overlijden van betrokkene,
    - **b.**dertig jaar nadat een einduitspraak als bedoeld in de artikelen 351 en 352, tweede lid, van het Wetboek van Strafvordering is gedaan in verband met een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van zes jaar of meer is gesteld, en in het kader van het misdrijf de gegevens zijn verwerkt of nadat een strafbeschikking wegens het misdrijf volledig ten uitvoer is gelegd, dan wel twintig jaar na het overlijden van betrokkene, of

Met vriendelijke groet,

5.1.2.e
Operationeel Specialist

Politie | Landelijke Eenheid | DSO|LFSC|Centrum voor Biometrie
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e
Werkdagen ma – do van 7-14.30 uur
vr van 7-11 uur

Van: 5.1.2.e)
Verzonden: maandag 22 maart 2021 17:09
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: RE: regels schonen BVH BVI

Beste allen.

5.1.2.e en ik hebben alweer lange tijd geleden de nodige energie gestopt in het achterhalen van de “hoe zit het nu”. Aanleiding van dit alles was de schoning die niet of onvolledig werd uitgevoerd en het feit dat we zo’n 100.000 foto’s in de DB van FCM hebben zitten die niet herleidbaar zijn naar een persoon (BVI). We hebben gekeken naar wetgeving, besluiten, protocollen etc. Dit alles hebben wij samengevat in een document “Verdachten Fotografie “proces tweeluik”. In het hoofdstuk 4.2 staat dit beschreven. We hebben in die periode (ergens in 2019) diverse mensen geïnterviewd. We hebben onder andere gesproken met 5.1.2.e , 5.1.2.e , een collega van BVI (weet echt niet meer wie), collega’s van Team TOP. 5.2.1

5.2.1 [redacted] . 5.2.1 [redacted]

5.1.2.e [redacted]
Senior Functioneel Beheerder Team Biometrie

06 – 5.1.2.e [redacted]
Werkdagen: ma, di, wo, do

Politie I Politiedienstencentrum I Dienst IM I Afdeling Functioneel Beheer
Boschdijktunnel 10, 5611 AG Eindhoven

Meer informatie? Kijk op:

Gebruikers Dashboard Havank of

Gebruikers Dashboard FCM & DPS/Photomatic

Van: 5.1.2.e [redacted]
Verzonden: maandag 22 maart 2021 15:09
Aan: 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>; 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>
CC: 5.1.2.e [redacted] 5.1.2.e [redacted] @politie.nl>
Onderwerp: RE: regels schonen BVH BVI

Goedmiddag 5.1.2.e [redacted]

Voor zover mijn informatie strekt is dit er niet, althans dat begreep ik van 5.1.2.e [redacted]
Daarom heb ik deze vraag neergelegd bij 5.1.2.e [redacted] .
Zijn reactie moet ik nog ontvangen want uiteraard moet dit duidelijk zijn en moeten we niet uitgaan van aannamen.
Zodra ik wat weet laat ik het weten.

Met vriendelijke groeten,
With kind regards,
Mit freundliche Grüße,

5.1.2.e [redacted]

Politie | IV-organisatie | Dienst Informatiemanagement | IV-Expert

M 06-5.1.2.e [redacted]
E 5.1.2.e [redacted] @politie.nl
Werkdagen: maandag t/m donderdag

druk deze e-mail alsjeblieft niet af als het niet nodig is

Van: 5.1.2.e
Verzonden: maandag 22 maart 2021 14:55
Aan: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: regels schonen BVH BVI

Hi 5.1.2.e
Ik had je gevraagd na te gaan hoe er nu wordt geschoond in BVH. 5.1.2.e gaf aan aandacht te gaan vragen voor het aan de voorkant schonen van foto's. Ik merk dat er nog steeds vragen leven over regels mbt schonen BVH en BVI. Als hier over geen duidelijke documentatie beschikbaar is, lijkt het mij zinvol om dit met deskundigen BVH-BVI hierover van gedachten te wisselen met mijn analisten. We gaan nu uit van aannames en dat kan tot verkeerde conclusies leiden. Concreet; weet jij of er info bestaat over deze regels en waar deze is te vinden, wie ik kan uitnodigen om hierover van gedachten te wisselen. Vanuit je recente onderzoek verwacht ik dat je de vraag wel kunt beantwoorden ☺

Met vriendelijke groet,

5.1.2.e
Operationeel Specialist

Politie | Landelijke Eenheid | DSO|LFSC|Centrum voor Biometrie
Europaweg 45, 2711 EM, Zoetermeer
Postbus 100, 3970 AC Driebergen
M 06 5.1.2.e
Werkdagen ma – do van 7-14.30 uur
vr van 7-11 uur

Van: 5.1.2.e
Aan: 5.1.2.e
Cc: 5.1.2.e ; 5.1.2.e ; 5.1.2.e
Onderwerp: GEB Havank 4 / Catch 2
Datum: vrijdag 29 april 2022 09:18:13
Bijlagen: GEB WPG Biometrievoorziening 1.0.docx

Hallo 5.1.2.e

Ik krijg je telefonisch nog niet te pakken dus alvast maar per mail.

Ruim anderhalf jaar geleden hebben we in Den Haag afspraken gemaakt over het logisch gescheiden opslaan van vreemdelingen foto's in de nieuwe Biometrievoorziening (Havank 4 en Catch 2). Toen is ook afgesproken dat wij onze politie Gegevens Bescherming Effectbeoordeling (GEB) voor de Biometrievoorziening ter review bij jullie zouden aanbieden. Inmiddels hebben we een voor de politie versie 1.0.

Kun jij ervoor zorg dragen dat deze GEB op korte termijn bij DGM wordt gereviewd op de voor jullie relevante punten?

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Politie | Politiedienstencentrum | Sector PPI

Zeisterweg 1, 3984 NH Odijk
Postbus 238, 3970 AE Driebergen
M 06 5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 26 april 2022 16:39
Aan: Riemen, John (J.A.J.M.) 5.1.2.i @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>
CC: 5.1.2.e 5.1.2.e @politie.nl>; 5.1.2.e
5.1.2.e @politie.nl>; 5.1.2.e 5.1.2.e @politie.nl>;
5.1.2.e 5.1.2.e @politie.nl>
Onderwerp: GEB Havank 4 / Catch 2

Beste John en 5.1.2.e

Hierbij de uiteindelijke versie van de GEB voor HAVANK 4 en CATCH 2. De versie met opmerkingen geeft nog de wijzigingen aan en antwoorden op opmerkingen in de vorige versie.

Enige waar mogelijk nog een aanpassing voor nodig is, is de rol van verwerkingsverantwoordelijke en vaststeller document. Nu staat deze op naam van John als beheerder Havank maar dit zou ook de hoofdportefeuillehouder Opsporing kunnen zijn (5.1.2.e).

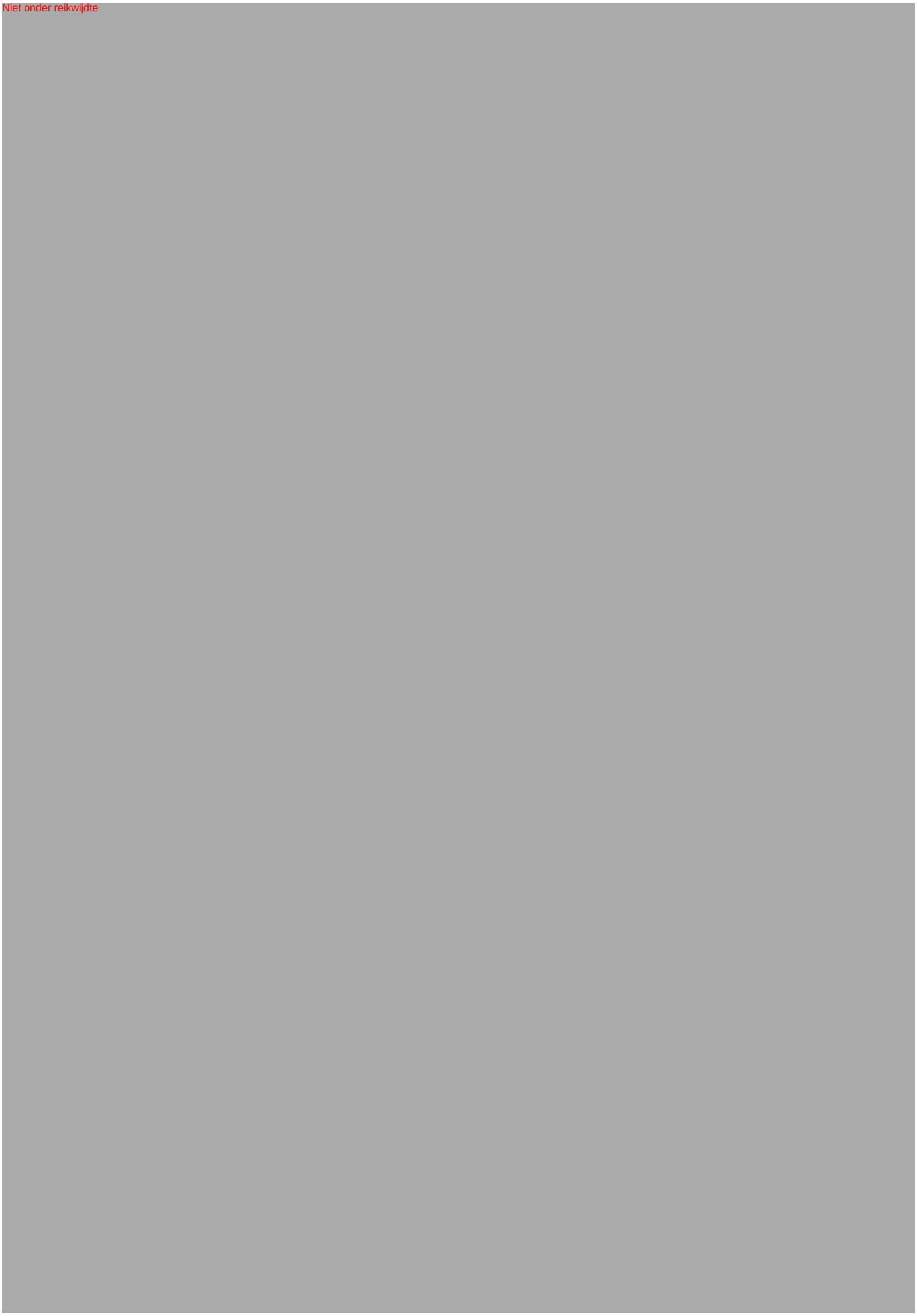
Met vriendelijke groet,

5.1.2.e
Adviseur informatiebeveiliging /risicomanagement

Politie | Politie Dienstencentrum |Sector Informatiebeveiliging i.o.
Ringbaan West 232, 5038 KE Tilburg
Postbus 8050, 5004 GB Tilburg

M +31 (0)6 5.1.2.e
E 5.1.2.i @politie.nl (loket informatiebeveiliging risicomanagement)
I http://intranet.politie.local/categorie/ondersteuning/onderwerpen/i/informatiebeveiliging/overzicht (intranetpagina)

Werkdagen: maandag, dinsdag, woensdag, donderdag tot 15 uur, vrijdagochtend


Niet onder reikwijdte