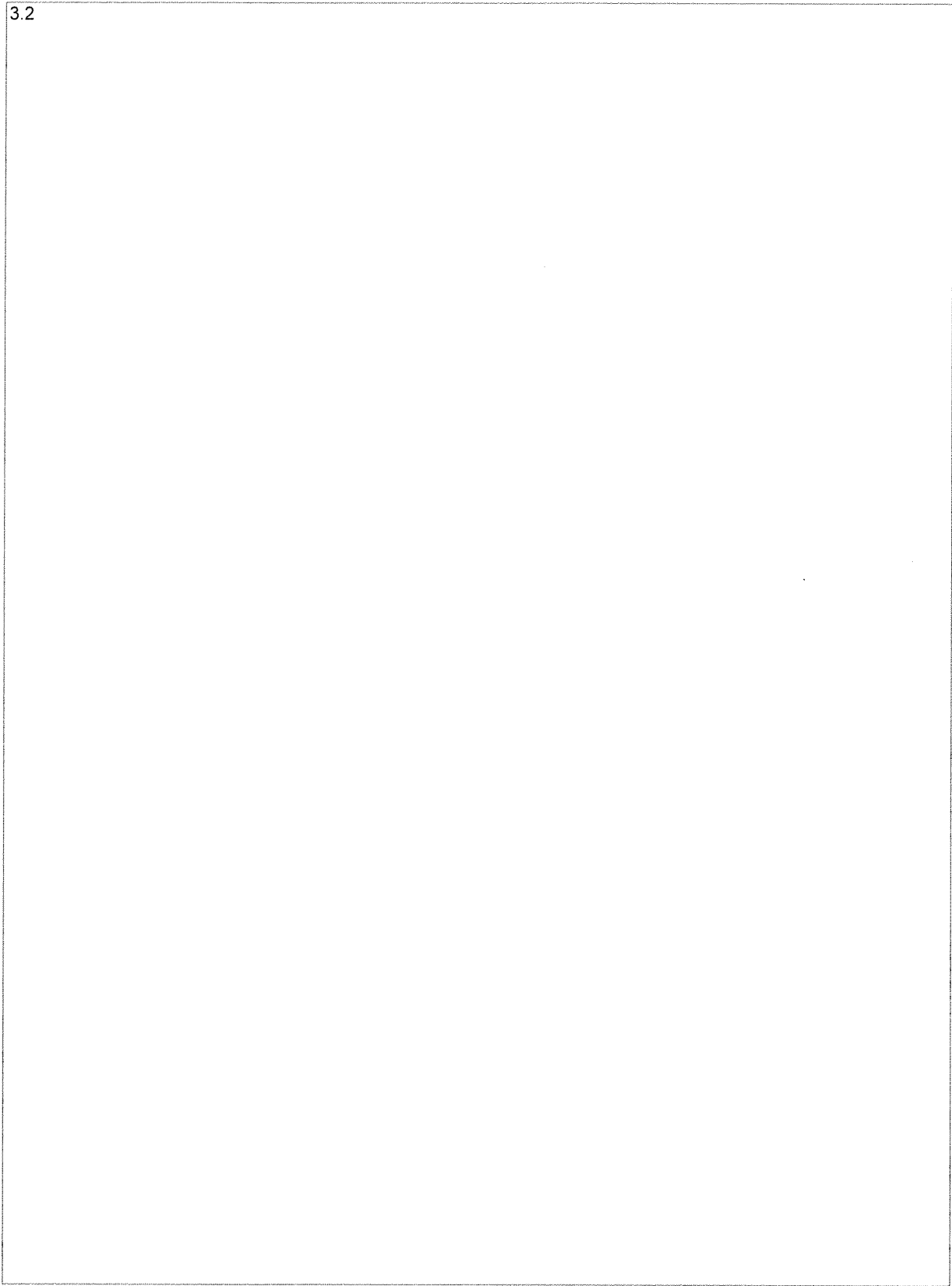


3.2

- 3. WPG userstories .....5
- 4. Blueview en Hansken userstories (input Politie & FIOD) .....6



3.2





### 3. WPG userstories

**Als** Compliancy officer,

**Wil ik** dat permissies in Hansken aan rollen van de politie en FIOD (buiten Hansken) gekoppeld kunnen worden **Zodat** autorisaties ingericht worden op basis van rollen (RBAC)

**Als** Compliancy officer,

**Wil ik** dat aan een bepaald gegevenstype door Hansken automatisch een voorgedefinieerd gegevensniveau wordt toegekend

**Zodat** er naast de permissies op basis van dit gegevensniveau kan worden geautoriseerd

**Als** Compliancy officer

**Wil ik** dat achteraf handmatig een toegekend gegevensniveau gewijzigd kan worden,

**Zodat** correcties kunnen worden toegepast in geval van een verkeerde toewijzing

**Als** Compliancy officer,

**Wil ik** dat Summ-IT het onderzoekskenmerk van een opsporingsonderzoek aan Hansken doorgeeft,

**Zodat** duidelijk is dat het in beide systemen over hetzelfde opsporingsonderzoek gaat

**Als** Compliancy officer,

**Wil ik** dat Summ-IT de status van een opsporingsonderzoek aan Hansken doorgeeft,

**Zodat** in Hansken ook de actuele status van een opsporingsonderzoek geregistreerd staat en gegevens verwijderd kunnen worden wanneer niet meer nodig

**Als** Compliancy officer,

**Wil ik** dat Hansken rekening houdt met de onderzoeks- en Wpg status (via Summ-IT) en op basis daarvan gegevens verwijderd/ niet meer toont aan gebruikers zodra een onderzoek in Wpg status 'Bewaren' is gekomen

**Zodat** politiegegevens niet langer in Hansken blijven staan dan toegestaan

***Let op:** Verwijderen betekent dat gegevens niet meer toegankelijk zijn voor reguliere gebruikers.*

*Vernietigen, betekent dat gegevens echt definitief worden weggehaald*

**Als** Compliancy officer,

**Wil ik** dat verwijderde gegevens indien nodig opnieuw beschikbaar kunnen worden gemaakt door de poortwachter,

**Zodat** in bijzondere gevallen de gegevens opnieuw kunnen worden doorzocht

**Als** Compliancy officer,

**Wil ik** dat verwijderde gegevens na 5 jaar bewaartermijn definitief vernietigd worden door te kijken naar de Wpg status van het gekoppelde Summ-IT onderzoek

**Zodat** politiegegevens niet langer bewaard blijven dan toegestaan.

**Als** eindgebruiker,

**Wil ik** over (toegankelijke) onderzoeken heen kunnen zoeken

**Zodat** ik (rekening houdend met mijn rol) de gegevens mag vinden waartoe ik ben geautoriseerd.

**Als** eindgebruiker,

**Wil ik** van onderzoeken waar ik geen toegang toe heb, hit/no hit resultaten zien indien er in deze onderzoeken iets relevants voorkomt op basis van mijn zoekvraag

**Zodat** ik - na contact met desbetreffende onderzoeksleider- de informatie uit andere onderzoeken kan gebruiken

**Als** eindgebruiker,

**Wil ik** van onderzoeken waar ik geen toegang toe heb, hit/no hit resultaten zien indien er in deze onderzoeken iets relevants voorkomt op basis van mijn zoekvraag

**Zodat** ik - na contact met desbetreffende onderzoeksleider- de informatie uit andere onderzoeken kan gebruiken

**Als** Compliance Officer

**Wil ik** dat alle logs worden opgeslagen in een separate omgeving,

**Zodat** analyses gedaan kunnen worden op bewaarde logs

**Als** Compliance Officer

**Wil ik** dat alle logging 2 jaar lang bewaard blijft,

**Zodat** gebruikershandelingen achteraf van een periode van 2 jaar kunnen worden nagetrokken.

**Als** Compliance Officer

**Wil ik** dat alle logging beveiligd is tegen mutaties,

**Zodat** bewezen kan worden dat de logging/ audittrail integer is

#### **4. Blueview en Hansken userstories (input Politie & FIOD)**

##### **Input Politie**

**A: Zoeken naar telefoonnummer in digitaal beslag**

**Situatie / achtergrond:**

Een mobiele telefoonnummer geeft bij CIOT-bevraging als resultaat: **no-hit / betreft prepaid-nummer**, zodat er geen NAW-gegevens bekend zijn van dit telefoonnummer.

**User Story 1 – telefoonnummer uit digitaal beslag aanwezig in lopende onderzoek(en):**

**Als** BVI gebruiker, zijnde een (tactisch) rechercheur,

**wil ik** in BVI kunnen zoeken naar een telefoonnummer waarbij, als ik dat aanvink/selecteer, ook gezocht wordt in alle digitaal beslag van de huidige lopende opsporingsonderzoek(en) waar ik deel van uit maak.

**Zodat** als het betreffende telefoonnummer ergens aanwezig is (bijvoorbeeld in een contactpersonen lijst / adresboek van een mobiele telefoon) in digitaal beslag er toch een naam / aanwijzing / indicatie gevonden kan worden van wie het telefoonnummer is.

**User Story 2 – telefoonnummer uit digitaal beslag aanwezig in lopende onderzoek(en) elders:**

**Als** BVI gebruiker, zijnde een (tactisch) rechercheur,

**wil ik** in BVI kunnen zoeken naar een telefoonnummer waarbij, als ik dat aanvink/selecteer, ook gezocht wordt in alle digitaal beslag van de huidige lopende opsporingsonderzoeken en hiervan een **hit-indicatie** krijgen indien dit telefoonnummer in een opsporingsonderzoek zit waarvoor ik niet geautoriseerd ben.

**Zodat** ik bij het betreffende onderzoeksteam navraag kan doen naar het betreffende telefoonnummer zodat mogelijk toch een naam / aanwijzing / indicatie gevonden kan worden van wie het telefoonnummer is.

**User Story 3 – telefoonnummer uit digitaal beslag aanwezig in onderzoeken van de afgelopen vijf jaar:**

**Als** BVI gebruiker, zijnde een infodesk rechercheur, analist of TCI medewerker,  
**wil ik** in BVI kunnen zoeken naar een telefoonnummer waarbij, als ik dat aanvink/selecteer, ook gezocht wordt in alle digitaal beslag van alle opsporingsonderzoeken.  
**Zodat** als het betreffende telefoonnummer ergens aanwezig is (bijvoorbeeld in een contactpersonen lijst / adresboek van een mobiele telefoon) in digitaal beslag er toch een naam / aanwijzing / indicatie gevonden kan worden van wie het telefoonnummer is/was.

### **B: Zoeken & signalering op unieke entiteiten in digitaal beslag**

#### **Situatie / achtergrond:**

Scenario uit december 2013: Vijf grote weborderbedrijven hebben al geruime tijd gedurende korte perioden serieuze DDOS-aanvallen die niet verklaard en niet afgeweerd kunnen worden. Vervolgens ontvangen deze vijf bedrijven elk afzonderlijk een mailtje waarin wordt bedreigd met een DDOS van een lange periode als niet binnen 10 dagen een aanzienlijk groot aantal Bitcoins wordt overgemaakt naar een bepaalde Bitcoin Wallets.

Onderzoek heeft beperkte aanknopingspunten:

- Bitcoin Wallets leiden tot een dood spoor
- Mailtjes zijn afkomstig vanaf geanonimiseerde maildiensten en leiden ook tot een dood spoor

In de aangifte / verkennend onderzoek worden de aanknopingspunten afgewogen en onderzoek gaat op de plank en komt er nooit meer van de plank.

#### **User Story 1 – Bitcoin Wallet uit digitaal beslag aanwezig in lopende onderzoek(en):**

**Als** BVI gebruiker, zijnde een infodesk rechercheur,  
**wil ik** in BVI kunnen zoeken naar een Bitcoin Wallet aanwezig in het digitaal beslag van alle lopende opsporingsonderzoeken (voor onderzoeken waar ik deel van uitmaak kan ik meteen de bijbehorende gegevens zien, voor onderzoeken waar ik geen deel van uit maak krijg ik een hit-indicatie.  
**Zodat** als het betreffende Bitcoin Wallet al ergens aanwezig is, er een heldere onderzoeksrichting gevonden kan worden.

#### **User Story 2 – Bitcoin Wallet komt voor in een nieuw (later toegevoegd) digitaal beslag:**

**Als** BVI gebruiker, zijnde een infodesk rechercheur,  
**wil ik** in BVI op unieke entiteiten (zoals bijvoorbeeld een Bitcoin Wallet) toekomstige signalering / abonnement kunnen plaatsen in toekomstig / nieuw toegevoegd digitaal beslag.  
**Zodat** als in een nieuw onderzoek in een nieuw toegevoegd digitaal beslag het betreffende Bitcoin Wallet ergens voor blijkt te komen er een signaal gegeven wordt dat het unieke Bitcoin Wallet dat ooit gezocht werd nu aangetroffen is in digitaal beslag.

Vergelijkbare scenario's zijn er eventueel ook te bedenken voor andere type entiteiten met unieke waarden, zoals mogelijk misschien:

- Emailadressen
- Telefoonnummers(?)
- IP-adressen(?)

### **INPUT FIOD**

#### **Als analist**

wil ik een bevraging op entiteiten in Blueview ook op Hansken plaats laten vinden zodat ik op die manier mijn bestaande informatie kan verrijken.

#### **Als analist**

wil ik een bevraging op entiteiten in Blueview ook op Hansken plaats laten vinden zodat ik weet of onderdelen mijn onderzoek ook voorkomen in andere lopende (politie) onderzoeken.

#### **Als analist**

wil ik een bevraging op entiteiten in Blueview ook op Hansken plaats laten vinden

zodat ik verbanden kan leggen met andere lopende onderzoeken.

Als onderzoeker

wil ik entiteiten die ik in Hansken aantref bevragen in blueview  
zo dat ik een zo compleet mogelijk beeld kan krijgen van mijn onderzoek.

Als onderzoeker

wil ik meta data uit blueview kunnen bevragen in de content van Hansken  
zodat ik een beter beeld van mijn onderzoek kan krijgen en nieuwe verbanden kan leggen.

Als onderzoeker

wil ik Blueview kunnen bevragen met entiteiten uit de content van Hansken in een onderzoek  
zodat ik een beter beeld van mijn onderzoek kan krijgen en nieuwe verbanden kan leggen.

**VOORDELEN:**

Je maakt de kans op fouten kleiner

Bevragingen worden objectiever

Doorlooptijd onderzoek wordt kleiner

Je krijgt een beter beeld bij criminele samenwerkingsverbanden