ONDERZOEK NAAR DE NATIONALE IMPLEMENTATIE VAN DE EUROPESE RICHTLIJN DATARETENTIE

ONDERZOEK NAAR DE NATIONALE IMPLEMENTATIE VAN DE EUROPESE RICHTLIJN DATARETENTIE

Ruud Boot, Johan van den Bosch (VKA)
Edwin Vervaet, Koos Varkevisser (Lucent Technologies)

9 oktober 2006

status Definitief
versie 3.0
interne toets Rene van den Assem

SAMENVATTING

In opdracht van de directeur Opsporing van het ministerie van Justitie heeft VKA tezamen met Lucent Technologies de nationale implementatie van de Europese richtlijn Dataretentie onderzocht. Deze richtlijn is na instemming door het Europees Parlement op 21 februari jongstleden aangenomen door de JBZ-raad.

Doelstelling van het onderzoek is het verzamelen van informatie over de technische en organisatorische aanpassingen bij aanbieders en behoeftestellers die bij toepassing van verschillende implementatieopties van de bewaarplicht en de daarmee samenhangende bevraging noodzakelijk zijn, inclusief de daaraan verbonden kosten. Op grond van de resultaten van het onderzoek kan de opdrachtgever in overleg met de betrokken departementen de eventuele alternatieven naar voorkeur rangschikken. Deze rangschikking kan de overheid vervolgens betrekken bij de besluitvorming rondom de implementatie van de Richtlijn en de inrichting van een mechanisme van dataretentie.

Voor het onderzoek hebben acht implementatieopties centraal gestaan waarbij er drie variabelen zijn:

- De keuze voor gecorreleerde of ongecorreleerde opslag van de informatie
- De keuze van de locatie van de opslag, te weten centraal of bij de aanbieder
- De keuze van de toegang tot de informatie bij bevraging, te weten door de aanbieder of door de behoeftesteller

Tabel 0-1: acht implementatieopties

	Gecorreleerde gegevensopslag	**Ongecorreleerde gegevensopslag**
Locatie van de opslag van gegevens en toegang tot informatie	Decentrale opslag, beantwoording door de aanbieder	Decentrale opslag, beantwoording door de aanbieder
	Decentrale opslag, directe toegang door de behoeftesteller	Decentrale opslag, directe toegang door de behoeftesteller
	Centrale opslag, directe toegang door de behoeftesteller	Centrale opslag, directe toegang door de behoeftesteller
	Hybride opslag, directe toegang door de behoeftesteller	Hybride opslag, directe toegang door de behoeftesteller

In de gekozen aanpak is er naar gestreefd om naast de inhoudelijke vakkennis van de onderzoekers en eerder gepubliceerd materiaal gebruik te maken van de kennis en kunde die bij de belanghebbende partijen aanwezig is.

Op 12 juni is middels een startbijeenkomst met behoeftestellers en aanbieders op basis van een kort vooronderzoek overeenstemming bereikt over de eisen en criteria die door elk van de belanghebbenden aan de implementatie gesteld worden.

In een uitgebreid veldonderzoek bij vijftien aanbieders is er informatie verzameld over ondermeer organisatie en processen, kosten, techniek en beveiliging. Er is daarbij gebruik gemaakt van interviews en een schriftelijk te beantwoorden vragenlijst.

In nauw overleg met de begeleidingscommissie is een beoordelingsmodel samengesteld waarmee een objectieve vergelijking van de verschillende implementatieopties mogelijk is. Het beoordelingsmodel bestaat uit twee delen: een kwantitatief deel voor het in beeld brengen van alle kosten en een kwalitatief deel voor het in beeld brengen van de mate waarin de optie voldoet aan kwalitatieve criteria. Het kwantitatieve model onderbouwt in detail de kosten voor een modelaanbieder met 125.000 klanten die een representatieve mix van diensten afnemen (in totaal 500.000 accounts voor vaste en mobiele telefonie, internet toegang en email). Vervolgens wordt deze geëxtrapoleerd om de kosten voor de gehele Nederlandse situatie in beeld te brengen. De kwalitatieve criteria zijn gebaseerd op de onderzoeksvragen en de eisen en criteria van de belanghebbenden. De criteria zijn ingedeeld in vijf categorieën en onderling gewogen. De gehanteerde weging is in overleg met de begeleidingscommissie tot stand gekomen. Door van een dergelijk model gebruik te maken is het mogelijk om de onderzoeksvragen in samenhang te beantwoorden en de belangen van de diverse criteria te wegen. Het kwalitatieve model leidt tot een puntenscore per implementatieoptie.

De acht implementatieopties zijn uitgewerkt op bedrijfsarchitectuur, informatiearchitectuur en technische architectuur. Daarbij is gebruik gemaakt van ontwerpeisen gebaseerd op de startbijeenkomst en de onderzoeksvragen rekening houdend met de bestaande situatie. Deze inhoudelijke uitwerking vormt de basis waarop de kosten zijn bepaald en de scores in het kwalitatieve model zijn vastgesteld. In alle implementatieopties is er uitgegaan van geautomatiseerde bevraging van de gegevens, wat een wijziging is ten opzichte van de huidige werkwijze. Hiervoor is gekozen omdat enerzijds de richtlijn stringentere eisen stelt die wijziging van de werkwijze impliceert en anderzijds omdat de operators in het veldonderzoek unaniem aangaven dat volledige automatisering de preferente oplossing vormt. Slechts voor de allerkleinste operators wordt uitgegaan van handmatige procedures, deze kosten zijn niet in detail uitgewerkt.

Tijdens het veldonderzoek kwam de gevraagde informatie pas eind augustus, begin september beschikbaar. De aangeleverde informatie over de dataset, opslag (inclusief kosten) en bevraging geeft een tamelijk volledig beeld, de informatie over acquisitie in combinatie met de huidige techniek en kosten is beperkt. Op basis van de eigen kennis van de onderzoekers en de aangeleverde informatie is er desalniettemin een objectief en afgewogen beeld ontstaan van de acht implementatieopties op nationaal niveau. De resultaten zijn als volgt.

Tabel 0-2: scoreoverzicht van het kwalitatief model

Categorie	Decentrale opslag beantwoording door aanbieder	Decentrale opslag directe toegang	Centrale opslag directe toegang	Hybride opslag directe toegang
Organisatie en processen	12	*9*	18	18
Technologie	18	10,2	20,1	20,1
Business Case	7,5	*0*	2,5	2,5
Informatiebeveiliging	4	11	20	15
Implementatie termijn	10	*0*	*0*	*0*
Totaal	**51,5**	**30,2**	**60,6**	**55,6**

Het kwalitatieve model geeft aan dat de Centrale implementatieoptie het hoogst scoort met 61 punten. De optie Decentrale opslag met directe toegang scoort duidelijk als laagste op de meeste criteria. Het is voor een genuanceerd beeld van de verschillen tussen de implementatie optie belangrijk om te kijken naar de oorsprong van de verschillen. Deze zijn in de uitkomsten van het kwalitatieve model opgenomen.

De uitkomst van het kwantitatieve model afgerond op € 10.000 is als volgt:

Tabel 0-3: kostenoverzicht van het kwantitatieve model.

Implementatie optie		In € over vijf jaar
Decentrale opslag, beantwoording door aanbieder	Gecorreleerd	€ 154.800.000
	Ongecorreleerd	€ 157.810.000
Decentrale opslag, directe toegang	Gecorreleerd	€ 141.580.000
	Ongecorreleerd	€ 146.100.000
Centrale opslag, directe toegang	Gecorreleerd	€ 133.800.000
	Ongecorreleerd	€ 135.350.000
Hybride opslag, directe toegang	Gecorreleerd	€ 148.320.000
	Ongecorreleerd	€ 147.340.000

Het financiële verschil tussen de duurste en goedkoopste implementatieoptie is 24 miljoen euro. Voor de Nederlandse samenleving is de centrale optie met directe toegang door de behoeftestellers de meest voordelige.

Het is echter te ongenuanceerd om op basis van deze uitkomsten tot de conclusie te komen dat de centrale optie dus de beste implementatieoptie is. Er zijn veel onderliggende details die het verschil tussen de diverse implementatieopties bepalen. Dit zijn details die voor belanghebbenden verschillend uitpakken en die verschillend gewogen zullen worden. Er is door de onderzoekers in overleg met de begeleidingscommissie voor een zo objectief mogelijke benadering gekozen bij de

kwalitatieve beoordeling. Zoals inmiddels duidelijk is geworden kan er met de uitkomsten van de beoordeling in de hand wel degelijk van mening worden verschild.

De afweging welke implementatieoptie de voorkeur verdient zal door het departement van Justitie in overleg met de departementen Binnenlandse Zaken, Defensie en Economische Zaken gemaakt worden. Naast de inhoudelijke aspecten die dit onderzoek inzichtelijk heeft gemaakt zullen ook bestuurlijke en politieke overwegingen daarbij een rol spelen.

Nadat de keuze voor de implementatieoptie is gemaakt en het wetgevingstraject zijn verdere vervolg krijgt is het aan te bevelen om begin 2007 op basis van de ingeslagen richting een vervolgonderzoek uit te voeren. Er kan dan meer specifiek ingegaan worden op het technisch ontwerp, organisatorische uitvoering, de implementatie planning en bijvoorbeeld een mogelijke pilot.

Inhoudsopgave

1 Inleiding

De Nederlandse rijksoverheid zal als gevolg van de Europese Richtlijn Dataretentie invulling geven aan de bewaarplicht en de daarmee samenhangende bevraging van identificerende gegevens en verkeersgegevens in de telecommunicatiesector. De nationale implementatie van deze bewaarplicht zal 1 september 2007 een feit moeten zijn [1]. Hiervoor wordt zowel een wetgevings- als een uitvoeringstraject doorlopen.

Ten behoeve van de nationale besluitvorming over het uitvoeringstraject hebben de betrokken ministers[2] aangegeven behoefte te hebben aan meer informatie rondom de implementatie. In dat kader heeft de directeur Opsporingsbeleid van het ministerie van Justitie als voorzitter van de interdepartementale Beleidsgroep voor interceptie, decryptie en signaalanalyse aan VKA opdracht gegeven voor de uitvoering van een onderzoek naar de verschillende implementatieopties voor deze bewaarplicht. Dit rapport geeft de bevindingen van dit onderzoek weer.

1.1 Achtergrond

Mede naar aanleiding van de terroristische aanslagen in Madrid en Londen, heeft de Raad Justitie en Binnenlandse Zaken (JBZ-raad), waar de Europese ministers van deze beleidsterreinen bij elkaar komen, verzocht om voorstellen te onderzoeken voor de bewaring van telecommunicatie-verkeersgegevens door aanbieders van elektronische communicatiediensten. De Europese Commissie stelt dat het bewaren van verkeersgegevens noodzakelijk is teneinde terroristische activiteiten effectief op te sporen, te onderzoeken en te bestrijden. Eind 2005 heeft het Europese Parlement, na enkele amendementen, ingestemd met een Europese bewaarplicht van verkeersgegevens. De JBZ-raad heeft vervolgens tijdens haar vergadering op 20 en 21 februari 2006 ingestemd met de Richtlijn Dataretentie (hierna: de Richtlijn). Nederland zal vervolgens de vereisten uit deze de Richtlijn in de nationale regelgeving moeten implementeren. Hiertoe zal een wetgevings- én een uitvoeringstraject bewandeld dienen te worden.

Dit onderzoek richt zich op het technische en organisatorische uitvoeringstraject. Doel van het uitvoeringstraject is om bij de inwerkingtreding van nationale regelgeving, waarmee de Richtlijn inzake dataretentie wordt geïmplementeerd, een werkend mechanisme voor opslag en bevraging van historische verkeersgegevens gereed te hebben, waarbij voldaan wordt aan alle toepasselijke regelgeving. De gekozen implementatieoptie moet echter niet alleen een werkende oplossing bieden die aan de regelgeving voldoet, maar ook een model zijn dat aan de industrie een zo efficiënt mogelijke oplossing biedt, dat wil zeggen de industrie zo min mogelijk (extra) belast.

1.2 Onderzoeksdoelstelling

Doelstelling van het onderzoek is het verzamelen van informatie over de technische en organisatorische aanpassingen bij aanbieders en behoeftestellers die bij toepassing van de verschillende modellen van implementatie (de implementatieopties) van de bewaarplicht

[1] Voor de internetgegevens bestaat de mogelijkheid de operationele invoering van de wetgeving voor een periode van 18 maanden uit te stellen.

[2] Justitie, Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Defensie

noodzakelijk zijn, gegeven de huidige set van verplichtingen en voorzieningen[3], alsmede de daaraan verbonden kosten. De juistheid van de gepresenteerde informatie moet door alle partijen worden gedeeld.

Op grond van de resultaten van het onderzoek kan de opdrachtgever in overleg met de betrokken departementen de eventuele alternatieven naar voorkeur rangschikken. Deze rangschikking kan de overheid vervolgens betrekken bij de besluitvorming rondom de implementatie van de Richtlijn en de inrichting van een mechanisme van dataretentie.

1.3 Onderzoeksvragen

In de aanvraag is de doelstelling van het onderzoek verder uitgewerkt middels een aantal vragen:

1. Welke eisen en criteria stellen de betrokken partijen (aanbieders, behoeftestellers) aan de opslag en bevraging van verkeersgegevens?
2. Hoe is de huidige werkwijze rond de opslag en bevraging van verkeersgegevens en voldoet die aan de genoemde eisen en criteria? Op welke punten schiet de bestaande werkwijze tekort en hoe kan dit worden ondervangen?
3. Wat is de impact op de aanbieders, respectievelijk de overheid, bij 4 verschillende modellen van opslag en bevraging van gegevens, waarbij wordt gekeken naar:
   - welke voorzieningen zijn reeds aanwezig;
   - welke uitbreiding op deze voorzieningen is nodig;
   - welke nieuwe voorzieningen moeten worden ontwikkeld.
4. Wat zijn de kosten die bij elk van deze 4 modellen horen?
5. Hoe (met welk(e) van de 4 beschreven modellen) kan het best worden gewaarborgd dat de gegevens:
   - niet toegankelijk zijn voor andere doeleinden dan die genoemd in de Richtlijn dataretentie;
   - uitsluitend worden geraadpleegd door personen die daarvoor vanwege hun wettelijke taakuitvoering in aanmerking komen;
   - na afloop van de bewaartermijn worden verwijderd of vernietigd, en;
   - beschikbaar zijn voor het leveren van statistieken aan de Commissie.
6. Hoe (met welk model) kan het beste worden gewaarborgd dat de in de richtlijn genoemde beginselen van gegevensbeveiliging in acht worden genomen?
7. Wat is de haalbaarheid in technische, organisatorische en juridische zin van de verschillende mogelijkheden?

De uitwerking van de onderzoeksvragen is als volgt geïnterpreteerd.

De uitwerking van de eerste twee onderzoeksvragen leidt tot een set wensen en criteria waaraan de toekomstige oplossing moet voldoen. Ook de onderzoeksvragen 5 tot en met 7 vertegenwoordigen criteria waaraan moet worden voldaan. Een antwoord op deze vragen voor iedere implementatieoptie is het meest zinvol wanneer het inzicht geeft in de onderlinge samenhang en rekening houdt met het verschil in gewicht (belang) van de criteria voor de belanghebbenden.

[3] Voortvloeiend uit de Telecommunicatiewet

De kosten die bij elke implementatieoptie horen zullen uniek zijn voor elke belanghebbende in de acquisitie, opslag en bevraging van de gegevens. Voor een onderbouwing van de beleidsbeslissing is inzicht van deze kosten op nationaal niveau benodigd in combinatie met inzicht in de effecten van de kosten op de marktpartijen.

De uitwerking van bovenstaande interpretatie heeft geleid tot een beoordelingsmodel dat in hoofdstuk 2 aan de orde komt en een set van ontwerpeisen dat in hoofdstuk 3 aan de orde komt.

De onderzoeksvragen verwijzen naar vier modellen of implementatieopties. Het betreft hier de keuze voor gecorreleerde en ongecorreleerde opslag en de keuze voor decentrale opslag met beantwoording door de aanbieders en centrale opslag met directe toegang door de behoeftestellers. Bij nadere uitwerking zijn er acht implementatieopties gedefinieerd die relevant zijn voor dit onderzoek. Deze worden kort toegelicht in hoofdstuk 2 en uitgebreid uitgewerkt in hoofdstuk 3 en 4.

1.4 Projectorganisatie

VKA is opdrachtnemer. Voor de uitvoering van het onderzoek werkt VKA samen met Lucent Technologies, een internationaal opererende leverancier van telecommunicatieapparatuur, managementsystemen en (multi-vendor) systeemintegratie.

Opdrachtgever is de Directeur Opsporingsbeleid van het ministerie van Justitie tevens voorzitter van de interdepartementale Beleidsgroep voor interceptie, decryptie en signaalanalyse.

De begeleidingscommissie dataretentie, bestaande uit vertegenwoordigers van de overheid en de telecommunicatieaanbieders, begeleidt het onderzoek en beoordeelt de uitkomsten van het onderzoek. Bijlage A bevat een overzicht van de organisaties die vertegenwoordigt zijn in de begeleidingscommissie.

Projectmanager aan de zijde van opdrachtnemer is Ruud Boot. Hij is hierbij ondersteund vanuit VKA door Johan van den Bosch en vanuit Lucent Technologies door Edwin Vervaet en Koos Varkevisser. Als inhoudelijk expert en tevens kwaliteitsbewaker treedt vanuit VKA principal consultant René van den Assem op.

1.5 Onderzoeksmethode

In de gekozen aanpak is er naar gestreefd om naast inhoudelijk vakkennis van de onderzoekers en eerder gepubliceerd materiaal intensief gebruik te maken van de kennis en kunde die bij de belanghebbende partijen aanwezig is. Er is om die reden uitgebreid aandacht besteed aan het raadplegen van zowel aanbieders van telecommunicatiediensten als behoeftestellers.

Verder is er veel aandacht besteed aan het objectiveren van de uitkomst gegeven de vele meningen die er op dit onderwerp leven. Het beoordelingsmodel aan de hand waarvan de verschillende implementatieopties kwalitatief en kwantitatief in beeld worden gebracht is in nauw overleg met de begeleidingscommissie samengesteld.

Het onderzoek is verdeeld in drie fases. Deze zijn gedurende de volgende periodes uitgevoerd:

Fase 1, voorbereiding en startbijeenkomst: 8 mei t/m 16 juni.
Fase 2, veldonderzoek, model ontwikkeling, oplevering conceptrapport: 19 juni t/m 22 september.
Fase 3, oplevering eindpresentatie en definitief rapport: 25 september – 29 september.

Fase 1 kent de volgende activiteiten:

- Literatuuronderzoek.
- Beknopt veldonderzoek ter voorbereiding van de startbijeenkomst. Dit betreft 3 interviews met behoeftestellers en departementen en vijf interviews met aanbieders.
- Startbijeenkomst met de begeleidingscommissie waarin eisen en criteria van de betrokken partijen worden vastgelegd en inzicht in de huidige werkwijze wordt verkregen.

Fase 2 kent de volgende activiteiten:

- Ontwikkeling van het kwantitatieve en kwalitatieve beoordelingsmodel aan de hand waarvan de verschillende implementatieopties in beeld worden gebracht. Als input voor de modelontwikkeling hebben ondermeer de onderzoeksvragen, de resultaten van de startbijeenkomst en de tussentijdse aanbevelingen van de begeleidingscommissie gediend.
- Analyse van de diverse mogelijkheden voor de inrichting van de nationale implementatie, er is daarbij ook gekeken naar mogelijke aanvullingen op de zes reeds geïdentificeerde mogelijkheden.
- Uitgebreid veldonderzoek bij vijftien operators (zie bijlage B voor de geraadpleegde aanbieders). De omvang van de operators varieert van klein tot groot, de marktsegmenten van de operators zijn vaste telefonie (KPN en diverse concurrenten waaronder kabelbedrijven), mobiele telefonie, internet providers en "overige" waaronder virtuele netwerk operators. Voor het veldonderzoek is gebruik gemaakt van interviews en een schriftelijk te beantwoorden vragenlijst.
- Inhoudelijke afstemmingen met de werkgroep wetgeving
- Verwerking tot concept rapportage en bespreking met de begeleidingscommissie.

Fase 3 kent de volgende activiteiten:

- Verwerking van de op en aanmerkingen van de begeleidingscommissie
- Presentatie van het eindrapport aan de opdrachtgever

In hoofdstuk 5 zal bij de algemene bevindingen ingegaan worden op opgedane ervaringen bij het uitvoeren van het onderzoek.

1.6 Afbakening

De nadruk in deze fase van implementatie ligt op het inzichtelijk maken van de kosten en de mate van vervulling van de kwalitatieve criteria voor elk van de implementatieopties. Deze informatie verschaft het departement (de departementen) de mogelijkheid om onderbouwd een keuze te maken voor één van de implementatieopties en dit te verwerken in het concept wetsvoorstel. Het is binnen deze context van belang om ook helder aan te geven waar de grenzen van dit onderzoek liggen. Het betreft daarbij zaken die voortvloeien uit de opdrachtformulering of die naderhand met de opdrachtgever en de begeleidingscommissie aan de orde zijn geweest.

Het rapport bevat geen advies welk van de opties te prefereren is. Het verschaft een zo objectief mogelijk beeld van kosten en kwalitatieve score van elk van de opties. In de besluitvorming door het departement zullen daarnaast bestuurlijke en politieke overwegingen een rol spelen. Dit advies is geen poging om partijen op voorhand op één lijn te krijgen.

De mate van detail bij uitvoeren van dit onderzoek is gericht op de keuze tussen de verschillende implementatieopties. Onderliggende details zoals exacte systeem- en softwarekeuze en leverancierskeuzes zijn niet gemaakt.

Bij het uitwerken van de kosten is er gekeken naar de activiteit die de kosten veroorzaakt en de partij die deze kosten maakt. Er is in het kader van dit onderzoek geen uitspraak gedaan of de partij die de kosten maakt ook degene is die deze kosten betaalt. Er is een aparte werkgroep die zich buigt over het vraagstuk van de vergoedingenstructuur.

Bij centrale en hybride opslag is er sprake van een intermediaire derde die gegevens opslaat en ter beschikking stelt voor directe toegang door de behoeftestellers. Deze intermediaire derde kan zowel een private partij zijn als een overheids(gebonden)instelling. De richtlijn Dataretentie legt de lidstaat op om uitvoering te geven aan de richtlijn, niet aan de sector. De keuze voor een private of een publieke organisatie als intermediaire derde is vrij. De afweging en keuze voor een private of publieke organisatie maakt geen deel uit van dit onderzoek.

De handhaafbaarheid van elke implementatieoptie is niet onderzocht. Wel wordt er een uitspraak gedaan over de te verwachten kwaliteit van het audit trail en de inspanning die benodigd is voor de audit.

De reikwijdte van de Richtlijn Dataretentie is beperkt tot de EU. Sommige diensten worden geleverd door een keten van aanbieders waarvan er bijvoorbeeld één buiten het werkingsgebied van de Richtlijn opereert. Zo kan een aanbieder van een emaildienst gebruik maken van een organisatie die in de Verenigde Staten van Amerika gevestigd is en daar ook de betreffende mailserver beheert. In de praktijk betekent het bijvoorbeeld dat aanbieders van veel gebruikte diensten zoals hotmail, Gmail en Skype mogelijk buiten het werkingsgebied van de richtlijn vallen. Dergelijke ketenvorming en de gevolgen hiervan voor de effectiviteit van de richtlijn zijn niet onderzocht..

De aanbieders hebben aangegeven dat bij bepaalde implementatieopties bij hen de behoefte ontstaat om zelf de informatie langer dan een jaar op te slaan. Deze behoeft is terug te voeren op hun plichten ten aanzien van privacy bescherming. Er is een risico dat er door fouten in (de verwerking van) informatie strafzaken gevoerd gaan worden waarvoor zij ter verantwoording worden geroepen. Er bestaat verschil van inzicht of dit juridisch noodzakelijk en toegestaan is. Ook over het hanteren van een vrijwaring als alternatieve oplossing lopen de meningen uiteen. Deze extra opslag of vrijwaring is niet meegenomen in de verdere uitwerking van de implementatieopties.

Er is een aparte werkgroep wetgeving die zicht buigt over de juridische vertaling van de Richtlijn Dataretentie. De juridische haalbaarheid en uitwerking valt buiten deze opdracht. Omdat het inhoudelijke resultaat van dit onderzoek van belang is voor de juridische verwerking is er een aantal maal gesproken met de werkgroep wetgeving.

1.7 Leeswijzer

Hoofdstuk 2, het beoordelingsmodel, licht na een korte introductie van de acht implementatieopties toe op welke wijze deze met elkaar vergeleken worden middels een kwalitatief en een kwantitatief beoordelingsmodel. Ook wordt de relatie met de onderzoekvragen toegelicht.

In hoofdstuk 3, de implementatieopties, wordt eerst het architectuurraamwerk geïntroduceerd aan de hand waarvan de implementatieopties worden uitgewerkt. Daarna wordt op het niveau van bedrijfsarchitectuur toegelicht hoe vier implementatieopties eruitzien, welke actoren erbij betrokken zijn, welke processen ze uitvoeren en welke producten ze leveren. Vervolgens worden de beveiligingsvereisten toegelicht waarna een overzicht volgt van de overige ontwerpeisen.

In hoofdstuk 4 wordt toegelicht hoe de implementatieopties er op het niveau van informatiearchitectuur en technische architectuur uitzien.

In hoofdstuk 5 wordt de uitkomst van het kwantitatieve model en het kwalitatieve model per implementatieoptie toegelicht en in verband gebracht met de onderzoeksvragen.

Hoofdstuk 6 sluit af met een korte conclusie

De onderzoeksvragen zijn middels het beoordelingsmodel en de ontwerpcriteria verwerkt in verschillende delen van het rapport. Tabel 1-1 op de volgende bladzijde geeft een overzicht waar in de verschillende hoofdstukken de onderzoeksvragen expliciet aan de orde komen. Voor iedere onderzoeksvraag geldt dat deze beantwoord wordt in hoofdstuk 5, uitkomsten.

Tabel 1-1: relatie tussen onderzoeksvraag, hoofdstuk en bijlage

Nummer van de Onderzoeksvraag	**Antwoord opgenomen in hoofdstuk / paragraaf / bijlage**
1	De vastgestelde lijst is opgenomen in bijlage C. De eisen en criteria zijn verwerkt in het kwalitatieve model in hoofdstuk 2, in de ontwerpeisen in hoofdstuk 3 en in hoofdstuk 5, uitkomsten.
2	De (mening over de) huidige werkwijze is niet apart beschreven maar verwerkt in het kwalitatieve model in hoofdstuk 2, in de ontwerpeisen in hoofdstuk 3, het ontwerp in hoofdstuk 4 en hoofdstuk 5, uitkomsten.
3	De impact op voorzieningen is opgenomen in hoofdstuk 4 de technische architectuur en hoofdstuk 5, uitkomsten.
4	De kosten zijn opgenomen in hoofdstuk 2 over het kwantitatieve beoordelingsmodel, in hoofdstuk 4 de technische architectuur en hoofdstuk 5, uitkomsten.
5	De waarborgen voor de omgang met de informatie zijn opgenomen in hoofdstuk 2 over het kwalitatieve beoordelingsmodel, in hoofdstuk 4 de technische architectuur en hoofdstuk 5, uitkomsten.
6	De gegevensbeveiliging is opgenomen in hoofdstuk 2 over het kwalitatieve beoordelingsmodel, in hoofdstuk 3 de implementatieopties (aparte paragraaf beveiliging), in hoofdstuk 4 de technische architectuur en hoofdstuk 5, uitkomsten.
7	De haalbaarheid is opgenomen in hoofdstuk 2 over het kwalitatieve beoordelingsmodel, en hoofdstuk 5, uitkomsten

2 Het beoordelingsmodel

In hoofdstuk 1 is ingegaan op de achtergrond, doelstelling en aanpak van het onderzoek naar de nationale implementatie van de richtlijn dataretentie. In dit hoofdstuk wordt ingegaan op de vraag hoe deze verschillende opties op basis van de gestelde onderzoeksvragen met elkaar op een objectieve wijze vergeleken kunnen worden. Daaraan voorafgaand wordt eerst in het kort ingegaan op de verschillende implementatieopties.

Voor het onderzoek staan vier modellen centraal waarbij er drie variabelen zijn:

- De keuze voor gecorreleerde of ongecorreleerde opslag van de informatie
- De keuze van de locatie van de opslag, te weten centraal of bij de aanbieder
- De keuze van de toegang tot de opgeslagen informatie bij bevraging, te weten door de aanbieder of door de behoeftesteller

De rankschikking van de variabelen resulteert uiteindelijk in acht mogelijke implementatieopties.

Tabel 2-1: overzicht van de acht implementatieopties

	Gecorreleerde gegevensopslag	**Ongecorreleerde gegevensopslag**
Locatie van de opslag van gegevens en toegang tot informatie	Decentrale opslag, beantwoording door de aanbieder	Decentrale opslag, beantwoording door de aanbieder
	Decentrale opslag, directe toegang door de behoeftesteller	Decentrale opslag, directe toegang door de behoeftesteller
	Centrale opslag, directe toegang door de behoeftesteller	Centrale opslag, directe toegang door de behoeftesteller
	Hybride opslag, directe toegang door de behoeftesteller	Hybride opslag, directe toegang door de behoeftesteller

Er zijn drie processen betrokken bij de opslag en bevraging van verkeersgegevens te weten Acquisitie van gegevens, Opslag van gegevens en Bevraging van gegevens. De actoren die betrokken zijn bij de uitvoering van deze processen zijn de aanbieders van telecommunicatiediensten, de behoeftestellers en eventueel een intermediaire derde. De implementatieoptie is bepalend voor welke actor welk proces uitvoert en met welke inhoud.

Hoofdstuk 3 en 4 gaan in detail in op de acht verschillende implementatieopties

De onderzoeksvragen die in paragraaf 1.3 zijn weergegeven hebben zowel een kwantitatief karakter als kwalitatief karakter. Bijvoorbeeld, onderzoeksvraag 4 naar de kosten van elke implementatieoptie heeft een puur kwantitatief karakter. Onderzoeksvraag 7 naar de haalbaarheid in technische, organisatorische en juridische zin van de verschillende mogelijkheden, is een vraag naar de waardering van een implementatieoptie op kwalitatieve aspecten. Om een bruikbaar beeld te krijgen op basis van de antwoorden op de onderzoeksvragen is het van belang deze voor iedere implementatieoptie gewogen en in samenhang met elkaar te beantwoorden.

De implementatieopties moeten op een zo objectief mogelijke wijze met elkaar worden vergeleken en gewaardeerd. Deze objectieve vergelijking kan alleen tot stand komen als de criteria waarop de vergelijking plaats vindt voor alle implementatieopties gelijk is. Daarom zijn de gestelde eisen en criteria tezamen met de overige onderzoeksvragen verwerkt in twee beoordelingsmodellen: een kwalitatief beoordelingsmodel en een kwantitatief beoordelingsmodel.

2.1 Kwalitatief beoordelingsmodel

Het kwalitatieve beoordelingsmodel is de uitwerking van de onderzoeksvragen 1, 2, 5, 6, en 7 (zie pararaaf 1.3). De vragen 1 en 2 staan stil bij de wensen en criteria die zijn vastgesteld bij de startbijeenkomst. De vragen 5 en 6 hebben betrekking op de mate waarin de verschillende implementatieopties waarborgen in zich dragen ten aanzien van informatiebeveiliging, gegevensvernietiging en rapportagemogelijkheden aan de Europese Commissie . Vraag 7 heeft betrekking op de technische, organisatorische en juridische haalbaarheid van de verschillende implementatieopties.

Tijdens het vooronderzoek zijn alle wensen, criteria en eisen bij de behoeftesteller en aanbieders geïnventariseerd. In de startbijeenkomst is deze inventarisatie gevalideerd. Vervolgens zijn alleen die criteria en eisen zijn in het beoordelingsmodel opgenomen die een *onderscheidend* karakter hebben bij de beoordeling van de implementatieopties en die dus bij de keuze tussen de implementatieopties doorslaggevend kunnen zijn.

De overige criteria en eisen zijn aangemerkt als *generiek* voor alle implementatieopties. Het zijn ontwerpeisen waaraan alle ontwerpen van de implementatieopties zoals deze in hoofdstuk 4 zijn beschreven volledige dienen te voldoen. De onderscheidende eisen en criteria zijn als variabelen gegroepeerd naar categorie: Organisatie en processen, Technologie, Business Case, (Informatie) Beveiliging en Implementatietermijn (haalbaarheid).

De onderscheidende criteria bevatten eveneens de belangrijkste geschilpunten tussen de behoeftesteller en de aanbieders en aanbieders onderling.
Dit maakt het kwalitatieve beoordelingsmodel eveneens bruikbaar om op die aspecten de discussie voort te zetten rond de belangrijkste thema's.

Opzet en werking van het kwalitatieve beoordelingsmodel
Er is een totaal van 100 punten verdeeld over de genoemde categorieën Organisatie en processen, Technologie, Business Case, (Informatie) Beveiliging en Implementatietermijn (haalbaarheid).
Elke categorie kent een maximale score die nooit hoger kan zijn dan het puntentotaal dat die categorie is toegekend. De puntenverdeling in de bovenstaande tabel is tot stand gekomen in overleg met de begeleidingscommissie en geeft het belang weer dat aan de categorieën is toegekend.

Tabel 2-2: overzicht van categorieën en onderwerpen in het kwalitatieve beoordelingsmodel.

Punten	Categorie	Onderwerpen voor meting
30	Organisatie en Processen	Flexibiliteit bij volumeverandering Efficiency van de bevraging Toetsing mogelijkheid aanbieder Rapportage mogelijkheden
30	Technologie	Aansluiting bij huidige gebruikte technologieën Toekomstvastheid van technologie
10	Business Case	Time to Market voor nieuw diensten Marktconsequenties voor kleine aanbieders
20	(Informatie) Beveiliging	Complexiteit van de Audit Trail Vertrouwelijkheid, Integriteit, Continuïteit Exclusiviteit van de opgeslagen gegevens
10	Implementatie termijn	Complexiteit is tijd
100		

Iedere categorie bestaat uit een aantal criteria en eisen. Per criterium en eis is aangegeven hoe gemeten kan worden in welke mate een implementatieoptie daaraan invulling geeft. De uitwerking van deze criteria (parameters) en de specifieke aspecten waarop de meting plaatsvindt met de waarde die daaraan wordt toegekend is opgenomen in bijlage D.

De criteria en eisen binnen elke categorie in relatie tot elkaar gewogen, elk criterium of eis draagt dus een gemaximeerd percentage bij aan de totale score van de categorie. De mate waarin aan de het criterium of eis wordt tegemoet gekomen is bepalend voor de bijdrage van het criterium of eis aan de totale score van de categorie.

Als een implementatieoptie dus maximaal aan alle criteria en eisen in het beoordelingsmodel voldoet scoort de betreffende implementatieoptie dus 100 punten in de kwalitatieve beoordeling.

Tabel 2-3: v*oorbeeld van de werking van het kwalitatieve beoordelingsmodel* voor één categorie

Wegings-factor Categorie	**Wegings-factor vraag**	**parameter**	**Waarde**	**Voorbeeld waarden voor optie A**	**Punten voor optie A**
Maximaal 30 punten	**(% van pnt)**	**Organisatie en processen**			
	33%	Efficiency van de bevraging	Snel=33% Gemiddeld=20% Langzaam=0	snel	10 punten
	33%	Mogelijkheid van toetsing op wettelijke grondslag door aanbieder	Ja=33% Nee=0%	nee	0 punten
	33%	Flexibiliteit om met fluctuatie van het bevragingsvolume om te gaan	Groot=33% Middel=20% Klein=0%	middel	6 punten
Score 16 punten					**16 punten**

Uitwerking van de berekeningswijze:

- De categorie 'organisatie en processen' draagt maximaal 30 punten bij aan de totaal score van de kwalitatieve beoordeling.
- Het criterium 'efficiency van de bevraging' draagt voor maximaal 33% bij aan de totaalscore van de categorie organisatie en processen.
- De efficiëntie van de implementatieoptie wordt (in dit voorbeeld) beoordeeld als *Snel*
- De berekening is als volgt: 33% van 30 punten is 10 punten.
- Betekenis van de score: In de categorie organisatie en processen draagt het criterium 'efficiency van de bevraging' 10 punten bij aan de totaalscore van de categorie en dus aan de totaalscore van de implementatieoptie.

Elke implementatieoptie wordt aan de hand van het kwalitatieve model beoordeeld. Dit leidt tot een score per categorie en een totaalscore. De scores geven een indruk hoe een implementatieoptie presteert ten opzichte van de eisen en criteria die gesteld worden.
Belangrijker is dat in een totaaloverzicht de scores van de implementatieopties naast elkaar worden gezet waardoor het mogelijk is om een indruk te krijgen hoe de opties ten opzichte van elkaar staan en op welke punten de verschillen zich concentreren. Hiermee worden de onderzoeksvragen in samenhang met elkaar beantwoord en is inzichtelijk op basis waarvan de waardering tot stand is gekomen. Daarbij moet in gedachten blijven dat het model een hulpmiddel vormt en de individuele belanghebbende een andere afweging kan maken voor wat betreft het belang van bepaalde scores.

2.2 Kwantitatief beoordelingsmodel

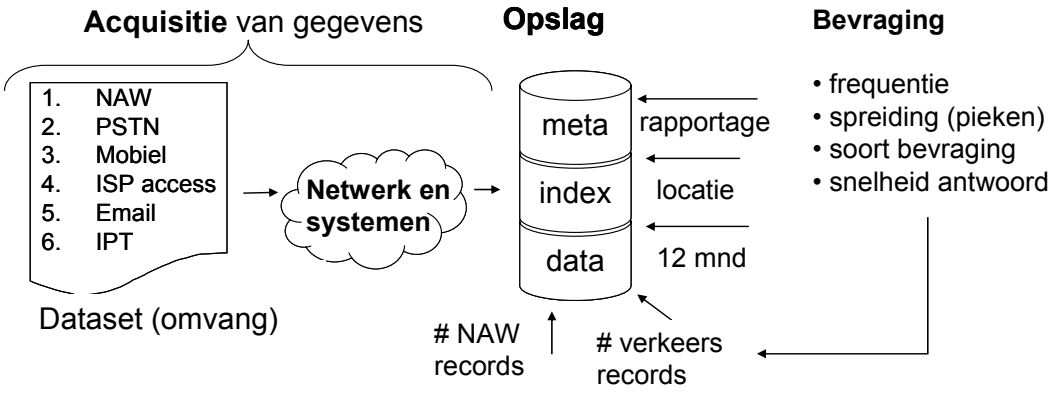
Het kwantitatieve beoordelingsmodel is de uitwerking van de onderzoeksvragen 3 en 4 naar de kosten van de implementatieopties en de financiële impact daarvan op de bedrijfsvoering van de aanbieders, de eventuele intermediaire derde en behoeftestellers. De belangrijkste uitdaging daarbij is om tot een kostenoverzicht op nationaal niveau te komen. Dit vraagt om een onderbouwing van onderaf maar ook om aggregatie tot op nationaal niveau.

In het kwantitatieve model zijn voor iedere implementatieoptie voor de processen 'acquisitie', 'opslag' en 'bevraging' per actor (behoeftesteller, aanbieder en eventuele intermediaire 3e) de kosten in beeld gebracht. Daarnaast is aangegeven hoe de kosten zich ontwikkelen in een periode van 5 jaar op de aspecten 'investering' (capital expenditure kortweg capex) en 'exploitatie' (operational expenses kortweg opex). Per implementatieoptie komt een dergelijk samengevat kostenoverzicht er als volgt uit te zien.

Betrokkene **Centrale opslag**	**kostensoort** **gecorreleerd**	**Jaar 1 CAPEX**	**Jaar 1 OPEX**	**Jaar 2 OPEX**	**Jaar 3 OPEX**	**Jaar 4 OPEX**	**Jaar 5 OPEX**	**Totaal 5 jaar**
Behoeftestellers	Acquisitie Opslag Bevraging Beheer							
Subtotaal Behoeftestellers								
Intermediaire derde	Acquisitie Opslag Bevraging Beheer							
Subtotaal Intermediaire 3de								
Aanbieders	Acquisitie Opslag Bevraging Beheer							
Subtotaal Aanbieders								
Totaal								

Figuur 2-1: samengevat kostenoverzicht op nationaal niveau

Onderliggend aan de bovenstaande presentatie van de kosten en kostenontwikkeling ligt een inventarisatie van de kosten op de diverse technische (dataset, database architectuur, hardware, sofware, infrastructuur) en organisatorische aspecten (beheer, beveiliging, faciliteiten) van elke implementatieoptie. Per implementatieoptie is gekeken naar welke omvang apparatuur en software noodzakelijk zijn, omvang van de beheerorganisatie, omvang van de organisatie voor bevraging en tot slot welke beveiligingsmaatregelen nodig zijn.



Figuur 2-2: kostenaspecten van de processen acquisitie, opslag en bevraging

Uit het veldonderzoek is gebleken dat huidige situatie per aanbieder qua bedrijfsomvang, bedrijfsmatige ontwikkeling, aangeboden diensten en technische infrastructuur zeer uitleen loopt. Zo is te verwachten dat de impact van de dataretentie richtlijn op de technische infrastructuur van aanbieders van traditionele vaste en mobiele telecommunicatiediensten relatief gezien matig is ten opzichte van de impact op de technische infrastructuur van aanbieders van IP access en email. Evenzeer is de bedrijfsmatige impact op relatief jonge, kleine en zeer kleine aanbieders groter dan op de grote en middelgrote aanbieders die al enige jaren in de markt actief zijn.

Om tot een hanteerbare modellering te komen is de bovenstaande berekening gemaakt voor een aanbieder met 125.000 klanten aan wie de aanbieder het volledige scala aan diensten levert dat onder de richtlijn dataretentie valt. Er is gerekend met 125.000 accounts vaste telefonie, 125.000 accounts mobiele telefonie, 125.000 accounts voor internet acces en 125.000 email accounts. Bijlage E bevat een gedetailleerd kostenoverzicht voor investeringen en operationele kosten voor deze aanbieder in het eerste jaar. Het is gebaseerd op de implementatieoptie centrale opslag, directe toegang en gecorreleerde opslag. Het model bevat ook de kostencomponenten voor de behoeftesteller en – voor deze optie - van de intermediaire derde. Omdat iedere implementatieoptie een andere opbouw en verdeling van kosten heeft zijn er acht van dergelijke modellen. Zoals blijkt uit het volgende overzicht kan deze aanbieder als middelgroot voor de Nederlandse markt worden beschouwd. In de bijlage komen ook de onderliggende details aan de orde zoals de dimensionering van de benodigde gegevensopslag, het gebruik van marktgegevens en gegevens uit het veldonderzoek.

Uit het jaarverslag van de OPTA over 2005 blijkt dat er zo'n 282 netwerkaanbieders zijn en 331 dienstaanbieders actief zijn. Op basis van de marktaandelen blijkt vervolgens dat de markt voor traditionele vaste en mobiele telefonie voor 95-99% in handen is van 3 tot 5 aanbieders. Het aantal klanten voor vaste telefonie dat deze aanbieders hebben varieert tussen 100.000 en 3,5 miljoen klanten. Voor mobiele telefonie ligt dit tussen de 1,7 miljoen en 5,7 miljoen klanten. In de markt van internetaanbieders hebben 4 grotere en 6 kleinere aanbieders circa 91% van de markt in handen. Het aantal klanten van deze aanbieders hebben varieert tussen 150.000 en 2 miljoen klanten. Dit betekent dat het overgrote deel van de aanbieders (het gaat om honderden aanbieders) kleine spelers zijn. Al deze aanbieders leveren tezamen 6,1 miljoen vaste telefonieaansluitingen, 4,9

miljoen internetaansluitingen, 16 miljoen mobiele aansluitingen (CBS getallen over 2005) en 7,9 miljoen actieve email accounts (op basis van veldonderzoek, exclusief hotmail, Gmail, etc.).

Voor de rekenkundige modellering van de kosten voor de aanbieders op nationaal niveau is een vertaling gemaakt van de markt. Het is dus géén weerspiegeling van de markt !

Tabel 2-4: aantallen grote, middelgrote en kleine aanbieders per dienst in Nederland, ten behoeve van de berekening van de kosten op landelijke schaal

Aanbieders *Gemiddeld aantal* *Accounts x 1000*	**Groot** *5000*	**Middel** *500*	**Klein** *1*
Vaste telefonie	1	5	30
Mobiel	4	5	10
Kabel	0	5	12
ISP	0	5	203
Totaal	5	20	255

Om te komen tot een berekening van de kosten op nationaal niveau is het model voor 500.000 accounts voor de grote aanbieders geëxtrapoleerd naar 5 miljoen accounts en voor de kleine aanbieders naar 1000 accounts. Daarbij zijn de kosten niet lineair met de omvang geëxtrapoleerd. Voor de extrapolatie naar 5 miljoen accounts is voor de kosten gerekend met 80% als gevolg van schaalgrootte voordelen. Deze voordelen zitten in hardware, software, infrastructuur en personeel. Voor de extrapolatie naar de kleine accounts is gerekend met 200%. Het relatieve nadeel voor de kleine operators is groot omdat in ze in veel gevallen sneller externe deskundigheid nodig zullen hebben en omdat de investeringen voor hard- en software per account naar verhouding groter zullen zijn.

In het geval van de kleine aanbieders is er bij de optie *decentrale opslag, beantwoording door de aanbieder* de mogelijkheid om op basis van bedrijfsmatige overwegingen te kiezen voor een handmatige bevraging van de databases. Het lage volume van bevragingen zal daarin leidend zijn, in het veldonderzoek is door aanbieders een ondergrens van 2 bevragingen per dag genoemd. De kostenonderbouwing van het model van 500.000 accounts is gebaseerd op geautomatiseerde bevraging, hoofdstuk 3 en 4 gaan daar verder op in. Door het extrapoleren van dit model voor de berekening van de kosten voor de kleine aanbieders is daardoor gerekend met een geautomatiseerde oplossing. In de praktijk zal een deel van deze aanbieders bij deze implementatieoptie kiezen voor handmatige bevraging van de database. De kosten voor de kleine aanbieders bedragen circa 2% van de totale kosten. Wanneer er van handmatige bevraging wordt uitgegaan zullen deze kosten veranderen maar het zal niet leiden tot een andere uitkomst .

Door het aantal aanbieders te vermenigvuldigen met het bijbehorende kostenmodel ontstaat een kostenoverzicht op nationaal niveau voor het eerste jaar. Doordat het model de kosten voor zowel de aanbieders, de behoeftestellers als –indien van toepassing – de intermediaire derde bevat zijn alle actoren in beeld gebracht.

Om tot een projectie te komen van vijf opeenvolgende jaren worden de operationele kosten van het eerste jaar vermenigvuldigt met een factor gebaseerd op drie componenten:

- Algemene prijsontwikkeling voor alle kosten, ingeschat op basis van CBS rapportages over historische algemene prijsontwikkeling op drie procent per jaar.
- Toename in het bevragingsvolume. Dit is een ontwikkeling vanuit de behoeftesteller. Overleg met Justitie leverde inzicht op in de drijfveren voor toename van het bevragingsvolume zoals toename in casussen waarvoor gevorderd kan worden, kortere cyclus per bevraging waardoor er per casus vaker bevraagd kan worden, het leren kennen van de uitgebreidere mogelijkheden tot bevraging door de opsporingsambtenaren en toename van het type bevragingen. Het levert bij Justitie een intuïtieve schatting voor de groei op van een factor 2 tot 4 in vijf jaar. In de berekeningen is uitgegaan van 20 procent groei in het bevragingsvolume per jaar.

- Toename in de omvang van de te bewaren gegevens als gevolg van toename van het gebruik, toename van mobiliteit van gebruikers over de aanbieders ("churn") en toename door substitutie van het ouderwetse PSTN naar VoIP (VoIP genereert veel meer te bewaren data dan PSTN). Het veldonderzoek heeft geen gedetailleerde informatie opgeleverd over bovenstaande ontwikkelingen. Voor de toename in omvang van te bewaren gegevens is uitgegaan van 20 procent volumegroei per jaar.

Omdat de beheerkosten niet in hetzelfde tempo groeien als de kosten voor bevraging en opslag is voor deze categorie kosten rekening gehouden met een groei van 8% per jaar (3% plus ¼ van 20%).

3 De implementatieopties

In Hoofdstuk twee is uiteengezet hoe de beoordeling van de verschillende implementatieopties tot stand komt. Dit hoofdstuk gaat in op de wijze waarop de implementatieopties in dit rapport worden uitgewerkt en het beschrijft op hoofdlijnen de werking van de opties op het niveau van bedrijfsarchitectuur. In het volgende hoofdstuk worden de opties verder uitgewerkt op het niveau van informatiearchitectuur en technische architectuur.

Voor de implementatie van de Europese Richtlijn Dataretentie zijn in de Nederlandse situatie meerdere oplossingsrichtingen denkbaar. De begeleidingscommissie dataretentie heeft voor het onderzoek de volgende oplossingrichtingen aangedragen:

- Decentrale opslag, beantwoording door de aanbieder
- Centrale opslag, directe toegang vanuit de behoeftesteller

Voor beide oplossingsrichtingen is de keuze voor correlatie van de data bij opslag toegevoegd waardoor er vier opties ontstaan: gecorreleerde opslag en ongecorreleerde opslag.

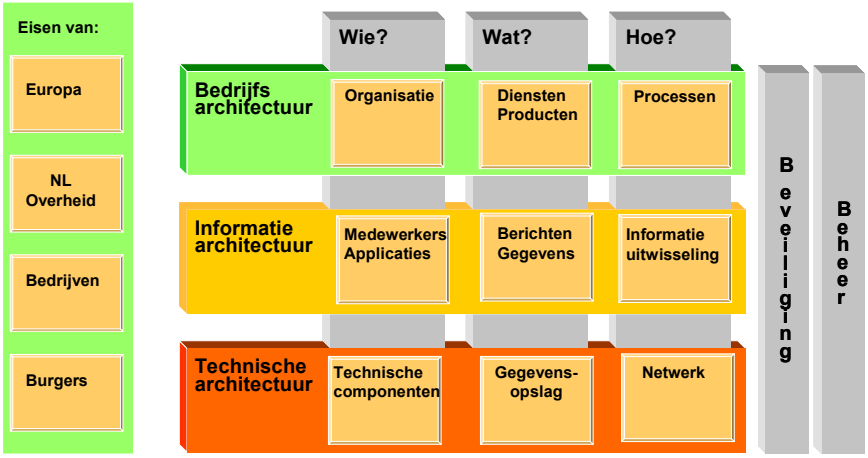
Omdat de decentrale opslag ook direct toegankelijk kan worden gemaakt voor de behoeftesteller zijn er op basis van deze indeling eigenlijk zes opties, drie oplossingsrichtingen met elk twee varianten. Het onderzoek is met deze zes opties als uitgangspunt gestart waarbij de mogelijkheid is open gelaten om ook mogelijke hybride oplossingsrichtingen te onderzoeken.
In de eerste fase van het onderzoek is er vanuit de gesprekken met de aanbieders en de behoeftestellers eveneens een vierde oplossingsrichting ontstaan omdat er bezien vanuit de opslag van data ook nog relevante hybride vormen denkbaar zijn. In het rapport zijn daarom acht implementatieopties uitgewerkt, vier oplossingsrichtingen met elk twee varianten:

Tabel 3-1: acht implementatieopties

	Gecorreleerde gegevensopslag	**Ongecorreleerde gegevensopslag**
Locatie van de opslag van gegevens en toegang tot informatie	Decentrale opslag, beantwoording door de aanbieder	Decentrale opslag, beantwoording door de aanbieder
	Decentrale opslag, directe toegang door de behoeftesteller	Decentrale opslag, directe toegang door de behoeftesteller
	Centrale opslag, directe toegang door de behoeftesteller	Centrale opslag, directe toegang door de behoeftesteller
	Hybride opslag, directe toegang door de behoeftesteller	Hybride opslag, directe toegang door de behoeftesteller

3.1 Referentiearchitectuur

Voor eenduidig begrip en voor de uitwerking in kosten en de kwalitatieve beoordeling is van belang om in meer detail te beschrijven hoe een optie precies werkt, wat de processen zijn, wie de actoren zijn, wat ze onderling uitwisselen en wat de onderliggende techniek is. Voor de beschrijving van de implementatieopties zal in deze verslaglegging gebruik worden gemaakt van het architectuurraamwerk zoals dat ook gebruikt wordt voor NORA[4] (Nederlandse OverheidsReferentieArchitectuur).



Figuur 3-1: het architectuurraamwerk van NORA

De bedrijfsarchitectuur richt zich op de organisaties die tezamen uitvoering geven aan de Richtlijn Dataretentie. Het beschrijft de processen die worden uitgevoerd en de producten en diensten die (onderling) worden geleverd. Het beschrijft de inrichtingsprincipes.

De informatiearchitectuur heeft betrekking op de inrichting van de informatiehuishouding. Het gaat daarbij over begrippen en gegevens, betekenis en definitie, de structuur en de wijze van uitwisseling.

De technische architectuur beschrijft het samenstel van machines, opslagvoorzieningen en netwerkcomponenten vanuit technische optiek.

De beschrijving volgens deze architectuur maakt op drie niveaus inzichtelijk hoe de implementatieopties werken. In dit hoofdstuk zullen de implementatieopties op het niveau van de bedrijfsarchitectuur worden beschreven. In hoofdstuk 4 zullen de implementatieopties op het niveau van informatiearchitectuur en technische architectuur beschreven worden.

[4] Zie Nederlandse OverheidsReferentieArchitectuur, samenhang en samenwerken binnen de elektronische overheid, versie 0.8, 31 maart 2006.

De eisen die aan de inrichting en de werking gesteld worden zijn weergeven aan de linkerzijde in figuur 3-1. Deze komen in dit hoofdstuk aan de orde in de paragraaf over de ontwerpeisen. In hoofdstuk 2 zijn de eisen aan de orde gekomen in relatie tot de uiteenzetting over het kwalitatieve beoordelingsmodel.

3.2 Actoren, processen, producten en diensten

De wijze waarop de implementatieopties werken zijn te beschrijven aan de hand van de actoren (wie?), de producten en diensten (wat?) en de processen (hoe?).

Bij de Nederlandse implementatie van de Richtlijn Dataretentie zijn de volgende actoren te onderscheiden:

- De behoeftestellers, te weten het Openbaar Ministerie (in de praktijk de opsporingsdiensten, o.a. KLPD en regiokorpsen, BOD'n) en de inlichtingen en veiligheidsdiensten (AIVD en MIVD).
- De aanbieders van vaste telefonie (zowel klassieke telefonie als IP telefonie), mobiele telefonie, internet providers en aanbieders van e-mail diensten
- Een eventuele intermediaire derde die in het proces van opslag, bevraging en beantwoording een actieve rol kan spelen (het huidige CIOT kan worden beschouwd als één van de vele vormen die een intermediaire derde kan aannemen)

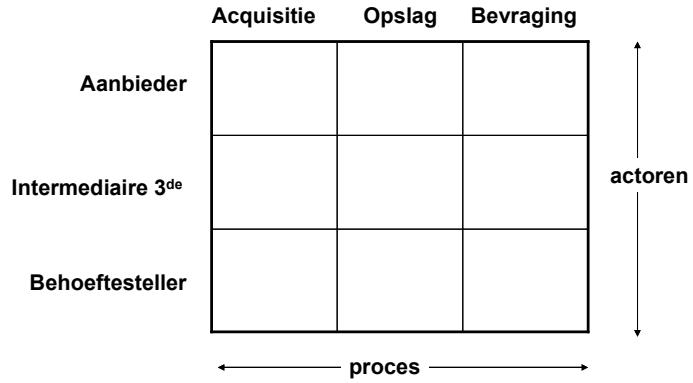
De volgende processen worden onderscheiden, mede op basis van informatie verkregen uit het veldonderzoek:

- Het *acquisitieproces* waarmee de te bewaren gegevens uit het netwerk en de business management systemen worden gehaald en – eventueel na conversie - aangeboden worden voor interne c.q. externe opslag.
- Het *opslagproces* van de gegevens inclusief het proces waarmee de gegevens na de vastgestelde bewaartermijn worden vernietigd.
- Het *bevragingsproces* vanuit de behoeftesteller inclusief de beantwoording door de bevraagde partij (de aanbieder dan wel de intermediaire derde).

Voor de heldere afbakening van verantwoordelijkheden van de actoren in de processen is het behulpzaam als vervolgens wordt gesproken over producten en diensten die tussen de actoren worden geleverd. De producten die tussen de actoren geleverd worden zijn de volgende:

- *Vraagstelling* (vordering) volgens een bepaald formaat, deze wordt door de behoeftesteller geleverd.
- *Antwoord op de vraagstelling* (vordering) volgens een bepaald formaat, deze wordt door de aanbieder of de intermediaire derde geleverd als dan niet via een geautomatiseerd proces.
- *Verlenen van toegang tot de opgeslagen gegevens* door de aanbieder of de intermediaire derde aan de behoeftesteller, dit is benodigd in het geval van de directe toegang.
- *Aanlevering van een gegevensbestand* met een bepaald formaat door de aanbieder.

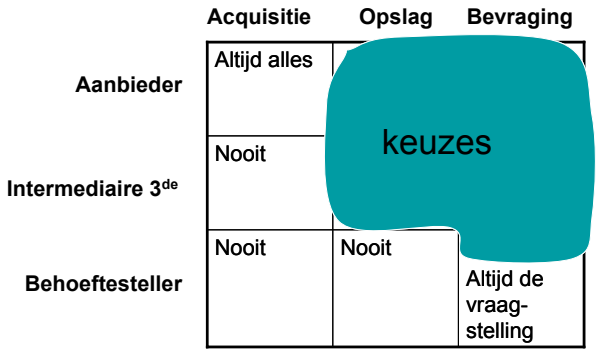
De processen en actoren kunnen uitgezet worden in een matrix waarmee inzichtelijk gemaakt kan worden welke actor een bepaald proces uitvoert.



Figuur 3-2: actoren en processen

Niet ieder proces is onder te brengen bij iedere actor, in een aantal gevallen ligt dit reeds vast gegeven de aard van het proces. Zo zal de acquisitie van gegevens altijd door de aanbieder worden uitgevoerd en is de behoeftesteller altijd de bron van een vraag.

Er blijft zo een kleiner speelveld over waar de keuzes gemaakt kunnen worden voor het onderbrengen van processen bij actoren. Daarbij gaat de keuze verder dan alleen door wie een proces wordt uitgevoerd, ook de wijze waarop deze wordt ingevuld is onderdeel van het keuzeproces en varieert per implementatieoptie. Het gaat dan bijvoorbeeld over de rol van de aanbieder in het beantwoordingproces. Het speelveld is weergegeven in figuur 3.



Figuur 3-3: Speelveld van de keuzemogelijkheden voor allocatie van processen bij actoren

Op het niveau van de bedrijfsarchitectuur zijn er vier opties:

- Decentrale opslag, beantwoording door de aanbieder
- Decentrale opslag, directe toegang door de behoeftesteller
- Centrale opslag, directe toegang door de behoeftesteller
- Hybride opslag, directe toegang door de behoeftesteller

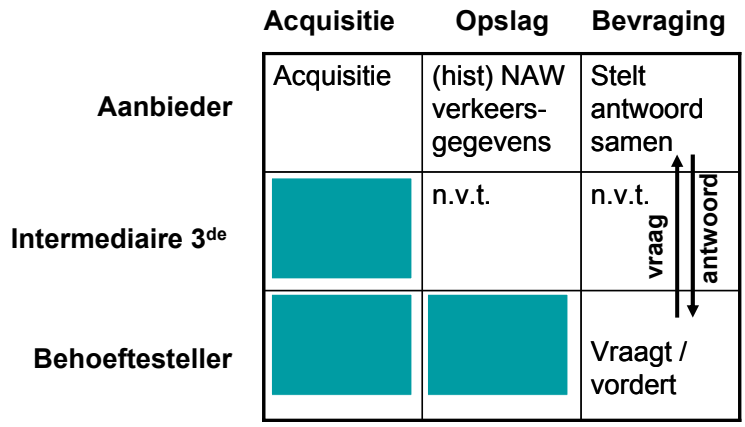
De keuze voor correlatie heeft betrekking op de technische inrichting van de opgeslagen informatie:

- Ingeval van *gecorreleerd opslag* is er in de database een koppeling aangebracht tussen de verkeersgegevens en de identificerende (NAW) gegevens.
- In het geval van *ongecorreleerde opslag* is er in de database geen koppeling aangebracht van verkeersgegevens en identificerende gegevens.

De keuze voor gecorreleerde opslag of ongecorreleerde opslag wordt als een keuze op het niveau van de informatiearchitectuur beschouwd en komt aan de orde in hoofdstuk 4.

3.3 Decentrale opslag, beantwoording door aanbieder

Deze implementatieoptie ziet er als volgt uit.



Figuur 3-4: decentrale opslag, beantwoording door de aanbieder.

Acquisitie

De aanbieder verzamelt de gegevens vanuit het netwerk, de netwerkmanagement systemen en de business management systemen. De gegevens worden geconverteerd naar een formaat dat de opslag van gegevens harmoniseert en bevraging vereenvoudigt.

Opslag

De aanbieder slaat de gegevens op, logisch en fysiek gescheiden van de operationele omgeving voor zover de beveiligingsmaatregelen dit vereisen. De toegang tot de informatie moet alleen mogelijk zijn voor daartoe geautoriseerd personeel van de aanbieder. Er is geen sprake van directe geautomatiseerde toegang door de behoefte steller dus zijn geen afspraken tussen de aanbieders en behoeftesteller nodig over de vorm waarin de opslag van gegevens plaats vindt. Iedere aanbieder kan zelf vorm van de gegevensopslag bepalen aan de hand van een bedrijfsmatige afweging over de efficiency van het bevragingsproces.

Doordat de aanbieder zelf de informatie opslaat ligt het eigendom van de opgeslagen informatie en de verantwoordelijkheid voor de juistheid en de bescherming ervan bij de aanbieder evenals de verantwoordelijkheid voor de vernietiging van de gegevens na de wettelijk vastgestelde termijn.

Bevraging en beantwoording

De behoeftesteller vordert de benodigde informatie bij de aanbieder. De vordering bevat gestandaardiseerde elementen om controles en de beantwoording efficiënter te laten verlopen. De vordering wordt aangeleverd in de vorm van een document (fax, secure e-mail) en verloopt volgens een vaste uniforme procedure. De procedure moet voorzien in controles op de aanwezigheid van de juiste grondslag van de vordering (wetsartikel), de autorisatie door de juiste ambtenaar (handtekening van een OvJ of RC) en de bron van herkomst van vordering (de authenticiteit van de opsporingsambtenaar die de vraag bij de aanbieder neerlegt).

De behoeftesteller legt het feit van de vordering van de gegevens inclusief de autorisatie daarvan vast in relatie tot het specifieke onderzoek waarop de vordering betrekking heeft. De rechtmatigheid van de vordering kan achteraf worden vastgesteld als onderdeel van de zogenoemde Audit Trail.

In het geval van decentrale opslag heeft de behoeftesteller een keuzeprobleem omdat het hij niet altijd kan vaststellen bij welke aanbieder het object van onderzoek diensten afneemt of heeft afgenomen. Doordat deze eenduidige vaststelling niet kan plaats hebben kunnen er een aantal iteraties over heen gaan voordat de juiste aanbieder gevonden is. Het is bij deze optie waarschijnlijk dat de huidige bevraging van actuele NAW gegevens bij het CIOT zal blijven bestaan.

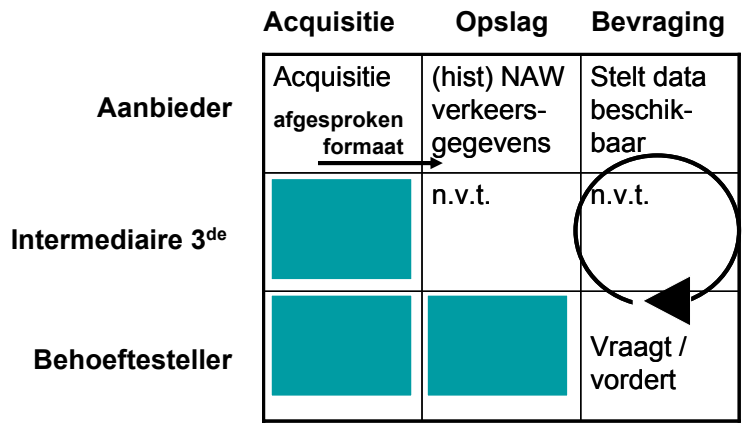
De aanbieder heeft een actieve rol bij de beantwoording, dat wil zeggen dat de aanbieder de gevraagde gegevens al dan niet geautomatiseerd bij elkaar zoekt en het antwoord doormiddel van de vastgestelde procedure (fax, secure e-mail) naar de behoeftesteller verzend.

De aanbieder is verantwoordelijk voor de juistheid van het antwoord op de vordering, er geen ander partij die dit voor hem doet. Er bestaat daardoor geen onduidelijkheid over de verantwoordelijkheid voor de juistheid van de verstrekte informatie. De vordering en de verstrekte informatie worden in relatie tot elkaar gearchiveerd als onderdeel van de inrichting van de zogenoemde Audit Trail ten behoeve van de controle achteraf op de juistheid en rechtmatigheid van de vordering en daarmee de juistheid en rechtmatigheid van de beantwoording.

Deze werkwijze laat overleg toe tussen behoeftesteller en aanbieder over de vordering en het antwoord. Hierdoor kan bijvoorbeeld sprake kan zijn van een actieve toetsing van de vordering door de aanbieder en kwaliteitsverbetering van de vordering en het antwoord door kennisuitwisseling over de interpretaties van de effectiviteit van de vordering en het antwoord op de vraagstelling.

3.4 Decentrale opslag, directe toegang

Deze implementatieoptie ziet er als volgt uit.



Figuur 3-5: decentrale opslag, directe toegang

Acquisitie

De aanbieder verzamelt de gegevens vanuit het netwerk, de netwerkmanagement systemen en de business management systemen. De gegevens worden geconverteerd naar een gestandaardiseerd en een voor alle aanbieders uniform formaat die de opslag van gegevens harmoniseert en daarmee geautomatiseerde bevraging mogelijk maakt.

Vanwege de noodzaak van standaardisatie bestaat in deze optie een sterkere onderlinge afhankelijkheid tussen de diverse actoren. De directe toegang kan alleen werken als de informatie in een gestandaardiseerde vorm worden aangeboden. Bij veranderingen in de door de aanbieder aangeboden diensten, de door de aanbieder aangeleverde informatie of veranderingen in de opslag en bevraging van de informatie zal door alle partijen rekening moeten worden gehouden met de bestaande afspraken. Eenzijdige afwijkingen hierin zullen tot problemen leiden in de verdere verwerking.

Opslag

De aanbieder slaat de gegevens op, logisch en fysiek gescheiden van de operationele omgeving voor zover de beveiligingsmaatregelen dit vereisen. De opslag vindt plaats volgens een afgesproken gestandaardiseerd formaat zodat er automatische bevraging door de behoeftestellers op kan plaatsvinden.

De toegang tot de informatie is niet mogelijk voor personeel van de aanbieder anders dan de systeembeheerder die het opslagsysteem en de bevragingsinterface moet kunnen testen op de juiste werking. De beheerder heeft alleen toegang voor zover zijn beheertaken dit vereisen en zijn activiteiten worden vastgelegd (gelogd en gearchiveerd) ter controle achteraf.
Het overige personeel van de aanbieder heeft geen faciliteiten om casus gerelateerde informatie op te vragen.

Doordat de aanbieder zelf de informatie opslaat ligt het eigendom van de opgeslagen informatie en de verantwoordelijkheid voor de juistheid en de bescherming ervan bij de aanbieder evenals de verantwoordelijkheid voor de vernietiging van de gegevens na de wettelijk vastgestelde termijn.

Bevraging en beantwoording
De behoeftesteller vordert de benodigde informatie bij de aanbieder. Daarvoor wordt directe toegang tot de opgeslagen gegevens gebruikt. De rol van de aanbieder bij het bevragingsproces is beperkt tot het beschikbaar stellen van de data en het verlenen van toegang tot de data. Er vindt geen actieve beantwoording door de aanbieder plaats, de aanbieder kan geen toetsing op de vordering uitvoeren en niet inhoudelijk bijdragen.

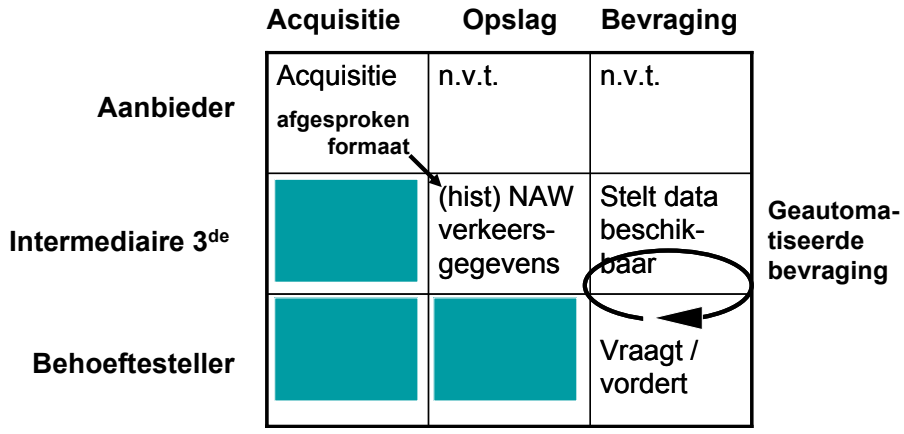
Een daartoe geautoriseerde opsporingsambtenaar heeft een werkstation (toepassing) tot zijn beschikking waarmee hij de diverse bestanden kan raadplegen. Iedere behoeftesteller zal zijn eigen werkstations hebben. De procedure moet voorzien in de juiste controles op de vordering (autorisatie op basis van de aanwezigheid van de vordering, grondslag, handtekeningen) én op de toegang tot de werkstations en de toepassing (autorisatie én authenticatie). De verantwoordelijkheid voor de juiste invulling hiervan ligt bij de behoeftestellers.
De procedure moet tevens voorzien in de archivering van het feit van de vordering van de gegevens inclusief de autorisatie daarvan. De archivering vindt plaats in relatie tot het specifieke onderzoek waarop de vordering betrekking heeft zodat de rechtmatigheid van de vordering achteraf kan worden vastgesteld (audit trail).

In het geval van decentrale opslag heeft de behoeftesteller een keuzeprobleem omdat het hij niet altijd kan vaststellen bij welke aanbieder het object van onderzoek diensten afneemt of heeft afgenomen. Doordat deze eenduidige vaststelling niet kan plaats hebben kunnen er een aantal iteraties over heen gaan voordat de juiste aanbieder gevonden is. Doordat de bevraging automatisch wordt doorlopen kan in een kortere tijd dan bij de handmatige procedure de juiste aanbieder worden gevonden. Het is ook bij deze optie waarschijnlijk dat de huidige bevraging van actuele NAW gegevens bij het CIOT zal blijven bestaan.

Doordat de aanbieder zelf niet meer het antwoord samenstelt wijzigt de situatie als het gaat om de verantwoordelijkheid voor de juistheid van de informatie. De aanbieder blijft verantwoordelijk voor de juistheid van de aangeboden informatie, de behoeftesteller heeft de verantwoordelijkheid om de juist vraag te stellen en daarmee het juiste antwoord samen te stellen.

3.5 Centrale opslag, directe toegang

Deze implementatieoptie ziet er als volgt uit.



Figuur 3-6: centrale opslag, directe toegang

Acquisitie

De aanbieder verzamelt de gegevens vanuit het netwerk, de netwerkmanagement systemen en de business management systemen. De gegevens worden geconverteerd naar een gestandaardiseerd en een voor alle aanbieders uniform formaat die de opslag van gegevens harmoniseert waarna de aanbieder de gegevens aanbiedt aan een intermediaire derde. De conversie is noodzakelijk om gecentraliseerde opslag en geautomatiseerde bevraging mogelijk te maken.

Vanwege de noodzaak tot standaardisatie bestaat ook in deze optie een sterke onderlinge afhankelijkheid tussen de diverse actoren. De centrale opslag en directe toegang kan alleen werken als de informatie in een gestandaardiseerde vorm wordt aangeboden en opgeslagen. Bij veranderingen in de door de aanbieder aangeboden diensten, de door de aanbieder aangeleverde informatie of veranderingen in de opslag en bevraging van de informatie zal door alle partijen rekening moeten worden gehouden met de bestaande afspraken. Eenzijdige afwijkingen hierin zullen tot problemen leiden in de verdere verwerking.

Opslag

Een intermediaire derde slaat de gegevens op. Deze intermediaire derde kan zowel een private partij zijn als een overheids(gebonden)instelling. De afweging en keuze voor een private of publieke organisatie is niet essentieel voor de praktische werking van de implementatieoptie en maakt geen deel uit van dit onderzoek.

De opslag vindt plaats volgens een afgesproken formaat zodat er automatische bevraging door de behoeftestellers op kan plaatsvinden.

Het personeel van de aanbieder heeft geen enkele toegang tot de opgeslagen gegevens en dus ook niet tot casus gerelateerde informatie. De toegang tot de informatie is niet mogelijk voor personeel

van de intermediaire derde anders dan de systeembeheerder die het opslagsysteem, de bevragingsinterface en bevragingstoepassing moet kunnen testen op de juiste werking. De beheerder heeft alleen toegang voor zover zijn beheertaken dit vereisen en zijn activiteiten worden vastgelegd (gelogd en gearchiveerd) ter controle achteraf (audit trail).

Doordat de aanbieder niet meer zelf de informatie opslaat is het eigendom en de verantwoordelijkheid voor de juistheid van de opgeslagen informatie niet zonder meer eenduidig. De aanbieder blijf verantwoordelijk voor de juistheid van de aan de intermediaire derde aangeboden informatie maar nadat de aanbieder zijn informatie heeft aangeboden is het aan de intermediaire derde om de opslag op de juiste wijze uit te voeren. Er is daarom voorzien in een geautomatiseerde controle om vast te kunnen stellen dat de door de aanbieder aangeboden informatie dezelfde is als de informatie die bij de intermediaire derde is ontvangen.

Vanuit de aanbieders is echter aangegeven dat de controle op de juistheid van de verzending van de gegevens door de ambiguïteit van de verantwoordelijkheidsstelling niet voldoende is. Daardoor ontstaat de behoefte bij de aanbieder om zelf de aan de intermediaire derde aangeboden informatie voor een langere periode op te slaan die de vastgestelde opslagtermijn kan overschrijden. De reden die daarvoor is opgegeven is dat in het geval van fouten in de gevorderde gegevens of fouten in de interpretatie daarvan de juistheid van het eigen handelen aangetoond moet kunnen worden. In een dergelijke bestandsvergelijking is in deze optie niet voorzien en maakt daarom geen deel uit van de audit trail (wel de gevorderde gegevens).
Daardoor voelen sommige aanbieders de noodzaak om de brongegevens langdurig op te slaan zodat ook na de periode van een jaar afdoende aangetoond kan worden dat er geen fouten zijn gemaakt. Deze extra opslag en de juridische noodzaak daarvan maken geen deel uit van dit onderzoek. Achterliggende aanname hiervoor is dat juridische dan wel technische maatregelen voldoende zullen blijken.

Bevraging en beantwoording
De behoeftesteller vordert de benodigde informatie bij de intermediaire derde. Daarvoor wordt directe toegang gebruikt. De rol van de aanbieder en van de intermediaire derde bij het bevragingsproces is beperkt tot het beschikbaar stellen van de data en het verlenen van toegang. Er vindt geen actieve beantwoording door de aanbieder of de intermediaire derde plaats, geen van beiden kan een actieve toetsing op de vordering uitvoeren of inhoudelijk bijdragen. De vraagstelling in de vordering is echter zodanig gestandaardiseerd dat in de bevragingstoepassing controles kunnen worden uitgevoerd op de relatie tussen de vraag en de juistheid van de wettelijke grondslag daarvan.

Een daartoe geautoriseerde opsporingsambtenaar heeft een werkstation (toepassing) tot zijn beschikking waarmee hij de diverse bestanden kan raadplegen. Iedere behoeftesteller zal zijn eigen werkstations hebben. De procedure moet voorzien in de juiste controles op de vordering (autorisatie op basis van de aanwezigheid van de vordering, grondslag, handtekeningen) én op de toegang tot de werkstations en de toepassing (autorisatie én authenticatie). De verantwoordelijkheid voor de juiste invulling hiervan ligt bij de behoeftestellers.

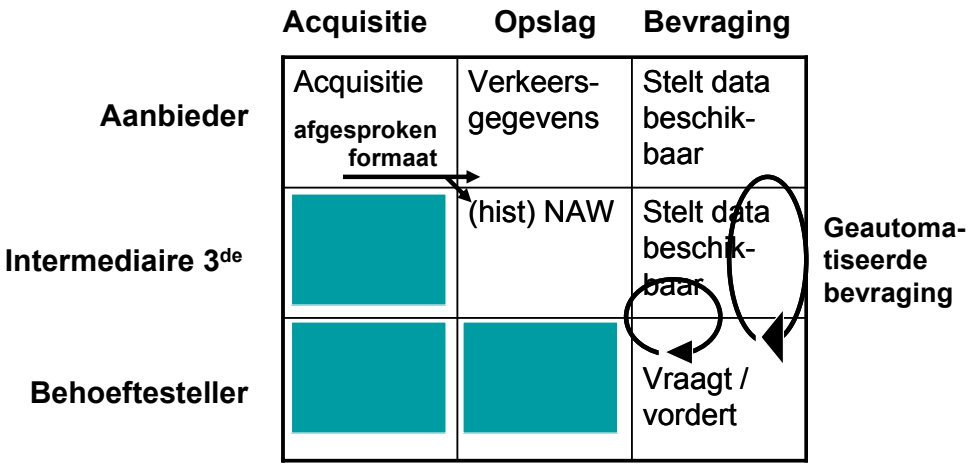
De procedure moet tevens voorzien in de archivering van het feit van de vordering van de gegevens inclusief de autorisatie daarvan. De archivering vindt plaats in relatie tot het specifieke onderzoek waarop de vordering betrekking heeft zodat de rechtmatigheid van de vordering achteraf kan worden vastgesteld (audit trail).

In het geval van centrale opslag heeft de behoeftesteller geen keuzeprobleem meer omdat er één plaats is waar kan worden vastgesteld van welke aanbieder het object van onderzoek diensten afneemt en heeft afgenomen.

Doordat de aanbieder geen actieve rol meer heeft in de beantwoording van een vordering en er geen opslag is voorzien van de aanboden gegevens ontstaat er een complexere situatie als het gaat om de juistheid van de informatie. De aanbieder blijft verantwoordelijk voor de juistheid van de aangeboden informatie, de intermediaire derde heeft de verantwoordelijkheid voor een juiste opslag en de juiste werking van de bevragingstoepassing, de behoeftesteller heeft de verantwoordelijkheid voor het stellen van de juiste vraag om het juiste antwoord te genereren.

3.6 Hybride opslag, directe toegang

De eerste drie opties zijn een weergave van de opties zoals deze in het offerteproces zijn benoemd. Tijdens de uitvoering van het onderzoek is er ook nog een vierde, hybride model ontwikkeld. Deze ziet er als volgt uit.



Figuur 3-7: hybride opslag, directe toegang.

De (historische) NAW gegevens worden gescheiden van de verkeersgegevens opgeslagen. De NAW gegevens worden centraal opgeslagen bij de intermediaire derde, de verkeersgegevens worden decentraal bij de aanbieder zelf opgeslagen. Dit biedt een aantal voordelen.

In de eerste plaats is er één centrale plaats waar de behoeftesteller kan nagaan bij welke aanbieder het object van onderzoek diensten afneemt of heeft afgenomen. Met deze informatie kan gericht de juiste aanbieder voor de verdere verkeersgegevens worden bevraagd.

In de tweede plaats blijven de verkeersgegevens bij de aanbieders. Deze gegevens worden door alle betrokkenen als gevoeliger beschouwd dan de NAW gegevens hetgeen bijvoorbeeld ook tot uiting komt in het feit dat verkeersgegevens uitsluitend door de officier van justitie kunnen worden gevorderd. Door deze in het bezit te laten van de aanbieder wordt een deel van de problematiek rond eigendom en verantwoordelijkheid vermeden.

Acquisitie
De aanbieder verzamelt de gegevens vanuit het netwerk, de netwerkmanagement systemen en de business management systemen. De gegevens worden geconverteerd naar een gestandaardiseerd en een voor alle aanbieders uniform formaat die de opslag van gegevens harmoniseert en daarmee geautomatiseerde bevraging gecentraliseerde opslag (NAW) mogelijk maakt.

Ook in de hybride situatie ontstaat er een sterke onderlinge afhankelijkheid tussen de diverse actoren. De hybride opslag en directe toegang kan alleen werken als de informatie in een gestandaardiseerde vorm wordt aangeboden en opgeslagen. Bij veranderingen in de door de aanbieder aangeboden diensten, de door de aanbieder aangeleverde informatie of veranderingen in de opslag en bevraging van de informatie zal door alle partijen rekening moeten worden gehouden met de bestaande afspraken. Eenzijdige afwijkingen hierin zullen tot problemen leiden in de verdere verwerking.

Opslag
Een intermediaire derde slaat de NAW gegevens op. Deze intermediaire derde kan zowel een private partij zijn als een overheids(gebonden)instelling. De afweging en keuze voor een private of publieke organisatie is niet essentieel voor de praktische werking van de implementatieoptie en maakt geen deel uit van dit onderzoek.

De aanbieder slaat zelf de verkeersgegevens op logisch en fysiek gescheiden van de operationele omgeving voor zover de beveiligingsmaatregelen dit vereisen.

De toegang tot de informatie is niet mogelijk voor personeel van de aanbieder anders dan de systeembeheerder die het opslagsysteem en de bevragingsinterface moet kunnen testen op de juiste werking. De beheerder heeft alleen toegang voor zover zijn beheertaken dit vereisen en zijn activiteiten worden vastgelegd (gelogd en gearchiveerd) ter controle achteraf. Het overige personeel van de aanbieder heeft geen faciliteiten om casus gerelateerde informatie op te vragen.

De toegang tot de informatie is niet mogelijk voor personeel van de intermediaire derde anders dan de systeembeheerder die het opslagsysteem en bevragingstoepassing moet kunnen testen op de juiste werking. De beheerder heeft alleen toegang voor zover zijn beheertaken dit vereisen en zijn activiteiten worden vastgelegd (gelogd en gearchiveerd) ter controle achteraf (audit trail).

De opslag vindt plaats volgens een afgesproken formaat zodat er automatische bevraging door de behoeftestellers op kan plaatsvinden.

Bevraging en beantwoording

De behoeftesteller vordert de benodigde NAW informatie bij de intermediaire derde. Daarvoor wordt directe toegang gebruikt. De verkeersgegevens vordert de behoeftesteller bij de aanbieder. De rol van beiden bij het bevragingsproces is beperkt tot het beschikbaar stellen van de data. Er vindt geen actieve beantwoording door de aanbieder of de intermediaire derde plaats, geen van beiden kan een toetsing op de vordering uitvoeren of inhoudelijk bijdragen. De vraagstelling in de vordering is echter zodanig gestandaardiseerd dat in de bevragingstoepassing controles kunnen worden uitgevoerd op de relatie tussen de vraag en de juistheid van de wettelijke grondslag daarvan.

Een daartoe geautoriseerde opsporingsambtenaar heeft een werkstation (toepassing) tot zijn beschikking waarmee hij de diverse bestanden kan raadplegen. Iedere behoeftesteller zal zijn eigen werkstations hebben. De procedure moet voorzien in de juiste controles op de vordering (autorisatie op basis van de aanwezigheid van de vordering, grondslag, handtekeningen) én op de toegang tot de werkstations en de toepassing (autorisatie én authenticatie). De verantwoordelijkheid voor de juiste invulling hiervan ligt bij de behoeftestellers.
De procedure moet tevens voorzien in de archivering van het feit van de vordering van de gegevens inclusief de autorisatie daarvan. De archivering vindt plaats in relatie tot het specifieke onderzoek waarop de vordering betrekking heeft zodat de rechtmatigheid van de vordering achteraf kan worden vastgesteld (audit trail).

Doordat de NAW gegevens centraal zijn opgeslagen is er één plek waar de behoeftesteller kan nagaan bij welke aanbieder de verdachte diensten afneemt of heeft afgenomen.

3.7 Beveiliging

De Europese Richtlijn

De beveiligingseisen die in artikel 7 van de Europese Richtlijn worden zijn gesteld in algemene bewoordingen geven aan de lidstaten ruimte voor tactische en operationele keuzen. Er wordt onder andere gesproken over de verplichting van de Lidstaten tot nemen van adequate technische en organisatorische maatregelen die:

- de data die wordt geacquireerd minimaal beschermen op minimaal het beveiligingsniveau van het netwerk (waarop de data wordt getransporteerd en uit worden ontrokken red.)
- de data (geacquireerd, opgeslagen en bevraagd red.) beschermen tegen ongeautoriseerde en onwettige opslag, bewerking en openbaring.
- de data beschermen tegen onbedoeld verlies, vernietiging of verandering.
- verzekeren dat de data die is opgeslagen, niet bedoeld wordt de data die wordt bevraagd en bewerkt, na de opslag termijn wordt vernietigd.

In het algemeen stelt de Richtlijn dat de data alleen mag worden gebruikt voor het doel waarvoor ze zijn opgeslagen.
Verderop in deze paragraaf wordt aangeven dat de eisen die in de richtlijn worden gesteld kunnen worden gedekt door bestaande uitwerkingen van de in algemene bewoordingen gestelde eisen.

De Nationale Context

Door de begeleidingscommissie van dit onderzoek is aangegeven dat beveiligingsnormering van ISO 17799 (wordt ISO 27000 serie) en de VIR (incl. VIR-BI) van toepassing moeten worden geacht. De internationaal geaccepteerde ISO normering voor beveiliging wordt in het bedrijfleven dus ook bij de aanbieders als uitgangspunt genomen voor de inrichting van hun eigen beveiligingsbeleid en bij de overheid is de nationale VIR en verdere operationele specificaties van de VIR-BI normering het uitgangspunt. Beide normeringen hebben hun oorsprong in de negentiger jaren van de vorige eeuw en zijn in de loop der jaren verder ontwikkeld. De verwachting is dat in 2007 een vernieuwde versie van de VIR wordt geaccepteerd die beter aansluit op de terminologie en uitgangspunten van de ISO beveiligingsnorm. De aard van de VIR normering en de ISO normering blijven echter wel verschillend. Daar waar de acceptatie van een ISO norm een vrije keuze is moet de VIR worden gezien als het interne beveiligingsbeleid van de Rijksoverheid. De grens van het werkingsgebied van de VIR is beperkt tot het verantwoordelijkheidsgebied van de Rijksoverheidsorganisatie.
Het proces van dataretentie overstijgt echter het directe werkingsgebied van de VIR en VIR BI.

Uitgangspunten voor het beveiligen van het proces van dataretentie: acquisitie, opslag en bevraging

In de startbijeenkomst is vanuit de behoeftesteller aangegeven dat het systeem van dataretentie moet voldoen aan de VIR en VIR-BI. Door de aanbieders is aangegeven dat de ISO norm voor beveiliging moet worden gevolgd. In deze paragraaf wordt ingegaan op de essenties van beide normen om vervolgens te komen tot een set van eisen voor de beveiliging van het systeem van dataretentie die in dit onderzoek gebruikt kan worden.

In de startbijeenkomst is door de I&V diensten aangegeven dat classificatie (in terminologie van de VIR: rubricering) van de gegevens in het proces van dataretentie op het niveau van Staatsgeheim zou moeten worden gesteld, er is geen verdere specificatie aangegeven (Stg Confidentieel, Stg Geheim, Stg Zeer Geheim). Een dergelijke rubricering heeft altijd betrekking heeft op 'gegevens' en op 'informatie'. De verdere rubricering is conform de VIR-BI essentieel voor de te specificeren beveiligingsmaatregelen.

Indien in het algemeen de rubricering Staatsgeheim wordt toegepast op de uitwerking van dataretentie moet men zich rekenschap geven dat hier een verschil optreedt met de wijze waarop met de activiteit aftappen wordt omgegaan. Binnenlandse Zaken heeft tot nu toe geen algemene verplichting tot een veiligheids-screening van de betrokken medewerkers van de aanbieders van toepassing verklaard. Slechts die medewerkers die betrokken zijn bij beantwoording van vraagstellingen van I&V diensten dienen tot op heden gescreend te zijn.
Hier staat tegenover dat indien de I&V diensten en behoeftestellers van hetzelfde systeem van bevraging gebruik maken (dit is onderdeel van een aantal implementatieopties) de rubricering Staatsgeheim van toepassing moet zijn op het gehele systeem van opslag en bevraging. De hoogste rubricering van informatie dat door een systeem wordt gegenereerd of bewerkt is immers van toepassing op de rubricering van het gehele systeem.

Zowel de VIR als de ISO normering gaan er vanuit dat een keuze voor te nemen beveiligingsmaatregelen gebaseerd moet zijn op een risicoafweging. In het VIR wordt gesproken van een verplichting om een Afhankelijkheids en Kwetsbaarheids Analyse uit te voeren als

uitgangspunt voor rubricering en de daarvan afgeleide maatregelen. In de nieuwe VIR 2007 wordt een vergelijkbare insteek gekozen als in de ISO beveiligingsnorm. De ISO norm hanteert een iets ruimere definitie en spreekt over het doen van een risicoanalyse die moet leiden tot een classificatie van het een te beveiligen object (gegevens, informatie en gerelateerde middelen en personeel), die classificatie is vervolgens richting gevend voor de keuze van beveiligingseisen die van toepassing zijn en de keuze voor de daarvan afgeleide maatregelen.

De vraag is dus welke risicoafweging moet worden gemaakt om:
- te bepalen in welke risico klasse het proces van dataretentie moet worden ingedeeld en;
- om daarvan afgeleid tot een juiste specificatie van beveiligingsmensen te komen.

Voor het proces van dataretentie moet op pragmatische wijze een adequate set van beveiligingseisen worden geformuleerd. Het uitvoeren van een A&K analyse of een risicoanalyse waarin alle betrokken partijen zitting hebben valt buiten de scope van dit onderzoek.

De oplossing voor de ontwerpen lijkt besloten te liggen in de eisen met betrekking tot een op essentiële punten vergelijkbaar proces die de overheid op een eerder moment heeft geformuleerd en vastgelegd namelijk in de bijlage van het Besluit Beveiliging Gegevens Aftappen Telecommunicatie (BBGAT, 18 oktober 2003):

1. de actoren die betrokken zijn bij dit proces zijn vrijwel dezelfde actoren als de betrokken bij het proces van dataretentie;
2. het betreft eveneens zeer gevoelige persoonsgegevens die ingeval van misbruik tot grote schade kunnen leiden voor het object van onderzoek en het imago van de betrokken actoren in het proces van dataretentie;
3. het belang van de actoren bij de juistheid en bescherming van de gegevens is vergelijkbaar;
4. het belang van de behoeftesteller bij de bescherming van bron van de vordering, identiteit van het object van onderzoek en de vergaarde informatie is vergelijkbaar.

In de bijlage van het Besluit Beveiliging Gegevens Aftappen Telecommunicatie zijn concrete beveiligingseisen opgenomen (Bijlage F) die, zij het met andere formuleringen en terminologie, inhoudelijk niet echt afwijken van de betreffende (selectie) beveiligingseisen uit de ISO normering.

Bij toepassing van de beveiligingsvereisten uit de BBGAT moet rekening worden gehouden met het volgende:

1. Bij de ontwerpen van de implementatieopties is er vanuit gegaan dat genoemde beveiligingseisen niet alleen op de aanbieder van toepassing zijn maar ook op de behoeftesteller en eventuele intermediaire derde, ongeacht de positionering daarvan binnen of buiten het verantwoordelijkheidsgebied van de Rijksoverheid;
2. De eisen (gerelateerd aan beveiliging) die de Europese richtlijn in artikel 7 stelt worden voldoende ingevuld door de meer geoperationaliseerde beveiligingseisen in de bijlage van het besluit. Toegevoegd zou moet worden de formulering van de eis ten aanzien van de vernietiging van de gegevens na de opslagtermijn.
3. De eisen die voortvloeien uit de Wet Bescherming Persoonsgegevens ten aanzien van het gebruik, de bescherming, opslag en vernietiging zijn niet specifiek (men spreek over adequate maatregelen). Indien aan de beveiligingseisen uit de Europese Richtlijn wordt voldaan wordt in

dezelfde mate aan de beveiligingseisen van de WBP wordt voldaan. Voor de WBP-eis tot vernietiging van de gegevens na de bewaartermijn geldt dat deze vergelijkbaar is met de zelfde eis in de Europese richtlijn. Eveneens is dat het geval voor de eis uit de WBP dat de gegevens alleen gebruikt mogen worden voor het doel waarvoor ze zijn opgeslagen. Voor andere verplichtingen uit de WPB dan de hierboven genoemde verplichtingen geldt dat deze in het kader van de uitwerking van de implementatieopties niet relevant zijn. Zo is bijvoorbeeld geen analyse gemaakt van de consequenties van de verplichting tot het aanmelding van bestanden bij het CBP indien deze langer dan de gegeven termijn worden opgeslagen etc.

4. Er is geen analyse gedaan van eventuele beveiligingseisen die in overige regelgeving of beleid zijn vastgelegd en mogelijk van toepassing zou kunnen zijn op delen van het proces of zelfs een enkele actor in het proces zoals bijvoorbeeld de regelgeving rond politieregisters. Voor zover deze eisen bestaan zijn ze dus niet expliciet in de ontwerpen van de implementatieopties meegnomen.

3.8 Ontwerpeisen

Naast de beveiligingsvereisten zijn er aanvullende eisen vanuit het wettelijk kader, de onderzoeksvragen en de criteria en wensen die door de behoeftestellers en door de aanbieders zijn gesteld (zie bijlage C). Iedere implementatieoptie dient invulling te geven aan deze eisen.

Daar waar een ontwerpeis in verschillende mate wordt ingevuld door de diverse implementatieopties is deze als onderscheiden criterium opgenomen in het kwalitatieve model.
Daar waar een ontwerpeis geen onderscheidend gevolg heeft op het ontwerp van de implementatieopties anders dan kosten, is deze als ontwerpeis beschreven.

Ontwerpeisen voor de bedrijfsarchitectuur
Op het niveau van bedrijfsarchitectuur gaat het ondermeer om de volgende ontwerpeisen:

- De opslag moet voldoen aan de dataset en overige voorwaarden zoals voorgeschreven door de richtlijn, zie bijlage G voor de gedefinieerde velden.
- In het onderzoek is met instemming van de begeleidingscommissie en de werkgroep wetgeving gerekend met een bewaartermijn van 1 jaar, na één jaar moeten de gegevens worden vernietigd.
- De bewaartermijn van één jaar is inclusief de actuele datum. Dat wil zeggen dat de set van NAW gegevens zoals deze momenteel door het CIOT wordt opgeslagen deel is van de identificerende gegevens zoals deze onder de richtlijn vallen.
- Het volume van de huidige bevraging van het CIOT op actuele NAW gegevens is voor alle opties buiten bij de modellering gehouden. In de decentrale varianten had opname van het bevragingsvolume geïmpliceerd dat het CIOT verdwijnt wat niet waarschijnlijk is. In de hybride en centrale variant is het onvermijdelijk dat CIOT en intermediaire derde samengaan. Om de opties vergelijkbaar te houden is gekozen voor het buitenbeschouwing laten van de bevraging van de actuele NAW gegevens. Hoofdstuk 5 staat stil bij de financiële overwegingen.
- De bevragingsprocedure moet voorzien in afdoende maatregelen ten aanzien van authenticatie en autorisatie van de ambtenaar die de vordering doet.

- De procedures moeten zorgvuldige dossiervorming ondersteunen ten behoeve van de inrichting van de audit trail (controles achteraf).
- Periodiek moet er een (onafhankelijke) audit worden gehouden om de juiste en daarmee rechtmatige uitvoering van de procedures vast te stellen.
- De bevragingsfrequentie voor (historische) verkeersgegevens en historische NAW gegevens ligt in het eerste jaar op 233 per maand voor de model aanbieder met 500.000 accounts en zal de jaren daarna met 20% toenemen. De inrichting en werking moet dit volume ondersteunen.
- De omvang van de te bewaren gegevens zal toenemen als gevolg van toename van het gebruik, toename van mobiliteit van gebruikers over de aanbieders ("churn") en toename door substitutie van het ouderwetse PSTN naar VoIP (VoIP genereert veel meer te bewaren data dan PSTN). Er is uitgegaan van 20% volumegroei per jaar. De inrichting en werking moet dit volume ondersteunen.
- De bevraging van verkeersgegevens is conform de huidige richtlijnen een set van enkelvoudige vragen (specifiek en gebaseerd op een casus), zie het vademecum Telecom van het OM.
- De tijdsduur tussen vordering van de gegevens en beantwoording is maximaal 5 dagen. Deze termijn is nu opgenomen in het vademecum Telecom, er is vanuit de eisen en criteria van behoeftestellers geen andere termijn genoemd anders dan dat men graag een korter tijdsduur zou willen. In de ontwerpen is uitgegaan van een periode van 48 uur.

Ontwerpeisen voor de informatie architectuur

Op het niveau van informatiearchitectuur gaat het ondermeer om de volgende ontwerpeisen:

- De specificatie van de gegevensvelden die conform de vastgestelde dataset door de aanbieder moeten worden geacquireerd en opgeslagen moet eenduidig zijn. Waar deze eenduidigheid ontbreekt in de dataset worden voor het onderzoek ontwerp keuzen gemaakt.
- Ten behoeve van de vergelijkbaarheid van de implementatieopties moet er sprake van eenduidige databasearchitectuur voor alle implementatieopties.
- De praktische uitwerking van gecorreleerde en ongecorreleerde gegevensopslag moet vanwege de vergelijkbaarheid tussen de implementatieopties op eenduidige en consequente wijze worden uitgewerkt.
- Zogenoemde 'data mining' door de actoren in het bevragingsproces moet in het ontwerp van de informatiearchitectuur worden voorkomen.
- In de informatiearchitectuur van de implementatieopties zijn de relevante maatregelen opgenomen om de te nemen beveiligingsmaatregelen in te vullen (zie paragraaf 3.7).
- De informatiearchitectuur moet de inrichting van een zogenoemde audit trail ondersteunen door middel van logging en archivering van de daarvoor essentieel geachte behandeling en bewerkingen van gegevens.
- De implementatieopties met directe toegang moeten uitgaan van een geautomatiseerde bevraging van gegevens en daarmee een standaardisatie van de berichtenuitwisseling. Dit heeft consequenties voor de gebruikte gegevensformaten, databasearchitectuur en ontwerp van de queries in de bevragingsmodules.

De overige eisen aan de informatiearchitectuur zijn als onderscheiden kenmerk van de implementatieopties opgenomen in het kwalitatieve beoordelingsmodel (bijlage D):

- De eisen aan de effectiviteit en snelheid van de gegevensuitwisseling die tot uiting komt in de mate van efficiency van het bevragingsproces.
- De eisen aan de schaalbaarheid en flexibiliteit van de informatiearchitectuur
- De eisen aan de toekomstvastheid van de informatiearchitectuur
- De eisen aan informatiearchitectuur ten aanzien van de effectiviteit van de gegevensvernietiging na de voorgeschreven opslagtermijn

Betekenis van de begrippen gecorreleerd en niet-gecorreleerd

De begrippen gecorreleerd en niet-gecorreleerd moeten in de ontwerpen als volgt worden uitgewerkt.:

- Gecorreleerd: Er is een geautomatiseerde koppeling gemaakt tussen de identificerende (NAW-nummer-dienst) gegevens en de verkeersgegevens.
- Niet-gecorreleerd: Er is geen geautomatiseerde koppeling gemaakt tussen de identificerende (NAW-nummer-dienst) gegevens en de verkeersgegevens.

Voor de bevraging van de gegevens betekent dit dat bij de gecorreleerde variant het mogelijk is om aan de hand van een identificerend gegeven zoals een telefoonnummer over een bepaalde periode in het verleden tegelijkertijd zowel de NAW gegevens op te vragen als bijbehorende verkeersgegevens. In de ongecorreleerde variant moet met hier voor twee vragen stellen. De eerste vraag betreft dan de NAW gegevens en in een tweede vraag kan men dan de verkeersgegevens opvragen.

Ontwerpeisen voor de technische architectuur

Op het niveau van de technische architectuur gaat het ondermeer om de volgende ontwerpeisen:

- De keuzen die in de technische architectuur moeten worden gemaakt ondersteunen de beschreven bedrijfsarchitecturen van de implementatieopties en de realisatie van de eisen aan de informatiearchitectuur. Daar waar deze leiden tot specifieke kenmerken van een implementatieoptie worden deze expliciet gemaakt.
- In de technische architectuur van de implementatieopties ondersteunt de implementatie van de relevante beveiligingsmaatregelen zoals die zijn aangegeven (zie par 3.7). De technische architectuur mag de maatregelen die niet op het niveau van de technische architectuur liggen ook niet in de weg staan. Daar waar dat mogelijk is moeten de kosten voor de te nemen beveiligingmaatregelen expliciet gemaakt worden.

De overige eisen aan de technische architectuur zijn als onderscheiden kenmerk van de implementatieopties opgenomen in het kwalitatieve beoordelingsmodel (bijlage D):

- De eisen aan de toekomstvastheid van de ingezette technologie met effect op de:
  - de schaalbaarheid van implementatieoptie
  - de inpassing van nieuwe diensten door de aanbieder
  - de inpassingen van nieuwe vraagstellingen door de behoeftesteller
- de eisen aan de aansluiting op de technologie met effect op:
  - de wijze van acquisitie van gegevens door de aanbieder
  - de wijze van opslag door de aanbieder
  - de wijze van bevraging door de behoeftesteller
  - de time to market voor de introductie van een nieuwe dienst door de aanbieder

- de tijd die nodig is voor implementatie van de implementatieoptie

Ontwerpeisen voor de beveiligingsarchitectuur

Op het niveau van de beveiligingsarchitectuur gaat het om de volgende eisen:

- De relevante de beveiligingsmaatregelen moeten onder andere worden afgeleid uit de beschreven bedrijfsarchitectuur, het gaat onder andere hierbij om:
  - eisen aan de juistheid en controleerbaarheid van de behandeling en bewerking van gegevens (o.a. inrichting van de audit trail en de daadwerkelijke uitvoering van audits)
  - eisen met betrekking tot de exclusiviteit (vertrouwelijkheid en integriteit) van gegevensuitwisselingprocessen en gegevensopslag (autorisatie en authenticatie)
  - eisen met betrekking tot de robuustheid van het bevragingsproces in de implementatie
  - eisen ter voorkoming van ongeoorloofde 'data mining', dat wil zeggen dat het in iedere implementatieoptie niet mogelijk moet zijn om aan de hand van één gegeven de hele 'doopceel' van een object van onderzoek te lichten. Er mag uitsluitend sprake zijn van beantwoording van (een set van) enkelvoudige vragen.
- De bijlage bij het Besluit Beveiliging Gegevens Aftappen Telecommunicatie (zie bijlage F) is richtinggevend voor de keuzen die op het niveau van het ontwerp van de beveiliging architectuur gemaakt moeten worden

Daar waar een ontwerpeis in verschillende mate wordt ingevuld door de diverse implementatieopties is deze als onderscheidend criterium opgenomen in het kwalitatieve model (zie bijlage D):

- eisen aan de vertrouwelijkheid van de relatie tussen de vraag en onderzoeker
- eisen aan de continuïteit van het bevragingsproces
- eisen aan de vertrouwelijkheid en integriteit van de opgeslagen data (risico op lek of manipulatie)
- eisen aan de inrichting van de Audit Trail conform het gewenste beveiligingsniveau
- eisen aan exclusiviteit van de toegang tot informatie en gegevens (risico van oneigenlijk gebruik)
- eisen aan de vernietiging van de gegeven na de bewaartermijn (risico op te lang bewaren)

Er wordt expliciet *niet* uitgesloten dat bij de implementatie van de opties additionele beveiligingsmaatregelen nodig kunnen zijn. Voorafgaande aan een implementatie van de Richtlijn dataretentie is het noodzakelijk met alle betrokken actoren in het proces een risicoanalyse of A&K analyse uit te voeren.

4 Architectuur van de implementatieopties

In Hoofdstuk drie is de werking van de verschillende implementatieopties op het niveau van bedrijfsarchitectuur beschreven. Dit hoofdstuk zet de uitwerking uiteen van de acht implementatieopties op het niveau van informatiearchitectuur en technische architectuur. Voor het begrip van de juiste context is het lezen van Hoofdstuk drie noodzakelijk.

De beschrijving van de implementatieopties vormt de basis voor de beantwoording van onderzoeksvragen 3 t/m 7. De inschatting van de kosten en de scores op de kwalitatieve criteria zijn bepaald op basis van deze ontwerpen.

Elke beschrijving van een optie start met een presentatie van de specifieke kenmerken en werking van de betreffende implementatieoptie. Beheer wordt als 'ketenkenmerk' besproken omdat deze op meerdere elementen van het NORA model betrekking hebben.

Er zijn onvoldoende gegevens verkregen om het hergebruik van bestaande systemen voor de acquisitie van gegevens te integreren in het technisch ontwerp. Daarom is bij het ontwerp van een zogenoemde 'greenfield situatie' uitgegaan. Deze keuze is mede ingegeven door de enorme diversiteit in de toegepaste techniek, systemen en procedures die tijdens het veldonderzoek bij de aanbieders is aangetroffen.

Om reden van de vergelijkbaarheid van de implementatieopties is de bestaande CIOT procedure niet in het ontwerp opgenomen. Bij de bespreking van de kosten van de verschillende implementatieopties wordt ingegaan op de relatie tussen de kosten van de implementatieopties en de kosten van het huidige CIOT.

Uit het veldonderzoek bij de aanbieders is naar voren gekomen dat in het algemeen de verwachting is dat een aanbieder die meer dan twee vragen om verkeersgegevens per dag krijgt van de behoeftestellers zeer waarschijnlijk het proces van bevraging op een of andere manier gaat automatiseren. Dit kan de vorm aannemen van een simpele standaard query op de ruwe data tot aan een specifieke applicatie op een gestructureerde database, ook bij decentrale opslag.
Op basis van gegevens uit het veldonderzoek is dat al gauw het geval indien een aanbieder 100-18.000 klanten (er lijkt sprake van een grote spreiding) heeft . Alle midden en grote aanbieders hebben meer dan het genoemde aantal klanten en hebben tezamen meer dan 90% van de markt in handen. In de ontwerpen zijn we daarom uitgegaan van een automatisering van de bevraging

Voor de implementatieoptie Decentrale opslag, beantwoording door aanbieders is aangenomen dat de aanbieders beneden de genoemde omvang kunnen kiezen om de bevraging handmatig te doen. Er zal altijd sprake zijn van een of andere vorm van opslag en gereedschap (tooling) om de bevraging van de data te kunnen doen.

4.1 Kenmerken van de architectuur van de implementatieopties

In deze paragraaf wordt ingegaan op de uitwerking van de ontwerpeisen zoals die in paragaaf 3.8 zijn verwoord naar kenmerken van de informatiearchitectuur, de technische architectuur en beveiligingen. De kenmerken zijn van toepassing op alle implementatie opties, daar waar er een verschil tussen de opties bestaat is dit aangegeven en wordt dit punt tevens in de beschrijving van de ontwerp aangegeven als specifiek kenmerk van de betreffende implementatieoptie.

4.1.1 Algemene kenmerken van de informatiearchitectuur

Bij de start van het onderzoek is uitgegaan van de dataset zoals aangegeven door de behoeftestellers. De aanbieders en behoeftestellers bleken vervolgens geen overeenstemming te hebben bereikt over de juridische basis (toegestaan binnen de EU richtlijn) van een aantal gegevens die daarin worden genoemd. Op verzoek van de opdrachtgever zijn alleen die gegevens in het onderzoek betrokken die binnen de scope van de Europese Richtlijn vallen (zie bijlage G).

Afbakening van de Dataset
Bij de afbakening van de dataset zijn een aantal keuzen gemaakt met betrekking tot de interpretatie van de dataset die in het onderzoek is betrokken. Deze keuzen zijn nodig omwille van de uitwerking in het databaseontwerp en het bepalen van de omvang van de gegevensrecords ten behoeve van de berekening van de benodigde opslagcapaciteit. Hieronder worden slechts de keuzen aangegeven die ten aanzien van een aantal datavelden zijn gemaakt, de volledige dataset die in het onderzoek is meegenomen is weergegeven in bijlage G.
Duidelijk moet zijn dat de betreffend keuzen die zijn gemaakt geen ander doel hebben dan om binnen het tijdsbestek van het onderzoek het database ontwerp te kunnen maken en de benodigde opslag capaciteit te kunnen berekenen.

A. NAW(+) gegevens (heeft betrekking op alle diensten c.q. verkeersgegevens)
B. Verkeersgegevens vaste telefonie, PSTN en IP based
C. Verkeersgegevens mobiele communicatie, GSM, GPRS en UMTS
D. Verkeersgegevens IP Access
E. Verkeersgegevens email

Ad. A Voor het onderzoek wordt bij NAW -dienstidentificatie uitgegaan van:
a. voor vaste telefonie het NAW aansluitadres en telefoonnummer,
b. voor mobiele telefonie de contractgegevens en telefoonnummer;
c. voor IP Access de contractgegevens en gebruikersnaam (namen)
d. voor E-mail de contractgegevens en gebruikersnaam (namen)

Ad B/C. Het onderzoek gaat bij ISDN-30 vanwege de technische- en juridische beperkingen uit van verkeersgegevens die op het hoofdnummer worden gegenereerd.

Naast gegevens per abonnement worden minimaal de volgende gegevens per gesprek vastgelegd:

- Inkomend/uitgaand
- Nummer(s) van de andere gespreksdeelnemer(s)
- Starttijd
- Stoptijd
- (bij mobiel) IMEI/IMSI nummer
- (bij VoIP) IP-adres
- Bearer service

Gedurende het veldonderzoek zijn ook de "niet geslaagde oproepen" ter sprake gekomen. Door de aanbieders is unaniem aangegeven dat er geen informatie bewaard blijft van oproeppogingen die niet tot een gesprek of verbinding met een voice mail geleid hebben. Om die reden is er in de berekening van het opslagvolume geen rekening gehouden met deze oproepinformatie.

Ad D. Voor het onderzoek wordt uitgegaan van de verkeersgegevens die worden gegenereerd door:
a. de log-on/log-of van een dsl-modem + IP/MAC-adres van het dsl-modem
b. de log-on/log-of van een inbelmodem + IP/MAC-adres van de computer

- Inlogtijd
- Uitlogtijd
- Uitgegeven IP-adres
- Protocol versie (IPv4/IPv6)
- Inlognaam
- MAC-adres van het client device (router, modem, PC)
- (bij WiFI) locatiegegevens van het access point

Ad E. Voor het onderzoek wordt uitgegaan van:
a. de e-mail die op de mail-server binnenkomt en wordt afgeleverd in de postbus.
b. de e-mail die via een Mail Transfer Agent wordt verzonden en de mailserver verlaat.
c. de afgevangen spam-e-mail die in relatie tot de postbus in een persoonlijke spam-box wordt opgeslagen.
N.B.: In de behoeftestelling is ook sprake van het opvragen van BCC-headers, deze zijn echter geen (technisch) onderdeel van het E-mail bericht dat wordt verzonden en daarmee door de aanbieder niet te traceren vanuit het perspectief van de verzender. Uiteraard wordt een BCC in de mailbox van de ontvanger wel getraceerd.

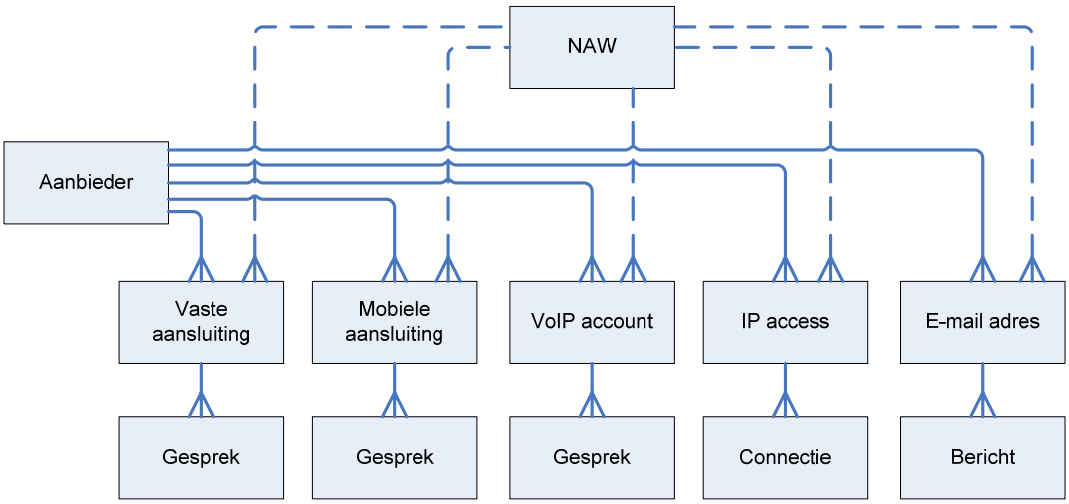
In de behoeftestelling is sprake van het eveneens vastleggen van 'niet geslaagde oproepen' Voor telefoongesprekken betreft dit oproepen die niet beantwoord worden, bij IP-sessies kunnen mislukte inlogpogingen vastgelegd worden.

Inrichting van het Data Model

Uitgangspunten
Het dat model is op een zodanig wijze gekozen dat dit flexibel is en schaalbaar. Voor de opslag van verkeersgegevens is voorzien in een database per dienst. Hiermee is het mogelijk dat een aanbieder die een bepaalde dienst wil gaan leveren alleen die database hoeft te implementeren die betrekking heeft op die dienst.

Voor elke implementatie optie is het mogelijk te werken met dezelfde architectuur.
In het geval men zich eventuele mengvormen van de implementatieopties zou willen voorstellen is de architectuur nog steeds bruikbaar.

Opzet en toepassing
Het data model gaat uit van een opzet waarin de verkeersgegevens van de verschillende diensten in aparte databases zijn opgenomen. De dienst VoIP moet in informatietechnische betekenis beschouwd worden als separate dienst wat ook betekent dat de VoIP verkeersgegevens in een aparte database worden ondergebracht.
Voor de vastlegging van de identificerende gegevens is gekozen voor hergebruik van de huidige databasestructuur van het CIOT (zie bijlage H voor het uitgewerkte databaseontwerp)



Figuur 4-1: globaal databaseontwerp

Het verschil tussen de gecorreleerde en de ongecorreleerde implementatievarianten is dat in de ongecorreleerde varianten de databases voor NAW en verkeersgegevens op verschillende systemen zijn opgeslagen. Dat betekent dat de gestippelde verbanden in bovenstaande figuur niet in de database zijn vastgelegd.

In het geval een aanbieder een nieuwe dienst gaat aanbieden die onder de Dataretentie Richtlijn valt, kan op een relatief eenvoudige wijze aan de retentieverplichting voldaan worden door een extra entiteit aan het data model toe te voegen,.

Voorkomen van 'data mining'
Bij de ontwerpeisen in hoofdstuk 3 is aangegeven dat in alle implementatie opties moet worden voorkomen dat er zogenoemde data mining plaats kan vinden. De mate van haalbaarheid daarvan is afhankelijk van de implementatieoptie. Het is dan ook veeleer een argument in de modelkeuze dan iets dat technisch voorkomen kan worden. Het kan echter wel met technische middelen bemoeilijkt worden. Zo kan geëist worden dat van bepaalde tabellen maximaal een bepaald aantal records per query wordt opgevraagd. Ook kan toegang tot tabellen of records worden beperkt door autorisatiemechanismen.

Zelfs dan kan, zeker in het centrale opslag model, niet voorkomen worden dat handmatig koppelingen en deelverzamelingen gemaakt worden door beheerders. Het voorkomen van ongeoorloofde data mining moet daarom niet alleen met technische middelen worden bestreden. Naast de genoemde maatregelen moet ook de juiste logging van handelingen door beheerders worden geïmplementeerd en de juiste procedures worden geïmplementeerd die voorkomen dat beheerders zonder directe controle (4 ogen principe) in hun eentje toegang tot de database kunnen hebben.

4.1.2 Algemene kenmerken van de technische architectuur

Automatisering van de bevraging
Bij de introductie van dit hoofdstuk is reeds ingegaan op de keuze voor geautomatiseerde bevraging.

In het ontwerp van de opties waarin sprake is van directe toegang door de behoeftesteller is uitgegaan van een bevragingsapplicatie die centraal ter beschikking wordt gesteld aan de behoeftesteller. Een randvoorwaarde voor geautomatiseerde bevraging is de realisatie van een verregaande standaardisatie van de vragen naar verkeersgegevens.

Toetsing op de juiste Autorisatie
Een nadrukkelijke eis bij alle ontwerpen is de zekerstelling dat misbruik en oneigenlijk gebruik van de verkeersgegevens wordt voorkomen. Er zijn in dit kader een drietal vragen met betrekking tot het onderwerp Autorisatie van belang zijn als het gaat om het verzekeren dat de persoon die gegevens opvraagt ook gemachtigd deze op te vragen:

a) Is de vraag van de onderzoeker getoetst door de Officier van Justitie of Rechter Commissaris?
b) Is de vraag van de onderzoeker naar verkeersgegevens op de juiste wettelijke grondslag gesteld?
c) Is de persoon die de gegevens opvraagt ook de persoon die hij of zijn zegt dat hij of zij is?

Ad a en b
Deze eisen zijn vooral procedureel van aard, en er zijn geen directe technische maatregelen te nemen om deze vragen te controleren anders dan deze op te nemen in de wijze waarop de bevrachtingapplicatie wordt opgebouwd.

Ad c
In het kader van deze eis hebben slechts die personen toegang die daartoe ook gemachtigd zijn. In de implementatie optie DBA wordt deze toets door de aanbieder op handmatige wijze uitgevoerd op de zelfde manier als dit in de huidige situatie het geval is (fax met CLI en PGP-secure E-mail).
In de overige opties is met behulp van een infrastructuur met "strong authentication" (certificaten en/of tokens) voorzien in een technische autorisatie oplossing.

Audit Trail
Met de beoordeling van de complexiteit van de inrichting van de Audit Trail is uitgegaan van het perspectief van de Auditeur. Dat betekent dat niet alleen de mate van eenvoud telt waarmee handelingen kunnen worden gelogd en gearchiveerd maar ook het aantal partijen waar loggings moeten worden opgevraagd en gecontroleerd in geval van een gehele systeem audit. Slechts de beschreven centrale opslag directe toegang variant (CDT) is de Audit Trail relatief eenvoudig omdat vrijwel alle belangrijke handelingen op 1 plaats worden gelogd. Het aspect dat ter plaatse bij de onderzoekers van de behoeftesteller een koppeling moet worden gemaakt (en gecontroleerd) tussen de vraag die gesteld is en het zaakdossier van de onderzoeker is in alle implementatieopties gelijk.

Van elke bevraging wordt vastgelegd:
- Wie heeft de vraag gesteld?
- Wie (OvJ/RC of hfd. IV dienst) heeft de vraag geautoriseerd?
- Op basis van welk wetsartikel is de vraag gesteld?
- Welke gegevens zijn gevraagd en geleverd?
- Wanneer is de vraag gesteld, respectievelijk het antwoordt geleverd?

Locatie en medium van de vastlegging verschillen per implementatieoptie.

Bij het ontwerp van de implementatieopties is de benodigde opslagcapaciteit voor de loggings meegenomen.

Acquisitie, Opslag en Bevraging
In de technische ontwerpen van de implementatieopties wordt een onderscheid gemaakt tussen acquisitie, conversie, correlatie, opslag en bevraging van gegevens. Conversie wordt in de ontwerpen gezien als een functie van acquisitie eveneens als de tijdelijke opslagcapaciteit die daarvoor nodig is.
De technische architectuur en informatiearchitectuur van het ontwerp van de implementatieoptie, de diversiteit van te verzamelen data en de omvang van de database zijn bepalend voor de uiteindelijke complexiteit en de werking van de implementatieopties.

Afhankelijk van het ontwerp liggen de genoemde functionaliteiten in zijn geheel of deels bij de aanbieder, een mogelijk intermediaire derde of bij de behoeftesteller. Acquisitie en conversie ligt in de ontwerpen altijd bij aanbieder. De allocatie van bevraging en opslag varieert per implementatieoptie.

4.1.3 Algemene kenmerken van het beheer

Elke vorm van automatisering brengt beheer van de automatiseringsmiddelen met zich mee. Daar waar in het ontwerp van de implementatieoptie zich de meeste automatiseringsmiddelen concentreren ligt ook het zwaartepunt van het beheer. De totale omvang van de beheerorganisatie voor het gehele systeem van acquisitie, opslag en bevraging hangt af van de mate van centralisatie van de automatiseringsmiddelen. Een bijzonderheid is dat wanneer uitgegaan wordt van een zeer

kleine aanbieder met een duizend klanten de omvang van de beheerorganisatie die gerelateerd is aan dataretentie slecht een marginaal deel van een taak is van een persoon. Daar het gaat om een zeer klein deel van de markt is de invloed hiervan echter gering als het om kosten gaat. Wel telt dit mee in de beoordeling van de vertrouwelijkheid van de bron van de vraag en object van onderzoek omdat het in dat kader gaat om personen die deze taak uitvoeren en niet om fte's.

4.1.4 Algemene kenmerken van de beveiliging

Beveiligingsstandaarden

Voor het ontwerp van de implementatieopties is zijn beveiligingseisen geformuleerd (zie hoofdstuk 3). Voor de invulling van de beveiligingseisen zijn algemene de volgende beveiligingsstandaarden gehanteerd:

- ISO 17799
- VIR, VIR-bi

Vertrouwelijkheid: Autorisatie en Authenticatie

Het ontwerp van vertrouwelijkheid of exclusiviteit is in de implementatieopties uitgewerkt t.a.v. :

- Het beheer van toegangsrechten tot het netwerk, bevragingsapplicatie en databases met daaraan gerelateerd:
  - De vertrouwelijkheid of exclusiviteit van de bron van de vraag
  - De vertrouwelijkheid of exclusiviteit van het object van onderzoek
  - De veranderbaarheid of integriteit van gegevens

Op het niveau van toegang tot de data is in de ontwerpen uitgegaan van de toepassing van Radius-achtige oplossingen, identity servers met PKI infrastructuur dan wel het gebruik van certificaten en tokens. Een dergelijke infrastructuur is in het geval van de opties waarin de bevragingsapplicatie centraal worden beheerd is dit een randvoorwaarde voor de werking.

Controleerbaarheid

Audit Trail

De begeleidingscommissie heeft bij aanvang van het onderzoek aangegeven waarom controleerbaarheid van grootbelang moet worden geacht:

- het gaat om persoonsgegevens van burgers die bij bewerking ook patronen van gedrag blootleggen.
- misbruik van dergelijke gegevens kan grote persoonlijke gevolgen hebben
- misbruik van de wetenschap dat er naar een individu een onderzoek wordt verricht kan voor het individu, de onderzoeker of de Staat der Nederlanden verstrekkende gevolgen hebben.
- het niet juiste gebruik van onderzoeksgegevens kan verstrekkende persoonlijke gevolgen hebben.

Het wordt daarom van belang geacht om alle handelingen die met een gegeven worden verricht achteraf te kunnen beoordelen op rechtmatigheid, juistheid en volledigheid. De details met betrekking tot de inrichting van de Audit Trail is reeds besproken in paragraaf 4.1.2.

Het uitgangspunt bij de beoordeling van de implementatieopties op dit aspect is dat naarmate de complexiteit van de inrichting van de Audit Trail toeneemt de controleerbaarheid van de naleving van genomen maatregelen afneemt.

Vernietiging
De Europese richtlijn stelt dat na de retentieperiode de opgeslagen gegevens moeten worden vernietigd. In de ontwerpen is dit voor zover mogelijk meegenomen. Men moet zich echter realiseren dat de controle op de vernietiging vooral procedureel van aard is en nauwelijks met technische middelen in absolute zin kan worden afgedwongen.

Continuïteit van het bevragingsproces
De continuïteit van het bevragingsproces wordt afgemeten aan de lengte van het proces, ofwel het aantal processtappen dat in een implementatie ontwerpt moet worden doorlopen. Naarmate het aantal processtappen toeneemt neemt ook de kwetsbaarheid van het proces toe.
Tussen de verschillende implementatieopties bestaat een soort trade off. Daar waar in het centrale model op eenvoudige wijze redundancy in het systeem kan worden ingebouwd om het robuuster te maken is de impact van een eventueel falen vele malen groter dan in een decentraal model. In een decentraal model is de impact van falen kleiner dan in een centraal model maar het aantal te doorlopen processtappen (iteraties) is vele malen groter dan in een centraal model. Redundancy is daarom een relatief belangrijk element van alle implementatie opties.

De kosten voor redundantie van de systemen zijn in de berekening niet meegenomen omdat deze sterk afhangen van de analyse van de risico's die met het technische ontwerp en het organisatorische ontwerp van een daadwerkelijke implementatie samenhangen. Er zouden teveel aannames gedaan moeten worden ten aanzien van de beschikbaarheideisen en de wijze waarop deze worden ingevuld (fit rates, MTBF, MTTR, RTO RPO etc.) en dus aannames over de noodzakelijke apparatuur.

Beveiliging van toegangsnetwerken
Bij het ontwerpen van de implementatieopties is uitgegaan van versleutelde verbindingen daar waar in het ontwerpen sprake is van verbinding over afstand. Voor verbindingen die gebruik maken van het publieke netwerk, is dit in de technische ontwerpen aangegeven met een sleutel.
Dit is echter niet de enige te nemen maatregel. Op lokaal nivo zal het netwerkverkeer gescheiden moeten zijn door VPN’s en/of VLAN constructies. Per optie is aangegeven wat de minimumeisen zijn

4.2 Decentrale opslag, beantwoording door aanbieder

Algemene kenmerken:

1. Alle opslag van alle gegevens, zowel de verkeersgegevens als de NAW gegevens vindt plaats bij de aanbieder.
2. De beantwoording van de vragen van de behoeftesteller wordt door de aanbieder verzorgd binnen een afgesproken termijn na binnenkomst van de vordering. De aanbieder heeft dus een infrastructuur in termen van organisatie en technische middelen om de afhandeling van de vordering te verzorgen.

4.2.1 Informatie architectuur

Acquisitie van gegevens

1. Na acquisitie van de gegevens worden de gegevens geconverteerd naar een gestandaardiseerd formaat en opgeslagen.

Opslag van gegevens

2. De structuur van de database en het gegevensformaat wordt door de aanbieder naar behoefte bepaald en kan dus per aanbieder verschillen. Voor de berekeningen en onderlinge vergelijkbaarheid van de opties zijn we uitgegaan van hetzelfde databaseontwerp (zie bijlage H)

Gecorreleerd en niet-gecorreleerd

3. In de gecorreleerde variant wordt tijdens de conversie een koppeling aangebracht tussen de NAW-dienst-nummer gegevens en de verkeersgegevens.
4. In de niet-gecorreleerde variant is er sprake van twee gescheiden databasestructuren. In de ene structuur zijn de NAW-dienst-nummer gegevens opgeslagen in de andere zijn de verkeersgegevens opgeslagen. De databases zijn fysiek en logisch van elkaar gescheiden.

Bevraging

5. De vordering wordt door de behoeftesteller in de vorm van een 'document' aangeboden via een medium zoals fax, beveiligde e-mail of koerier.
6. Het antwoordt van de aanbieder wordt via hetzelfde medium verzonden als de vordering.

Gecorreleerd en niet-gecorreleerd

7. In de niet-gecorreleerde variant legt de aanbieder geen geautomatiseerde koppeling tussen de NAW gegevens en de verkeersgegevens van de dienst die de klant afneemt. Dit betekent dat de aanbieder twee vorderingen krijgt en twee applicaties moet raadplegen om tot een volledig antwoord te komen indien het onderzoek dit vereist.
8. In de gecorreleerde variant heeft de aanbieder één applicatie voor bevraging.

De snelheid van het bevragingsproces is in de gecorreleerde variant hoger dan in de niet-gecorreleerde variant. Dit heeft meerdere oorzaken:

- De behoeftesteller moet meerdere vragen stellen om zowel de NAW-dienst-nummer gegvens als de juiste (periode) verkeersgegevens te verkrijgen.
- De behoeftesteller heeft geen gegevens over bij welke aanbieder het object van onderzoek in de gevraagde periode klant was. Zelfs in het geval (variant Centrale Opslag) de behoeftesteller wel over de actuele NAW gegevens beschikt zoals in de huidige CIOT situatie wordt issue maar zeer ten dele opgelost gezien de verminderde trouw van de consument aan één leverancier.

4.2.2 Technische architectuur

De voornaamste kenmerken van deze implementatie liggen in het feit dat vrijwel alle kosten liggen binnen het domein van de aanbieder. De aanbieder houd hiermee een volledig overzicht over de bevragingen. Correlatie en opslag liggen bij de aanbieder. De aanbieder zal voor de eigen

organisatie een front-end moeten bieden om de bevraging op de database te doen. De kosten voor de daadwerkelijke bevraging zijn beduidend hoger aan de kant van de bevrager (zelf zoeken in de database) maar niet noodzakelijk lager voor behoeftesteller.

Acquisitie

De wijze waarop gegevens worden ontrokken aan de bronsystemen wordt bepaald door de ICT huishouding van de aanbieder.

Opslag

In gecorreleerde variant bestaat er een koppeling tussen de database met NAW gegevens dit in tegenstelling tot de niet gecorreleerde variant.

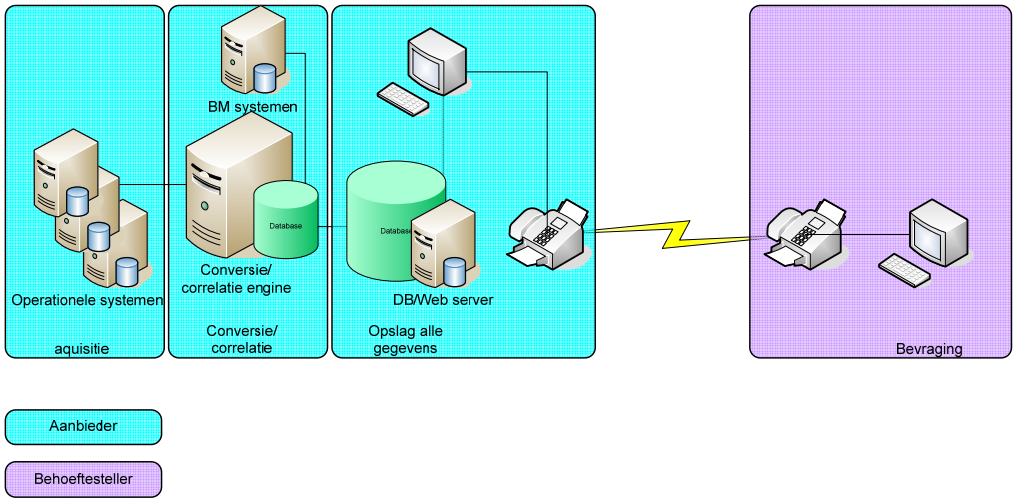
Bevraging

Bevraging vanuit de behoeftesteller vindt plaats met een niet geautomatiseerde user interface. Bij de aanbieder wordt gebruik gemaakt van een bevragingsapplicatie. In de gecorreleerde varianten is met één identificerend gegeven en in één vraagstelling zowel de volledige NAW gegevens op te vragen als de verkeersgegevens van de dienst. Voor alle ontworpen bedrijfsarchitecturen met geautomatiseerde bevraging geldt dat vanwege de eis van het voorkomen van 'data mining' de beperking is ingebouwd dat niet met één identificerend gegeven voor meerdere afgenomen diensten verkeersgegevens zijn op te vragen.

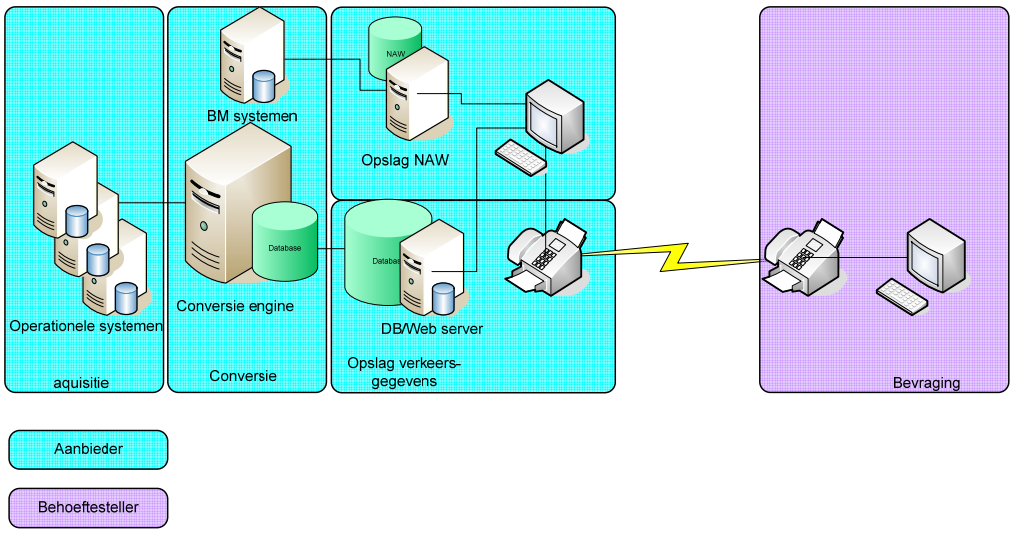
Procesconsequenties: Toetsing rechtmatigheid

De toetsing van de rechtmatigheid van de vordering (getoetst door OvJ/RC of hfd IV), juiste wetsartikel, vrager geautoriseerd) vindt per verzoek handmatig plaats door de organisatie van de aanbieder door het beoordelen van de inhoud van de vordering en de identiteit van de betrokken functionarissen.

De vaststelling van de authenticiteit van de vragensteller gebeurd op de traditionele manier door een combinatie van elementen: handtekening op een fysiek document, CLI van de fax dan wel de gecontroleerde authenticiteit van de beveiligde E-mail



Figuur 4-2: De gecorreleerde variant decentrale opslag beantwoording door aanbieder



Figuur 4-3: De niet gecorreleerde variant decentrale opslag beantwoording door aanbieder

4.2.3 Beheer

Kenmerken van het beheer

1. Er is geen verschil tussen de gecorreleerde en niet-gecorreleerde variant.
2. het zwaartepunt van de beheer ligt vrijwel geheel bij de aanbieder

4.2.4 Beveiliging

Kenmerken van de beveilging

Indien gebruik gemaakt wordt van een fax om de vordering en de beantwoording te verzenden is dit een zwak punt in de beveiliging omdat fouten gemaakt kunnen worden met de nummer invoer. Overwogen moet worden de fax in zijn geheel niet meer te gebruiken. Wanneer gebruikt wordt gemaakt van beveiligde e-mail is dit risico ondervangen. Fouten kunnen dan eveneens worden gemaakt echter de ontvanger kan zonder sleutel het bericht niet lezen.

In deze optie rust de vertrouwelijkheid van de bron van de vraag en het object van onderzoek op de integriteit van de betreffende medewerkers van de aanbieder. Indien de classificatie staatsgeheim voor het gehele bevragingsproces wordt gehanteerd dienen deze medewerkers te worden gescreend.

Toegang tot systemen

De systemen bij de aanbieder waarop de gegevens worden opgeslagen, bevinden zich in een aparte beveiligde zone van het netwerk zonder andere applicaties. Dit netwerkgedeelte is controleerbaar van de rest van het aanbiedernetwerk gescheiden door tenminste een firewall die alleen het versturen van verkeersgegevens uit de productiesystemen toelaat. De bevragingsterminal

bevindt zich eveneens in deze afgeschermde zone en heeft verder geen andere communicatiemogelijkheden, behoudens het verzenden en ontvangen van E-mail die voor het proces noodzakelijk is.
Voor het inloggen op de bevragingsterminal is "strong authentication" vereist.

Audit Trail
De controleerbaarheid is in deze optie afhankelijk van een eenduidige set van eisen met betrekking tot de procesinrichting, archivering en rapportage aan de kant van zowel de aanbieder als de behoeftesteller. De inrichting van de audit trail is omvangrijk en door de hoeveelheid minder of meer autonome partijen aan de kant van de aanbieders en behoeftestellers de complexiteit van uitvoering van een gedegen controle op groot.

De aanbieder bewaart de aanvraag en een kopie van de gegeven antwoorden. Het bevragingsproces bij de aanbieder is zodanig dat gelogd wordt welke gegevens uit de database(s) worden opgevraagd en door wie.

Continuïteit
De continuïteit van het bevragingsproces is afhankelijk van de maatregelen die door de individuele aanbieder zijn genomen. De impact van een verstoring bij een aanbieder is afhankelijk van de ernst van het onderzoek dat door de behoeftesteller is ingesteld en het belangt van de opgevraagde gegevens voor dat onderzoek. Het is echter onwaarschijnlijk dat het bevragingsproces als geheel verstoord wordt.
Zie voor overige informatie paragraaf 4.1.4. met betrekking tot de *continuïteit van het bevragingsproces*.

4.3 Decentrale opslag, directe toegang

4.3.1 Informatie architectuur

Acquisitie van gegevens
1. Na acquisitie van de gegevens worden de gegevens geconverteerd naar een gestandaardiseerd landelijk uniform formaat.

Opslag van gegevens
2. De gegevens worden na conversie en opgeslagen in een database(s) die voldoen aan een op landelijk niveau vastgestelde architectuur (zie database ontwerp in bijlage H).

Gecorreleerd en niet-gecorreleerd
3. In de gecorreleerde variant is er sprake van twee gescheiden databasestructuren. In de ene structuur zijn de NAW-dienst-nummer gegevens opgeslagen in de andere zijn de verkeersgegevens opgeslagen. De databases zijn fysiek en logisch van elkaar gescheiden.

Bevraging

4. In deze optie wordt één applicatie voor de bevraging gebruikt met een gestandaardiseerde user interface.
5. Het antwoordt van de aanbieder wordt in dezelfde applicatie aangeboden.

Gecorreleerd en niet-gecorreleerd

6. In de gecorreleerde variant kan de behoeftesteller aan de hand van een identificerend gegeven in één vraag stellen met betrekking tot de periode waarover de verkeersgegevens worden opgevraagd.
7. In de niet-gecorreleerde variant betekent dit dat de aanbieder twee vragen moet stellen om tot een antwoord te komen indien de vordering dit vereist.
8. De snelheid van het bevragingsproces is in de gecorreleerde variant is gelijk aan de snelheid in de niet-gecorreleerde variant.

Toetsing rechtmatigheid

1. De vordering wordt door de behoeftesteller in de bevragingsapplicatie ingevoerd met gebruik van de gestandaardiseerde user interface.
2. Na invoer dient de vraag geauthoriseerd te worden door de Officier van Justitie of de Rechter Commissaris. Deze doet dat in de betreffende applicatie. Deze moet dus onderscheid kunnen maken tussen functionarissen die geautoriseerd zijn een vraag te stellen en die de vraag mogen goedkeuren. In de stap vind ook de verificatie van het juiste wetsartikel plaats.
3. De applicatie stelt de vraag aan de database van de betreffende aanbieder en presenteert het antwoord aan de bevrager.

Opgemerkt zij dat in deze variant de aanbieder geen inhoudelijke controle op de rechtmatigheid van de vraag kan doen.

4.3.2 Technische architectuur

Acquisitie

Geen bijzonderheden.

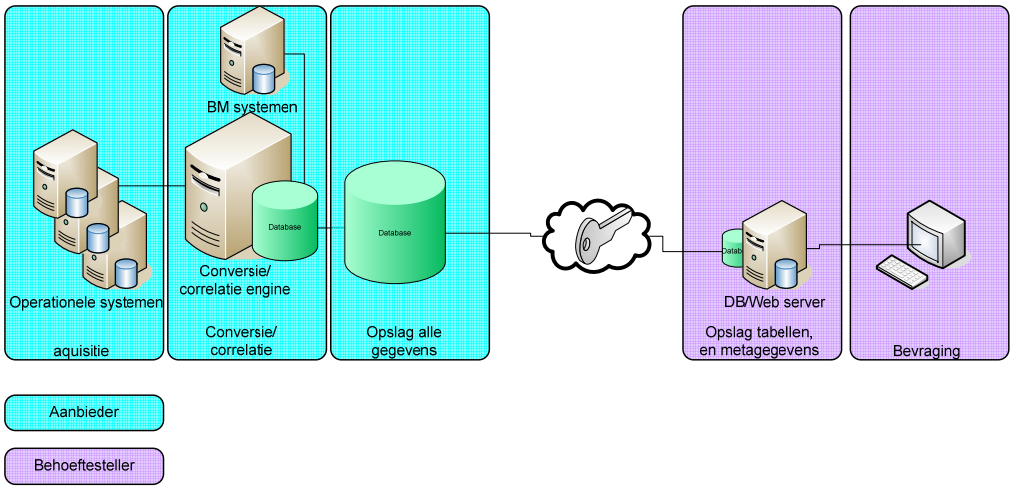
Opslag

In deze optie is sprake van een gestructureerde opslag van data conform een uniform database model.
De implementatie optie gaat uit aan de kant van de behoeftesteller uit van de opstelling van een machine die fungeert als portal voor de bevraging en een centrale databaseserver met daarin de paden naar de verschillende decentrale databases van de aanbieders.

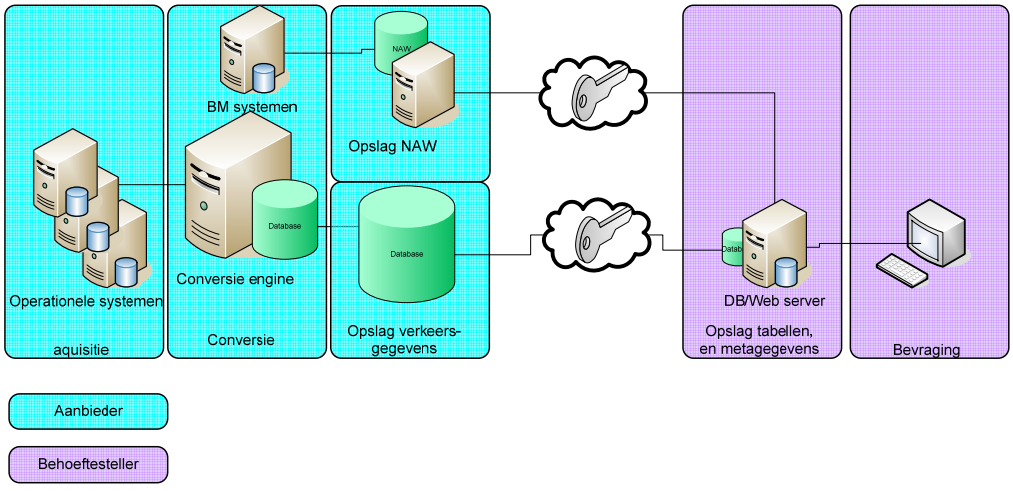
Bevraging

In deze optie is voorzien in een centraal beheerde bevragingsapplicatie welke de verbinding tussen de behoeftesteller en aanbieder verzorgt.

Bijzonder kenmerk van de optie is dat door het ontbreken van directe kennis aan de kant van de behoeftesteller van welke persoon in een bepaalde periode klant is geweest van een bepaalde aanbieder het bevraginssysteem de vraag van de behoeftesteller aan de databases van meerdere aanbieders stelt totdat de juiste aanbieder is gevonden. Over het netwerk vindt er dus veel verkeer plaats dat niet direct leidt tot een antwoordt op de vordering. Beantwoording van een vraag kan dus kort of langer duren (maximaal ongeveer een half uur) afhankelijk van hoe snel de juiste aanbieder is gevonden. In de niet gecorreleerde variant duurt het hele proces van bevraging van verkeersgegevens langer dan in de gecorreleerde variant.



Figuur 4-4: De gecorreleerde variant decentrale opslag en directe toegang



Figuur 4-5: De niet gecorreleerde variant decentrale en directe toegang

4.3.3 Beheer

Het beheer van deze bedrijfsarchitectuur is een complexe zaak door het ontbreken van duidelijke centrale regie. Er zijn veel partijen die allen een deel van de totale werking van de implementatieoptie verzorgen.

In de optie is er vanuit gegaan dat het beheer van de bevragingsapplicatie op een centraal punt bij de behoeftesteller plaatsvindt. Er is geen technische belemmering om de gezamenlijke aanbieders het beheer op zich te laten nemen maar omdat het belang van de bevraging bij de behoeftesteller ligt leek het plausibel het beheer daar onder te brengen.

4.3.4 Beveiliging

Het beheer van autorisaties en de authenticatie van de 'bevrager' verloopt via het beheer van de bevragingsapplicatie waar ook de logging plaatsvindt van de bevragingshandelingen.

Audit trail

Centraal in de bevragingsapplicatie wordt gelogd:

- Inhoud van de vraag
- Verkregen antwoord
- Toepasselijk wetsartikel
- Identiteit van de vraagsteller
- Identiteit van de goedkeurende OvJ/RC
- Tijdstip van vraag
- Tijdstip van goedkeuring
- Tijdstip van beantwoording

In de database van de aanbieder wordt gelogd:

- Inhoud van de vraag
- Verstuurde antwoord
- Identiteit van de vraagsteller
- Tijdstip van vraag/beantwoording

Toegang tot de systemen

De systemen bij de aanbieder waarop de gegevens worden opgeslagen, bevinden zich in een aparte beveiligde zone van het netwerk zonder andere applicaties. Dit netwerkgedeelte is controleerbaar van de rest van het aanbiedernetwerk gescheiden door tenminste een firewall die alleen het versturen van verkeersgegevens uit de productiesystemen, en het opzetten van een VPN vanuit de behoeftesteller, toelaat.

De communicatie tussen behoefsteller en aanbieder verloopt via een VPN (IPSEC) over internet waarbij de VPN-routers zich aan elkaar identificeren met certificaten. Deze VPN-routers bevinden zich direct aan het beveiligde netwerkgedeelte.

De bevragingsterminal en de portal bij de behoeftesteller bevinden zich eveneens in een afgeschermde zone en heeft verder geen andere communicatiemogelijkheden. Voor het inloggen op de bevragingsterminal is "strong authentication" vereist

De OvJ/RC heeft toegang tot de applicatie nodig voor het goedkeuren van aanvragen. Deze toegang vindt plaats via een webinterface over een beveiligde (SSL) verbinding. Er moet ingelogd worden door middel van strong authentication.

Continuïteit

Zie voor overige informatie paragraaf 4.1.4. met betrekking tot de *continuïteit van het bevragingsproces*.

4.4 Centrale opslag, directe toegang

4.4.1 Informatie architectuur

Acquisitie

Na de onttrekking en conversie van gegevens worden de data tijdelijk opgeslagen bij de aanbieder.

Opslag

De tijdelijk opgeslagen gegeven worden dagelijks via een beveiligde verbinding verzonden naar de centrale databases van de intermediaire 3e.

De consequenties van een gecorreleerde of niet gecorreleerde opslag zijn eerder beschreven.

Bevraging

Er is in deze optie voorzien in een centraal beheerde bevragingsapplicatie.

Toetsing rechtmatigheid

Vindt op dezelfde manier plaats als bij de vorige optie.

4.4.2 Technische architectuur

Acquisitie

Na de onttrekking en conversie van gegevens worden de data tijdelijk opgeslagen bij de aanbieder.

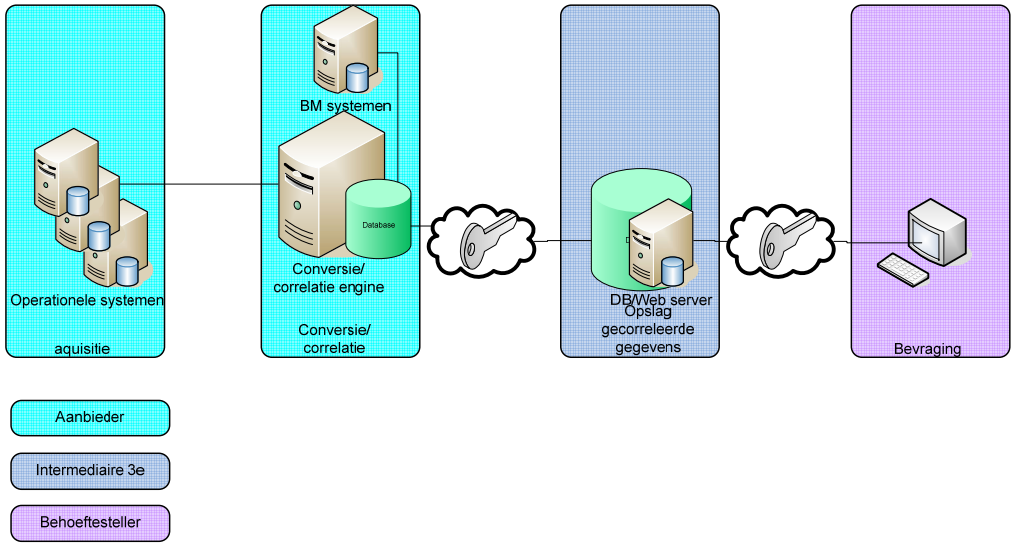
Opslag

De tijdelijk opgeslagen gegeven worden dagelijks via een VPN verbinding verzonden naar de centrale databases van de intermediaire behoeftesteller. Door de hoeveelheid data die moet worden verzonden is in het ontwerp van de optie rekening gehouden met voldoende netwerk capaciteit. Hoewel er (logisch) sprake is van centrale opslag bij een intermediair derde kan de database deels fysiek decentraal opgeslagen zijn.

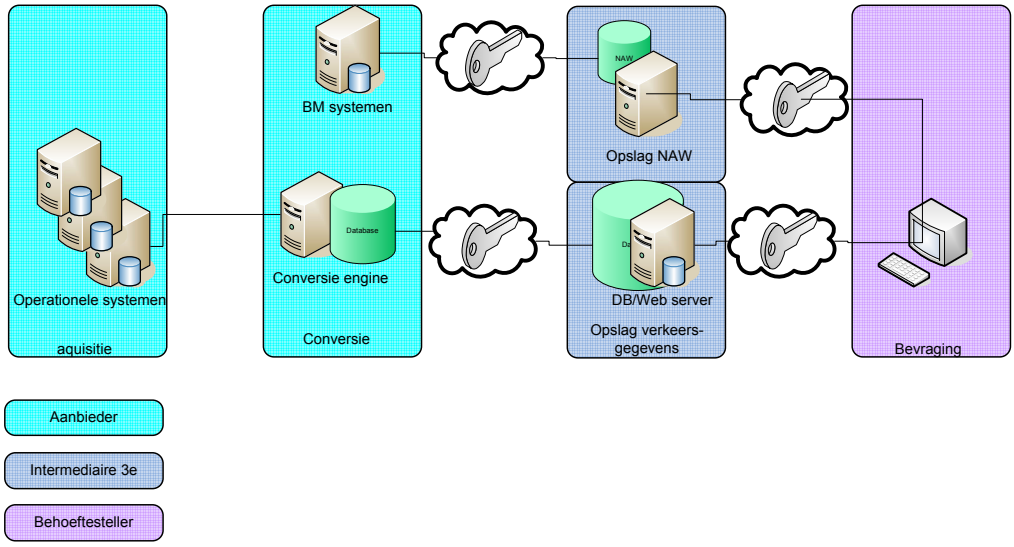
De consequenties van een gecorreleerde of niet gecorreleerde opslag zijn eerder beschreven.

Bevraging

Er is in deze optie voorzien in een centraal beheerde bevragingsapplicatie.



Figuur 4-6: De gecorreleerde variant Centrale opslag en direct toegang



Figuur 4-7: De niet gecorreleerde variant Centrale opslag en directe toegang

4.4.3 Beheer

In deze optie ligt het zwaartepunt van het beheer bij de intermediaire 3e.

4.4.4 Beveiliging

In deze optie is kenmerkend dat aan de ene kant er een grote impact te verwachten is van het falen van beveiligingsmaatregelen (inbeuk op de exclusiviteit, continuïteit van het bevragingsproces en misbruik van gegevens) maar ander andere kant door de overzichtelijke situatie het ook vrij eenvoudig is om maatregelen te nemen.

Bijzondere aandacht voor de controleerbaarheid, de Audit Trail is in deze optie noodzakelijk omdat zonder adequate maatregelen een eventueel oneigenlijk gebruik van gegevens gemakkelijk over het hoofd kan worden gezien. Het daadwerkelijk uitvoeren van periodieke onafhankelijke audits is noodzakelijk om te gemoet te komen aan de eisen die worden gesteld.

Ook is van belang in deze optie binnen welk domein de intermediaire 3e wordt geplaats, in geval van een onafhankelijke intermediaire derde zijn de mogelijkheden om de controleerbaarheid vorm te geven groter dan in het geval de intermediaire 3e zich binnen het domein van de behoeftesteller bevindt. Het genoemde verschil komt voort door de scheiding van verantwoordelijkheden en bevoegdheden die dan mogelijk is tussen de belanghebbende partij bij het verkrijgen van informatie (de behoeftesteller) en een belanghebbende partij die slechts de verantwoordelijkheid heeft om deze informatie op een controleerbare en juiste wijze te verstrekken.

Audit trail

Centraal in de bevragingsapplicatie wordt gelogd:

- Inhoud van de vraag
- Verkregen antwoord
- Toepasselijk wetsartikel
- Identiteit van de vraagsteller
- Identiteit van de goedkeurende OvJ/RC
- Tijdstip van vraag
- Tijdstip van goedkeuring
- Tijdstip van beantwoording

In de database van de intermediair wordt gelogd:

- Inhoud van de vraag
- Verstuurde antwoord
- Identiteit van de vraagsteller
- Tijdstip van vraag/beantwoording

Toegang tot de systemen

De systemen bij de intermediair waarop de gegevens worden opgeslagen, bevinden zich in een aparte beveiligde zone van het netwerk zonder andere applicaties. Dit netwerkgedeelte is controleerbaar van de rest van het aanbiedernetwerk gescheiden door tenminste een firewall die alleen het versturen van verkeersgegevens uit de productiesystemen, en het opzetten van een VPN vanuit de aanbieder en behoeftesteller, toelaat.

De communicatie tussen behoefsteller en aanbieder enerzijds en de intermediair anderzijds verloopt via een VPN (IPSEC) over internet waarbij de VPN-routers zich aan elkaar identificeren met certificaten. Deze VPN-routers bevinden zich direct aan het beveiligde netwerkgedeelte. Voor het afleveren van gegevens door de aanbieder aan de intermediair wordt Secure FTP (SFTP) gebruikt.

De bevragingsterminal en de portal bij de behoeftesteller bevinden zich eveneens in een afgeschermde zone en heeft verder geen andere communicatiemogelijkheden. Voor het inloggen op de bevragingsterminal is "strong authentication" vereist.

Toegang tot de systemen van de intermediair, anders dan voor afleveren van gegevens of uitvoeren van bevragingen, is voorbehouden aan gescreend beheerpersoneel van de intermediair.

De OvJ/RC of hoofd I&V dienst heeft toegang tot de applicatie nodig voor het goedkeuren van aanvragen. Deze toegang vindt plaats via een webinterface over een beveiligde (SSL) verbinding. Er moet ingelogd worden door middel van strong authentication.

Continuïteit
De centrale systemen bij de intermediair moeten mogelijk redundant zijn uitgevoerd. Zie voor overige informatie paragraaf 4.1.4. met betrekking tot de *continuïteit van het bevragingsproces*.

4.5 Hybride opslag, directe toegang

4.5.1 Informatie architectuur

Acquisitie
Na de onttrekking en conversie van gegevens worden de NAW data tijdelijk opgeslagen bij de aanbieder. De verkeersgegeven worden permanent opgeslagen bij de aanbieder.

Opslag
In deze implementatie optie vindt de oplag van NAW gegevens plaats bij een intermediaire 3e en de opslag van verkeersgegevens binnen het domein van de aanbieder.
De NAW data worden via een beveiligde verbinding van de aanbieder naar intermediaire derde verzonden waarna deze de gegevens NAW gegevens opslaat.

Bevraging
De wijze van bevraging is gelijk aan de wijze van bevraging in de centrale optie.

Toetsing rechtmatigheid
Vindt op dezelfde manier plaats als bij de vorige optie.

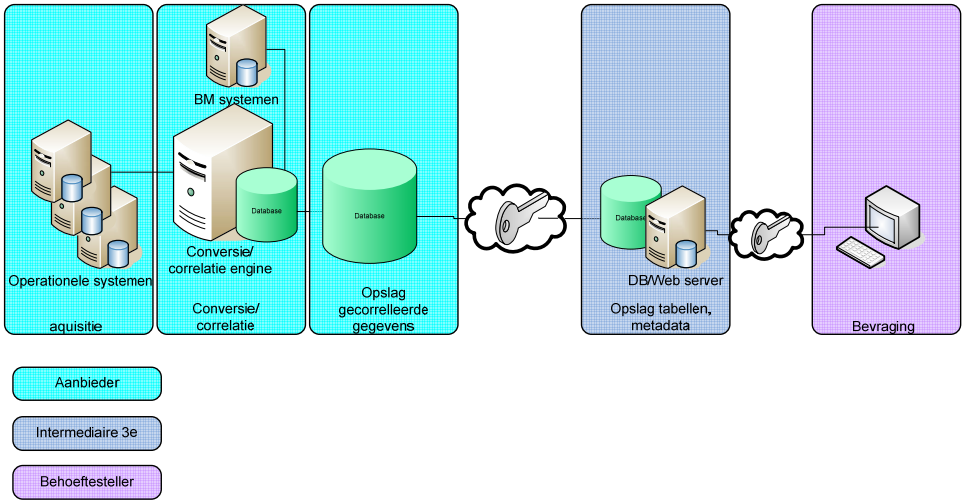
4.5.2 Technische architectuur

Acquisitie
Geen bijzonderheden ten opzichte van de andere opties.

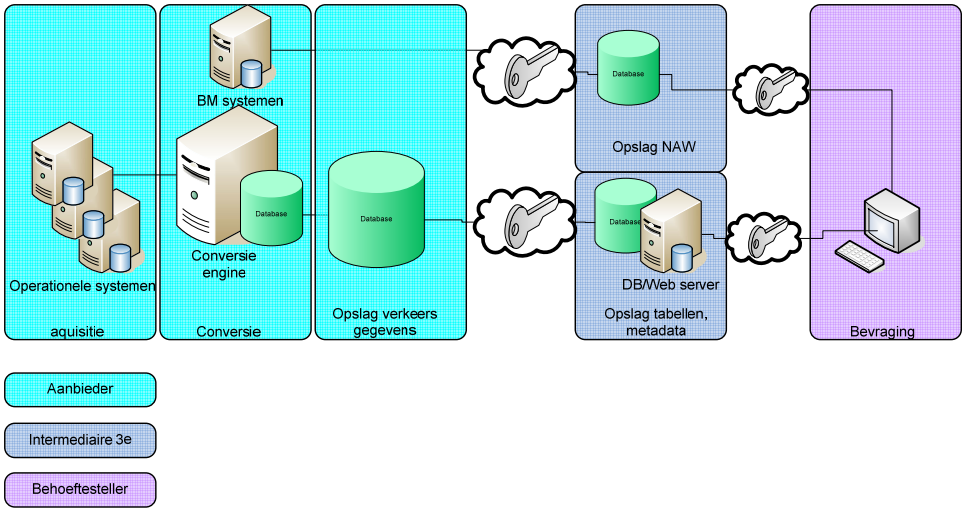
Opslag
In deze optie is er sprake van een opslagsysteem voor de NAW gegevens bij de intermediaire derde en heeft elke aanbieder een opslagsysteem voor de verkeersgegevens.

Bevraging

De bevraging wordt op de zelfde wijze vorm gegeven als in de centrale optie. Zij het dat hier een beveiligde verbinding van het domein van de aanbieder naar de decentrale database in het domein van de aanbieder is gemaakt om de opgeslagen te kunnen bevragen.



Figuur 4-8: De gecorreleerde variant Hybride Opslag en directe toegang



Figuur 4-9: De niet gecorreleerde variant Hybride opslag en directe toegang

4.5.3 Beheer

In deze bedrijfsarchitectuur is het beheer van alle automatiseringsmiddelen verdeeld tussen de intermediaire derde en de aanbieder.

4.5.4 Beveiliging

De beveiliging is vrijwel gelijk aan de beveiliging in de centrale optie zijn het dat vanwege het feit dat de verkeersgegevens bij de aanbieder zijn opgeslagen deze ook het beheer heeft van de beveiligingsvoorzieningen die in zijn domein noodzakelijk is. Het betekent ook dat in afwijking tot de centrale optie de beheerder van de aanbieder instaat moet zijn de bevragingsinterface in relatie tot de opgeslagen data moet kunnen testen.

Audit Trail

Centraal in de bevragingsapplicatie wordt gelogd:

- Inhoud van de vraag
- Verkregen antwoord
- Toepasselijk wetsartikel
- Identiteit van de vraagsteller
- Identiteit van de goedkeurende OvJ/RC of hfd IV dienst
- Tijdstip van vraag
- Tijdstip van goedkeuring
- Tijdstip van beantwoording

In de database van de intermediair wordt gelogd:

- Inhoud van de vraag
- Verstuurde antwoord
- Identiteit van de vraagsteller
- Tijdstip van vraag/beantwoording

In de database van de aanbieder wordt gelogd:

- Inhoud van de vraag
- Verstuurde antwoord
- Identiteit van de vraagsteller
- Tijdstip van vraag/beantwoording

Toegang tot de systemen

Hiervoor geldt hetzelfde als beschreven bij de vorige optie.

Continuïteit

De centrale systemen bij de intermediair moeten mogelijk redundant zijn uitgevoerd. Zie voor overige informatie paragraaf 4.1.4. met betrekking tot de *continuïteit van het bevragingsproces*.

5 Uitkomsten

In hoofdstuk 4 is een uiteenzetting gegeven over de informatiearchitectuur en technische architectuur voor elk van de implementatieopties. Deze vormen de basis voor de kostenschattingen in het kwantitatieve model en voor de beoordeling over de mate waarin aan diverse eisen en criteria wordt voldaan in het kwalitatieve model.

In dit hoofdstuk wordt voor elk van de implementatieopties de uitkomst van het kwantitatieve en kwalitatieve model gegeven met een korte toelichting over hoe de resultaten geïnterpreteerd kunnen worden.

5.1 Algemene bevindingen

Bij aanvang van het onderzoek is voor de te bewaren data uitgegaan van de dataset opgesteld door de behoeftestellers. Deze dataset stuitte op veel weerstand bij de aanbieders. Belangrijkste argumenten van de aanbieders waren de uitbreiding van de te bewaren informatie in vergelijking met de richtlijn dataretentie en de onduidelijke definitie van sommige velden. Na overleg tussen aanbieders, behoeftestellers en justitie op 22 juni jongstleden zijn op advies van de werkgroep wetgeving een aantal velden verwijderd. De velden waarom het gaat zijn betalingsgegevens, paalnummers of locatiegegevens gedurende een communicatie en de locatie waar de lijn is gemonteerd. Deze moeizame start heeft belemmerend gewerkt bij de uitvoering van het onderzoek.

De doelstelling van het veldonderzoek is geweest om concrete, door de aanbieders gedragen informatie te verzamelen over organisatie en processen, technische haalbaarheid, kosten en beveiligingsaangelegenheden. Daarbij is gebruik gemaakt van interviews en een vragenlijst die schriftelijke beantwoord kon worden. Er zijn 14 aanbieders benaderd voor het maken van een afspraak op locatie van de aanbieder. Tijdens het eerste gesprek is in anderhalf uur een toelichting gegeven op het onderzoek en de vragenlijst en wat van de aanbieder verwacht wordt aan op te leveren informatie. Tijdens het veldonderzoek kwam de gevraagde informatie laat beschikbaar, pas in de loop van augustus, begin september is een deel van de gevraagd informatie aangeleverd. Meer concreet in getallen uitgedrukt is de response op de vragenlijst als volgt.

Tabel 5-1: response op de vragenlijst

Vragenlijst veldonderzoek met response	# Volledig beantwoord	# Gedeeltelijk beantwoord	# Niet beantwoord
Organisatie			
Geef een zo compleet mogelijk overzicht van uw huidig klanten bestand, diensten en gegenereerde verkeersgegevens met mutaties.	10	3	1
Welke organisatorische aanpassingen zijn nodig voor de invoering.	5	4	5
Welke velden kunnen opgevraagd worden (en welke niet).	4	6	4
Techniek			
Wat is er technisch nodig om de info uit de netwerk systemen te halen.	5	6	3
Hoeveel systemen zijn hierbij betrokken.	5	4	5
Hoeveel verschillende opslag formaten zijn er.	3	4	7
Welke koppelingen zijn er nodig om te converteren en bevragen.	3	6	5
Opslag			
Wat is de omvang om alle gegevens 1 jaar op te slaan.	3	7	4
Wat is de benodigde FTE capaciteit om gegevens op te slaan.	5	7	2
Wat zijn de Hardware kosten voor opslag.	2	7	5
Bevraging			
Wat is de inspanning om gegevens uit het netwerk te halen.	5	5	4
Welke tools worden nu gebruikt voor bevraging.	3	7	4
Wat is de benodigde FTE capaciteit om gegevens op te vragen.	3	5	6
Wat wordt er op dit moment bevraagd (aantallen + type bevraging)	7	3	4
Wat zijn de Hard- en software investeringen voor bevraging.	3	4	7
Beveiliging			
Heeft u een beveiligingsplan voor deze activiteit.	7	5	2
Verwacht u issues m.b.t. de beveiliging als gevolg van de uitbreiding van de bewaarplicht (en zo ja welke?)	2	4	8
Heeft u specifieke maatregelen genomen voor de continiteit.	3		11

Bovenstaand resultaat is gebaseerd op 9 ontvangen vragenlijsten, 8 schriftelijk en 1 telefonisch. Het feit dat op onderdelen soms meer dan 9 antwoorden zijn is het gevolg van de gesprekken die met de aanbieders gevoerd zijn. Deze gesprekken zijn gehouden voorafgaand aan het invullen van de lijst en naderhand ter toelichting of verificatie van gegevens. Het aantal gevoerde gesprekken is als volgt:

Tabel 5-2: aantal en doel gesprekken met aanbieders

Gesprekken met aanbieders	**Aantal**
interview op locatie van de aanbieder	9
Telefonisch interview	4
Telefonische beantwoording van de vragenlijst	1
Mondelinge toelichting op de schriftelijk beantwoordde vragenlijst, waarvan 1gesprek op locatie aanbieder	5
Telefonische verificatie op volledigheid en juistheid van ontwerpuitgangspunten en modellering	4

Alle geïnterviewde aanbieders hebben aangegeven dat de implementatie van de richtlijn dataretentie een zware en complexe uitdaging wordt die veel tijd en grote investeringen met zich mee brengt en een grote impact heeft op de bedrijfsvoering. Goede afstemming en planning is noodzakelijk vooral omdat de huidige bevraging ook al veel vragen oproept. Indien over een jaar de

wet ingevoerd gaat worden, dan zullen de meeste aanbieders volgens de onderzoekers nog niet klaar zijn om hieraan volledig te voldoen.

Voor de groep van kleinste ISP aanbieders is vanuit meerdere bronnen aangegeven dat zij niet in staat zijn om investeringen groter dan € 10.000 voor hun rekening te nemen. Deze stelling is door de onderzoekers niet bij de individuele bedrijven geverifieerd.

Er is de aanbieders veel aan gelegen om een goed proces voor de bevraging en autorisatie te implementeren. Het belang ervan is vooral groot bij de implementatieopties waarbij er geen inhoudelijke betrokkenheid van de aanbieder is bij casus. Regelmatige audits worden van groot belang van belang om vertrouwen in de rechtmatigheid en zorgvuldigheid van de gevolgde procedures te behouden.

De omvang van de totale opslag is berekend op 365 TB aan informatie aan het eind van het eerste jaar.

De aandacht in het onderzoek is sterk gericht geweest op de toekomstige situatie. Zowel tijdens het vooronderzoek als het veldonderzoek is gebleken dat de betrokkenen gefocusseerd waren op de toekomst en de consequenties van de Richtlijn Dataretentie. De eisen en wensen van de aanbieders en behoeftestellers reflecteren wel de onvrede met de huidige werkwijze voor opslag en bevraging van identificerende gegevens en verkeersgegevens.

5.2 Scoreoverzicht van de beoordeling

Overzicht van de scores van de kwalitatieve beoordeling
Het verschil tussen de gecorreleerde en niet gecorreleerde variant van een implementatie optie bleek niet voldoende groot om relevant te zijn voor de kwalitatieve beoordeling. De verschillen tussen de vier hoofdvormen van de implementatieopties bleek vele malen groter. Daarom wordt in de onderstaande tabel de vier hoofdvormen van de implementatieopties weergegeven. De hoogste scores voor iedere categorie zijn **vet** gedrukt de laagste scores *italic*.

Tabel 5-3: Totaal overzicht van de kwalitatieve beoordeling

Categorie	Decentrale opslag beantwoording door aanbieder	Decentrale opslag directe toegang	Centrale opslag directe toegang	Hybride opslag directe toegang
Organisatie en processen	12	*9*	**18**	**18**
Technologie	18	10,2	**20,1**	**20,1**
Business Case	**7,5**	*0*	2,5	2,5
Informatiebeveiliging	4	11	**20**	15
Implementatie termijn	**10**	*0*	*0*	*0*
Totaal	51,5	30,2	**60,6**	55,6

De implementatieoptie Decentrale opslag, beantwoording door aanbieder scoort veel hoger dan de decentrale optie met directe toegang. Op de categorie informatiebeveiliging laat deze optie echter punten liggen. Hierbij moet worden opgemerkt dat deze score alleen gebaseerd is op de onderliggende criteria van het model en niet een uitspraak doet over het gehele beveiligingsniveau van de implementatieoptie. Op de categorie implementatietermijn is deze optie binnen een jaar na de start van de implementatie te realiseren

De implementatie optie Decentrale opslag en directe toegang scoort het laagst op bijna alle categorieën. Alleen in de categorie informatiebeveiliging neemt deze optie een lage middenpositie in.

De implementatie optie Centrale opslag met directe toegang scoort in bij alle categorieën (mede) als hoogste. De implementatietermijn wordt geschat op meer dan een jaar na de start van de implementatie.

De implementatieoptie Hybride opslag en directe toegang scoort in vrijwel alle categorieën gelijk aan de optie Centrale opslag directe toegang. In de categorie informatiebeveiliging scoort deze optie iets lager maar wel weer hoger dan de andere opties. Ook bij deze optie wordt ingeschat dat de implementatietermijn langer is dan een jaar.

In pagraaf 5.3 wordt de betekenis van de kwalitatieve uitkomsten voor de beantwoording van de onderzoeksvragen uitgewerkt en de implementatieopties in meer detail besproken.
In de Bijlage I vindt u het totaaloverzicht van de scores van de kwalitatieve beoordeling.

Overzicht van de scores van de kwantitatieve beoordeling
Voor het globale scoreoverzicht zijn de scores van CAPEX en vijf jaar OPEX voor alle drie de processen en actoren bij elkaar opgeteld weergegeven. Ook zijn de puntenscores van het kwalitatieve model ter vergelijk weergegeven. De beste (meest voordelige) scores zijn vet weergegeven.

Tabel 5-4: scoreoverzicht voor de acht implementatieopties

Implementatie optie		**In € over vijf jaar**	**punten**
Decentrale opslag, beantwoording door aanbieder	Gecorreleerd	€ 154.800.000	51.5
	Ongecorreleerd	€ 157.810.000	51.5
Decentrale opslag, directe toegang	Gecorreleerd	€ 141.580.000	30.2
	Ongecorreleerd	€ 146.100.000	30.2
Centrale opslag, directe toegang	Gecorreleerd	**€ 133.800.000**	**60.6**
	Ongecorreleerd	€ 135.350.000	**60.6**
Hybride opslag, directe toegang	Gecorreleerd	€ 148.320.000	55.6
	Ongecorreleerd	€ 147.340.000	55.6

Het financiële verschil tussen de duurste en goedkoopste implementatieoptie is 24 miljoen euro. De centrale opslag met directe toegang leidt zowel tot de laagste kosten als tot de hoogste score in het

kwantitatief model. Het is echter al te eenvoudig om op basis van deze getallen tot de conclusie te komen dat de centrale optie dus de beste implementatieoptie is. De volgende paragrafen gaan aan de hand van de onderzoeksvragen dieper in op de achterliggende informatie.

5.3 Beantwoording van de onderzoeksvragen op basis van het kwalitatieve model

Onderzoeksvraag 1
Welke eisen en criteria stellen de betrokken partijen (aanbieders, behoeftestellers) aan de opslag en bevraging van verkeersgegevens?

Beantwoording onderzoeksvraag 1
De inventarisatie van eisen en wensen die in de fase van het vooronderzoek is gedaan is in de startbijeenkomst bij de betrokken partijen geverifieerd. Het overzicht van deze eisen en wensen is weergegeven in bijlage C.

Bij de opbouw van de kwalitatieve beoordeling zijn de onderscheidende en keuzebepalende eisen opgenomen in het kwalitatieve beoordelingsmodel (zie bijlage D). Veel van de criteria in het model zijn terug te voeren op de eisen en criteria vanuit de aanbieders en de behoeftestellers. De overige criteria in het beoordelingsmodel zijn direct terug te voeren op overige onderzoeksvragen.

Onderzoeksvraag 2
Hoe is de huidige werkwijze rond de opslag en bevraging van verkeersgegevens en voldoet die aan de genoemde eisen en criteria? Op welke punten schiet de bestaande werkwijze tekort en hoe kan dit worden ondervangen?

Beantwoording onderzoeksvraag 2
De huidige werkwijze lijkt op globaal niveau, wanneer niet naar de meer technisch inhoudelijke componenten wordt gekeken, veel op de manier van werken in de implementatieoptie Decentrale opslag beantwoording door aanbieder. In redelijkheid is aan te nemen dat de huidige situatie in het kwalitatieve model veel overeenkomsten zal vertonen met de scores van de optie Decentrale opslag beantwoording door aanbieder.

De aandacht van alle partijen in het onderzoek is vooral gericht geweest op de toekomstige situatie. Het is gebleken dat alle betrokkenen gefocusseerd waren op de toekomst en de consequenties daarvan. De eisen en wensen van de aanbieders en behoeftestellers die naar voren zijn gekomen reflecteren wel de onvrede met sommige punten in de huidige situatie. Dit heeft zijn weerslag gevonden in bijvoorbeeld de wens van de behoeftesteller om het bevragingsproces sneller te laten verlopen en de wens van de aanbieders om een actieve toetsing te kunnen blijven doen op de rechtmatigheid van een vordering.

Onderzoeksvraag 3

Wat is de impact op de aanbieders, respectievelijk de overheid, bij 4 verschillende modellen van opslag en bevraging van gegevens, waarbij wordt gekeken naar:

- welke voorzieningen zijn reeds aanwezig;
- welke uitbreiding op deze voorzieningen is nodig;
- welke nieuwe voorzieningen moeten worden ontwikkeld.

Beantwoording van onderzoeksvaag 3

Op basis van de globale ontwerpen van de implementatieopties is een inschatting gemaakt van de impact van de verschillende implementatieopties. Daarbij is gebruik gemaakt van de kennis van de onderzoekers over situatie bij de aanbieders en het CIOT onder meer verkregen tijdens het vooronderzoek en veldonderzoek.

In het kwalitatieve beoordelingsmodel is deze onderzoeksvraag ondergebracht in de categorie Technologie, aansluiting van de gebruikte technologie op de huidige situatie en toekomstvastheid van de gebruikte technologie.
We zien dat de voor wat betreft de impact een drietal opties een vrijwel gelijk aantal punten halen en alleen de optie Decentrale Opslag met Directe toegang duidelijk minder scoort.
De overige deelvragen zijn inhoudelijk verwerkt in de ontwerpen van de Implementatieopties. In alle opties is het duidelijk is dat gegevens bij de aanbieders aan een diversiteit aan bronnen moet worden onttrokken. Indien er wordt gekozen voor geautomatiseerde bevraging door de behoeftesteller moet rekening gehouden worden met de noodzaak tot gestandaardiseerde gegevensopslag. Dit betekent dat voor die implementatieopties waarin sprake van is geautomatiseerde bevraging door de behoeftesteller, rekening gehouden moet worden met aanzienlijke nieuwbouw. In de kwantitatieve beantwoording is dit in de kostenverschuivingen tussen de actoren in het veld weergegeven.

Onderzoeksvragen 5 en 6

(5) Hoe (met welk(e) van de 4 beschreven modellen) kan het best worden gewaarborgd dat de gegevens:

- niet toegankelijk zijn voor andere doeleinden dan die genoemd in de Richtlijn dataretentie;
- uitsluitend worden geraadpleegd door personen die daarvoor vanwege hun wettelijke taakuitvoering in aanmerking komen;
- na afloop van de bewaartermijn worden verwijderd of vernietigd, en;
- beschikbaar zijn voor het leveren van statistieken aan de Commissie.

(6) Hoe (met welk model) kan het beste worden gewaarborgd dat de in de richtlijn genoemde beginselen van gegevensbeveiliging in acht worden genomen?

Onderzoeksvragen 5 en 6 zijn vrijwel in zijn geheel als in het kwalitatieve model opgenomen in de categorie 'Informatiebeveiliging'. De vraag over de levering van statistieken aan de Europese Commissie is ondergebracht binnen de categorie 'Organisatie en processen':

Beantwoording van de onderzoeksvragen 5 en 6

- De implementatie opties Centrale opslag en Hybride opslag met directe toegang scoren het hoogst op de criteria voor het waarborgen van autorisatie en authenticatie zodat 'gegevens

uitsluitend worden geraadpleegd door personen die daarvoor vanwege hun wettelijke taakuitvoering in aanmerking komen' en niet 'toegankelijk zijn voor andere doeleinden dan bedoelt in de Richtlijn'. Reden hiervoor is dat de bevraging centraal is geregeld wordt beheer van toegangsrechten op een gecentraliseerde plaats kan worden beheerd en ondersteund door adequate technische middelen.

- De implementatieoptie Decentrale opslag en beantwoording door aanbieder scoort het laagst van als het gaat om de verzekering dat de opgeslagen gegevens na afloop van de bewaartermijn worden vernietigd. Niet omdat dit niet even makkelijk of moeilijk kan worden gerealiseerd maar vooral omdat in deze optie de controle op de vernietiging het erg omvangrijk is als men volledigheid nastreeft. De overige opties scoren op dit punt gelijk omdat een bepaalde mate van controle op afstand mogelijk wordt.
- Geen enkele optie is inherent onveilig. Implementatieoptie Centrale Opslag met directe toegang scoort het hoogst als het gaan om de *mogelijkheden* tot het beveiligen van de informatie. Door de centralisatie van de opslag en het beheer is het nemen van maatregelen eenvoudiger dan in de andere opties. Toch is deze optie ook de gene die, juist door die centralisatie, tevens het meest kwetsbaar is voor discontinuïteit van het bevragingsproces, misbruik en oneigenlijk gebruik van gegevens. De risico's kunnen deels worden gemitigeerd met een aantal relatief eenvoudige technische maar ook relatief kostbare maatregelen (redundantie in bij de opslag- en bevragingsmiddelen). Centrale optie vereist om de zelfde redenen echter ook stevige organisatorische beveiligingsmaatregelen zoals regelmatige controles op kwetsbaarheden en naleving van procedures om de genoemde risico's te mitigeren en een onafhankelijke Audit op het gehele dataretentieproces .
- De Decentrale implementatieopties scoren het laagst op beschikbaarheid van statistieken voor de Europese commissie. De andere twee opties scoren op dit criterium in gelijke mate als beste omdat er betere mogelijkheden zijn dan in de decentrale varianten voor geautomatiseerde gegevensverzameling ten behoeve van de statistieken.

Onderzoeksvraag 7

Wat is de haalbaarheid in technische, organisatorische en juridische zin van de verschillende mogelijkheden?

Beantwoording van onderzoekvraag 7

- De enige optie die met betrekking tot de haalbaarheid in organisatorische en technische zin als twijfelachtig moet worden beschouwd is de implementatieoptie Decentrale Opslag bij de aanbieder en directe toegang voor de behoeftesteller. Dit heeft met name te maken met het ontbreken van een punt waar de regierol kan worden belegd voor de implementatie. Er is in deze implementatieoptie erg veel overleg en afstemming nodig over praktische keuzen zodat een dergelijke 'natuurlijke' rol noodzakelijk is. De overige opties moeten in termen van haalbaarheid op de aspecten organisatie en techniek als gelijkwaardig worden gezien.
- Als het gaat om de kortst mogelijke termijn waarin een implementatie optie kan worden geïmplementeerd is de verwachting dat de alleen de implementatie van de optie Decentrale toegang en beantwoording door aanbieder binnen een jaar na aanvang van de implementatie kan worden afgerond. Reden hiervoor is dat in alle meer geautomatiseerde implementatieopties er veel afstemming en overleg nodig is over technische details, standaardisatie van vraag en antwoord en organisatorische keuzen om tot een succesvolle afronding te kunnen komen.

- De deelvraag naar de haalbaarheid in juridische zin is niet in dit onderzoek meegenomen zoals dat in de afbakening van het onderzoek is aangegeven (paragraaf 1.6)

Toelichtingen per Implementatieoptie

De onderbouwing van de beoordelingen in het kwalitatieve model zijn voor het belangrijkste deel terug te vinden in hoofdstuk 3 en 4 waar de implementatieopties op het niveau van bedrijfsarchitectuur, informatiearchitectuur en technische architectuur zijn beschreven. Daarnaast is de beoordeling ook ingegeven door het 'professional judgement' van de onderzoekers.
De onderliggende weging van de categorieën en criteria is tot stand gekomen in overleg met de bereidingscommissie. Het is niet uitgesloten dat individuele partijen afhankelijk van hun eigen belangen tot andere afwegingen zouden zijn gekomen en dus tot andere uitkomsten. De waarde van de kwalitatieve model moet vooral gezocht worden in het feit dat de belangrijkste criteria die de besluitvorming een rol spelen in het model zijn opgenomen. Het kwalitatieve beoordelingsmodel ondersteunt daarmee de discussie door focus aan te brengen en biedt een eenduidige manier om afwegingen te beargumenteren.

Hieronder worden de uitkomsten per implementatieoptie besproken op die punten waarin de optie sterke verschillen vertoont ten opzichte van de andere opties.

Implementatieoptie: Decentrale opslag, beantwoording door aanbieder

In de totaalscore is deze optie gerangschikt als derde maar staat dichter bij de twee hoogst scorende opties dan bij de laagst scorende implementatieoptie.

Tabel 5-5: overzicht van kwalitatieve scores decentrale opslag, beantwoording door aanbieder

Punten per categorie	Categorie	Gecorreleerde opslag	Ongecorreleerde opslag
30 ptn	Organisatie en processen	12	12
30 ptn	Technologie	18	18
10 ptn	Business Case	7,5	7,5
20 ptn	Informatiebeveiliging	4	4
10 ptn	Implementatie termijn	10	10
100 pnt	**Totaal**	**51,5**	**51,5**

De score op de business case is hoog vanwege relatief geringere invloed op de doorlooptijd van de introductie van nieuwe diensten door de aanbieder. Er is geen standaardisatie nodig waardoor de aanbieder alles naar eigen inzicht kan implementeren en minder afhankelijk is van afspraken tussen de aanbieders en behoeftesteller. Hetzelfde argument geldt voor de implementatietermijn: als enige is deze optie waarschijnlijk uitvoerbaar binnen een jaar na de start van de implementatie omdat de aanbieder alleen rekening hoeft te houden met zijn eigen voorzieningen en er geen afstemmingen met andere partijen nodig zijn. De aanbieder kan zelf bepalen hoe de implementatie van de richtlijn

technisch vorm wordt gegeven en heeft daarmee de gelegenheid deze maximaal te laten aansluiten bij zijn huidige wijze van werken.

Deze optie is de enige die positief scoort bij Organisatie en Processen op de mogelijkheid van de aanbieder om actief te toetsen op rechtmatigheid van de vordering en om inhoudelijk bij te dragen aan de beantwoording van de vordering omdat de vraag van de behoeftesteller niet via geautomatiseerde systemen verloopt, maar op papier of in de (beveiligde) e-mail wordt aangeleverd.

Op het gebied van informatiebeveiliging scoort deze optie relatief laag als gevolg van het criterium dat er veel personeel van de aanbieder persoonlijk betrokken is bij de beantwoording van vorderingen. Dit personeel is op de hoogte van zowel de bron van de vordering als het object van onderzoek. Eveneens is er in deze optie sprake van en veelheid aan beheerders van de opgeslagen data waarmee, geredeneerd vanuit het gehele systeem, de controleerbaarheid van de beheerders afneemt. De conclusie dat op dit criterium de optie als slecht moet worden beoordeeld is echter niet aan de orde omdat juist door de decentrale opslag de impact van het risico op informatielekkage beperkter is dan in de centrale optie (men heeft immers slechts toegang tot een heel klein deel van het totaal) en men ook niet geconfronteerd wordt met *alle* vorderingen maar slechts een zeer klein deel.
De inrichting van de audit trail en de uitvoering van audits is complex en omvangrijk doordat er veel partijen in het gehele systeem actief zijn en moeten worden gecontroleerd. Ook zullen deze partijen allen op hun eigen wijze invulling hebben gegegeven aan de eisen waardoor de eenduidigheid van de beoordeling door een auditeur moeilijker is vorm te geven. Op veel locaties bevinden zich relevante loggings in een diversiteit aan systemen.
De controleerbaarheid van de vernietiging van de gegevens na de bewaartermijn is omvangrijk door de grote hoeveelheid aanbieders die op diverse manieren informatie hebben opgeslagen.

Implementatieoptie: Decentrale opslag, directe toegang

In de totaalscore is deze optie gerangschikt als vierde op grote afstand van de overige implementatieopties.

Tabel 5-6: overzicht van kwalitatieve scores decentrale opslag, directe toegang

Punten per categorie	**Categorie**	**Gecorreleerde opslag**	**Ongecorreleerde opslag**
30 ptn	Organisatie en processen	9	9
30 ptn	Technologie	10,2	10,2
10 ptn	Business Case	0	0
20 ptn	Informatiebeveiliging	11	11
10 ptn	Implementatie termijn	0	0
100 pnt	**Totaal**	**30,2**	**30,2**

Deze optie scoort op alle categorieën (mede) als laagste. Er zijn op het gebied van technologie vrijwel geen mogelijkheden voor hergebruik van bestaande mechanismen dus zal in deze optie omvangrijke nieuwbouw noodzakelijk zijn. De categorie business case scoort laag doordat er vergaande standaardisatie nodig is om deze optie te laten werken terwijl het ontbreekt aan en partij die de regie voert. Dit kost veel tijd en geld voor afstemming, wat met name de kleine aanbieder raakt en alle aanbieders belemmert bij de introductie van nieuwe diensten.

De implementatie termijn scoort even laag als de centrale en hybride opties maar door het ontbreken van sterke centrale regie vanuit een intermediaire derde bestaat de kans dat deze optie nog meer tijd vergt in het geval van de centrale en hybride optie.

De categorie informatiebeveiliging scoort hoger dan in de optie Decentrale opslag beantwoording door aanbieder omdat het personeel van de aanbieder niet in de gelegenheid is kennis te nemen van de inhoud van de vordering. Overigens scoort het criterium exclusiviteit van de toegang (voorkomen van oneigenlijk gebruik) als enige van de opties zeer laag vanwege de technische complexiteit van de optie, er is sprake van geautomatiseerde bevraging maar het ontbreekt aan een centrale partij die eenduidig toezicht kan houden op het totale autorisatiebeheer van de toegang tot de opgeslagen informatie.

Centrale opslag, directe toegang

In de totaalscore is deze optie gerangschikt als eerste maar staat relatief dicht bij de implementatieoptie die als tweede is gerangschikt.

Tabel 5-7: overzicht van kwalitatieve scores centrale opslag, directe toegang

Punten per categorie	**Categorie**	**Gecorreleerde opslag**	**Ongecorreleerde opslag**
30 ptn	Organisatie en processen	18	18
30 ptn	Technologie	20,1	20,1
10 ptn	Business Case	2,5	2,5
20 ptn	Informatiebeveiliging	20	20
10 ptn	Implementatie termijn	0	0
100 pnt	**Totaal**	**60,6**	**60,6**

De centrale optie scoort op alle categorieën (mede) het hoogst. Op organisatie en processen is dat met name het gevolg van de efficiency van de bevragingsprocedure en de flexibiliteit om met fluctuaties in het bevragingsvolume om te gaan. Ook de aanlevering van rapportages aan de Europese Commissie zal door de mogelijkheid van gecentraliseerde loggings eenvoudig zijn. De optie sluit maar ten dele aan op bestaande werkwijzen en technologieën, is wel goed schaalbaar en

in de toekomst goed te onderhouden. Door de combinatie van centralisatie en automatisering van gegevensoverdracht is de score op informatiebeveiliging van deze optie hoog.

Deze optie scoort als hoogste in de categorie informatiebeveiliging. Hier moet echter worden opgemerkt dat deze score tot stand is gekomen doordat in de optie de mogelijkheid is om op eenvoudige wijze de juiste maatregelen te nemen om oneigenlijk gebruik, misbruik en manipulatie van de opgeslagen data te voorkomen en continuïteitsrisico's te beheersen. Aan de andere kant is deze optie door de centralisering juist wel het meest kwetsbaar voor oneigenlijk gebruik, misbruik en manipulatie en continuïteitsrisico's. De centrale optie is dus niet inherent veiliger.

Door de vergaande standaardisering scoort de optie laag op de categorie business case: het belast de kleine aanbieders relatief zwaar. Het beïnvloed de introductie van nieuwe diensten minder dan de decentrale variant met directe toegang maar wel meer dan de decentrale variant met beantwoording door aanbieder. Ook de implementatietermijn zal langer dan een jaar zijn.

Hybride opslag, directe toegang

In de totaalscore is deze optie gerangschikt als duidelijke tweede maar staat relatief dicht bij implementatieopties die als eerste en derde zijn gerangschikt.

Tabel 5-8: overzicht van kwalitatieve scores hybride opslag, directe toegang

Punten per categorie	Categorie	Gecorreleerde opslag	Ongecorreleerde opslag
30 ptn	Organisatie en processen	18	18
30 ptn	Technologie	20,1	20,1
10 ptn	Business Case	2,5	2,5
20 ptn	Informatiebeveiliging	15	15
10 ptn	Implementatie termijn	0	0
100 pnt	**Totaal**	**55,6**	**55,6**

De hybride optie scoort in het kwalitatieve model vrijwel gelijk aan de centrale optie. De daar genoemde opmerkingen zijn ook hier van toepassing. Het verschil met de optie voor centrale opslag dat de complexiteit van de in te richten audit trail toeneemt ten opzichte van de centrale optie. Op dit punt scoort de hybride optie wel weer beter dan de optie Decentrale opslag en beantwoording door aanbieder.
De hybride implementatieoptie scoort op de overige criteria gelijk aan het centrale model omdat voor wat betreft de beveiligingsrisico's en de type maatregelen die getroffen moeten worden de opties vergelijkbaar zijn.

5.4 Beantwoording van de onderzoekvragen op basis van het kwantitatieve model

Deze paragraaf geeft het antwoord op onderzoeksvraag 4 te weten de kosten die bij elk van de implementatieopties horen. Daarnaast gaat het in op het kostenaspect van onderzoeksvraag 3 voor zover hergebruik van bestaande voorzieningen mogelijk is en zich vertaald in een kostenvoordeel.

Bij de beschouwing van de kosten is het vooral van belang om na te gaan hoe de kosten van de diverse implementatieopties zich tot elkaar verhouden. Dit zal dat vanuit diverse invalshoeken gebeuren zodat er een beeld ontstaat waar de belangrijkste verschillen zitten. Daarbij wordt er gebruik gemaakt van drie overzichten: totale kosten per implementatieoptie, investeringskosten per implementatieoptie en operationele kosten per implementatieoptie. Alle drie de overzichten geven deze kosten verdeeld over de actoren en per actor verdeeld over de processen. Beheer is er als apart proces aan toegevoegd omwille van een correcte extrapolatie over vijf jaar.

De overzichten maken gebruik van de volgende afkortingen:

DBA	Decentrale opslag, beantwoording door aanbieder
DDT	Decentrale opslag, directe toegang
CDT	Centrale opslag, directe toegang
HDT	Hybride opslag, directe toegang
GC	Gecorreleerde opslag
OC	Ongecorreleerde opslag

Betrokkene	kosten-soort	Investeringen en operationele kosten over 5 jaar							
		DBA GC	DBA OC	DDT GC	DDT OC	CDT GC	CDT OC	HDT GC	HDT OC
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 6.100.000	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 14.960.000	€ 14.960.000	€ 20.050.000	€ 20.050.000	€ 16.600.000	€ 16.600.000	€ 16.600.000	€ 16.600.000
	Beheer	€ 7.490.000	€ 7.490.000	€ 7.490.000	€ 7.490.000	€ 7.490.000	€ 7.490.000	€ 7.490.000	€ 7.490.000
Subtotaal Behoeftestellers		€ 22.440.000	€ 22.440.000	€ 27.530.000	€ 33.630.000	€ 24.080.000	€ 24.080.000	€ 24.080.000	€ 24.080.000
Intermediaire 3de	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 20.310.000	€ 21.850.000	€ 1.930.000	€ 3.320.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 5.910.000	€ 5.910.000	€ 5.910.000	€ 5.910.000
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 8.610.000	€ 8.610.000	€ 11.130.000	€ 11.130.000
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 34.820.000	€ 36.350.000	€ 18.950.000	€ 20.350.000
Aanbieders	Acquisitie	€ 60.760.000	€ 62.270.000	€ 62.960.000	€ 63.360.000	€ 59.020.000	€ 59.020.000	€ 62.250.000	€ 62.250.000
	Opslag	€ 29.060.000	€ 30.550.000	€ 27.870.000	€ 25.900.000	€ 0	€ 0	€ 27.160.000	€ 24.780.000
	Bevraging	€ 15.020.000	€ 15.020.000	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 27.520.000	€ 27.520.000	€ 23.210.000	€ 23.210.000	€ 15.880.000	€ 15.880.000	€ 15.880.000	€ 15.880.000
Subtotaal Aanbieders		€ 132.380.000	€ 135.370.000	€ 114.050.000	€ 112.460.000	€ 74.920.000	€ 74.920.000	€ 105.300.000	€ 102.920.000
Totaal		€ 154.800.000	€ 157.810.000	€ 141.580.000	€ 146.100.000	€ 133.800.000	€ 135.350.000	€ 148.320.000	€ 147.340.000

Figuur 5-1: totale kosten per implementatieoptie over vijf jaar

Betrokkene	kosten-soort	Investeringen							
		DBA GC	DBA OC	DDT GC	DDT OC	CDT GC	CDT OC	HDT GC	HDT OC
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 40.000	€ 40.000	€ 4.570.000	€ 4.570.000	€ 1.120.000	€ 1.120.000	€ 1.120.000	€ 1.120.000
	Beheer	€ 3.380.000	€ 3.380.000	€ 3.380.000	€ 3.380.000	€ 3.380.000	€ 3.380.000	€ 3.380.000	€ 3.380.000
Subtotaal Behoeftestellers		€ 3.410.000	€ 3.410.000	€ 7.950.000	€ 7.950.000	€ 4.500.000	€ 4.500.000	€ 4.500.000	€ 4.500.000
Intermediaire 3de	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 18.050.000	€ 16.680.000	€ 1.370.000	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 3.450.000	€ 3.450.000	€ 3.450.000	€ 3.450.000
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 4.290.000	€ 4.290.000	€ 6.810.000	€ 6.810.000
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 25.780.000	€ 24.420.000	€ 11.620.000	€ 10.260.000
Aanbieders	Acquisitie	€ 30.390.000	€ 30.390.000	€ 30.390.000	€ 30.390.000	€ 30.390.000	€ 30.390.000	€ 30.390.000	€ 30.390.000
	Opslag	€ 25.130.000	€ 21.560.000	€ 23.940.000	€ 21.560.000	€ 0	€ 0	€ 23.940.000	€ 21.560.000
	Bevraging	€ 8.020.000	€ 8.020.000	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 14.800.000	€ 14.800.000	€ 14.800.000	€ 14.800.000	€ 7.470.000	€ 7.470.000	€ 7.470.000	€ 7.470.000
Subtotaal Aanbieders		€ 78.340.000	€ 74.770.000	€ 69.120.000	€ 66.740.000	€ 37.860.000	€ 37.860.000	€ 61.800.000	€ 59.420.000
Totaal		€ 81.750.000	€ 78.180.000	€ 77.070.000	€ 74.690.000	€ 68.140.000	€ 66.780.000	€ 77.920.000	€ 74.170.000

Figuur 5-2: investeringskosten per implementatieoptie

Betrokkene	kosten-soort	Operationele kosten over 5 jaar							
		DBA GC	DBA OC	DDT GC	DDT OC	CDT GC	CDT OC	HDT GC	HDT OC
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 6.100.000	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 14.920.000	€ 14.920.000	€ 15.480.000	€ 15.480.000	€ 15.480.000	€ 15.480.000	€ 15.480.000	€ 15.480.000
	Beheer	€ 4.110.000	€ 4.110.000	€ 4.110.000	€ 4.110.000	€ 4.110.000	€ 4.110.000	€ 4.110.000	€ 4.110.000
Subtotaal Behoeftestellers		€ 19.030.000	€ 19.030.000	€ 19.580.000	€ 25.680.000	€ 19.580.000	€ 19.580.000	€ 19.580.000	€ 19.580.000
Intermediaire 3de	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 2.260.000	€ 5.170.000	€ 560.000	€ 3.320.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 2.460.000	€ 2.460.000	€ 2.460.000	€ 2.460.000
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 4.320.000	€ 4.320.000	€ 4.320.000	€ 4.320.000
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 9.040.000	€ 11.930.000	€ 7.330.000	€ 10.090.000
Aanbieders	Acquisitie	€ 30.370.000	€ 31.880.000	€ 32.570.000	€ 32.970.000	€ 28.630.000	€ 28.630.000	€ 31.860.000	€ 31.860.000
	Opslag	€ 3.930.000	€ 8.990.000	€ 3.930.000	€ 4.340.000	€ 0	€ 0	€ 3.220.000	€ 3.220.000
	Bevraging	€ 7.000.000	€ 7.000.000	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 12.720.000	€ 12.720.000	€ 8.410.000	€ 8.410.000	€ 8.410.000	€ 8.410.000	€ 8.410.000	€ 8.410.000
Subtotaal Aanbieders		€ 54.040.000	€ 60.600.000	€ 44.930.000	€ 45.720.000	€ 37.060.000	€ 37.060.000	€ 43.500.000	€ 43.500.000
Totaal		€ 73.050.000	€ 79.630.000	€ 64.510.000	€ 71.410.000	€ 65.660.000	€ 68.570.000	€ 70.400.000	€ 73.170.000

Figuur 5-3: operationele kosten per implementatieoptie over vijf jaar

De overzichten van investeringskosten en operationele kosten per implementatieoptie zijn opgenomen in bijlage J, deze worden verder niet besproken.

Het kosteneffect van correlatie
De keuze voor gecorreleerde opslag leidt bij zes van de acht implementatieopties tot eenzelfde beeld: de totale kosten over vijf jaar zijn voor gecorreleerde opslag iets lager dan voor ongecorreleerde opslag. De investeringen vallen voor gecorreleerde opslag wat hoger uit maar dit wordt terugverdiend in de operationele kosten. Afhankelijk van de implementatieoptie is gecorreleerde opslag tussen de 1% en 3% goedkoper. Alleen in het geval van de hybride implementatieoptie maken de lagere operationele kosten in het geval van gecorreleerde opslag de hogere investeringen niet helemaal goed. Het verschil in kosten tussen gecorreleerde en ongecorreleerde opslag is zo klein dat deze keuze marginaal lijkt.

Bij de verdere bespreking van de kosten concentreert de analyse zich daarom op de verschillende bedrijfsarchitecturen.

De duurste implementatieoptie
De duurste implementatieoptie is decentrale opslag, beantwoording door aanbieder. Investeringen in portal en database servers en bijbehorende ontwikkelkosten leiden tot een relatief hoog investeringsbedrag. Daarnaast zijn de operationele kosten hoog doordat de kosten van bevraging bij de aanbieder niet gecompenseerd worden door lagere kosten voor bevraging bij de behoeftestellers.

De goedkoopste implementatieoptie
De goedkoopste implementatieoptie is centrale opslag, directe toegang. De investeringen voor opslag, bevraging en beheer zijn verhoudingsgewijs laag. De investeringskosten voor acquisitie zijn vergelijkbaar met de overige implementatieopties. De som van operationele kosten is eveneens het laagst.

De duurste en goedkoopste implementatieoptie vanuit het perspectief van de aanbieder
De decentrale opslag, beantwoording door de aanbieder heeft de hoogste kosten voor de aanbieder tot gevolg. Zoals eerder aangegeven zijn de kosten van bevraging een belangrijke component daarin, ook de operationele kosten voor beheer zijn hoog in vergelijking met de andere implementatieopties.

Centrale opslag, directe toegang leidt voor de aanbieders tot de meest voordelige oplossing. De investeringen in opslag kunnen achterwege blijven, de operationele kosten zijn laag doordat de aanbieder geen casusgerichte activiteiten meer hoeft te verrichten.

Naast kosten spelen uiteindelijk ook vergoedingen een rol. Deze analyse houdt geen rekening met een eventuele toekomstige vergoedingstructuur.

De duurste en goedkoopste implementatieoptie vanuit het perspectief van de behoeftesteller
De meest voordelige implementatieoptie voor de behoeftestellers is decentrale opslag, beantwoording door aanbieders. Lage investeringen dragen daar toe bij, de operationele kosten blijven op vergelijkbaar niveau met de overige implementatieopties.

De duurste oplossing voor de behoeftestellers is decentrale opslag, directe toegang en ongecorreleerde opslag. Dit wordt veroorzaakt door hoge operationele kosten doordat de behoeftesteller zelf de correlatie in de opgevraagde informatie moet aanbrengen, er is geen aanbieder of intermediaire derde die dit doet.

Bewaartermijn

In het onderzoek is met instemming van de begeleidingscommissie en werkgroep wetgeving gerekend met een bewaartermijn van een jaar. Op verzoek van de werkgroep wetgeving is er op basis van de huidige modellering gekeken naar een kortere c.q. een langere bewaartermijn.

De kosten die door een wijziging van de bewaartermijn direct beïnvloed worden hangen samen met de opslag van de gegevens dus de disks en de daarmee samenhangende besturingslogica. Ook de beheerkosten zullen iets wijzigen.

Op basis van de implementatieoptie centrale opslag, directe toegang zijn de additionele kosten van twee jaar opslag circa € 14 miljoen euro waarvan € 500.000 operationele kosten over een periode van vijf jaar. Voor de overige implementatieopties is een vergelijkbaar bedrag van toepassing.

Op basis van dezelfde implementatieoptie is in het geval van een bewaartermijn van een half jaar een verlaging van de kosten van bijna € 7 miljoen te verwachten waarvan € 400.000 operationele kosten over een periode van vijf jaar. Voor de overige implementatieopties is een vergelijkbaar bedrag van toepassing.

Een verhoging c.q. verlaging van bevragingsvolume en de daarmee samenhangende kosten is niet meegenomen in de berekening.

Bestaande voorzieningen

Uit het veldonderzoek is onvoldoende informatie gekomen om voor het acquisitie en opslag proces een uitspraak te doen over de kostenbesparingen die met hergebruik bereikt worden. De diversiteit in het veld is enorm. Niet alleen in netwerktechniek maar ook in de toegepaste netwerkmanagement en businessmanagement systemen waaruit een deel van de informatie moet komen. Een gemiddelde uitspraak over hergebruik zou weinig waarde toevoegen, beter is het om de kosten als greenfield te beschouwen.

De bestaande voorzieningen die te maken hebben met de informatieverstrekking aan het CIOT verdienen nog een aparte toelichting.

Wanneer tot een decentrale variant wordt besloten is het onwaarschijnlijk dat het CIOT opgeheven wordt. Niet alleen vanwege kapitaalsvernietiging maar vooral vanuit operationele overwegingen: het CIOT dient voor de behoeftestellers als belangrijk centraal punt voor een groot volume van bevragingen op actuele NAW gegevens. Voor de decentrale varianten moeten de kosten voor het CIOT er dus bij opgeteld worden. Voor 2006 is het budget circa 2,5 miljoen euro.

Voor de hybride en centrale variant is het zeer waarschijnlijk dat de taken van het CIOT zullen opgaan in de intermediaire derde. Wellicht kan een deel van de bestaande voorzieningen

hergebruikt worden wat leidt tot een bescheiden reductie van de investeringskosten. Omdat het volume van de huidige CIOT bevragingen niet in de operationele kosten van bevraging zijn meegenomen zullen deze nog bij de kosten voor de hybride en centrale opties komen. Dit zal een deel van de eerder genoemde 2,5 miljoen euro zijn. Voor de beheerkosten treden er geen wijzigingen op.

6 Conclusies

Met de invoering van de Europese Richtlijn Dataretentie staat Nederland voor een omvangrijke operatie. De implementatie van de richtlijn is voor alle betrokkenen een grote uitdaging.

Alle geïnterviewde aanbieders hebben aangegeven dat de implementatie van de richtlijn dataretentie een zware en complexe uitdaging wordt die veel tijd en grote investeringen met zich mee brengt en een grote impact heeft op de bedrijfsvoering.

De resultaten van dit onderzoek geven aan dat de invoering omvangrijk is. Over een periode van vijf jaar varieert de optelsom van investering en operationele kosten tussen de 133 miljoen euro en 157 miljoen euro afhankelijk van de gekozen implementatieoptie.

Implementatie optie		**In € over vijf jaar**	**punten**
Decentrale opslag, beantwoording door aanbieder	Gecorreleerd	€ 154.800.000	51.5
	Ongecorreleerd	€ 157.810.000	51.5
Decentrale opslag, directe toegang	Gecorreleerd	€ 141.580.000	30.2
	Ongecorreleerd	€ 146.100.000	30.2
Centrale opslag, directe toegang	Gecorreleerd	€ 133.800.000	60.6
	Ongecorreleerd	€ 135.350.000	60.6
Hybride opslag, directe toegang	Gecorreleerd	€ 148.320.000	55.6
	Ongecorreleerd	€ 147.340.000	55.6

Tabel 6-1: overzicht totale kosten en score voor iedere implementatieoptie.

Voor de Nederlandse samenleving is de centrale optie met directe toegang door de behoeftestellers de meest voordelige. De overige implementatieopties zijn duurder en belasten vooral de aanbieder zwaarder. Niet alleen financieel maar ook operationeel. Hoe de financiële belasting voor de aanbieder in de praktijk uitvalt is overigens op basis van het kosten overzicht niet te zeggen, dit hangt in belangrijke mate af van de vergoedingenstructuur waartoe nog besloten gaat worden.

De keuze die mogelijk gemaakt gaat worden voor een implementatieoptie of een variant daarvan zal niet alleen op basis van kostenoverwegingen gemaakt kunnen worden. Uit het kwalitatieve model blijkt dat de centrale optie met directe toegang ook het hoogst scoort op de gehanteerde criteria.

Het is echter te eenvoudig om op basis van deze uitkomsten tot de conclusie te komen dat de centrale optie dus de beste implementatieoptie is. Er zijn veel onderliggende details die het verschil tussen de diverse implementatieopties bepalen. Dit zijn details die voor belanghebbenden verschillend uitpakken en die verschillend gewogen zullen worden. Er is door de onderzoekers in overleg met de begeleidingscommissie voor een zoveel mogelijk objectiveerbare benadering gekozen bij de kwalitatieve beoordeling. Toch kan er met de uitkomsten van de beoordeling in de hand wel degelijk van mening worden verschild.

De afweging welke implementatieoptie de voorkeur verdient zal door het departement van Justitie in overleg met de departementen Binnenlandse Zaken, Defensie en Economische Zaken gemaakt worden. Naast de inhoudelijke aspecten die dit onderzoek inzichtelijk heeft gemaakt zullen ook bestuurlijke en politieke overwegingen daarbij een rol spelen.

Nadat de keuze voor de implementatieoptie is gemaakt en het wetgevingstraject zijn verdere vervolg krijgt is het aan te bevelen om begin 2007 op basis van de ingeslagen richting een vervolgonderzoek uit te voeren. Er kan dan meer specifiek ingegaan worden op het technisch ontwerp, organisatorische uitvoering, de implementatie planning en bijvoorbeeld een mogelijke pilot.

September 2006.

GERAADPLEEGDE LITERATUUR

95/46/EG Richtlijn van het Europees parlement en de raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

2002/58/EG Richtlijn van het Europees parlement en de raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie

2006/24/EC Richtlijn van het Europees parlement en de raad betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten

Opinie 3/2006 WP 119 van de 'Article 29 Data Protection Working Party' op de Richtlijn 2006/24/EC

Hoofdstuk 13 Telecommunicatiewet.

Besluit bijzondere vergaring nummergegevens telecommunicatie.

Besluit aftappen openbare telecommunicatienetwerken en –diensten.

Regeling aftappen openbare telecommunicatienetwerken en –diensten.

Besluit verstrekking gegevens telecommunicatie.

Besluit vorderen gegevens telecommunicatie.

Besluit aanwijzing toezichthouders telecommunicatiewet.

Besluit beveiliging gegevens aftappen telecommunicatie (BBGAT).

Stratix, Onderzoek ‘Bewaren Verkeersgegevens door Telecommunicatieaanbieders’, juni 2003.

KPMG, 'Onderzoek naar de opslag van historische verkeersgegevens van telecommunicatieaanbieders', november 2004.

De wet bescherming persoonsgegevens en de opinie van het College Bescherming Persoonsgegevens.

Artikel 126m t/m 126ng, tappen en vorderen gegevens bij telecomaanbieders / derden, Wetboek van strafvordering.

Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI).

Wet op de Inlichtingen- en Veiligheidsdiensten (WIV).

Vademecum Telecommunicatie voor rechterlijke macht en opsporingsdiensten, 2006, landelijk parket OM.

De digitale economie 2005, Centraal Bureau voor de Statistiek (CBS)

Marktmonitor elektronische communicatie en post 2005, OPTA.

A Leden van de begeleidingscommissie

De volgende organisaties zijn vertegenwoordigd geweest in de begeleidingscommissie Dataretentie:

Associatie van Competitieve Telecomoperators (ACT)

Casema

Essent Kabelcom

Internet Service Provider Overleg (ISPO)

Korps Landelijke Politiediensten (KLPD)

KPN Telecom

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Defensie, Militaire Inlichtingen en Veiligheidsdienst

Ministerie van Economische Zaken

Ministerie van Justitie

Nationale Beheersorganisatie Internet Providers (NBIP)

Nationaal Coördinator Terrorismebestrijding (NCTB)

Openbaar Ministerie (OM)

T-Mobile

UPC

Vodafone

B Geraadpleegde aanbieders

Bij de voorbereiding van de startbijeenkomst zijn de volgende (vertegenwoordigers van) aanbieders geraadpleegd:

1. Associatie van Competitieve Telecomoperators (ACT)
2. Casema
3. KPN Telecom
4. T-Mobile
5. Wanadoo

Tijdens het veldonderzoek zijn de volgende (vertegenwoordigers van) aanbieders geraadpleegd:

1. Debitel
2. Enertel
3. Essent Kabelcom
4. KPN Telecom
5. Nationale Beheersorganisatie Internet Providers (NBIP)
6. Microsoft
7. Planet Internet
8. Scarlet
9. T-mobile
10. UPC
11. Versatel
12. Vodafone
13. Wanadoo / Orange
14. Zeelandnet

C Eisen en criteria startbijeenkomst

Lijst eisen en wensen aanbieders:

	Wet- en Regelgeving
	Waarborging bescherming privacy klant
	Voorkomen van succesvolle aansprakelijkheidstelling van de Aanbieder door onterecht vermeende fouten in de aangeleverde data
	Vooraf toetsen van de rechtmatigheid van de vordering (door de aanbieder)
	Eenduidigheid dataset: dataset vanuit behoeftestellers of EU-set
	Bewaartermijn eenduidig vastgesteld
	De data vallend onder de Dataretentie richtlijn zal niet bevraagd worden via andere procedures dan overeengekomen en wettelijk vastgelegd bij de implementatie van deze richtlijn
	Vooraf toetsen op de juiste autorisatie van bevrager (door de aanbieder)
	Er moet voldoende tijd zijn voor operationele implementatie van de bewaarplicht na instellen van wetgeving

	Organisatie en processen
	Centraal/decentraal is onder andere afhankelijk van de gestelde waarborgen (privacy/aansprakelijkheid)
	Voorkeur voor decentrale opslag en bevraging.
	3e partij denkbaar maar afhankelijk van gestelde waarborgen (privacy/aansprakelijkheid)
	‘Toetsing vooraf’ in proces/procedures opnemen
	Er zal rekening moeten worden gehouden met andere bevragingsprocessen voor informatie die buiten de richtlijn dataretentie valt.
	(democratische) Controle, Audit en rol CBP
	Standaardisering van de vraag/Kennis bij de behoeftesteller
	Sanctioneren behoeftesteller indien ‘misbruik’ wordt gemaakt van de opsporingsmogelijkheden (autonomie politieregio’s)
	Operationele impact in het oog houden

	Technologie
	Eenduidigheid dataset, specificatie gegevensvelden met correlaties zijn noodzakelijk voor de inrichting databases en dus implementatie door aanbieder (voorbeeld IPnummer, MAC adres correleert met?)
	Vastgestelde bewaartermijn is noodzakelijk voor bepalen opslagcapaciteit
	Implementatie termijn vergelijkbaar met introductie nieuwe dienst
	Eenduidigheid van verantwoordelijkheid in de keten voor opslag van gegevens bepalend voor technische implementatie
	Time-to-Market nieuwe dienst mag niet worden beïnvloed door implementatie

	dataretentie richtlijn

Businesscase	
	Kosten voor softwarelicenties in de operationele omgeving moeten expliciet gemaakt worden
	Indien derde partij, bij overname activiteiten ook overname personeel of deel van de kosten

	CAPEX	OPEX	
		Beheer	Bevraging
Behoefte-stelling	• Infrastructuur • Hardware • Software	• Organisatie • Mensen, • ICT System/infra • Locatie	• Organisatie • Mensen, • ICT System/infra • Locatie
Service Providing	• Infrastructuur • Hardware • Software	• Organisatie • Mensen, • ICT System/infra • Locatie	• Organisatie • Mensen, • ICT System/infra • Locatie

Informatiebeveiliging	
	Standaard ISO 17799 (of 27001)
	Autorisatie/Authenticatie van bevrager (behoeftesteller)
	Vertrouwelijkheid van verkeersgegevens hoger geclassificeerd dan NAW-nummer gegevens
	Schenden privacy van klanten door opvraag van verkeerde gegevens voorkomen
	Het Besluit Beveiliging moet ondersteund worden.

Lijst eisen en wensen behoeftestellers:

Wet- en Regelgeving	
	Toets rechtmatigheid bevraging ligt bij behoeftestellers
	Vrijwaring hoeft niet apart worden geregeld want is in de wet verankerd door opname van de verplichting
	Foutieve interpretatie of gebruik van gegevens is verantwoordelijkheid van behoeftestellers
	Dataset van de behoeftestellers is leidend met in achtneming van de wijzigingen naar aanleiding van de kwaliteitsslagen.
	Implementatietijd voor wetgeving en implementatie in het veld gelijk

	Organisatie en processen
	Geen principiële voorkeur voor centrale of decentrale opslag
	Snelle afhandeling van vragen
	Standaardisering van de vraag en antwoord door training 'bevragers' noodzakelijk (vademecum en technisch achtergrond van een 'gegeven').
	Snelheid, kosten effectiviteit, vertrouwelijkheid van de vraag, integriteit van antwoorden zijn belangrijk, hiervoor mogelijke oplossing in geautomatiseerde bevraging
	Controle/Audit en mogelijke rol CBP
	(AIVD) Geen open communicatie/samenwerking bij onderzoeken
	Intermediaire 3e partij is denkbaar

	Technologie
	Geen specifieke voorkeur centraal/decentraal: logisch centraal kan fysiek decentraal zijn
	Wat er niet is kan niet worden opgeslagen en bevraagd (wel aantonen dat het er niet is)
	Betekenis gecorreleerd/ niet gecorreleerd betekent niet 'CSI Miami'. Alleen een specifieke vraag leidt tot een specifiek antwoord. Ook geen data mining.

	Businesscase
	Toevoegen 3e intermediair (indien aan de orde): – NBIP achtig model – CIOT achtig model

	CAPEX	OPEX	
		Beheer	Bevraging
Behoeftestelling	• Infrastructuur • Hardware • Software	• Organisatie • Mensen, • ICT System/infra • Locatie	• Organisatie • Mensen, • ICT System/infra • Locatie
Intermediaire derde (indien aan de orde)	• Infrastructuur • Hardware • Software	• Organisatie • Mensen, • ICT System/infra • Locatie	• Organisatie • Mensen, • ICT System/infra • Locatie
Service Providing	• Infrastructuur • Hardware • Software	• Organisatie • Mensen, • ICT System/infra • Locatie	• Organisatie • Mensen, • ICT System/infra • Locatie

	Informatiebeveiliging
	Standaard VIR en VIR-bi
	Referentie met ISO is nodig
	Verkeersgegevens en NAW-nummer: Hoogste classificatie Geheim/Staatsgeheim
	Verkeersgegevens zwaarder beveiligen dan NAW gegevens
	Vertrouwelijkheid van de vraag (i.v.m. onderzoek) is zeer belangrijk
	Autorisatie/Authenticatie van bevrager is essentieel
	Sterke verankering van de vraag in het onderzoeksdossier (beter dan nu) i.v.m. hardheid audit-trail.

D Kwalitatief beoordelingsmodel

Wegingsfactor , twee invalshoeken: per categorie (totaal van de categorieën = 100 punten) en per vraag (totaal = 100% per categorie)
Parameter is een vertaling van de requirements die in de kwalitatieve beoordeling een rol spelen
Meting geeft aan hoe de parameter wordt 'gemeten'
Waarde geeft de wijze aan waarop er ranking plaatsvindt, de waarde is gekoppeld aan wegingsfactor vraag. Maximale = 100% van weging vraag

Onderwerp	# vragen	waardering
Organisatie & Processen	5	30
Techniek	6	30
Business Case	2	10
Beveiliging	6	20
Implementatietermijn	1	10
Totaal	20	100

Wegings-factor categorie	**Wegings-factor vraag**	**Parameter**	**Meting**	**Waarde**
30 punten	**(% van pnt)**	**Organisatie en processen**		
	20%	Efficiency van de bevraging bevragingsprocedure	Aantal verschillende processtappen (iteraties) die doorlopen moeten worden voor een antwoord op een samenhangende enkelvoudige vragen	Snel= 20% Gemiddeld= 10% Langzaam=0
	20%	Mogelijkheid van toetsing vordering op wettelijke grondslag door de aanbieder	Ondersteunt het proces een actieve (handmatige) toetsing door de aanbieder wiens gegevens gevorderd / bevraagd worden	Ja = 20% Nee = 0%
	20%	Mogelijkheid van inhoudelijke ondersteuning door de aanbieder bij beantwoording van de vordering /bevraging	Ondersteunt het proces een actieve (handmatige) inhoudelijke ondersteuning door de aanbieder wiens gegevens gevorderd / bevraagd worden	Ja = 20% Nee = 0%
	20%	Flexibiliteit om met fluctuatie van de bevragingsvolume om te gaan	Afhankelijkheid beantwoording van menselijke handelingen én mate van centralisatie. Centralisatie = +, menselijke handeling = -	Groot = 20% Middel= 10% Klein= 0%
	20%	Mate waarin op	Hoe meer gegevens geautomatiseerd	Geautomatiseerd,

		eenvoudige wijze de verplichte rapportages aan de commissie kunnen worden opgeleverd	en centraal aanwezig zijn des te eenvoudiger zijn de gevraagde rapportages op te leveren	centraal = 20% Handmatig, decentraal = 0%

Wegings-factor categorie	**Wegings-factor vraag**	**Parameter**	**Meting**	**Waarde**
30 punten		**Technologie**		
	17%	Aansluiting op de huidig huidige technologieën	Impact op het beheer en de wijze van opslag door de aanbieder. Is er vrijwel volledig hergebruik mogelijk van technologie en procesorganisatie of sprake van deels hergebruik of vrijwel gehele vervanging.	Hergebruik = 17% Deels hgb = 9% Vervanging = 0%
	17%	Aansluiting op de huidig huidige technologieën	Impact op het beheer en de wijze van acquisitie door de aanbieder Is er vrijwel volledig hergebruik mogelijk van technologie en procesorganisatie of sprake van deels hergebruik of vrijwel gehele vervanging.	Hergebruik = 17% Deels hgb = 9% Vervanging = 0%
	17%	Aansluiting op de huidig huidige technologieën	Impact op het beheer en de wijze van bevraging door de behoeftesteller Is er vrijwel volledig hergebruik mogelijk van technologie en procesorganisatie of sprake van deels hergebruik of vrijwel gehele vervanging.	Hergebruik = 17% Deels hgb = 9% Vervanging = 0%
	16%	Toekomstvastheid van de gebruikte technologie	Schaalbaarheid van implementatieoptie	Goed = 16% Middel = 8% Slecht = 0%
	16%	Toekomstvastheid van de gebruikte technologie	Inpasbaarheid van nieuwe diensten	Goed = 16% Middel = 8% Slecht = 0%
	16%	Toekomstvastheid van de gebruikte technologie	Inpasbaarheid van nieuwe vraagstellingen	Goed = 16% Middel = 8% Slecht = 0%

Wegings-factor categorie	Wegings-factor vraag	Parameter	Meting	Waarde
10 punten		**Business Case**		
	50%	Mate van beïnvloeding van de huidige marktverdeling tussen aanbieders	Kleine aanbieders kunnen de implementatieoptie aan.	Geen = 50% Licht = 25% Groot = 0%
	50%	Mate van beïnvloeding van 'time to market' voor nieuwe diensten	Verwachting t.a.v. de relatie tussen complexiteit/flexibiliteit en toekomstvastheid van de technologie	Licht = 50% Matig = 25% Groot = 0%

Wegings-factor categorie	Wegings-factor vraag	Parameter	Meting	Waarde
20 punten		**Informatiebeveiliging**		
	10%	Vertrouwelijkheid van de relatie tussen de vraag en onderzoeker (Risico op informatielekkage)	Bron van de vraag en/of het object van onderzoek bij aanbieder / I3de bekend. Regel: Hoe meer mensen / processtappen des te meer risico op publiek worden van de geheimen.	Ja = 0% Nee = 10%
	10%	Continuïteit van het bevragingsproces (Risico van het niet-tijdig beschikbaar zijn van gegevens)	Aantal Single Points Of Failure in het ontwerp van de optie. Impact van falen Mogelijkheden voor maatregelen.	Goed = 10% Middel = 5% Slecht = 0%
	10%	Vertrouwelijkheid en integriteit van de opgeslagen data (risico op lek of manipulatie)	Controleerbaarheid van beheerders dat toegang heeft tot de data in het bevragingsproces. Regel: Hoe meer beheerders hoe moeilijker te controleren.	Goed = 10% Middel = 5% Slecht = 0%
	50%	De Audit Trail is in te richten conform gewenst beveiligingsniveau	Mate van complexiteit van de Audit Trail (proces, procedure en techniek) Regel: hoe meer processtappen des te complexer; hoe meer partijen des te complexer.	Complex = 0% Middel = 25% Eenvoudig = 50%
	10%	Exclusiviteit van toegang (risico van oneigenlijk gebruik)	Controleerbaarheid van het beheer van toegangsrechten. Regel: hoe groter het aantal mutaties in de toegekende rechten hoe moeilijker te controleren.	Complex = 0% Middel = 5% Eenvoudig = 10%

	10%	Vernietiging van de informatie na de bewaartermijn (risico op te lang bewaren)	Complexiteit van de controleerbaarheid van de naleving	Complex = 0% Middel = 5% Eenvoudig = 10%

Wegings-factor categorie	**Wegings-factor vraag**	**Parameter**	**Meting**	**Waarde**
10 punten		**Implementatie termijn**		
	100%	Tijd benodigd voor implementatie	Implementatie termijn <jaar is: 85-90% van de markt (aandelen) voldoet voor 90% aan de richtlijn. Inschatting op basis van: complexiteit techniek complexiteit organisatie en proces complexiteit Audit Trail	< 1 jaar = 100% > 1 jaar = 0%

E Overzicht van kosten van een aanbieder met 500.000 accounts

Om te komen tot een kostenschatting is gebruik gemaakt van diverse bronnen van informatie. De onderbouwing van kosten is van onderaf gedaan, dat wil zeggen vanuit de informatie architectuur en technische architectuur voor elk van de implementatieopties.

Database omvang en kosten

1. Bepaling gegevensset en gegevensdefinitie (zoals veldlengten).
2. Bepaling gegevensstructuur in een databaseontwerp
3. Bepaling grootte van de records voor NAW, telefonie, mobile telefonie, internet access en emails
4. Bepaling van het aantal maal dat deze records in een jaar gegenereerd worden, een combinatie van de omvang van de markt en de intensiteit van het gebruik.

Bovenstaande berekening leidt tot een grootte van database en op basis daarvan kan een schatting gemaakt worden van de opslagkosten. In de modellering kan een proportioneel deel aan de fictieve aanbieder met 125.000 klanten toegekend worden en – indien relevant voor de optie - aan de intermediaire derde

De gehanteerde marktgegevens zijn als volgt:

Tabel E-1: marktgegevens

	Eind 2005 (Bron: CBS) Aantallen x 1000
Aantal huishoudens	7.100
Percentage huishoudens met vaste telefonie	86%
Aantal vaste aansluitingen	6.106
Percentage huishoudens met Internet aansluiting	70%
Aantal Internetaansluitingen	4.970
Percentage huishoudens met inbel verbinding	16%
Aantal inbel verbindingen	795
Percentage huishoudens met ADSL aansluiting	47%
Aantal ADSL aansluitingen	2.343
Percentage huishoudens met Kabel aansluiting	37%
Aantal kabel aansluitingen	1.831
Mobiele Telefonie	16.000
E-mail accounts (markt maal 1,6; Bron: veldonderzoek)	7.952
Totaal aantal aansluitingen	***35.028***

In tabelvorm is het resultaat van de bovenstaande berekening met gebruikmaking van de marktgegevens als volgt, voor elk van de gehanteerde gegevens is de bron weergegeven:

Tabel E-2: berekening omvang totale gegevens bestand

Vaste telefonie		
Aantal gesprekken vast per dag	5	Bron: Aanbieders. KPMG rapport (data begin 2004 gaat nog uit van 8.2)
Omvang Database record	238 Byte	Bron: Databaseontwerp
Omvang Database Gehele markt	2.470 Gb	Berekening: # Vaste aansluitingen*5*365*238
Mobiele telefonie		
gesprekken mobiel p/d	12	Bron: Aanbieders
sms p/d	20	Bron: Aanbieders
database record	238 Byte	Bron: Databaseontwerp
Gehele markt	4.740Gb	Berekening: # Mobiele aansluitingen*32*365*238
Internet access		
Ipaccess (**dialin**)		
Database record	726 Byte	Bron: Databaseontwerp
Aantal inlogsessies p/d	12	Bron: Aanbieders
Gehele markt	21.915 Gb	Berekening: Aantal inbellers*12*365*726
Ipaccess (**Breedband)**		
Database record	726 Byte	Bron: Databaseontwerp
inlogsessies p/d	0,1	Bron: Aanbieders
Gehele markt	103 Gb	Berekening: Aantal breedbandaansluitingen*0,1*365*726
Email		
Aantal email aliases	5	
Database record	3925 Byte	Bron: Databaseontwerp
messages p/d	32	Bron: Aanbieders
Gehele markt	339.515 Gb	Berekening: aantal email messages*aantal internetaansluitingen*365*3925
NAW gegevens		
Database Record	443 Byte	Bron: Databaseontwerp
Gehele markt :	5.274 Gb	Aantal gebruikersaccounts*365*443

De omvang van de database records volgt uit de omvang van de respectievelijke velden, welke gebaseerd zijn op de het door het CIOT voorgeschreven formaat. Bron: Document Bestandslayout Aanlevering versie 1.8. Het databaseontwerp (zie bijlage H) maakt gebruikt van dit voorgeschreven formaat.

De totale omvang van de database komt uit op 365 terabyte. De totale omvang van de database is vervolgens geverifieerd door zowel aanbieders als een Lucent Data Base Administrator.

De kosten per terabyte opslag zijn circa € 34.000 (Bron: SUN International) hetgeen neerkomt op € 12,4 miljoen euro voor opslag voor de gehele markt gedurende een jaar. Deze kostenreferentie betreft de disks en het RAID.

Integrale kosten

De kosten voor de opslag van de gegevens is slechts een fractie van de totale kosten. Zoals in de technische architectuur aangegeven is er een uitgebreidere infrastructuur noodzakelijk om voor de aanbieders, de behoeftestellers en de intermediaire derde het geheel te laten werken. Daar horen infrastructuur, computers, software licenties en werkstations bij maar ook de ontwikkelinspanning om alles te laten werken en in de bestaande organisatie en systemen te laten landen.

In bijgaande tabellen is te zien welke kostenposten zijn gebruikt voor het maken van de totale kosteninschatting. Het voorbeeld heeft betrekking op implementatieoptie Centrale Gecorreleerde Opslag, directe toegang door de behoeftesteller. Het bevat de kostenelementen voor de aanbieder, de behoeftesteller en de intermediaire derde tezamen.

De aanbieder is in dit geval een fictieve aanbieder met 125.000 klanten die elke dienst afnemen (vaste telefonie, mobiele telefonie, internet toegang en email diensten). De onderbouwing voor het acquisitieproces is opgedeeld in drie tabellen:

Tabel E-3: uitwerking investeringskosten voor het proces Acquisitie

	Investeringskosten - deel 1 (Capex)							
Aquisitie	Ontwikkeling	Acquisitie ontwikkeling	Acquisitie HW	Acquisitie SW	Acquisitie Installatie	Acquisitie Project Management	Conversie ontwikkeling	Conversie HW
Aquisitie/Conversie uit de verschillende systemen		€ 184.500	€ 10.000	€ 24.000	€ 5.000	€ 10.000	€ 137.500	€ 32.000
Beheer/infra/backup/procedures/management	€ 11.000	€ -	€ -	€ -	€ -	€ -	€ -	€ -
Beveiliging	€ 16.000	€ -	€ -	€ -	€ -	€ -	€ -	€ -

Tabel E-4: uitwerking investeringskosten voor het proces Acquisitie

	Investeringskosten - deel 2 (Capex)							
Aquisitie	Conversie SW	Conversie Installatie	Conversie Project Management	hardware	software	installatie	Project Management	Overig
Aquisitie/Conversie uit de verschillende systemen	€ 45.000	€ 21.500	€ 28.500	€ -	€ -	€ -	€ -	€ -
Beheer/infra/backup/procedures/management	€ -	€ -	€ -	€ 16.000	€ 7.000	€ 12.500	€ 15.000	€ 3.000
Beveiliging	€ -	€ -	€ -	€ 15.000	€ 4.000	€ 7.000	€ 8.000	€ 8.000

Tabel E-4: totale investeringskosten en operationele kosten jaar 1 voor het proces Acquisitie

Aquisitie	CAPEX totaal	OPEX
Aquisitie/Conversie uit de verschillende systemen	€ 498.000	€ 80.000
Beheer/infra/backup/procedures/management	€ 64.500	€ 14.500
Beveiliging	€ 58.000	€ 9.000
Totaal	**€ 620.500**	**€ 103.500**

Tabel E-5: investeringskosten en operationele kosten jaar 1 voor het proces Opslag

		Investeringskosten (CAPEX)						
Opslag	CAPEX totaal	Ontwikkeling	hardware	software	installatie	PM	Overig	OPEX
Database/opslag	€ 344.786	€ 16.000	€ 258.286	€ 20.000	€ 17.500	€ 33.000	€ -	€ 19.000
correlatie	€ 39.000	€ 8.000	€ 6.000	€ 5.000	€ 10.000	€ 10.000	€ -	€ 2.000
Beheer/infra/backup/procedures/management	€ 136.500	€ 35.000	€ 14.000	€ 33.500	€ 10.000	€ 37.000	€ 7.000	€ 13.000
Beveiliging	€ 58.000	€ 16.000	€ 15.000	€ 4.000	€ 7.000	€ 8.000	€ 8.000	€ 8.000
Totaal	**€ 578.286**							**€ 42.000**

Tabel E-6: investeringskosten en operationele kosten jaar 1 voor het proces Bevraging

		Investeringskosten (CAPEX)						
Bevraging	CAPEX totaal	Ontwikkeling	hardware	software	installatie	PM	Overig	OPEX
Consoles/webserver/bevraging	€ 72.000	€ 22.000	€ 10.000	€ 15.000	€ 15.000	€ 10.000	€ -	€ 58.000
Beheer/infra/backup/procedures/management	€ 29.500	€ 6.000	€ 7.000	€ 4.000	€ 4.500	€ 5.000	€ 3.000	€ 8.000
Beveiliging	€ 63.000	€ 21.000	€ 15.000	€ 4.000	€ 7.000	€ 8.000	€ 8.000	€ 12.000
Totaal	**€ 164.500**							**€ 78.000**

Onderliggend aan bovenstaande tabellen zijn verder detailleringen in apparatuurlijsten, ureninschattingen, etc.

Voor alle personele inzet is gerekend met een standaard uurtarief, waarbij gerekend is met een manuur tarief van 100 Euro all-in (bron: veldonderzoek). Dit tarief kan als marktconform gezien worden (bron: marktonderzoek).

De kosten voor bevraging zijn gebaseerd op de kosten welke gemaakt moeten worden om een bevraging in het systeem in te voeren en gebaseerd op 88 bevragingen per maand bij 125.000 klanten (bron: marktonderzoek) waarbij per bevraging ongeveer een half uur werk besteed wordt (bron: aanbieders).

De ontwikkelingskosten (bron: veldonderzoek, EMC, SUN) bestaan uit het ontwikkelen en ontwerpen van de verschillende componenten (technisch en functioneel ontwerp, bouw en

implementatie), waarbij een duidelijk zwaartepunt is te vinden bij de acquisitie en conversie van de gegevens (bron: veldonderzoek).

De kosten voor de verschillende hardware componenten zijn bepaald op basis van de gegevens uit het veldonderzoek tezamen met gegevens uit de markt (bron: Cisco, SUN, HP, EMC) en gegevens van soortgelijke implementaties binnen Lucent. De kosten voor bijvoorbeeld infrastructuur, Project Management, Installatie, Training, monitoring en server ruimte zijn aannames gebaseerd op ervaringscijfers binnen Lucent.

Om tot de nationale kosten te komen moeten bovenstaande kostenramingen uitgesplitst worden naar de drie actoren te weten de aanbieder, de behoeftesteller en de intermediaire derde. Na die uitsplitsing kan de vermenigvuldiging plaatsvinden volgens de matrix die is toegelicht in hoofdstuk 2. Deze uitsplitsing en berekening is voor ieder implementatiemodel uitgevoerd.

De verdeling van de kosten is gebaseerd op de technische uitvoering van de betreffende implementatieoptie. Het onderliggende kostenmodel maakt het mogelijk om kosten welke bij een specifieke taak in de keten horen onder te brengen bij de actor die de taak uitvoert. Bijvoorbeeld: bij centrale opslag, zullen de kosten voor de centrale toegang (webportal) toegekend zijn aan de intermediaire derde. Bij decentrale opslag met directe bevraging, komen deze kosten ten laste van de behoeftesteller.

Het overzicht van de uitgesplitste kosten voor de aanbieder, de intermediaire derde en de behoeftesteller staat op de volgende bladzijde.

Behoeftestellers		CAPEX	OPEX	
Centrale opslag	Gecorreleerd		Beheer	Bevraging
Acquisitie				
Conversie				
Correlatie				
Opslag				
Bevraging				€ 54.000
	Console	€ 32.000		€ 2.000
Beheer		€ 19.000	€ 6.000	
Beveiliging		€ 63.000	€ 12.000	
Infra		€ 14.500	€ 2.000	
Subtotaal behoeftesteller		**€ 128.500**	**€ 20.000**	**€ 56.000**

Intermediaire derde				
Acquisitie	ontwikkeling			
	Hardware			
	Software			
	Installatie			
	Project Management			
	Algemeen			
Conversie	ontwikkeling			
	Hardware			
	Software			
	Installatie			
	Project Management			
	Algemeen			
Correlatie		€ 39.000	€ 2.000	
Correlatie handmatig		€ 0		€ 0
Opslag		€ 286.286	€ 9.000	
Bevraging	Database	€ 58.500	€ 10.000	
	webserver	€ 40.000	€ 2.000	
Beheer		€ 120.000	€ 8.000	
Beveiliging		€ 58.000	€ 6.000	
Infra		€ 16.500	€ 7.000	
Subtotaal Intermediaire derde		**€ 618.286**	**€ 44.000**	**€ 0**

Aanbieders				
Acquisitie	ontwikkeling	€ 184.500	€ 80.000	
	Hardware	€ 10.000		
	Software	€ 24.000		
	Installatie	€ 5.000		
	Project Management	€ 10.000		
	Algemeen			
Conversie	ontwikkeling	€ 137.500		
	Hardware	€ 32.000		
	Software	€ 45.000		
	Installatie	€ 21.500		
	Project Management	€ 28.500		
	Algemeen			
Correlatie				
Opslag				
Bevraging				
Beheer		€ 50.000	€ 12.500	
Beveiliging		€ 58.000	€ 9.000	
Infra		€ 14.500	€ 2.000	
Subtotaal Aanbieders		**€ 620.500**	**€ 103.500**	**€ 0**

F Bijlage bij het Besluit Beveiliging Gegevens Aftappen Telecommunicatie

NB De in dit rapport voorgestelde toepassing van de beveiligingseisen die in de onderstaande bijlage worden beschreven is gericht op de aanbieder, de behoeftesteller en de eventuele intermediaire 3e.

Bijlage als bedoeld in artikel 2, derde lid, van het Besluit beveiliging gegevens aftappen telecommunicatie

I. Beveiligingseis algemeen

Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. De functionaris voert daartoe regelmatig controles uit en legt de resultaten daarvan vast.

II. Beveiligingseisen ten aanzien van personeel

a. In de functiebeschrijving van personeel dat belast is met de verwerking van de informatie en gegevens wordt de verantwoordelijkheid voor de beveiliging daarvan beschreven.
b. Personeel dat in aanraking komt met de informatie en gegevens tekent een geheimhoudingsverklaring.
c. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens heeft toegang tot de informatie en de gegevens.

III. Fysieke beveiliging en beveiliging van de omgeving

a. De informatie en de gegevens worden zoveel mogelijk binnen één ruimte geconcentreerd.
b. De ruimte waarbinnen de informatie en de gegevens aanwezig zijn is deugdelijk fysiek beveiligd.
c. De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.
d. Toegang tot de ruimte waar de gegevens of de informatie zich bevindt is uitsluitend toegestaan aan daartoe geautoriseerde personen voorzover dit voor hun functie noodzakelijk is.
e. Het binnentreden en verlaten van de ruimte moet zodanig zijn geregeld dat er sprake is van gecontroleerde en achteraf herleidbare toegang op individueel niveau.
f. Documenten waarin, dan wel verwisselbare gegevensdragers waarop, de informatie en de gegevens zijn vastgelegd worden in deugdelijk beveiligde opbergmiddelen bewaard.
g. Personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de informatie en de gegevens zich bevinden worden door eigen geautoriseerd personeel begeleid.

IV. Beheer van communicatie- en bedieningsprocessen

a. De status/rubricering van de informatie en de gegevens (staatsgeheim of vertrouwelijk) dient te allen tijde kenbaar te zijn.
b. Reproductie van de informatie of de gegevens is alleen toegestaan door daartoe geautoriseerde personen en uitsluitend voor zover dat nodig is voor de goede uitvoering van de bijzondere last dan wel toestemming op grond van de Wet op de

inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, van de wet dan wel een verzoek op grond van artikel 13.4 van de wet.
c. De informatie of de gegevens worden niet buiten de normale ruimte gebracht, tenzij dat voor de goede voortgang van de werkzaamheden noodzakelijk is. In dat geval wordt de verblijfplaats van de informatie of de gegevens geregistreerd.
d. De verwijdering en vernietiging van de informatie en gegevens geschiedt op een onomkeerbare wijze. Van de verwijdering en vernietiging wordt een rapport opgemaakt, dat in afschrift wordt gezonden aan de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie.

V. Toegangsbeveiliging van geautomatiseerde informatiesystemen

a. De toegang tot geautomatiseerde informatiesystemen waarin de informatie en de gegevens worden verwerkt is op deugdelijke wijze beveiligd, onder meer door middel van persoonsgebonden authenticatie.
b. De logische beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.
c. Het aantal foutieve inlogpogingen is beperkt tot drie. Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering, welke uitsluitend door de functionaris, bedoeld in onderdeel I van deze bijlage, kan worden opgeheven. Het voorgaande is niet van toepassing op de systeembeheerder, met dien verstande dat bij drie foutieve inlogpogingen een hernieuwde inlogpoging slechts kan plaatsvinden via een voor noodsituaties ingericht account en persoonsgebonden authenticatie voor het gebruik waarvan door de functionaris, bedoeld in onderdeel I van deze bijlage toestemming moet worden verleend.
d. Het geautomatiseerde systeem, waarin de gegevens en de informatie worden verwerkt, wordt niet eerder verlaten dan nadat een (handmatig of automatisch) toegangsbeveiligingsmechanisme in werking is gesteld.
e. Alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem worden persoonsgebonden vastgelegd teneinde onderzoek mogelijk te maken.
f. Toegang tot het geautomatiseerde informatiesysteem is uitsluitend voorbehouden aan daartoe geautoriseerd personeel.
g. De toegangsrechten van de gebruikers worden periodiek geëvalueerd.
h. De autorisaties van alle gebruikers worden vastgelegd.

VI. Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

a. Alle wijzigingen in apparatuur, software of procedures die de beveiliging van de gegevens en informatie kunnen beïnvloeden zijn controleerbaar, dat wil zeggen bekend en beoordeeld door of namens de aanbieder als zijnde aanvaardbaar.
b. Het onderhouden van geautomatiseerde informatiesystemen, voor zover deze nog toegang verschaffen tot gegevens en informatie, vindt op locatie plaats.
c. In afwijking van onderdeel b, is het op afstand onderhouden van geautomatiseerde informatiesystemen slechts toegestaan, indien dit wordt uitgevoerd door daartoe geautoriseerde personen als bedoeld in onderdeel II van deze bijlage, en slechts op tijdstippen waarvoor door de functionaris, bedoeld in onderdeel I, onder a, van deze bijlage, toestemming is verleend en er aantoonbaar voldoende waarborgen bestaan voor het handhaven van het beveiligingsniveau van de gegevens en informatie.
d. Reparatie aan het geautomatiseerde informatiesysteem waarin de informatie en de gegevens worden verwerkt vindt op locatie plaats. Van de eerste volzin kan worden afgeweken indien de informatie en gegevens zijn verwijderd en niet te achterhalen zijn.

G Dataset te bewaren gegevens op basis van aangepaste opgave van de behoeftestellers.

Uitwerking Nederlandse behoeftestelling van de Richtlijn Data retentie

Bijgaande lijst is gebaseerd op de lijst van gegevens zoals door het ministerie van Justitie aan VKA toegestuurd op 16 mei 2006 (kenmerk 024/PIDS/2006). Na overleg tussen aanbieders en behoeftestellers op 22 juni jongstleden zijn op advies van de werkgroep wetgeving een aantal velden verwijderd. De velden waarom het gaat zijn betalingsgegevens, paalnummers of locatiegegevens gedurende een communicatie en de locatie waar de lijn is gemonteerd.

Nationale vereisten:

- Een aanbieder dient voor elke dienst die deze levert de verkeersgegevens te bewaren. Per dienst worden de te bewaren verkeersgegevens in onderstaande lijst gespecificeerd. Ter illustratie: bij het versturen van E-mail via UMTS zijn 3 diensten van toepassing, te weten mobiele communicatie, IP access en E-mail.
- Datum en tijdstip dienen gebaseerd te zijn op ISO-normering.
- Telefoonnummers dienen in eenduidig formaat (E164) aangeleverd te worden.
- A, B, C nummers conform ETSI-definiëring.
- Alle elementen dienen voorzien te zijn van datum en tijd.
- Bij conference call dienen de gegevens van alle deelnemers te worden bewaard.
- Onder NAW gegevens worden verstaan de gegevens als vermeld in de telefoongids (naam, adres, woonplaats) en de gegevens van de contractant (naam, adres , woonplaats) en de afgenomen diensten/soort abonnement,

Te bewaren gegevens:

<u>Vaste telefonie</u>

Per gesprek (alsmede niet geslaagde oproepen) dienen de navolgende gegevens te worden bewaard:

- A-nummer
- B-nummer
- C-nummers
- NAW-gegevens
- Datum en tijdstip van start en einde communicatie
- Bearer service

<u>Mobiele communicatie</u>

Per gesprek (alsmede niet geslaagde oproepen) dienen de navolgende gegevens te worden bewaard:

- A-nummer
- B-nummer
- C-nummers

- NAW-gegevens
- Datum en tijdstip van start en einde communicatie
- Bearer/ teleservices (UMTS, GPRS, etc.)
- IMEI/IMSI
- In geval van anonieme prepaid service: datum/tijd van de initiële activering van de dienst en paalnummer (incl. x/y- coördinaten) waar vandaan de activering is gemaakt.
- Gegevens benodigd om de geografische locatie van zendmasten te bepalen.

IP access

Bij een log-on en log-off van een directe en/of indirecte verbinding met het internet dienen de navolgende gegevens te worden bewaard:

- Inlognaam / onderscheidend kenmerk
- NAW-gegevens
- IP-adres(sen)
- Datum en tijdstip van de log-on of log-off
- Gegevens om eindpunt te identificeren, in geval van :
- Inbellen - Telefoonnummer waarmee de klant inbelt;
- Wifi - MAC-adres netwerkkaart en ID/locatie Hotspots;
- DSL - Telefoonnummer en/of poortnummer;
- Kabel -MAC adres modem of ander identificerend kenmerk;
- VPN/tunnel - IP adres tunnel endpoint van de klant;
- GSM/UMTS/GPRS -telefoonnummer en Cell ID tijdens opzetten verbinding (NB ook het genoemde onder “mobiele communicatie” is van toepassing.

NB. Het voornaamste doel van deze gegevens is om zo veel mogelijk vast te kunnen stellen welk persoon/ systeem gebruik maakt van een bepaald IP adres.

E-mail

Per mailbericht dat door een aanbieder wordt verwerkt (alsmede niet geslaagde oproepen), dienen de navolgende gegevens te worden bewaard:

- IP-adres, of ander identificerend kenmerk indien verbinding niet over IP gaat, waarmee een mailbericht wordt opgehaald of verstuurd.
- E-mail adres verzender (ook het “FROM:” veld uit header en in geval van SMTP: “MAIL FROM:”)
- E-mail adres beoogde ontvangers (ook de “TO:” en “Cc:” velden uit de header en in geval van SMTP: “RCPT TO:”)
- De “Bcc:” adressen in het geval van het versturen van e-mail
- Andere e-mail adressen/aliassen van de klant
- Datum en tijdstip van communicatie
- Inlognaam/user ID
- NAW-gegevens (indien aanwezig)
- Wijze waarop mail wordt verzonden/ontvangen (POP, IMAP, SMTP, webmail, etc.)

NB. De verkeersgegevens van een mail dienen te worden bewaard op het moment dat een mail door een aanbieder tbv. een klant wordt verstuurd, op het moment dat een mail door een aanbieder

tbv. een klant wordt ontvangen en op het moment dat een mail door een aanbieder bij een klant wordt afgeleverd. Ook het versturen en lezen van mail via webmail vallen hieronder.

Internet telefonie

Per gesprek (alsmede niet geslaagde oproepen) dienen de navolgende gegevens te worden bewaard:

- Identificerend kenmerk van initiator (vgl. A-nummer)
- Identificerend kenmerk van opgeroepen persoon/ systeem (vgl. B-nummer)
- Identificerend kenmerk(en) waarnaar de verbinding is doorgeleid (vgl. C-nummers)
- IP adressen van alle gesprekspartners (ook wanneer deze niet identificerend zijn, vanwege routing/derde partijen)
- NAW-gegevens
- Datum /tijdstip van start en einde communicatie
- Inlognaam/onderscheidend kenmerk waarmee gebruiker te benaderen is.
- Codec (G711, MPEG4, etc.)
- Protocol (SIP, H323, etc.)
- Bij diensten met een PSTN-gateway: het door de gateway gebruikte PSTN-nummer.

H Gedetailleerd database ontwerp

Het databaseontwerp is uitgewerkt in apart bij te voegen Visio bestand.

I Scores per implementatieoptie in de kwalitatieve beoordeling

Wegings-factor categorie	Wegings-factor vraag	Parameter	DBA	DDT	CDT	HDT
30 punten	**(%)**	**Organisatie en processen**				
	20%	Efficiency van de bevraging bevragingsprocedure	Langzaam 0	Middel 3	Snel 6	Snel 6
	20%	Mogelijkheid van toetsing vordering op wettelijke grondslag door de aanbieder	Ja 6	Nee 0	Nee 0	Nee 0
	20%	Mogelijkheid van inhoudelijke ondersteuning door de aanbieder bij beantwoording van de vordering /bevraging	Ja 6	Nee 0	Nee 0	Nee 0
	20%	Flexibiliteit om met fluctuatie van de bevragingsvolume om te gaan	Klein 0	Groot 6	Groot 6	Groot 6
	20%	Mate waarin op eenvoudige wijze de verplichte rapportages aan de commissie kunnen worden opgeleverd	handmatig en decentraal 0	handmatig en decentraal 0	automatisch en centraal 6	automatisch en centraal 6
	100%	**Totaal**	**12**	**9**	**18**	**18**

Wegings-factor categorie	Wegings-factor vraag	Parameter	DBA	DDT	CDT	HDT
30 punten		**Technologie**				
	17%	Aansluiting op de huidig technologieën t.a.v. acquisitie	Deels 2,7	Deels 2,7	Deels 2,7	Deels 2,7
	17%	Aansluiting op de huidige technologieën t.a.v. opslag	Deels 2,7	Vervanging 0	Deels 2,7	Deels 2,7
	17%	Aansluiting op de huidig huidige technologieën t.a.v. bevraging	Hergebruik 5,1	Vervanging 0	Deels 2,7	Deels 2,7
	16%	Toekomstvastheid technologie t.a.v. schaalbaarheid	Middel 2,7	Middel 2,7	Goed 4,8	Goed 4,8
	16%	Toekomstvastheid technologie inpassing nieuwe diensten	Goed 4,8	Slecht 0	Middel 2,4	Middel 2,4
	16%	Toekomstvastheid technologie inpassing nieuwe vraagstellingen	Slecht 0	Goed 4,8	Goed 4,8	Goed 4,8
	100%	**Totaal**	**18**	**10,2**	**20,1**	**20,1**

Wegings-factor categorie	Wegings-factor vraag	Parameter	DBA	DDT	CDT	HDT
10 punten		**Business Case**				
	50%	Mate van beïnvloeding van de huidige marktverdeling tussen aanbieders	Licht 2,5	Groot 0	Groot 0	Groot 0
	50%	Mate van beïnvloeding van 'time to market' voor nieuwe diensten	Licht 5	Groot 0	Matig 2,5	Matig 2,5
	100%	**Totaal**	**7,5**	**0**	**2,5**	**2,5**

Wegings-factor categorie	Wegings-factor vraag	Parameter	DBA	DDT	CDT	HDT
20 punten		**Informatiebeveiliging**				
	10%	Vertrouwelijkheid van de relatie tussen de vraag en onderzoeker (Risico op informatielekkage)	Ja 0	Nee 2	Nee 2	Nee 2
	10%	Continuïteit van het bevragingsproces (risico van het niet-tijdig beschikbaar zijn van onderzoeksdata)	Middel 1	Middel 1	Goed 2	Goed 2
	10%	Vertrouwelijkheid en integriteit van de opgeslagen data (risico op lek of manipulatie)	Middel 1	Middel 1	Goed 2	Goed 2
	50%	De Audit Trail is in te richten conform gewenst beveiligingsniveau	Complex 0	Middel 5	Eenvoudig 10	Middel 5
	10%	Exclusiviteit van toegang (risico van oneigenlijk gebruik)	Middel 2	Complex 0	Eenvoudig 2	Eenvoudig 2
	10%	Vernietiging van de informatie na de bewaartermijn (risico op te lang bewaren)	Complex 0	Eenvoudig 2	Eenvoudig 2	Eenvoudig 2
	100%	**Totaal**	**4**	**11**	**20**	**15**

Wegings-factor categorie	Wegings-factor vraag	Parameter	DBA	DDT	CDT	HDT
10 punten		**Implementatie termijn**				
	100%	Tijd benodigd voor implementatie	< 1 jaar 10	> 1 jaar 0	> 1 jaar 0	> 1 jaar 0
	100%	**Totaal**	**10**	**0**	**0**	**0**

Totaalscore per implementatieoptie

Categorie	Decentrale opslag beantwoording door aanbieder	Decentrale opslag directe toegang	Centrale opslag directe toegang	Hybride opslag directe toegang
Organisatie en processen	12	9	18	18
Technologie	18	10,2	20,1	20,1
Business Case	7,5	0	2,5	2,5
Informatiebeveiliging	4	11	20	15
Implementatie termijn	10	0	0	0
Totaal	**51,5**	**30,2**	**60,6**	**55,6**

J Financiële overzichten per implementatiemodel

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 40.000	€ 1.890.000	€ 2.320.000	€ 2.860.000	€ 3.520.000	€ 4.330.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 3.410.000	€ 2.590.000	€ 3.080.000	€ 3.680.000	€ 4.400.000	€ 5.280.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Aanbieders	Acquisitie	€ 30.390.000	€ 4.880.000	€ 5.270.000	€ 5.690.000	€ 6.150.000	€ 8.380.000
	Opslag	€ 25.130.000	€ 670.000	€ 720.000	€ 780.000	€ 850.000	€ 910.000
	Bevraging	€ 8.020.000	€ 4.030.000	€ 660.000	€ 710.000	€ 770.000	€ 830.000
	Beheer	€ 14.800.000	€ 2.170.000	€ 2.340.000	€ 2.530.000	€ 2.730.000	€ 2.950.000
Subtotaal Aanbieders		€ 78.340.000	€ 11.750.000	€ 9.000.000	€ 9.720.000	€ 10.490.000	€ 13.080.000
Totaal		€ 81.750.000	€ 14.340.000	€ 12.080.000	€ 13.390.000	€ 14.890.000	€ 18.350.000

Figuur k-1: Decentrale opslag, beantwoording door aanbieder, gecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 40.000	€ 1.890.000	€ 2.320.000	€ 2.860.000	€ 3.520.000	€ 4.330.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 3.410.000	€ 2.590.000	€ 3.080.000	€ 3.680.000	€ 4.400.000	€ 5.280.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Aanbieders	Acquisitie	€ 30.390.000	€ 4.880.000	€ 5.270.000	€ 5.690.000	€ 6.150.000	€ 9.890.000
	Opslag	€ 21.560.000	€ 1.280.000	€ 1.490.000	€ 1.750.000	€ 2.050.000	€ 2.420.000
	Bevraging	€ 8.020.000	€ 4.030.000	€ 660.000	€ 710.000	€ 770.000	€ 830.000
	Beheer	€ 14.800.000	€ 2.170.000	€ 2.340.000	€ 2.530.000	€ 2.730.000	€ 2.950.000
Subtotaal Aanbieders		€ 74.770.000	€ 12.360.000	€ 9.760.000	€ 10.680.000	€ 11.700.000	€ 16.100.000
Totaal		€ 78.180.000	€ 14.950.000	€ 12.850.000	€ 14.360.000	€ 16.100.000	€ 21.370.000

Figuur k-2: Decentrale opslag, beantwoording door aanbieder, ongecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 4.570.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 7.950.000	€ 2.660.000	€ 3.170.000	€ 3.780.000	€ 4.530.000	€ 5.440.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Aanbieders	Acquisitie	€ 30.390.000	€ 5.550.000	€ 6.000.000	€ 6.480.000	€ 6.990.000	€ 7.550.000
	Opslag	€ 23.940.000	€ 670.000	€ 720.000	€ 780.000	€ 850.000	€ 910.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 14.800.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 69.120.000	€ 7.660.000	€ 8.270.000	€ 8.930.000	€ 9.650.000	€ 10.420.000
Totaal		€ 77.070.000	€ 10.320.000	€ 11.440.000	€ 12.710.000	€ 14.180.000	€ 15.860.000

Figuur k-3: Decentrale opslag, directe toegang, gecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 770.000	€ 950.000	€ 1.170.000	€ 1.440.000	€ 1.770.000
	Bevraging	€ 4.570.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 7.950.000	€ 3.430.000	€ 4.120.000	€ 4.950.000	€ 5.970.000	€ 7.210.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Subtotaal Intermediaire 3de		€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
Aanbieders	Acquisitie	€ 30.390.000	€ 5.430.000	€ 5.950.000	€ 6.520.000	€ 7.170.000	€ 7.900.000
	Opslag	€ 21.560.000	€ 550.000	€ 680.000	€ 830.000	€ 1.020.000	€ 1.260.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 14.800.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 66.740.000	€ 7.410.000	€ 8.170.000	€ 9.030.000	€ 10.000.000	€ 11.110.000
Totaal		€ 74.690.000	€ 10.850.000	€ 12.290.000	€ 13.980.000	€ 15.970.000	€ 18.320.000

Figuur k-4: Decentrale opslag, directe toegang, ongecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 1.120.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 4.500.000	€ 2.660.000	€ 3.170.000	€ 3.780.000	€ 4.530.000	€ 5.440.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 18.050.000	€ 390.000	€ 420.000	€ 450.000	€ 480.000	€ 520.000
	Bevraging	€ 3.450.000	€ 420.000	€ 450.000	€ 490.000	€ 530.000	€ 570.000
	Beheer	€ 4.290.000	€ 740.000	€ 790.000	€ 860.000	€ 930.000	€ 1.000.000
Subtotaal Intermediaire 3de		€ 25.780.000	€ 1.540.000	€ 1.660.000	€ 1.800.000	€ 1.940.000	€ 2.100.000
Aanbieders	Acquisitie	€ 30.390.000	€ 4.880.000	€ 5.270.000	€ 5.690.000	€ 6.150.000	€ 6.640.000
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 7.470.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 37.860.000	€ 6.320.000	€ 6.820.000	€ 7.370.000	€ 7.960.000	€ 8.590.000
Totaal		€ 68.140.000	€ 10.520.000	€ 11.650.000	€ 12.940.000	€ 14.420.000	€ 16.130.000

Figuur k-5: Centrale opslag, directe toegang, gecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 1.120.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 4.500.000	€ 2.660.000	€ 3.170.000	€ 3.780.000	€ 4.530.000	€ 5.440.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 16.680.000	€ 740.000	€ 860.000	€ 1.000.000	€ 1.180.000	€ 1.390.000
	Bevraging	€ 3.450.000	€ 420.000	€ 450.000	€ 490.000	€ 530.000	€ 570.000
	Beheer	€ 4.290.000	€ 740.000	€ 790.000	€ 860.000	€ 930.000	€ 1.000.000
Subtotaal Intermediaire 3de		€ 24.420.000	€ 1.890.000	€ 2.100.000	€ 2.350.000	€ 2.630.000	€ 2.960.000
Aanbieders	Acquisitie	€ 30.390.000	€ 4.880.000	€ 5.270.000	€ 5.690.000	€ 6.150.000	€ 6.640.000
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 7.470.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 37.860.000	€ 6.320.000	€ 6.820.000	€ 7.370.000	€ 7.960.000	€ 8.590.000
Totaal		€ 66.780.000	€ 10.870.000	€ 12.090.000	€ 13.500.000	€ 15.120.000	€ 16.990.000

Figuur k-6: Centrale opslag, directe toegang, ongecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 1.120.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 4.500.000	€ 2.660.000	€ 3.170.000	€ 3.780.000	€ 4.530.000	€ 5.440.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 1.370.000	€ 70.000	€ 90.000	€ 110.000	€ 130.000	€ 160.000
	Bevraging	€ 3.450.000	€ 420.000	€ 450.000	€ 490.000	€ 530.000	€ 570.000
	Beheer	€ 6.810.000	€ 740.000	€ 790.000	€ 860.000	€ 930.000	€ 1.000.000
Subtotaal Intermediaire 3de		€ 11.620.000	€ 1.230.000	€ 1.330.000	€ 1.450.000	€ 1.590.000	€ 1.730.000
Aanbieders	Acquisitie	€ 30.390.000	€ 5.430.000	€ 5.870.000	€ 6.330.000	€ 6.840.000	€ 7.390.000
	Opslag	€ 23.940.000	€ 550.000	€ 590.000	€ 640.000	€ 690.000	€ 750.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 7.470.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 61.800.000	€ 7.410.000	€ 8.010.000	€ 8.650.000	€ 9.340.000	€ 10.090.000
Totaal		€ 77.920.000	€ 11.300.000	€ 12.510.000	€ 13.880.000	€ 15.450.000	€ 17.260.000

Figuur k-7: Hybride opslag, directe toegang, gecorreleerde opslag

Betrokkene	kostensoort	Jaar 1 CAPEX	Jaar 1 OPEX	Jaar 2 OPEX	Jaar 3 OPEX	Jaar 4 OPEX	Jaar 5 OPEX
Behoeftestellers	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Bevraging	€ 1.120.000	€ 1.960.000	€ 2.410.000	€ 2.970.000	€ 3.650.000	€ 4.490.000
	Beheer	€ 3.380.000	€ 700.000	€ 760.000	€ 820.000	€ 880.000	€ 950.000
Subtotaal Behoeftestellers		€ 4.500.000	€ 2.660.000	€ 3.170.000	€ 3.780.000	€ 4.530.000	€ 5.440.000
Intermediaire derde	Acquisitie	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Opslag	€ 0	€ 420.000	€ 520.000	€ 640.000	€ 780.000	€ 960.000
	Bevraging	€ 3.450.000	€ 420.000	€ 450.000	€ 490.000	€ 530.000	€ 570.000
	Beheer	€ 6.810.000	€ 740.000	€ 790.000	€ 860.000	€ 930.000	€ 1.000.000
Subtotaal Intermediaire 3de		€ 10.260.000	€ 1.580.000	€ 1.760.000	€ 1.980.000	€ 2.240.000	€ 2.530.000
Aanbieders	Acquisitie	€ 30.390.000	€ 5.430.000	€ 5.870.000	€ 6.330.000	€ 6.840.000	€ 7.390.000
	Opslag	€ 21.560.000	€ 550.000	€ 590.000	€ 640.000	€ 690.000	€ 750.000
	Bevraging	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
	Beheer	€ 7.470.000	€ 1.430.000	€ 1.550.000	€ 1.670.000	€ 1.810.000	€ 1.950.000
Subtotaal Aanbieders		€ 59.420.000	€ 7.410.000	€ 8.010.000	€ 8.650.000	€ 9.340.000	€ 10.090.000
Totaal		€ 74.170.000	€ 11.650.000	€ 12.940.000	€ 14.410.000	€ 16.110.000	€ 18.060.000

Figuur k-8: Hybride opslag, directe toegang, ongecorreleerde opslag