AANBIEDINGSFORMULIER VOOR ONDERRADEN

13

Onderraad: MICIV

handtekening:

Minister van Binnenlandse Zaken en Koninkrijksrelaties
Minister van Grote Steden - en Integratiebeleid

02G430540

coördinerend bewindspersoon Minister van BZK

(eventueel namens deze) minister van Financiën

1a Datum indiening bij onderraad: ') 10 april 2002 1b Kenmerk coördinerend bewindspersoon: ')	10. Het voorstel - is aangekondigd in de regeringsverklaring - de troonrede - de begroting - het parlement - hangt samen met verplichtingen op grond van internationale verdragen en met name Europese regelgeving - komt voort uit een gedachtewisseling in het SG-Beraad die naar aanleiding van de gebeurtenissen van 11 september 2002 is gevoerd
2a Datum verzending naar coördinerend bewindspersoon: 10 april 2002 2b Kenmerk/Afdeling: IOS/IC2002/N67004	11. Korte titel: Beveiligd communiceren tussen bewindspersonen en ambtenaren
3. Motivering indien moet worden afgeweken van de 10-dagentermijn: ') n.v.t.	12. Korte inhoud en doelsteling: In de notitie Veilig Communiceren (VeCom) wordt geschetst hoe op korte termijn enkele acute knelpunten op het gebied van beveiliging van de communicatie tussen bewindspersonen en hun ambtenaren opgelost kunnen worden. Deze korte-termijnoplossingen worden geplaatst in een lange-termijn-perspectief.
4. Hamerstuk	
5. Datum evt. voorgaande behandeling:	
4. Aan EU-notificatieverplichting voldaan: N.v.t.	
7. Advies uitgebracht door adviescollege(s): CVIN	
8. Interdepartementaal voorbereid met: - Financiën (DG Rijksbegroting): ☐ - Justitie (wetgevingstoets incl. deregulering): ☐ - Overige departementen: - Departementen die deel uitmaken van CVIN Overeenstemming bereikt: 4. Ja	13. Voorgestelde conclusies: De volgende beslispunten liggen voor: - Akkoord gaan met de aanschaf van de voorgestelde secure GSM's - Akkoord gaan met versleuteling van de kosten voorafgaand aan de opdrachtverlening naar rato van afname - Verlenen van medewerking aan het zo spoedig mogelijk definitief vaststellen van het per departement te bestellen aantal toestellen - onderschrijft u in beginsel de behoefte aan een besloten netwerk voor e-mail dat elektronisch en fysiek is afgesloten van andere communicatiemiddelen; - bent u in beginsel bereid, indien in het DTO-onderzoek (incl. risico-analyse) nut, noodzaak en haalbaarheid van TopNet onomstotelijk wordt vastgesteld, (ook in financiële zin) mee te werken aan de realisatie van TopNet.
9. Behandeld in ambtelijk voorportaal: ') - SG-Beraad (20 maart) - CVIN (29 maart)	
Overeenstemming bereikt: 4. Ja ')	

14. 14. Gevolgen voor de rijksbegroting op korte of lange termijn voor de meerjarenafspraken, voor de sociale lasten, eventuele financiële gevolgen voor lagere publieksrechtelijke lichamen of betrokken instellingen:
geen

NB Op grond van art. 15 Comptabiliteitswet dient bij voorstellen van wet met financiële gevolgen en bij mededelingen aan de Staten-Generaal over voorgenomen beleidsvoorstellen, het standaardformulier 'overzicht van de financiële gevolgen voor de rijksbegroting' te zijn gevoegd.

15. Gevolgen voor de arbeidsmarkt:
een beslag van ca. 4 man van de capaciteit van DTO in drie maanden.

Gevolgen voor het rijksapparaat:
geen

- personeelsbezetting:
geen

- huisvesting:
geen

- millenniumtoets:
geen

17. Aanvullende opmerkingen:

18. Naam en telefoonnummer contactpersoon:

)Getekend aanbiedingsformulier in originali (enkelvoud) te verzenden aan de coördinerend bewindspersoon, die de rubrieken 1, 3, 9 en eventueel 17 invult.

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

Datum
10 april 2002

Ons kenmerk
IOS/IC2002/U67004

Onderdeel
DGOB/IOS/I&C

Inlichtingen

Uw kenmerk

Blad
1 van 2

Aantal bijlagen
1

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Aan de voorzitter en leden van de MICIV

Onderwerp
Veilig Communiceren

Hierbij zend ik u de notitie Veilig Communiceren, waarin wordt geschetst hoe op korte termijn enkele acute knelpunten in de beveiliging van de communicatie tussen bewindspersonen en ambtenaren opgelost kunnen worden. Deze korte-termijn-oplossingen worden geplaatst in een lange-termijn-perspectief.

Uitgangspunt voor de langere termijn is de verwachting dat door stapsgewijze integratie van een aantal bouwstenen als RYX, NAFIN, de Haagse Ring, CERT en PKI gekomen kan worden tot een hoger beveiligingsniveau van de Rijksbrede datacommunicatie. Het ambitieniveau is de elektronische communicatie binnen de gehele Rijksoverheid zo te beveiligen dat langs één Rijksbrede infrastructuur alle informatie waar nodig tot en met het niveau Stg. Confidentieel elektronisch uitgewisseld kan worden. De notitie schetst hoe deze integratie op middellange termijn gerealiseerd zou kunnen worden, maar geeft tevens aan dat door het ontbreken van financiële middelen er nog geen zicht is op uitvoering van dit Integratietraject. Op dit vlak worden daarom nu geen concrete beslispunten aan u voorgelegd.

Daarnaast is er echter op korte termijn dringend behoefte aan veilige interdepartementale uitwisseling van gevoelige informatie tussen bewindspersonen en hun naaste adviseurs. De huidige uitwisseling van papieren documenten is in principe veilig, maar beantwoordt onvoldoende aan de huidige dynamische informatiebehoeften. De beschikbare vaste telefonieverbindingen zijn onvoldoende veilig. Hetzelfde geldt voor het e-mailverkeer via openbare netwerken. Daarom zijn in dit verband twee terreinen geïdentificeerd waarop onmiddellijk actie nodig is: mobiele telefonie en e-mail. In de notitie staan de voorgestelde beslispunten concreet aangegeven. Ik verwijs u daarnaar.

Op langere termijn is voor de beveiliging van dit soort communicatietoepassingen de inrichting van een cryptofaciliteit randvoorwaarde. Ook hieraan besteedt de notitie voor het integrale beeld aandacht, zij het dat de besluitvorming hierover een separaat traject volgt.

Over de financiering wil ik nog het volgende opmerken. Omdat het om een Rijksbreed project gaat waar ieder departement belang bij heeft, ligt het niet voor de hand dat de financiering op de schouders van één of enkele departementen komt. Omdat bij beveiliging het geheel net zo sterk is als de zwakste schakel, biedt een integrale aanpak, ook in de financiering, de meeste kans op succes. Tenslotte is haast geboden vanwege de risico's die de huidige telefonische en elektronische communicatie tussen bewindpersonen en hun naaste adviseurs met zich meebrengen.
BZK heeft evenals Defensie en BuZa in de begrotingsbrief aandacht gevraagd voor generale compensatie van de incidentele en structurele kosten voortvloeiende uit de in notitie beschreven projectvoorstellen. In het overleg tussen de ministers van Financiën, BZK en GSI is echter geconcludeerd dat er vooralsnog geen ruimte is voor generale compensatie. Daarom worden in de notitie op de verschillende onderdelen verschillende financieringsvoorstellen gedaan.

De notitie is besproken in het SG-Beraad van 20 maart en de CVIN van 29 maart. Zowel SG-Beraad als CVIN onderschreven de noodzaak om de in de notitie beschreven problemen aan te pakken en konden instemmen met de voorgestelde oplossingen met de aantekening dat definitieve besluitvorming over aanschaf secure gsm's en het vaststellen van de behoefte aan TopNet in de Ministerraad moet plaatsvinden.
T.a.v. TopNet hebben de in het SG-Beraad en CVIN vertegenwoordigde ministeries de principiële bereidheid uitgesproken om mee te doen aan de ontwikkeling van TopNet en daaraan ook financieel bij te zullen dragen als het door DTO uit te voeren onderzoek, inclusief risicoanalyse, nut en noodzaak van TopNet uitwijst. Een separate en op basis van de uitkomst van het onderzoek uitgewerkte go/no go beslissing - ook ten aanzien van de financiering - dient dan aan SG-beraad en Ministerraad te worden voorgelegd.

DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES,

K.G. de Vries

[redacted]

Veilig Communiceren (VeCom)

Beveiligde communicatie tussen bewindspersonen en ambtenaren

1 Aanleiding: context en opzet van deze notitie

Ongewenste verspreiding van informatie, bijvoorbeeld als gevolg van afluisteren of hacken, kan een bedreiging vormen voor de eenheid van de Kroon en het regeringsbeleid, de veiligheid van de Staat of economische belangen. Dergelijke informatie wordt derhalve beveiligd door middel van administratieve, bouwkundige, technische en personele maatregelen. De moderne communicatietechnologie vergemakkelijkt en versnelt de uitwisseling van informatie en biedt daardoor – ook binnen de overheid - kansen voor een efficiënte wijze van communicatie. Tegelijkertijd wordt echter steeds meer duidelijk, dat de veiligheid van de informatiewisseling niet (meer) op alle onderdelen voldoende is gewaarborgd.

Het op grote schaal afluisteren van telecommunicatie in het zgn. Echelon-programma stond in 2001 zowel op nationaal als Europees niveau in de belangstelling. Het kabinet heeft de TK hierover in de brief van 19 januari 2001 (27591, nr. 1) geïnformeerd en vervolgens op 14 juni 2001 (27591, nr 2) de vragen van de TK naar aanleiding van deze brief beantwoord. Tevens is de ambtelijke Taskforce Echelon ingesteld waarvan recent het Plan van Aanpak door de Ministerraad is goedgekeurd.

De gebeurtenissen van 11 september 2001 en de internationale strijd tegen het terrorisme hebben het belang van beveiliging, in alle opzichten, extra onderstreept. Het kabinet onderkent in het Actieplan Terrorismebestrijding en Veiligheid dat op 5 oktober 2001 (27925, nr 10) aan de TK is aangeboden, dat terroristische organisaties intensief gebruik maken van moderne technologie. Daarom is het noodzakelijk dat de overheid de meest geavanceerde technische hulpmiddelen inzet om (elektronisch) afluisteren door terroristische en criminele organisaties te voorkomen.

Mede naar aanleiding daarvan hebben de SG's/DG's van de meestbetrokken departementen (BZK, Def, BuZ, VW, Fi) op initiatief van de SG AZ in 2001 besloten tot een analyse van de knelpunten in en oplossingsmogelijkheden voor VEilig COMmuniceren (VECOM) binnen de rijksoverheid (hierna te noemen: VECOM-stuurgroep). Daaruit is onder meer gebleken, dat de communicatie tussen bewindspersonen onderling en met hun (top-)ambtenaren, zowel via de telefoon als elektronisch, kwetsbaar is voor afluisteren. Daarnaast sluit het aanbod van optimaal beveiligde moderne telecommunicatiemiddelen onvoldoende aan bij de behoefte.

Bij veilig communiceren zijn alle departementen betrokken. Een rijksbrede benadering is derhalve essentieel. Alvorens oplossingen te implementeren, is het van belang dat de noodzaak van veilig communiceren, en de huidige knelpunten daarin, breed worden onderschreven. Vervolgens is "commitment" van alle departementen onontbeerlijk voor de aanpak van deze knelpunten. De oplossingsrichtingen die door de VECOM-stuurgroep zijn geïdentificeerd, geven hiertoe de aanknopingspunten.

De opzet van de notitie is als volgt. In hoofdstuk 2 wordt de huidige situatie op het gebied van beveiligde communicatie geschetst. Daarbij wordt tevens ingegaan op de noodzaak om veilig te kunnen communiceren, en de knelpunten die ten aanzien daarvan zijn geïdentificeerd.
Hoofdstuk 3 schetst vier oplossingsrichtingen voor de korte en de lange termijn. Daarvan hebben de projecten Mobiele telefonie en Topnet betrekking op de korte termijn. Zij behelzen de aanschaf resp. realisatie van een concreet communicatiemiddel (nl. secure GSM's en een beveiligd e-mail-netwerk) voor een beperkte groep van gebruikers (nl. bewindspersonen en top-ambtenaren). De twee laatste projecten hebben betrekking op de langere termijn. Zo is het project Cryptofaciliteit van belang voor de

waarborging van een adequaat beveiligingsniveau van communicatie. Zonder Nederlandse encryptie is het niet mogelijk de veiligheid van vertrouwelijke tot (zeer) geheime communicatie te garanderen. Dit project kan derhalve op langere termijn worden beschouwd als een randvoorwaarde, die continuering van beveiligde communicatie op topniveau mogelijk moet maken. Het laatste project Integratie richt zich op de verhoging van het beveiligingsniveau binnen en verbreding naar de gehele Rijksoverheid.
In hoofdstuk 4 wordt een aanzet gegeven voor de projectstructuur, waaronder de aansturing, planning en financiering. Hierin is uitgegaan van betrokkenheid van alle departementen, waarbij BZK het voortouw heeft.

Alleen voor de projecten Mobiele Telefonie en TopNet worden beslispunten aan u voorgelegd.
Besluitvorming over de Cryptofaciliteit vindt plaats in een afzonderlijk traject. Besluitvorming over het project Integratie is nog niet aan de orde, omdat er geen zicht is op financiering van de eerste onderzoeksfase, noch het gehele Integratietraject. Voor de financiering van dit traject was een claim ingediend bij Financiën in het kader van de Voorjaarnota/Kaderbrief-besluitvorming. In het overleg tussen de bewindslieden van Financiën, BZK en GSI is echter geconcludeerd dat er voor de uitvoering van dit traject vooralsnog geen middelen beschikbaar zijn en dat het op een later moment (NJN 2002 dan wel begrotingsvoorbereiding 2004) opnieuw geagendeerd kan worden.

2 De noodzaak van veilige communicatie: huidige situatie en knelpunten

De noodzaak tot beveiliging van informatie en communicatie binnen de rijksoverheid vloeit voort uit een aantal belangen die bescherming behoeven. Hierbij moet onder meer gedacht worden aan informatie waarvoor geldt dat kennisname door niet gerechtigden schade kan toebrengen aan het belang van de staat of zijn bondgenoten, zoals gegevens met betrekking tot de krijgsmacht en de inlichtingen- en veiligheidsdiensten, het te voeren regeringsbeleid en de eenheid van de Kroon: de zogenaamde staatsgeheimen. In dit verband worden de notulen van de ministerraad als Staatsgeheim-Zeer geheim gerubriceerd en geldt een strikt regime ten aanzien van de verspreiding hiervan. Daarnaast dient de overheid zorgvuldig om te gaan met vertrouwelijke informatie afkomstig van derden. Voorkomen moet worden dat onbevoegden kennis kunnen nemen van deze informatie.

Dergelijke informatie zal veelal op een hoog politiek en ambtelijk niveau worden uitgewisseld. Daarom bestaat er juist op dit niveau een acute noodzaak voor een adequate beveiliging.

2.1 Regelgeving

De regelgeving die ziet op de beveiliging van informatie binnen de Rijksoverheid is vastgelegd in het Voorschrift Informatiebeveiliging Rijksdienst (VIR). Daarnaast zijn in de aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst (AAR-9) specifieke regels vastgelegd voor de beveiliging van staatsgeheimen. Deze uit 1989 daterende regeling bevat nauwelijks aanwijzingen met betrekking tot de huidige ICT-omgeving. Ten aanzien van de overdracht van staatsgeheimen via telecommunicatiemiddelen is in de AAR-9 vastgelegd dat dit uitsluitend mag geschieden indien gebruik wordt gemaakt van een veilige verbinding en/of een vercijfersysteem die door de voormalige Nationale Verbindingsbeveiligingsraad is goedgekeurd voor de betreffende rubricering. Daarnaast geldt als eis dat zeer geheim gerubriceerde gegevens in principe slechts mogen worden verwerkt op apparatuur die exclusief voor die opdracht is toegewezen.
Op dit moment wordt de AAR-9 herzien. In de herziene regeling - het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) - is ten aanzien van de ICT-omgeving vastgelegd dat de ICT-beveiligingsapparatuur die gebruikt wordt voor de beveiliging van staatsgeheimen moet zijn goedgekeurd door de minister van Binnenlandse Zaken en Koninkrijksrelaties.

Tevens is vastgelegd dat netwerken waarover informatie op het niveau Staatsgeheim Geheim en hoger wordt gecommuniceerd noch direct noch indirect mogen zijn gekoppeld aan externe netwerken. Bij het laatste moet worden gedacht aan internet. Dit betekent dat – zonder het treffen van adequate beveiligings- en cryptovoorzieningen - geen gebruik kan worden gemaakt van het Rijksoverheidsintranet voor uitwisseling van informatie die als Staatsgeheim-Geheim en -Zeer geheim zijn gerubriceerd.

2.2. De huidige praktijk

Naast de beveiligde (gerubriceerde) schriftelijke informatie-uitwisseling, kan thans door een beperkte groep personen (bewindspersonen en hoge ambtenaren) slechts gebruik worden gemaakt van het ministersnet. Dit bestaat uit een vaste telefoonverbinding. Ooit betrof dit een aparte ringlijn met een beperkt aantal aansluitingen die werd beheerd door een zeer beperkt aantal medewerkers van de toenmalige PTT. Tegenwoordig echter valt de lijn onder het reguliere netwerkbeheer van KPN. Nieuwe aansluitingen zijn in de loop der tijd (gedeeltelijk) gerealiseerd via het reguliere KPN-net. Het ministersnet is dus onvoldoende veilig.
Bovendien is het concept van vaste aansluitingen inmiddels achterhaald. Bewindslieden en hoge ambtenaren maken in toenemende mate gebruik van mobiele – en dus onbeveiligde telefoons.

Daarnaast wordt in toenemende mate van e-mail gebruik gemaakt. Het is immers sneller en eenvoudiger dan het versturen van schriftelijke stukken. Het is echter ook relatief eenvoudig door derden af te tappen. In de praktijk is reeds nu al niet te voorkomen dat ook op hoog politiek en ambtelijk niveau van dit communicatiemiddel gebruik wordt gemaakt voor informatie die vanwege de inhoud gerubriceerd zou moeten zijn. In plaats van te trachten dit te beperken, ligt het in de rede het beveiligingsniveau hiervan te optimaliseren.

3 Oplossingsrichtingen

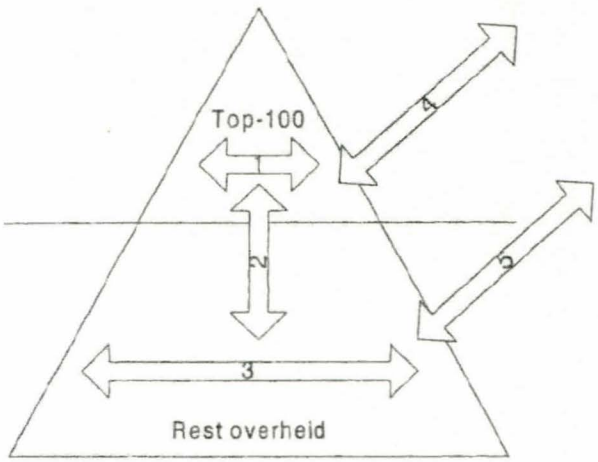
3.1 De ideale situatie

Een adequaat beveiligde communicatie binnen de rijksoverheid omvat meer dan de communicatie tussen bewindspersonen en hoge ambtenaren Zij communiceren ook met hun beleidsambtenaren en deze communiceren weer onderling met elkaar. Allen communiceren ook met de buitenwereld. In de optimale situatie zou op alle niveaus veilig dienen te kunnen worden gecommuniceerd, ook als dit informatie betreft die de eenheid van de Kroon, het regeringsbeleid of de veiligheid van de Staat raakt of als het commercieel vertrouwelijke informatie betreft. Dit heeft betrekking op de volgende informatiestromen (in volgorde van prioriteit, zie ook figuur 1):

1. communicatie tussen top-100 onderling;
2. communicatie tussen top-100 en ambtenaren
3. communicatie tussen ambtenaren onderling
4. communicatie van top-100 naar buiten
5. communicatie ambtenaren naar buiten

Deze informatiestromen bestaan en zijn reeds ingevuld. Op de meeste departementen heeft iedereen Internet (e-mail), van ambtenaar tot en met minister (informatiestromen 4 en 5). Aan informatiestroom 3 wordt reeds inhoud gegeven door middel van RYX (het intranet voor de gehele Rijksoverheid) in combinatie met departementale netwerken. De informatiestroom tussen bewindslieden en hun ambtenaren (informatiestroom 2) wordt daarmee ook belangrijk, want bewindslieden zullen ook met hun medewerkers willen kunnen communiceren. De ervaring leert dat als personen op verschillende niveaus van beveiliging niet transparant met elkaar kunnen communiceren, die communicatie zich niet

via de beveiligde verbindingen afspeelt, maar dat de makkelijkste en dus vaak onbeveiligde weg wordt gekozen, hetgeen ongewenst is. Dit is ook een technisch probleem, maar vooral een psychologisch; de belangrijkste en meest onderschatte voorwaarde voor het tot een succes maken van een technische innovatie. Dit geldt au fond ook voor de communicatie naar buiten: ministers en ambtenaren communiceren ook met de buitenwereld. Dit stelt enerzijds eisen aan de gebruikersvriendelijkheid van de oplossing, anderzijds aan de beveiligingszin van de gebruikers.



Figuur 1. Communicatiepiramide van de Rijksoverheid.

3.2 Beveiligingsniveau

Het ambitieniveau zou idealiter moeten zijn om alle communicatie tussen bewindslieden en ambtenaren en tussen ambtenaren onderling over de volle breedte van de Rijksdienst maximaal te beveiligen, zodat ook informatie die tot Stg. Zeer geheim is gerubriceerd, door betrokkenen kan worden gewisseld. Dat is echter op korte termijn vanuit technisch en financieel oogpunt niet haalbaar. Voorgesteld wordt derhalve een onderscheid te maken tussen oplossingsrichtingen die op korte termijn kunnen worden geïmplementeerd en oplossingen voor de lange termijn.

Voor de korte termijn ligt het in de rede prioriteit te geven aan beveiliging van communicatie binnen de Top-100. Immers, juist op dat niveau wordt informatie uitgewisseld waarvan ongewenste verspreiding de belangen van de Staat ernstig kan aantasten. Het is van groot belang dat de bewindspersonen en hoge ambtenaren op beveiligde wijze kunnen communiceren.

Aan twee soorten communicatiemiddelen bestaat op korte termijn behoefte binnen de Top-100: (mobiele) telefonie en datacommunicatie (e-mail).

3.3 Korte termijn

3.3.1 GSM

Het is mogelijk op korte termijn een oplossing te realiseren voor mobiele (en vaste) telefonie die voorziet in beveiliging tot en met Stg-confidentieel. Deze oplossing kan relatief snel gerealiseerd worden.

Door de Noorse overheid is een secure GSM, de NSK 200, ontwikkeld die qua beveiliging hoog scoort in vergelijking met de op de markt beschikbare secure GSM's. Deze NSK 200 is ook goedgekeurd voor gebruik binnen de NAVO (tot en met de classificatie 'NATO-secret'). Het is het enige beschikbare toestel dat volgens het NBV voldoende beveiliging biedt voor communicatie van bijzondere informatie.

De NSK 200 is niet alleen als GSM te gebruiken voor mobiel bellen, maar ook als een vast toestel op het bureau (met een zogenaamd 'DECT'-basisstation).

Het toestel is ontworpen met beveiliging als primair uitgangspunt. Daardoor is het een zeer goed beveiligd toestel. De spraak wordt versleuteld door middel van een Noorse cryptografische chip in het toestel. Dit is een belangrijk nadeel. Het betekent dat rekening gehouden moet worden met de mogelijkheid van Noorse manipulatie (waarvan de VS weet kan hebben omdat zij de evaluatie voor de NAVO-goedkeuring uitgevoerd hebben en daartoe alle technische details van het systeem onder ogen hebben gehad). Door middel van een Nederlandse evaluatie van het systeem en door het gebruik van Nederlandse sleutels daar waar mogelijk, kan het nadeel van het gebruik van Noorse cryptografie (i.p.v. Nederlandse) in zekere mate ondervangen worden. Het ontbreken van een Nederlands cryptohart in de NSK 200 betekent dat het toestel met een oorspronkelijk hoge beveiligingswaarde ('NATO-secret') in de Nederlandse context niet zomaar beschouwd kan worden als een communicatiemiddel voor informatie tot en met 'Stg. Geheim'. Met in achtneming van het genoemde nadeel zou het toestel gebruikt kunnen worden als een 'interim confidentieel' oplossing.

Een definitieve oplossing (voor communicatie tot en met Stg. Geheim) is alleen mogelijk als de Cryptofaciliteit een Nederlandse cryptochip realiseert die in een secure GSM past. Dit vergt dus een lange-termijn oplossing. Project 3 (Cryptofaciliteit) schept hiervoor de randvoorwaarden.

Met de aanschaf van deze GSM's wordt op een termijn van drie tot zes maanden dus voorzien in beveiligde telefonie, die ook mobiel kan worden gebruikt. Naar verwachting zullen deze GSM's voor ca. 3 tot 4 jaar worden gebruikt, waarna de definitieve oplossing kan worden gerealiseerd. Aanschaf van deze GSM's is slechts te rechtvaardigen indien hiervan in de praktijk door betrokkenen ook daadwerkelijk gebruik wordt gemaakt. Dit is mede afhankelijk van het gebruiksgemak. Het toestel is in vergelijking met reguliere GSM's relatief groot en zwaar. Derhalve wordt hierbij een voorbeeld van het toestel voorgelegd.

Het beveiligingsniveau, de gebruiksduur en het gebruiksgemak moeten worden afgewogen tegen de kosten. Deze bedragen per toestel eenmalig bij aanschaf € 7.300,--. Dit is inclusief DECT-station, sleutelmanagement, mogelijkheid tot aansluiting op het vaste net en beheer. Voor de financiering wordt voorgesteld de aanschaf- en structurele kosten, voorafgaand aan de opdrachtverlening, naar rato van het aantal per departement aan te schaffen toestellen te versleutelen over de departementen.

Omdat bij beveiliging het geheel net zo sterk is als de zwakste schakel is het van belang dat departementen zich voordat de aanschaforder wordt geplaatst, verbinden tot aanschaf van de toestellen voor en gebruik door alle bewindspersonen en top-ambtenaren uit de doelgroep. Immers zodra één persoon uit de doelgroep via een ander toestel communiceert met andere personen uit de doelgroep, is de communicatie per definitie onveilig. De consequentie van de beslissing tot aanschaf en gebruik is derhalve dat alle bewindspersonen en top-ambtenaren alleen nog dit toestel gebruiken voor al hun telefoongesprekken. Het toestel vervangt zowel hun huidige vaste als mobiele telefoons. Het vaststellen van de preciese omvang van de doelgroep per departement en daarmee het aantal per departement aan te schaffen toestellen, zal de eerste stap in het aanschaftraject zijn.

Beslispunten

- ***Akkoord gaan met de aanschaf van de voorgestelde secure GSM's***
- ***Akkoord gaan met versleuteling van de kosten voorafgaand aan de opdrachtverlening naar rato van afname***
- ***Verlenen van medewerking aan het zo spoedig mogelijk definitief vaststellen van het per departement te bestellen aantal toestellen***

3.3.2 *Beveiligd elektronisch communiceren voor bewindspersonen (TopNet)*

Met de huidige stand van techniek kan een oplossing voor elektronische communicatie (e-mail-verkeer) worden gerealiseerd voor informatie die is gerubriceerd tot en met STG Geheim. Elektronische datacommunicatie voor het niveau STG Zeer Geheim is binnen enkele jaren technisch niet mogelijk.

Dit betekent dat TopNet voorziet in een datanetwerk voor een selecte groep van 100 tot 150 gebruikers (bewindspersonen, top-ambtenaren en hun secretaresses) met mogelijkheden voor onderlinge e-mail en het raadplegen van elektronische dossiers op de vaste kantoorlocaties. Op de werkstations zullen de gebruikelijke ondersteunende applicaties zoals tekstverwerking beschikbaar zijn. Overige functionaliteiten zijn later toe te voegen zoals: videoconferencing, adressengids, elektronische agenda, inscannen van documenten, chatten etc.

TopNet kan gebruikt worden in besluitvormingscircuits waarin veel gerubriceerde documenten binnen de doelgroep moeten worden uitgewisseld. Een voorbeeld van zo'n circuit is de besluitvorming in Ministerraad, Onderraden en Ministeriele commissies.
Op grond van het maximaal haalbare beveiligingsniveau kan Topnet in dit kader worden gebruikt voor:

- Agenda van de ministerraad, onderraden en ministeriele commissies;
- Besluitenlijst van de ministerraad, onderraden en ministeriele commissies;
- Voorstellen aan de ministerraad, onderraden en ministeriele commissies (MR-stukken)
- Vertrouwelijke correspondentie en gedachtenuitwisseling tussen bewindspersonen en hoge ambtenaren en hoge ambtenaren onderling rond deze stukken.

Gelet op het huidige rubriceringsniveau van de ministerraadsnotulen (Stg. Zeer Geheim) kan voor de verspreiding hiervan in beginsel geen gebruik worden gemaakt van Topnet.
De verspreiding van MR-stukken via Topnet biedt het voordeel dat stukken die te laat worden aangeleverd, maar toch in de MR moeten worden besproken, tijdig en veilig bij de betrokkenen (bewindspersonen en secretariaat ministerraad) kunnen worden aangeleverd. Er is echter ook een aantal nadelen. Zo is het niet praktisch als alle MR-stukken standaard elektronisch worden verspreid. Dit zou een inefficiënt kopieerproces binnen de departementen en het secretariaat ministerraad tot gevolg hebben. Daarnaast worden MR-stukken door de beleidsambtenaren op lager niveau voorbereid. Door het gesloten karakter van Topnet kunnen deze documenten niet op eenvoudige wijze elektronisch op Topnet worden overgezet.

Topnet leent zich bij uitstek voor formele en informele communicatie in situaties waarin snelheid én geheimhouding van cruciaal belang zijn. Gedacht kan worden aan internationale crisissituaties waarin snel een gecoördineerd standpunt moet worden bepaald door meerdere bewindspersonen en top-ambtenaren t.a.v. politieke en/of militaire aspecten. Of aan nationale crisissituaties. Ook in internationale onderhandelingen en overleg kan er behoefte zijn aan een veilig kanaal om snel informatie te kunnen terug koppelen en tekstvoorstellen te kunnen uitwisselen en becommentariëren. Daarbij zal Topnet tot extra versnelling kunnen leiden in situaties waarin ambtenaren uit de doelgroep zijn gehuisvest op een andere lokaties dan hun bewindspersonen, zoals bijv. de BVD t.o.v. BZK. Die dislokatie kan tot onwenselijke vertraging in de communicatie leiden indien niet elektronisch kan worden gecommuniceerd.

Tenslotte is de verwachting dat zodra TopNet in gebruik de communicatiepatronen van de leden van de doelgroep zullen verschuiven. Voor hun onderlinge communicatie zal minder gebruik worden gemaakt van telefoon en van niet-beveiligde e-mail.

Binnen de departementen zullen TopNet en de bijbehorende werkstations gescheiden worden van de overige (inter-)departementale ICT-voorzieningen. De gebruikers krijgen dus een tweede PC op of onder het bureau. Met behulp van een schakelkastje kunnen ze wel gebruik maken van één gemeenschappelijk beeldscherm, toetsenbord en muis. TopNet-werkstations en overige vitale TopNet-componenten zullen worden opgesteld binnen de beveiligde zones van de departementen. Het TopNet kan worden gezien als een netwerk dat deze beveiligde zones met elkaar verbindt. Hiertoe wordt een eigen infrastructuur met geëvalueerde encryptiemiddelen en betrouwbaar systeembeheer ingericht. Het dataverkeer zal lopen over een eigen vezel in de Haagse Ring: de glasvezelkabel die momenteel wordt aangelegd tussen de departementen en de Hoge Colleges van Staat.

Uit beveiligingsoogpunt is zo'n gescheiden netwerk een voordeel vanwege de beheersbaarheid. Daar staat echter een belangrijk nadeel tegenover. Bewindspersonen en top-ambtenaren zullen niet alleen onderling elektronisch willen communiceren, maar nog veel meer met medewerkers buiten de gebruikersgroep van TopNet. De vraag is dus hoe deze gebruikersgroep uitgebreid kan worden met handhaving van het beoogde beveiligingsniveau Stg Geheim. Daar is onderzoek voor nodig.
Maar elke uitbreiding van de gebruikersgroep kent zijn grenzen. Bij welk aantal die grens ook wordt getrokken, altijd zullen er departementsmedewerkers buiten de gebruikersgroep van TopNet blijven met wie gebruikers van TopNet al dan niet regelmatig elektronisch berichten en documenten willen uitwisselen. Dat betekent dat de interfaces tussen TopNet en de elektronische en/of papieren communicatiestromen moeten worden gecontroleerd. Op deze grensvlakken moeten organisatorische en technische maatregelen worden getroffen om gerubriceerde informatie uit TopNet op een gecontroleerde wijze en met inachtneming van alle daarvoor geldende voorschriften verder het ambtelijk apparaat in te kunnen leiden. Ook daarvoor is nader onderzoek nodig.

De afweging van de voor- en nadelen, de haalbaarheid, de risico's en de kosten en baten van TopNet kan nu nog niet definitief gemaakt worden. Daarvoor is eerst nader onderzoek nodig. Datzelfde geldt voor de analyse van de behoeftestelling, de hoeveelheid dataverkeer, de omvang van de doelgroep en het aanbod van technische mogelijkheden. Voorgesteld wordt door DTO een onderzoek te laten uitvoeren dat medio dit jaar zal leiden tot een onderbouwd voorstel aan het SG-Beraad en de Ministerraad voor een go/no-go-beslissing over de aanleg van TopNet. De kosten van dit onderzoek zullen gezamenlijk gedragen worden door AZ, BZ, Defensie en BZK.

Zo'n onderzoek is echter alleen zinvol als alle departementen (ook hier geldt dat het geheel net zo sterk is als de zwakste schakel) nut en noodzaak van TopNet inzien. Daarom wordt reeds nu, als noodzakelijk te vervullen voorwaarde voor de start van het onderzoek, van u gevraagd de behoefte aan TopNet te onderschrijven en de intentie uit te spreken mee te werken (ook in financiële zin) aan de realisatie van TopNet indien nut en noodzaak in het DTO-onderzoek glashelder worden aangetoond.

Beslispunten:

- ***onderschrijft u in beginsel de behoefte aan een besloten netwerk voor e-mail dat elektronisch en fysiek is afgesloten van andere communicatiemiddelen;***
- ***bent u in beginsel bereid, indien in het DTO-onderzoek (incl. risico-analyse) nut, noodzaak en haalbaarheid van TopNet onomstotelijk wordt vastgesteld, (ook in financiële zin) mee te werken aan de realisatie van TopNet.***

3.4 Randvoorwaarde lange termijn: cryptofaciliteit

Uit het oogpunt van staatsveiligheid is het noodzakelijk te kunnen beschikken over apparatuur door middel waarvan de beveiliging van staatsgeheimen en andere gevoelige gegevens gegarandeerd wordt. Veel van de apparatuur die tot nu toe voor dat doel werd ingezet, werd ontwikkeld en geleverd

door Philips Crypto B.V. Door inkrimping bij Philips Crypto richten zij zich nu vooral op het leveren en ondersteunen van bestaande apparatuur. Grootschalige ontwikkeling van nieuwe producten is niet meer goed realiseerbaar. Hierdoor ontstaat er een aanzienlijk en urgent probleem op het gebied van informatiebeveiliging.
Als oplossing voor dit probleem wordt voorgesteld een Cryptofaciliteit bij de BVD te realiseren. Deze faciliteit stimuleert, coördineert en levert bijdragen aan het realiseren van betrouwbare systemen en (cryptografische) producten of onderdelen daarvan voor de bijzondere informatie van de Rijksoverheid. Concreet kan daarbij worden gedacht aan de behoeften zoals die worden gesteld in het VECOM-traject (secure mobiele telefonie, e-mailtoepassingen, etc.).

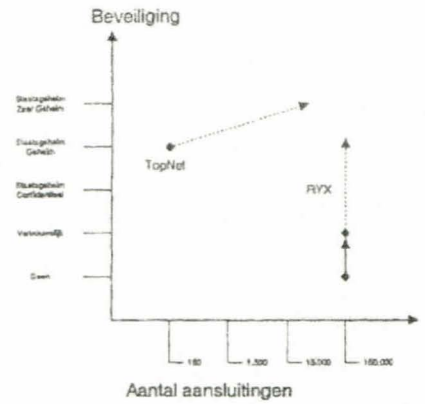
De voorbereiding van de Cryptofaciliteit wordt reeds langer in een separaat besluitvormingstraject door de BVD voorbereid ten behoeve van de MICIV. Omdat de opzet van een Cryptofaciliteit en derhalve de continuering van de productie van Nederlandse encryptietechnologie onlosmakelijk verbonden is met het streven naar veiliger communiceren, is de Cryptofaciliteit voor het volledige beeld in deze notitie opgenomen. Dit laat echter onverlet dat de verdere voorbereidingen en besluitvorming (incl. financiering) hun beslag zullen krijgen in dit separate traject en dat de realisatie van de Cryptofaciliteit separaat zal worden aangestuurd vanuit de MICIV en door de BVD worden uitgevoerd.

3.5 Lange termijn perspectief / Integratie datacommunicatie-bouwstenen

Op de lange termijn dient zowel een verbreding van de communicatie plaats te vinden naar de gehele Rijksoverheid als een verhoging van het beveiligingsniveau van de communicatie binnen de gehele Rijksoverheid. Deze verbreding kan worden ingevuld met RYX dat tot doel heeft iedere Rijks- en Defensieambtenaar met elkaar te verbinden. Daartoe dient echter wel een verdere verhoging van het beveiligingsniveau van RYX én de daarop aangesloten departementale netwerken te worden bereikt.

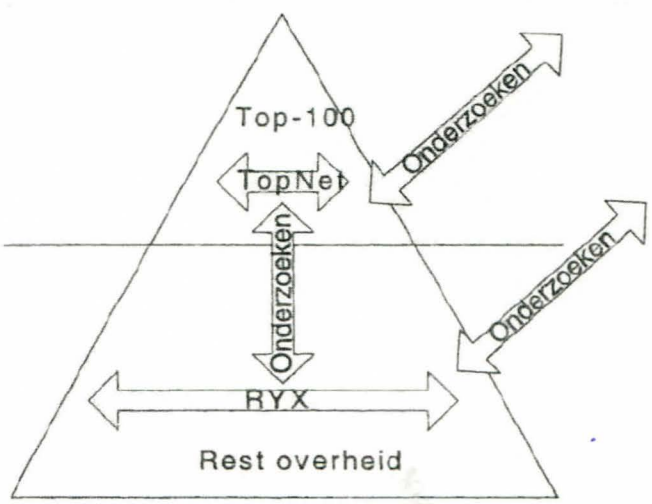
Op dit moment wordt gewerkt aan de verhoging van het beveiligingsniveau van RYX naar het niveau vertrouwelijk. Voor een verder verhoging van het beveiligingsniveau is integratie van bestaande bouwstenen nodig. Het betreft NAFIN (het landelijk dekkende, besloten en specifiek beveiligde netwerk van Defensie), de Haagse ring (de glaskabel die wordt aangelegd tussen alle departementen en de Hoge Colleges van Staat), CERT (voorkomen van virussen en ander elektronisch onheil) en PKI (de inrichting van een infrastructuur die vertrouwelijkheid en authenticiteit van elektronische berichten alsmede de identiteit van de communicatiepartners middels elektronische handtekeningen moet garanderen). Een haalbaarheidsonderzoek/definitiestudie leidend tot een stappenplan zal duidelijk moeten maken of en hoe deze integratie vorm kan krijgen.

In figuur 2 wordt de samenhang van het project Integratie met RYX en TopNet getoond. Als TopNet is aangelegd, is er een netwerk waarmee minstens ca. 150 personen (bewindslieden en top-ambtenaren) en mogelijk meer op het niveau Stg-geheim met elkaar kunnen communiceren. De beweging zou moeten zijn naar een niveau van Stg-Zeer geheim. Dit kan echter met de huidige technische mogelijkheden niet worden gerealiseerd.
RYX is van meet af aan bedoeld voor alle ca. 150.000 rijksambtenaren. De huidige versie van RYX biedt niet meer beveiliging dan dat de gebruikersgroep besloten (150.000 mensen!) is. Het dataverkeer loopt nu nog over openbare netwerken. Binnen het lopende project RYX wordt echter gewerkt aan een opwaardering van het beveiligingsniveau naar vertrouwelijk. Daartoe zal het dataverkeer over de Haagse Ring gaan lopen. Verder zullen zowel RYX zelf als de departementale netwerken waarop RYX draait, worden geaudit op basis van het Voorschrift Informatiebeveiliging Rijksdienst (VIR).
Het project Integratie heeft tot doel een beweging in gang te zetten die ervoor moet zorgen dat TopNet meer mensen kan bereiken en dat zo mogelijk het niveau van beveiliging nog wordt verhoogd en tevens dat het basisniveau van beveiliging van de elektronische communicatie tussen alle Rijksambtenaren waar nodig wordt verhoogd van vertrouwelijk naar Stg-Confidentieel en zo mogelijk Stg-Geheim.



Figuur 2. De relatie tussen de projecten TopNet, RYX en integratie. De pijlen geven de richting van de projecten weer, niet hun exacte uitkomst.

In het vooronderzoek voor het project TopNet zullen ook indicatief scenario's worden opgesteld voor de opschaling van TopNet naar een grotere doelgroep. Maar voor een goed onderbouwde go/no-go-beslissing voor de uitvoering van het Integratietraject is een gedegen definitiestudie nodig. Deze studie zou moeten opleveren een stappenplan waarin wordt aangegeven of en hoe TopNet en RYX geleidelijk naar elkaar kunnen toegroeien. In onderstaande figuur 3 is dat weergegeven met de verticale pijl in de piramide. Maar bewindslieden en top-ambtenaren communiceren ook met de buitenwereld. Dat geldt uiteraard ook voor alle overige ambtenaren. In de definitiestudie zal daarom ook onderzocht worden hoe die communicatiestromen zo goed mogelijk beveiligd kunnen worden, opdat wordt voorkomen dat informatie onbedoeld via die kanalen bij de buitenwereld terecht komt en dat andersom langs die weg virussen of ander elektronische onheil de piramide binnen dringen.



Figuur 3. De oplossingsrichtingen in de communicatiepiramide.

De uitvoering van dit project, te beginnen met de definitiestudie, zal echter pas worden gestart zodra er zicht is op financiering van het gehele Integratietraject. Vooralsnog is dat zicht er niet.

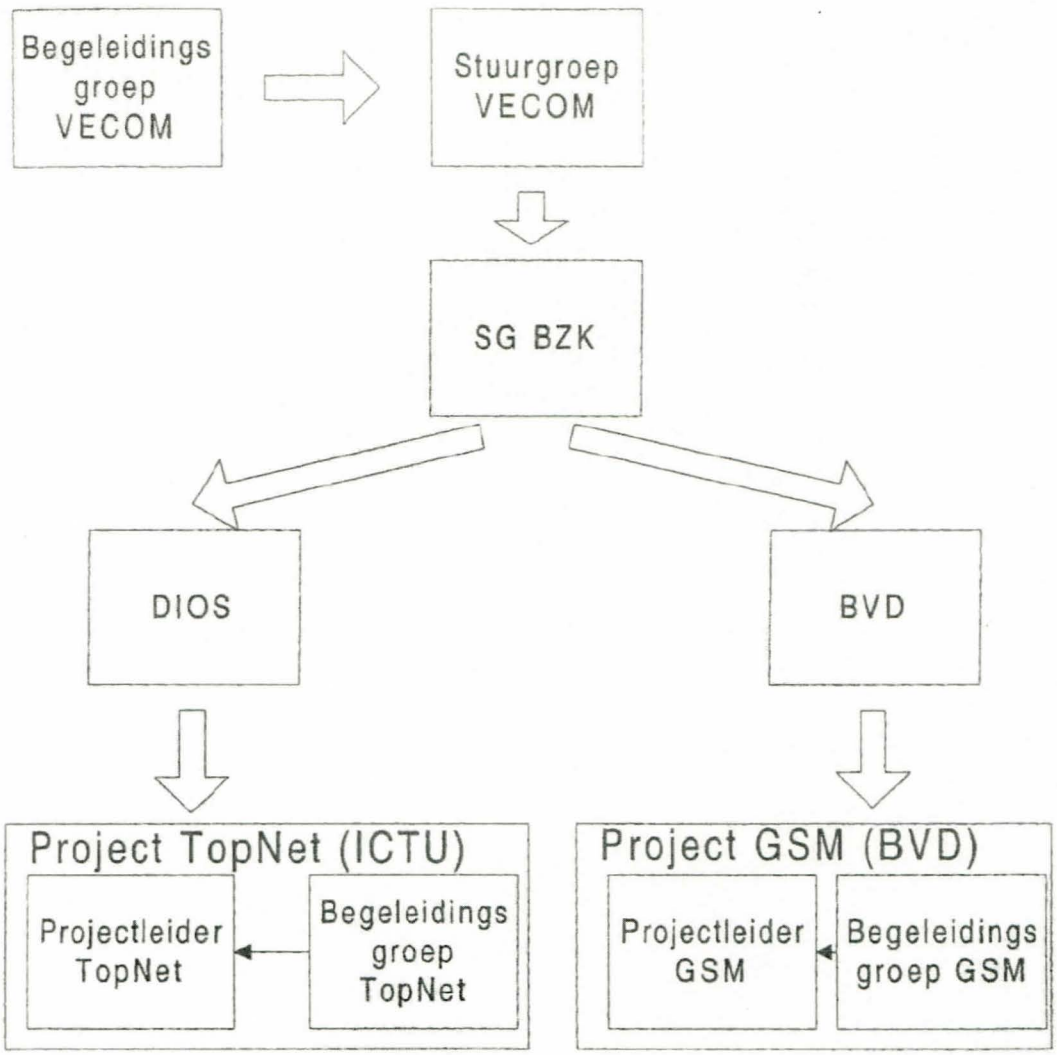
4 Projectstructuur

4.1 Aansturing

Voor de aansturing van de projecten TopNet en Beveiligde Telefonie wordt voorgesteld de stuurgroep VeCom (bestaande uit de sg's AZ, BZK, Def., BZ en V&W, de dg Rijksbegroting en de hoofden BVD en MID) te continueren. Deze stuurgroep wordt ondersteund door een Begeleidingsgroep bestaande uit medewerkers van deze sg's. SG-BZK zal fungeren als opdrachtgever.
De uitvoering van het project TopNet wordt gedelegeerd aan BZK/DIOS; het project Beveiligde telefonie aan de BVD. Voor het project TopNet wordt een projectleider aangetrokken, die bij de ICTU wordt gestationeerd. Deze projectleider wordt geassisteerd door een begeleidingsgroep. Omdat de implementatie van TopNet impact heeft op alle departementen wordt voorgesteld alle departementen deel te laten nemen aan deze begeleidingsgroep. De projectstructuur voor het project Beveiligde telefonie is vergelijkbaar. Hiervoor zal eveneens een begeleidingsgroep worden gevormd, die de bij de BVD te stationeren projectleider zal ondersteunen.

Binnen ieder departement dient ook de interne aansturing geregeld te worden. Daartoe wordt voorgesteld per departement één VeCom-coördinator aan te wijzen. Deze coördinator wordt gemandateerd door de SG. Hij/zij coördineert de informatiestroom betreffende VeCom (d.w.z. voor de projecten TopNet en Beveiligde telefonie) binnen het departement en is eerste aanspreekpunt van het departement op VeCom-gebied.

Anders van opzet is de Cryptofaciliteit. Dat is een voorziening van structurele aard, waarvan in de aansturing wordt voorzien door het MICIV, en dat onder verantwoordelijkheid van de SG-BZK door de BVD zal worden ingevuld. Daar de Cryptofaciliteit ook Rijksoverheidsbreed produkten en diensten zal genereren is het van belang te voorzien in een goede afstemming met aanpalende rijksbrede ontwikkelingen, zoals andere activiteiten die aansluiten bij het VeCom-traject.



Figuur 4. Voorgesteld model voor de aansturing van VeCom.

N.B. De cryptofaciliteit wordt separaat aangestuurd via het MICIV- (CVIN-)traject door SG-BZK en uitgevoerd door de BVD.

4.2 Planning

De vier projecten zijn op te splitsen in een definitie-, een realisatie- (c.q. project-) en een exploitatiefase.

Voor het project secure GSM is de definitiefase reeds afgerond. De realisatiefase kan starten zodra achtereenvolgens SG-Beraad, CVIN, MCIV en Ministerraad hebben ingestemd met de aanschaf én de financiering is geregeld. De doorlooptijd is 6 maanden. Bij een start rond 1 mei 2002 kan het aanschaf- en implementatietraject ca. 1 november 2002 zijn afgerond.
Ook voor de oprichting van de Cryptofaciliteit is de definitiefase reeds afgerond. Ook hiervoor geldt dat de realisatie, de oprichting en bemensing van de structurele Cryptofaciliteit, kan starten zodra de inhoudelijke besluitvorming is afgerond én de financiering is geregeld. Realisatie en exploitatie lopen hier naadloos in elkaar over.

Voor het projecten TopNet zal de definitie/onderzoeksfase binnenkort starten. Deze fase zal ca. 1 september worden afgerond. Vervolgens zal een onderbouwd voorstel voor een go/no-go-beslissing worden voorgelegd aan het SG-Beraad en vervolgens aan de Ministerraad.
Voor het project Integratie is nog geen startmoment voorzien.

In tabel 1 wordt het bovenstaande samengevat.

Tabel 1. Overzicht van de geschatte duur van de activiteiten.

Project	Activiteit	Duur (mnd)	Afgerond (bij start 1-5-02)
Secure GSM	Realisatie	6	1-11-02
	Exploitatie	structureel	
TopNet	Definitiefase	4	1-9-02
	Realisatie	9 a 12	1-9-03
	Exploitatie	structureel	
Cryptofaciliteit	Realisatie/exploitatie	structureel	
Project integratie	Definitiefase	4	pm
	Realisatie	12	pm
	Exploitatie	structureel	

4.3 Kosten

Voor de vier projecten is een kostenraming opgesteld die loopt tot en met 2005. Die begroting is onderverdeeld in een incidentele post en een structurele post (zie de tabel op de volgende bladzijde).

	KOSTE NRAMING 20-02-2002 (in m€)										
Nr	Project	Activiteit	Incidenteel					Structureel			
			2002	2003	2004	2005	Totaal	2002	2003	2004	2005
1.1	**TopNet**	Onderzoek	0,60				0,60				
1.2		Investeringen	6,70	3,30			10,00				
1.3		Exploitatie							4,00	4,00	4,00
2.1	**Telefonie**	Ontwikkeling	PM	PM	PM	PM	PM				
2.2		Aanschaf	1,00				1,00				
2.3		Sleutelgeneratie	0,10				0,10				
2.3		Exploitatie						PM	PM	PM	PM
3.1	**Cryptofac.**	Personeel/Organisatie							0,85	0,85	0,85
3.2		Basisinvesteringsbudget						0,50	1,00	2,00	2,00
3.3		Additionele Investeringen						PM	PM	PM	PM
4.1	**Integratie**	Opstellen stappenplan	0,40				0,40				
4.2		**PKI/eNIK**									
4.2.1		PKI/eNIK (Certificaten, Lezers, Voorlichting, eNIK, Kenniscentrum)		15,00	15,00		30,00				
4.2.2		Exploitatiekosten PKI								6,00	12,00
4.2.3		PKI t/m STG Confidentieel	0,00	p.m.	p.m.	p.m.	p.m.	0,00	p.m.	p.m.	p.m.
4.3		**Upgraden CERT**					0,00	1,25	1,25	1,25	1,25
		Upgraden RYX									
4.4.1		RYX TPM-verklaring standaardbeveiliging									
4.4.1.1		Maatregelen m.b.t. serverpark, portiersysteem en externe koppelingen, netwerk, TPM verklaring	0,20				0,20		0,10	0,10	0,10
4.4.1.2		Monitoring tool	0,30				0,30		0,10	0,10	0,10
4.4.2		RYX t/m Departementaal Vertrouwelijk (beveiliging)									
4.4.2.1		Intrusion Detection System op het netwerk		0,20			0,20		0,05	0,05	0,05
4.4.2.2		Encryptie t.b.v. EU Extranet informatie	0,30	0,20			0,50		0,10	0,10	0,10
4.4.2.3		Overige maatregelen Voorschrift Bijzonder Informatie Beveiliging (opvolger AAR-9)		0,50	0,30	0,10	0,90			0,10	0,10
4.4.2.4		PKI-geschikt maken RYX applicaties	0,10	0,30	0,10		0,50				
4.4.3		RYX t/m Staatsgeheim Confidentieel			p.m.	p.m.	p.m.				p.m.
4.4.4		Implementatie beveiligde interdepartementale e-mail op RYX		0,50			0,50		0,30	0,30	0,30
4.4.5		Uitbreiden RYX naar andere overheidsorganisaties (project, software, hardware, datacommunicatie, bevelliging)			p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
4.5		**Overige centrale voorzieningen**									
4.5.1		Onderhoud en beheer firewalls, beveiligingsdiensten		1,50			1,50	1,50	1,50	1,50	1,50
4.5.2		Betere landelijke dekking m.b.v. NAFIN		1,00			1,00	0,50	1,00	1,00	1,00
4.5.3		Gemeenschappelijke Internet e-mail koppeling		0,50			0,50		0,50	0,50	0,50
4.5.4		Gemeenschappelijke Internet www-services		2,00			2,00		2,00	2,00	2,00
4.5.5		Gemeenschappelijke Inbeldienst		0,90			0,90			0,90	0,90
4.5.6		Gemeenschappelijke overige koppelingen (o.a. overheid)		1,00			1,00		1,00	1,00	1,00
4.6		**Overige decentrale voorzieningen**									
4.6.1		Invoering Basisbeveiligingsniveau Rijksdienst									
4.6.1.1		Inventarisatie	0,20				0,20				
4.6.1.2		Ontwikkeling Basisbeveiligingsniveau		0,30			0,30				
4.6.1.3		Departementale implementatie (systeembeheer, antivirus, intrusion detection, beveiliging van werkstations, laptops en organizers, externe koppelingen, etc etc), beheer en onderhoud.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
4.6.2		Invoering Beveiligingsniveau Departementaal Vertrouwelijk bij de Rijksdienst	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
4.6.3		Invoering Beveiligingsniveau STG Confidentieel bij de Rijksdienst	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
4.6.4		Departementale voorzieningen t.b.v. bev.interdep.e-mail via RYX	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
5	**Project-organisatie**	**Uitvoeringskosten ICTU**	1,50	1,50	1,50		4,50				
			11,40	28,70	16,90	0,10	57,10	3,75	13,75	21,75	27,75