Bylage 1

PKI taskforce

Ib99/PKI009

PKI taskforce

Plan van Aanpak
(concept)

Plan van aanpak PKI Taskforce

In het vorige IB-beraad is ingestemd met het instellen van een Taskforce voor een Public Key Infrastructure[1] die tot taak krijgt om, gegeven de conclusies van beide voorgaande onderzoeken (Beveiligde Email en Ttp-diensten voor de overheid), in relatief korte tijd (ong. 3 jaar) een werkbare betrouwbare infrastructuur voor TTP diensten voor de communicatiebehoefte van de (Rijks)overheid te realiseren. Het ministerie van Financiën heeft reeds een wens in die richting te kennen gegeven. Vanuit het ministerie van BZK, als coördinerend ministerie voor de informatiebeveiliging leeft dezelfde wens. Uiteraard kunnen alle geïnteresseerde ministeries aan deze Taskforce deelnemen. Het gaat immers over een infrastructuur die voor alle departementen dienstbaar is en die vanuit de wens van het IB-beraad in gezamenlijkheid wordt opgezet.

Daarbij is de vraag gesteld door het IB-beraad om op korte termijn kennis te kunnen nemen van een meer gedetailleerd plan van aanpak van deze PKI Taskforce. Teneinde dit plan op te kunnen stellen is op 9 en 10 september een eerste bijeenkomst geweest van vertegenwoordigers van departementen en uitvoeringsorganisaties. Tijdens deze bijeenkomst stond het voorbereiden van een dergelijk plan van aanpak centraal. De resultaten van de beraadslagingen zijn in dit plan van aanpak opgenomen.

De hoofdtaak van deze Taskforce zal dan zijn om vanuit het Interdepartementaal overheidsdomein scenario te komen tot een generieke, voor ieder departement te benutten, infrastructurele oplossing voor het betrouwbaar en integer kunnen communiceren met elkaar en met andere partijen en het gebruik digitale handtekeningen op grote schaal mogelijk te maken.

Uitgangspunten voor de Taskforce zullen zijn:

- De Taskforce richt zich niet alleen op de communicatie tussen Overheid en Overheid, maar tevens op de communicatie tussen Overheid en bedrijfsleven en Overheid en Burger. Oplossingen zullen generiek moeten zijn en overdraagbaar van het ene domein naar het andere.

- Het gebruik van de PKI door organisaties zal afhankelijk zijn van hun applicaties; de PKI is een "enabler" van oplossingen die in het eigen individuele domein gekozen kunnen worden. De PKI richt zich dan ook niet op de mogelijkheden die de PKI biedt voor de back-office op het gebied van herinrichting van bestaande processen, deze verantwoordelijkheid blijft in handen van de eigen organisatie

- Het moet mogelijk zijn om met de PKI infrastructuur 80% van de normale overheidscommunicatie en dienstverlening uit te kunnen voeren. De resterende 20% waarvoor wellicht zwaardere beveiligingseisen kunnen gelden (denk aan Staatsgeheim,

[1] De Canadese Overheid heeft in het kader van haar eigen Nationaal Actie Programma ook een PKI Taskforce ingesteld, met als opdracht een PKI infrastructuur voor de Canadese Overheid

politiebestanden etc.) zal een zwaarder regime vergen, maar de oplossing voor de PKI in het normale domein moet dusdanig zijn dat deze interoperabel blijft met het zwaardere regime (transparantie voor de gebruiker)

- De Taskforce PKI zal een gezamenlijk gezicht van de Overheid naar buiten dienen te tonen. Daarvoor zal zowel commitment van de deelnemende partijen nodig zijn, waarbij als uitgangspunt het principe van "Gezamenlijk, en niet vrijblijvend" gehanteerd dient te worden. Daartoe bevat het Plan van Aanpak voorstellen in de zin van de begeleiding van de Taskforce door diverse gremia, het gebruiken van ervaringen die reeds in andere trajecten worden opgedaan[2] en het ondersteunen van initiatieven.

- Een belangrijk punt zal zijn de communicatie (zowel intern naar de partners als extern naar anderen) over:
  - Wat is nu eigenlijk een PKI
  - Wat betekenen de definities
  - Wat heb je eraan
  - Waarom zou je het willen
  - etc.

- Voor de vrager van PKI diensten voor zijn eigen proces moet het gebruik van de PKI infrastructuur laagdrempelig zijn.

In het plan van aanpak wordt aan de hand van actielijnen en middelen een en ander ingekaderd worden.

[2] Met inbegrip van de aan de Tweede Kamer aangeboden TTP-nota over uitgangspunten en randvoorwaarden voor TTP-dienstverlening in Nederland

Doelstelling van de Taskforce

Het realiseren van een werkbare betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de (Rijks)overheid en transparant is voor de gebruikers.

Uitwerking doelstelling

Met PKI–diensten worden diensten bedoeld die direct of indirect bijdragen aan het waarborgen van de authenticiteit (identificatie/oorsprong), integriteit (juistheid) en exclusiviteit (vertrouwelijkheid) van elektronische communicatie en het mogelijk maken om digitale handtekeningen op grote schaal te gebruiken. Voor wat betreft de Digitale handtekeningen zal rekening worden gehouden met de Europese richtlijn digitale handtekeningen.

Onder een infrastructuur voor PKI-diensten wordt de combinatie van bestuurlijke, organisatorische en technische componenten verstaan die nodig zijn voor het leveren van de PKI-diensten.

Met de term vastgesteld beveiligingsniveau wordt aangegeven dat er een keuze moet worden gemaakt voor de betrouwbaarheid van de PKI-diensten. Des te hoger het beveiligingsniveau van de PKI-diensten, des te meer toepassingen kunnen worden ondersteund. De kosten nemen echter toe met een hoger beveiligingsniveau terwijl de flexibiliteit veelal afneemt. De Taskforce stelt zich tot doel om PKI-diensten te realiseren die 80% van de normale overheidscommunicatie en dienstverlening kan ondersteunen.

De term communicatiebehoefte van de overheid omvat zowel de communicatie tussen Overheid en Overheid als die tussen Overheid en Bedrijfsleven en tussen Overheid en Burger.

Met transparantie wordt bedoeld dat de overheid zicht naar buiten toe met één gezicht presenteert. Er moet voor het bedrijfsleven, burgers en bijvoorbeeld uitvoeringsinstanties geen technisch onderscheid zijn in de communicatie met de verschillende departementen of overheidsinstellingen.

Afbakening

De PKI-diensten faciliteren een grote hoeveelheid toepassingen (applicaties). Of een toepassing daadwerkelijk gebruik kan maken van de PKI hangt ondermeer af van de betrouwbaarheid van de PKI (beveiligingsniveau). Een toepassingsaanbieder (organisatie) moet als verantwoordelijke voor de toepassing de beslissing nemen of de PKI kan worden gebruikt. De inrichting van de processen van de toepassingsaanbieder valt dan ook buiten de verantwoordelijkheid van de Taskforce. Wel dient de Taskforce uiteraard de noodzakelijke

informatie aanleveren waarop de toepassingsaanbieder kan beslissen en het gebruik van de PKI door de toepassingsaanbieder onderstenen.

- Het begrip 80% van de overheidscommunicatie is uitgangspunt voor het geboden beveiligingsniveau. De resterende 20% waarvoor wellicht zwaardere beveiligingseisen kunnen gelden (denk aan Staatsgeheim, politiebestanden etc.) zal een zwaarder regime vergen, maar de oplossing voor de PKI in het normale domein moet bij voorkeur dusdanig zijn dat deze interoperabel blijft met het zwaardere regime (transparantie voor de gebruiker)

De Taskforce zal een beperkte levensduur hebben. Dit betekent dat zij zorg zal moeten dragen voor de overdracht van eindproducten naar staande organisatie-onderdelen.

Actielijnen

Inleiding

Tijdens de verschillende discussies binnen de klankbordgroep van het project "TTP-diensten voor de Rijksoverheid" en de Taskforce-bijeenkomst is duidelijk gebleken dat er ook op (zeer) korte termijn trajecten zijn binnen de overheid waarbij PKI-diensten noodzakelijk zijn. Binnen de Belastingdienst zijn er zelfs enkele toepassingen die nu reeds gebruik maken van PKI-diensten. Het is belangrijk voor het bereiken van de doelstellingen van de Taskforce dat deze trajecten op korte termijn geïnventariseerd en ondersteund worden vanuit de Taskforce. Door snel op deze concrete behoefte in te spelen kan al spoedig een draagvlak voor de doelstellingen van de Taskforce worden gecreëerd. Gebeurt dit niet, dan zullen deze trajecten eigen oplossingen creëren waardoor een aantal geïsoleerde PKIs zullen ontstaan. Dit is zowel uit het oogpunt van draagvlak voor de Taskforce als financieel (voor de overheid) nadelig.

Daar staat tegenover dat voor de verwezenlijking van het einddoel van de Taskforce een langer traject noodzakelijk is waarbij de belangen van alle betrokken partijen, ook op middellange termijn, uitgewogen dienen te worden opgenomen. De praktijkervaring die binnen de kortte termijn trajecten opgedaan wordt, zal echter belangrijk kunnen bijdragen aan een optimaal werkbare PKI-dienstverlening voor de overheid.
Om deze redenen is er een tweedeling gemaakt in de activiteiten van de Taskforce:

- De hoofdactielijn gericht op het bereiken van het uiteindelijke doel op middellange termijn (binnen de voorziene looptijd van de taskforce van 3 jaar).
- Een actielijn gericht op de korte termijn oplossingen.

Daarnaast zijn twee -voor beide actielijnen- belangrijke sub-actielijnen benoemd:

- toetsing wet en regelgeving
- communicatie en PR

Hoofdactielijn

De doelstelling van deze actielijn is het realiseren van het doel van de PKI Taskforce: Het realiseren van een werkbare betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de rijksoverheid en transparant is voor de gebruikers.

Binnen de hoofdactielijn worden de volgende kernactiviteiten onderscheiden:

- Zekerstellen van de betrokkenheid van alle relevante (maatschappelijke) partijen (overheidsorganisaties, gebruikersorganisaties, belangengroepen, bedrijfsleven)
- Vaststellen van het vereiste betrouwbaarheidsniveau en het opstellen van een Certificate Policy voor de overheids-PKI
- Selectie ten aanzien van de te leveren PKI-diensten
- Liaison met nationale en internationale activiteiten
- Opstellen van Contracten, convenanten e.d.
- Selectie producten en/of diensten, aanbesteding
- Voorbereiding en uitvoering van een introductie- en invoeringsplan
- Overdracht naar staande organisatie (lijn)

Korte termijn actielijn

Doelstelling:
Snel bedienen van bestaande initiatieven door ondersteuning te bieden aan de concrete vraag naar PKI-diensten.

Beoogde effecten:
- Snel creëren van een draagvlak voor de doelstellingen van de Taskforce.
- Bundelen van bestaande kennis op het gebied.
- Praktijkervaring opdoen die zal bijdragen aan het uiteindelijke doel.
- Voorkomen van een wildgroei aan lokale PKIs.
- Kostenbesparing op korte termijn door gezamenlijk gebruik PKI-diensten.

Daarbij wordt er bewust een keuze gemaakt voor een tijdelijke PKI-infrastructuur waarbij eventueel concessies worden gedaan aan het beoogde uiteindelijke beveiligingsniveau. Tijdelijk houdt hier in dat de hier bedoelde PKI-infrastructuur of zal worden uitgefaseerd of (waarschijnlijk) zal migreren naar de definitieve PKI.

Deze actielijn wordt voor een belangrijk deel bepaald door de vraagzijde. Wat niet wil zeggen dat het niet denkbaar is dat vanuit de Taskforce experimenten worden geïnitieerd.

Binnen de korte-termijn actielijn worden de volgende kernactiviteiten onderscheiden:

- Inventarisatie van relevante initiatieven en projecten
- Zekerstellen van de betrokkenheid van Taskforce en initiatiefnemers (liaison) bij relevante initiatieven en projecten
- Vaststellen van het geschikte betrouwbaarheidsniveau en het opstellen van een voorlopig Certificate Policy voor een eventueel tijdelijke overheids-PKI. Een tijdelijke PKI is daarbij geen consessie aan het beoogd beveiligingsniveau, maar zoals gezegd slechts tijdelijk.
- Opstellen van Contracten, convenanten e.d.
- Selectie producten en/of diensten, eventueel aanbesteding
- Invoering tijdelijke PKI-diensten
- Operationeel beheer van de tijdelijke PKI
- Migratie naar eindoplossing c.q. uitfasering

Sub-actielijnen

Uit de voorgaande Hoofd- en Korte termijn actielijnen volgen een tweetal aspecten die bijzondere aandacht vergen. Het betreft de toetsing van de bestaande Nationale en Internationale wet- en regelgeving en de communicatie over de activiteiten van de Taskforce en PKI-diensten.

Toetsing wet- en regelgeving

Belangrijk in dit opzicht is met name de status – en daarmee de gebruiksmogelijkheden – van de Digitale Handtekening. Voor een optimale inzetbaarheid van de PKI binnen toepassingen is het mogelijk dat in enkele gevallen de wet- en/of regelgeving belemmeringen opwerpen. In het civiele recht is in enkele gevallen een vormvoorschrift van toepassing. Dit betekent dat alleen een handgeschreven document (en handtekening) geldig is. In het bestuursrecht gelden voor meerdere handelingen dergelijke vormvoorschriften.
Ofschoon het niet binnen de directe mogelijkheden maar ook doelstellingen van de Taskforce lijkt te liggen om wetswijzigingen daadwerkelijk door te doen voeren, aangezien dit meer speelt bij het gebruik dat men van de PKI gaat maken (de toepassingen) en niet bij de PKI zelf, ligt er wel een belangrijke taak in het signaleren van probleemgebieden en het initiëren van activiteiten om de problemen op te lossen. Afstemming zal dan ook gezocht worden met bestaande trajecten zoals de activiteiten die voortkomen uit de nota Wetgeving op de Digitale Snelweg van het Ministerie van Justitie en de Europese Richtlijn digitale handtekeningen.

Communicatie

Reeds in de voorbereidende discussies is gebleken dat het moeilijk is om eenduidig en begrijpelijk te communiceren over PKI-diensten en hun relatie met toepassingen. Aangezien acceptatie door een breed publiek een belangrijke factor is voor het tot stand brengen van een voorziening voor betrouwbare elektronische communicatie, is het noodzakelijk vanaf het begin voldoende aandacht te besteden aan dit aspect. Het vermijden van jargon en het gebruiken van consistente en eenduidige begrippen is van groot belang. De activiteiten van de Taskforce en de rol van de PKI dienen duidelijk te worden gecommuniceerd. Presentaties, folders en een PKI website zullen daaraan bijdragen.

Kritische Succes/faalfactoren:

Hieronder wordt een korte opsomming gegeven van Kritische trajecten, met waar mogelijk een nadere invulling.

Succesfactoren:

- Commitment :Het commitment dat "als we wat met PKI gaan doen, we dat doen via de Taskforce" zal duidelijk moeten worden gemaakt. Daarvoor kan de formele instelling middels een instellingsbesluit van de minister voor GSI een eerste aanzet vormen. Maar ook kan gedacht worden aan convenanten, die door partijen met de Taskforce worden gesloten. Een verdere invulling van het commitment wordt verkregen door het daadwerkelijk deelnemen aan de Taskforce door departementen en organisaties
- Zichtbaarheid: Communicatie over en bekendheid met de doelen en activiteiten van de Taskforce bij de aanbieders van nieuwe diensten, gebruikersgroepen. Een van de eerste activiteiten zal dan ook zijn het inschakelen -intern en extern- van communicatie-deskundigen op het terrein van ICT.
- Snelheid: Bij de korte-termijn actielijn dient een operationele PKI voor het ondersteunen van de vraagzijde beschikbaar te zijn. Daarbij kan mogelijk efficiënt gebruik worden gemaakt van de PKI-initiatieven van nu reeds aangemelde deelnemers aan de Taskforce..

Risicofactoren:

- (Maatschappelijke) acceptatie: voor het grootschalig invoeren van een PKI, met name in de communicatie tussen overheid en burger is een brede maatschappelijke acceptatie noodzakelijk. Daarbij kan de privacygevoeligheid (big-brother idee), indien niet goed in acht genomen, een remmende factor zijn. Wel kan de PKI eventueel een rol spelen bij het gebruiken van Privacy Enhancing Technologies, wat de bezwaren voor een groot gedeelte kan wegnemen.
- Beveiligingsniveau: Een te laag niveau levert beveiligingsrisico's op die kunnen leiden tot imageschade en daarmee een afbreukrisico. Een te hoog niveau leidt tot hoge(re) kosten, complexe(re) procedures en belemmerd daarmee het praktische gebruik. Gegeven de doelstelling van 80% en de mogelijkheid om via de korte-termijn actielijn middels experimenten tot een meer generiek beveiligingsniveau te komen zal hieraan bijzondere aandacht moeten worden geschonken. Daarbij zal in nauwe samenwerking met betrokkenen, het bedrijfsleven en met inachtneming van internationale ontwikkelingen gewerkt dienen te worden.
- Volume: de tijd en middelen zijn beperkt. Het bedienen van een te grote vraag kan de uitvoering belemmeren. Prioriteitstelling kan ertoe leiden dat organisaties teleurgesteld worden. Hier zal het voorgestelde dagelijks bestuur en het ICT-beraad een cruciale rol spelen.

Planning (indicatie)

Start Taskforce: 1-11-1999

Einde Taskforce: k4/2003

Communicatie en PR: k4/1999

Beschikbaarheid Korte termijnoplossing: 1-11-2000

Concept totaaloplossing: k3-2000

Pilots/proefdraaien totaaloplossing: k3/2001

Invoering totaaloplossing: k2/2002

	4/99	1/00	2/00	3/00	4/00	1/01	2/01	3/01	4/01	1/02	2/02	3/02	4/02	1/03	2/03
Start Tf	X														
Comm +PR	X	X	X	X	X	X	X	X	X	X	X	X			
KT oplossing					X	X	X	X	X	X	X	X			
Concept PKI				X											
Test PKI									X	X	X				
Invoering PKI											X	X	X	X	X
Overdracht lijn											X	X	X	X	X

Plan van aanpak:

Middelen

1. Budget:

De **PKI** zal een "enabling service" zijn die door de gehele overheid gebruikt kan worden voor het doelmatig en doeltreffend organiseren van eigen of interdepartementale applicaties. Daarom ligt het voor de hand om voor de financiering van de PKI Taskforce te zoeken naar een departement-overstijgende oplossing. Een oplossing daarvoor is het financieel onderbrengen van de PKI Taskforce in het Nationale ActieProgramma Elektronische Snelwegen; actielijn Elektronische Overheid, pijler C.1. Overheidscommunicatie.

Voor het jaar **1999** is een bedrag van f. 600,000,- gereserveerd, dat uiteenvalt in:
- Opstartkosten (startconferenties, overleggen)
- Personeelskosten kernbezetting Taskforce
- Huisvesting (incl. apparaatskosten)
- Communicatie en PR

Voor het jaar **2000** is een bedrag voorzien van f. 2.000.000 dat uiteenvalt in:

- Personeelskosten
- Huisvesting
- Communicatie en PR (incl. conferenties)
- Short-track invoering van een eerste versie van de PKI, inclusief aanbesteding, beheer en ondersteuning
- Experimenten

Voor het jaar **2001** is een bedrag voorzien van f. 4.000.000 dat uiteenvalt in:

- Personeelskosten
- Huisvesting
- Communicatie en PR
- Long-track invoering van een volwaardige PKI
- Beleggen van beheer en ondersteuning

Voor het jaar **2002** is een bedrag voorzien van f. 4.000.000 dat uiteenvalt in:
(voortzetting van vorig jaar)
- Personeelskosten
- Huisvesting
- Communicatie en PR
- Long-track invoering van een volwaardige PKI
- Beleggen van beheer en ondersteuning

de posten voor het jaar 2003 zijn P.M.

2. Bezetting Taskforce:

De bezetting van de taskforce zal bestaan uit speciaal daartoe aan te trekken medewerkers en uit door de departementen ter beschikking gestelde medewerkers. Ten aanzien van de eerste categorie zal het normale departementale proces van werving en selectie gevolgd worden. Omdat het in de bedoeling ligt om zo snel mogelijk met de werkzaamheden van de Taskforce te kunnen beginnen, zullen deze functies zo snel mogelijk moeten worden opengesteld, danwel intern worden ingevuld. Het gaat dan om:

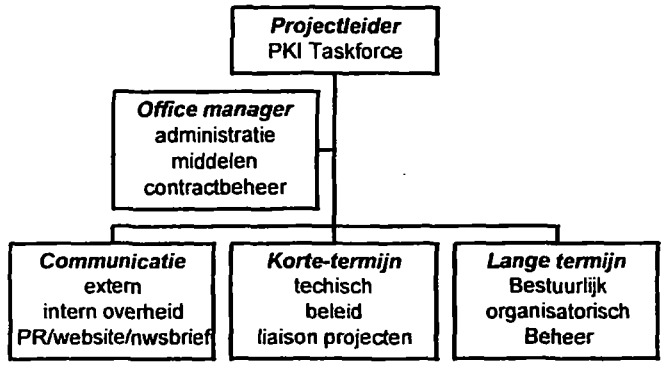
- Projectleider PKI Taskforce:
  - - Dagelijkse leiding
  - - Synergie
  - - Overleg
- Medewerker:
  - - Ondersteuning deeltaken/ secretaris
- Medewerker:
  - - Contacten/experimenten
- Medewerker Juridische expertise
  - (Toetsing uitgangspunten, contractbegeleiding, toetsing generieke en specifieke wetgeving
- Medewerker Bestuurlijke expertise
  - (koppeling politiek, voorbereiding/begeleiding gremia)
- Medewerker Beleidsmatige expertise
  - (overleg, contacten)
- Medewerker Technische expertise
  - (beoordeling voorstellen/oplossingen, technische kennis van PKI's)
- Medewerker Communicatie en PR expertise
  - (begeleiden externe bureaus, voorbereiden conferenties, persberichten)
- Office manager/ secretariaat:
  - - secretariaatswerkzaamheden
  - - contractbeheer

Bij de inventarisatie van mogelijke deelnemers vanuit de departementen zal gekeken worden naar modaliteiten van deelname:

- Detachering/ andere vormen
- part-time/full-time
- voorwaarden
- datum van overgang

Een concept organigram zou dan zijn:

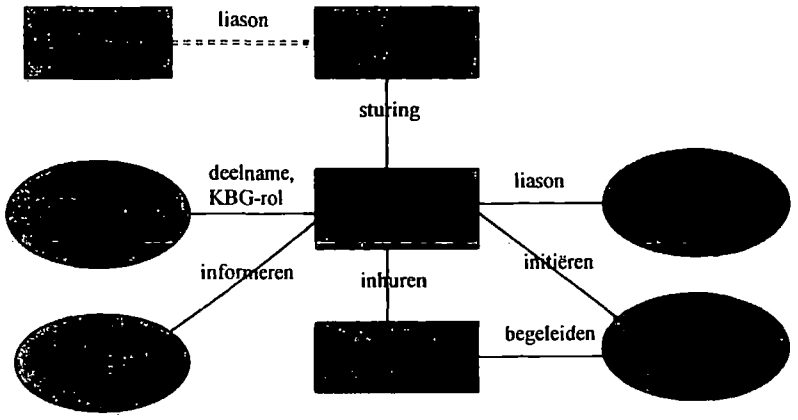
PKI Taskforce Organigram



3. Bestuurlijk positionering:

Ten aanzien van de bestuurlijke organisatie is het volgende schema besproken tijdens de eerste bijeenkomst van de PKI taskforce

Schema PKI-taskforce



workshop 9/10 september 1999

De opdrachtgever van de PKI Taskforce zal het ICT-beraad zijn. Omdat het ICT-beraad slechts 4 keer per jaar bijeenkomt is het voorstel om uit het ICT beraad een soort van "Dagelijks Bestuur" te formeren. Dit dagelijks bestuur, bestaande uit 3 tot 4 leden van het ICT beraad zal het eerste aanspreekpunt zijn voor de Taskforce op het terrein van bestuurlijke aspecten.

Vanuit de deelnemende organisaties aan de Taskforce zal behoefte zijn aan een Klankbordgroep (KBG)-overleg teneinde de juiste koers veilig te stellen en de juiste keuzes te kunnen bespreken. Voor de volgers, diegenen die geen directe betrokkenheid hebben of willen, maar wel geïnteresseerd zijn in de voortgang, zal d.m.v. conferenties, nieuwsbrieven etc. informatie worden verstrekt.

Voor wat betreft de lopende projecten (reeds opgestarte initiatieven) zal gezorgd moeten worden voor een goede liaison-functie binnen de Taskforce, zodat er een goede kennis is van reeds ontwikkelde oplossingen en de daarbij vergaarde informatie ook ter beschikking kan komen van de Taskforce. Daarnaast kunnen de ontwikkelde producten van de Taskforce ook optimaal bijdragen aan de lopende projecten, en kan vroegtijdig worden ingeschat of en hoe migratiestrategieen een goede kans van slagen hebben.

Specifieke kennis kan en zal ingehuurd worden door de Taskforce om bepaalde deelgebieden uit te werken danwel om grotere gehelen uit te werken en uit te voeren.

Experimenten zullen door de Taskforce geïnitieerd dan wel ondersteund worden, bijvoorbeeld aan de hand van concrete wensen en behoeften in het short-track traject. Daarbij zal waar nodig en mogelijk uiteraard gebruik worden gemaakt van specifieke expertise uit de markt.