



Ministerie van Binnenlandse Zaken
DIR IOS; Afd. Infrastructuur en Continuïteit
[REDACTED]
Postbus 20011
2500 EA DEN HAAG

Utrecht, 3 november 2000
Kenmerk: 2655000-40617/MF/IvdH

Geachte heer [REDACTED]

Zoals u weet is Kenniscentrum CIBIT de afgelopen maanden zeer actief geweest in het ontwerpen en organiseren van een Masterclass Information Security Management. U heeft daar ook een bijdrage aan geleverd, of doet dat nog, waarvoor wij u bijzonder erkentelijk zijn.

Op dit moment is de outline van de masterclass rond en zijn wij met betrokken partijen de diverse onderdelen van het programma verder aan het uitwerken. Het is verheugend om te zien dat wij daarbij op medewerking van vele prominente partijen en personen in de markt mogen rekenen. Het programma ziet er thans qua onderwerpenverdeling, als volgt uit:

- Selling Security (Awareness)
- Managing Security
- ICT law & Ethics
- Security Standards & best practices
- Risk analysis in the value chain
- Business continuity
- Security techniques
- E-security

De inhoud van het programma is gebaseerd op de stof voor het door ISC² gecertificeerde CISSP-examen. Als CIBIT besteden we bovendien extra aandacht aan de couleure locale van Europa in het bijzonder Nederland. Daarbij moet vooral gedacht worden aan recht en ethiek, maar ook aan de meer op regelgeving gebaseerde cultuur.


Binnenkort zullen wij beginnen met het produceren van marketingmateriaal en de start van een wervingscampagne. De bedoeling is het programma te laten starten rond maart 2001. De opleiding bestaat uit 15 dagen, die worden gespreid over vijf blokken van drie dagen.

Het is voor Kenniscentrum CIBIT bijzonder belangrijk om de kwaliteit van de opleiding direct vanaf de start op een hoog niveau te brengen en te houden. Om dat te garanderen hanteren wij uiteraard onze eigen kwaliteitseisen en procedures. Ook de continue inbreng van gastdocenten met recente ervaring uit de praktijk waarborgt een deel van de kwaliteit.

Een belangrijk aspect in ons kwaliteitsproces evenwel, is de betrokkenheid van onafhankelijke derde partijen. Deskundigen op hun gebied, met voeling voor de ontwikkelingen in de markt. Bij onze Master of Science opleidingen hebben wij op deze wijze external examiners en validatie-panels. Voor de Masterclass ISM willen wij met dit doel graag een *Advisory Board* instellen.

Ik en alle collega's die bij dit project zijn betrokken zouden het bijzonder op prijs stellen indien u zitting zou willen nemen in deze Advisory Board. De overige leden die zijn uitgenodigd, vindt u onderaan deze brief. Onze verwachting is dat de Board jaarlijks maximaal 2 keer bijeen zal komen. Tijdens deze bijeenkomsten zullen belangrijke ontwikkelingen in het vakgebied worden gerelateerd aan de opzet en inhoud van de Masterclass en eventueel gewenste wijzigingen worden besproken. Ook zullen de evaluaties van deelnemers tot dan toe aan de orde komen. Tot slot zullen de leden van de Board als zodanig worden vermeld in onze marketinguitingen rondom de Masterclass. Uiteraard ontvangen de leden van de Board een passende vergoeding voor hun inspanningen.

Uw bijdrage aan de Advisory Board betekent voor ons een belangrijke stap in het uiteindelijke succes van de Masterclass ISM. Een positieve reactie op ons verzoek wordt dan ook bijzonder gewaardeerd.

Indien u vragen heeft vóór u beslist, dan kunt u te allen tijde contact opnemen met mij of mijn collega 



Ik zie met bijzondere belangstelling uit naar uw reactie.

Met vriendelijke groet,
Kenniscentrum CIBIT


opleidingen

NB:

Deze uitnodiging is tevens verstuurd aan:

- , Informatie Technologie Centrum , (ING)
- , faculteit technische wiskunde en informatica, TU Delft)



Datum
9 februari 2001

Ons kenmerk
DIOS/IC2001/U53453

Onderdeel
Directie Informatiebeleid
Openbare Sector

Inlichtingen
T (070) 426
F (070) 426 7600

Uw kenmerk
2655000-40617/MF/1

Blad
1 van 1

Aantal bijlagen

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Kenniscentrum CIBIT
t.a.v. Opleidingen
De heer
Postbus 19210
3501 DE UTRECHT

Minuut

Onderwerp
uw brief d.d. 3 november 2000

Van

Lijnparaaf Medeparaaf
dIOS

Afschrift aan

Archief

12/2

Kamer

H 524

Afschrift aan

Kamer

Visie

Weer voorleggen

Datum

Geldelijk bezwaar

Begrotingsjaar

Begrotingsartikel

Bedrag

fl.

Budgetregel

Verzendgegevens

Uiterste verzenddatum

Aanwijzingen

- Aantekenen
 Per expresse
 Per koerier
 Per e-mail

- Per fax
 Internet
 Staatscourant

- Diplomail Aruba
 Diplomail Curaçao
 Diplomail St. Maarten

Verzonden door

Naam

Verzenddatum

12-2-2000

Bijzonderheden



Datum
9 februari 2001

Ons kenmerk
DIOS/IC2001/U53453

Onderdeel
Directie Informatiebeleid
Openbare Sector

Inlichtingen
T (070) 426 7600
F (070) 426 7600

Uw kenmerk
2655000-40617/MF/lvdH

Blad
1 van 1

Aantal bijlagen

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Kenniscentrum CIBIT
t.a.v. de Opleidingen
De heer
Postbus 19210
3501 DE UTRECHT

Onderwerp
uw brief d.d. 3 november 2000

Geachte heer

In reactie op uw brief van 3 november 2000 maakt u melding dat de outline van de masterclass Information Security Management rond is. Een belangrijk initiatief van Kenniscentrum CIBIT om een opleiding op het gebied van informatiebeveiliging te ontwikkelen van kwalitatief hoog niveau. Graag verneem ik kennis van de verdere inhoudelijke uitwerking van het programma.

Ik ben gaarne bereid om zitting te nemen in de Advisory Board voor deze Masterclass ISM. Ik heb geen bezwaar om als extern deskundige en lid van de Board opgenomen te worden in brochures rondom de Masterclass. In verband met drukke agenda word ik graag tijdig op de hoogte gesteld van de bijeenkomsten. Ik zie de eerste bijeenkomst met belangstelling tegemoet.

Met vriendelijke groet,



ckp 2/27/2

> Registratiekamer
T.a.v. de heer [redacted]
Postbus 93374
2509 AJ DEN HAAG

Datum : 26 februari 2001
Onderwerp : rapport "Sleutels van vertrouwen"

Ons kenmerk : DIOS/IC2001/U58219

Geachte heer [redacted]

Onlangs heeft PKI overheid een laatste concept van het rapport "Sleutels van vertrouwen" ontvangen. Gezien onze taak om PKI diensten voor de overheid te realiseren voelen wij ons uiteraard zeer betrokken bij het onderwerp van het rapport. Op een eerdere versie van het rapport hebben wij reeds uitgebreid gereageerd middels een notitie en een gesprek met de heren [redacted] van uw organisatie. Dit vanuit een gedeelde mening dat privacy bescherming een belangrijk aspect is waar, binnen het ontwerp van een PKI, de nodige aandacht moet worden besteed.

In het ontwerp hebben wij de nodige maatregelen getroffen om de privacy te beschermen, waaronder de keuze voor een 'kaal' certificaat. Ons commentaar komt voornamelijk voort uit het feit dat de PKI voor de overheid zich met name richt op de identificatie van personen en in het bijzonder op de elektronische handtekening. Dit vergt een werkbaar mechanisme voor het uniek identificeren van een persoon. In het rapport "Sleutels van Vertrouwen" zowel als in het boek van S.A. Brands ("Rethinking Public Key Infrastructuur and Digital Certificates") wordt geconstateerd dat unieke, onomstotelijke identificatie in bepaalde gevallen noodzakelijk is. Het ontbreekt echter zowel in de tekst als de aanbevelingen aan nuancering zodat al snel de stemming wordt gekweekt dat unieke identificatie en PKI een onoverkomelijke bedreiging vormen voor de privacy. Unieke identificatie is mogelijk door persoonsgerelateerde gegevens op te nemen als NAV-gegevens en geboortedatum of een uniek nummer. Vooralsnog geeft PKI overheid de voorkeur aan een nummer boven het opnemen van aanvullende persoonsgebonden gegevens.

Gezien de toch op essentiële vlakken verschillende uitgangspunten tussen PKI Overheid en het rapport "Sleutels van Vertrouwen", welke verschillen ook tijdens het eerder genoemde gesprek zijn aangegeven, is het enigszins ongelukkig dat PKI Overheid en een medewerker, de heer [redacted] in het rapport wordt genoemd, zonder dat daarbij wordt opgemerkt dat het rapport niet noodzakelijkerwijs de meningen van de betrokkenen weergeeft.

Postadres:
Postbus 20011
2500 EA DEN HAAG

Bezoekadres:
Herengracht 17-19
2511 EG DEN HAAG

tel: 070-346 22 88
fax: 070-312 36 12
internet: www.PKIoverheid.nl

COMMUNICEREN IN VERTROUWEN



- Overigens vinden wij het spijtig dat het rapport de positieve aspecten voor de privacy die volgen uit de toepassing van PKI, nauwelijks belicht. Men denke bijvoorbeeld aan het voorkomen van identiteitsfraude en de bijbehorende schade aan de persoonlijke levenssfeer.

Dat deze privacyzaak de Taskforce PKI Overheid na aan het hart ligt, is u uit eerdere contacten en verzoeken tot het leveren van een bijdrage aan het oplossen van deze problematiek genoegzaam bekend. Wij steunen daarom de Registratiekamer in haar streven om de negatieve gevolgen van een digitale identiteit voor de privacy weg te nemen of tot acceptabele proporties terug te brengen. Wij zien hierin ook een actieve rol voor de Taskforce PKI Overheid weggelegd. Wij treffen in uw rapport echter nog weinig aangrijpingspunten aan, die helpen om dit streven te realiseren. Uw concrete aanbevelingen wijken te ver af van de huidige stand van zaken op het gebied van TTP-dienstverlening en PKI. Graag zoeken wij daarom met u naar begaanbare wegen in dit gezamenlijk streven.

Met vriendelijke groet

[Redacted signature]

Taskforce PKI Overheid

COMMUNICEREN IN VERTROUWEN IN COMMUNICEREN



Datum
4 december 2001

Ons kenmerk
DIOS/IC2001/u99562

Onderdeel
Directie Informatiebeleid
Openbare Sector

Inlichtingen

T [REDACTED]
F [REDACTED]

Uw kenmerk

Blad
1 van 1

Aantal bijlagen
1

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Deelnemers PKI Workshop Migratie

Onderwerp
Notulen PKI workshop Migratie

Geachte workshop deelnemer,

Op 8 november 2001 jongstleden werd in de Van Limburg Stirumzaal van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties de workshop "PKI migratie" gehouden. Hierbij treft u de notulen aan van deze bijeenkomst.

Hartelijk dank voor uw deelname.

Met vriendelijke groet,

[REDACTED]

Notulen PKI Workshop Migratie

Datum: 8-11-2001

Tijdstip: 9:30-12:00

Locatie: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Van Limburg Stirumzaal

Deelnemers: [REDACTED] (HEC - voorzitter)
[REDACTED] (BAC)
[REDACTED] (BAC)
[REDACTED] (BZK/BPR)
[REDACTED] (BZK/DIOS)
[REDACTED] (BZK/DIOS)
[REDACTED] (Defensie)
[REDACTED] (DTO)
[REDACTED] (Justitie)
[REDACTED] (Justitie)
[REDACTED] (PKIoverheid)
[REDACTED] (PKIoverheid)
[REDACTED] (Senter)
[REDACTED] (Senter)
[REDACTED] (SZW)
[REDACTED] (V&W)

[REDACTED] (voorzitter) heet iedereen welkom en geeft aan dat de focus van de workshop gericht is op proces eigenaren.

Presentatie Belastingdienst

[REDACTED] (Belastingdienst) geeft een korte presentatie over de pilot Aangifte Via Internet (AVI). De proef is gestart na een Bestuursbesluit in 1997. Aan de proef hebben ongeveer 1000 ondernemers meegewerkt; voorwaarde voor deelname was dat degene die de aangifte verzorgde tevens degene was die de betaling verrichtte. De proef heeft tot eind 2001 geduurd. De belangrijkste problemen die zich tijdens de proef hebben voorgedaan hangen samen met de uitgifte en gebruik van certificaten. Ca. 20% van de certificaten zijn opnieuw uitgegeven wegens het verlies van pincode of het in ongereede raken van het softwarecertificaat op de pc. Het down zijn van de CA heeft soms voor problemen gezorgd waardoor op het papieren traject is teruggevallen. In verband met het ontbreken van een elektronisch archief dat voldoet aan alle juridische eisen, zijn aan het einde van de proef alle resultaten op papier uitgedraaid.

Presentatie justitie

[REDACTED] (Bestuursdepartement Justitie) geeft een korte toelichting op de PKI-pilots binnen Justitie. Justitie omvat ca. 40.000 werkplekken verspreid over 450 lokaties. Vertrouwelijkheid staat voor Justitie hoog in het vaandel, wat ook blijkt uit de pilots die er binnen Justitie lopen. De belangrijkste pilots binnen Justitie zijn Directie Informatie (intern), [REDACTED] (Rechterlijke Organisatie), MOT (Meldpunt ongebruikelijke transacties), DBZ (Dir: Bestuurszaken; gratieverzoeken, testamentenregister, verklaring v goed gedrag), CIOT (Centraal Informatiepunt Onderzoek Telecom), VK (Vreemdelingenketen)

[REDACTED] heeft ander karakter dan de andere projecten. [REDACTED] maakt vanwege de strenge eisen aan de

vertrouwelijkheid gebruik van biometrie (vingerafdruk); er is besloten zelf de CA-uitvoering in te richten. De RA-functie is decentraal ingericht en is bij informatiebeveiligingsfunctionarissen van arrondissementen belegd.

De voorzitter meldt wat hem tijdens deze presentaties is opgevallen:

- Hoewel de projecten verschillen, blijkt dat PKI zich in het beginstadium van ontwikkeling bevindt.
- De verschillende bedrijfsprocessen kennen hun eigen eisen en leiden tot aparte opzet van PKI.
- In deze presentaties worden de certificaten met name door eigen medewerkers en bedrijven gebruikt, niet door burgers.

Toelichting op notitie

De voorzitter geeft kort de twee scenario's uit notitie weer. In de discussie kunnen eventueel nog andere scenario's naar voren worden gebracht.

_____ geeft aan dat deze discussie is aangezwengeld door Justitie. Justitie heeft het voorbehoud alleen gemaakt voor het domein OVERHEID-OVERHEID en niet voor de overige domeinen. In dit domein is het zijns inziens ook mogelijk deel uit te maken van de vertrouwelijkheidsstructuur op basis van lagere eisen gecombineerd met aanvullende maatregelen.

_____ geeft een korte toelichting op de notitie. Het is de bedoeling een generieke PKI in te richten, rekening houdend met internationale ontwikkelingen. De afweging nu gaat tussen ofwel het uiteindelijke, gemeenschappelijk niveau nastreven en daar eventueel in individuele trajecten naar toe groeien, ofwel tussentijds een gezamenlijk niveau hanteren. Bij de laatste optie rijst echter onmiddellijk de vraag welk niveau of welke hoogte dit niveau zal hebben. De PKI-markt is op dit moment nog niet rijp, waardoor er individuele trajecten zullen ontstaan. Deze trajecten kunnen door de taskforce ondersteund worden, maar zullen in eerste instantie geen deel uitmaken van de PKI voor de overheid, en zullen daar individueel naar toe migreren.

_____ gaat kort in de ontwikkelingen rond de eNIK. Het paspoort zal voorzien worden van een biometrisch kenmerk in verband met beveiliging. De eNIK zal voorzien zijn van certificaten en biometrie. Volgend jaar zullen twee grootschalige pilots plaatsvinden om de eNIK te beproeven: Kiezen op Afstand en een pilot bij één gemeente (met ca. 30.000 deelnemers aan de pilot). In het najaar van 2002 staan de keuze voor type biometrie en het besluit voor uitrol van de eNIK op de agenda.

De voorzitter vraagt expliciet naar het generieke aspect van de PKI voor de overheid en naar het eindniveau van deze PKI. _____ Het generieke aspect is vooral van belang voor de eindgebruikers; met meerdere niveaus wordt het onbegrijpelijk voor de burgers en ambtenaren. Het eindniveau voor de elektronische handtekening wordt bepaald door de eisen in de Europese Richtlijn; voor vertrouwelijkheid wordt uitgegaan van alle informatie met uitzondering van gerubriceerde informatie.

_____ wijst er op dat een PKI in een grote organisatie gefaseerd ingevoerd moet worden: eerst ervaring opdoen met softwarecertificaten. Justitie is onderdeel van de overheid en het kan toch niet zo zijn dat Justitie in dat geval geen onderdeel zou uitmaken van vertrouwensstructuur van de overheid. De heer _____ heeft de indruk dat deze overgangssituatie reeds eerder door Stuurgroep is toegezegd.

_____ geeft aan dat verschillende niveaus in één infrastructuur een probleem oplevert: de zwakste bepaalt het niveau van het geheel. Het is altijd mogelijk op technisch en/of organisatorisch niveau afspraken te maken tussen PKI's van verschillende niveaus. _____ noemt het risico dat er na het maken van separate afspraken geen behoefte meer is aan een gemeenschappelijke PKI.

Discussie

De voorzitter stelt voor het voorstel voor het migratietraject als uitgangspunt te nemen en wil graag tot een voorkeursadvies komen. Komende discussie wil hij gebruiken in hoeverre we het er over eens zijn. En op welke punten er nog een discussie gevoerd moet worden. De voorzitter vraagt de aanwezigen (organisaties) of zij zich in het voorstel voor het migratietraject kunnen vinden.

Senter _____ Graag een realistisch traject uitzetten. Eerst pilots uitvoeren en dan het eindniveau

bepalen met gemeenschappelijk draagvlak. De kaarten die de Kamer van Koophandel aan bedrijven gaat uitgeven zijn bedoeld voor meerdere e-diensten. Er is een vliegwieleffect nodig om een kritische massa te kunnen bereiken. En dat desnoods zonder nog te voldoen aan de standaarden. Maar daarbij wel het kwaliteitsniveau bewaken. Het doel moet helder neergezet worden.

Belastingdienst - [redacted]: Is het eens met de opmerkingen van Senter. Voegt daar aan toe dat het bewerken van de markt noodzakelijk is teneinde een maatschappelijk breder draagvlak te verkrijgen.

Justitie - [redacted] wil zichzelf niet herhalen; de eerder gemaakte opmerkingen blijven staan. [redacted] Hoewel de Rechterlijke Organisatie (RO) zijn eigen belang heeft, is er weinig verschil met de voorgestelde PKI voor de overheid. Voor de RO geldt een hoog niveau om alles goed af te kunnen dekken. Dit houdt niet in dat de RO afstand zal nemen van de gemeenschappelijke standaarden; het vasthouden aan industriële standaarden is hierbij van belang. Er worden slechts beperkte migratieproblemen voorzien om aan te haken bij de PKI voor de overheid. [redacted] Justitie is een grote organisatie. De Directie Informatievoorziening (DI) wil ook voldoen aan de eindtermen, maar voorziet een gefaseerde benadering. Maar het is niet acceptabel als wij niet in de gemeenschappelijke vertrouwensstructuur kunnen meedoen.

Voorzitter: Ook met onderlinge, gemeenschappelijke afspraken is het mogelijk vertrouwen te verkrijgen.

Defensie - [redacted]: Op basis van de eigen ervaringen met de PKI-pilot wil Defensie aansluiten bij de uitgangspunten van de taskforce. En daarmee aansluiten bij de Europese richtlijn. Voor Defensie is ook een hoger niveau van belang (Nato-vertrouwelijk). [redacted] Met behulp van aanvullende eisen is het wellicht mogelijk ook de hogere niveaus (STG) af te dekken. Het intern gebruiken van meerdere niveaus is nog in onderzoek.

SoZaWe - [redacted] Uw klanten zijn mijn klanten: interoperabiliteit is dan ook een voorwaarde. Marktconformiteit is belangrijk. Zowel interoperabiliteit en marktconformiteit zal over de landsgrenzen heen goed moeten werken. Geen bezwaar tegen gedifferentieerde migratiestrategieën.

Verkeer en Waterstaat - [redacted] Het redeneren vanuit de bedrijfsprocessen is een goede invalshoek. Om het einddoel te bereiken kan een kenniscentrum PKI een goede rol spelen: individuele hulp, kennis en geld. De moeilijkheid van PKI is een risicofactor. Het is belangrijk PKI en de aandachtspunten in begrijpelijke termen uit te leggen aan stuurgroepen / SG's zodat de problemen goed bespreekbaar zijn.

Justitie - [redacted] aanvulling op het kenniscentrum: Taskforce zou een generiek business plan ter beschikking kunnen stellen aan partijen.

BPR - [redacted] Er wordt nu al aan gewerkt om de ontwikkeling eNik tegelijk te laten oplopen met ontwikkeling van diensten. De Taskforce doet mee met de pilots, brengt deskundigheid in en kijkt mee; BPR verwacht een inhoudelijke inbreng van de taskforce. BPR heeft zelf budget gekregen voor de pilots.

Taskforce - [redacted] Wij ondersteunen pilots wanneer ze het commitment hebben te migreren naar het eindniveau: Programma van Eisen (PvE). Wij leren ook van pilots, ook - of misschien wel juist - wanneer ze afwijken van het PvE.

Binnenlandse Zaken - [redacted] In het verleden is in het ICT beraad de afspraak gemaakt dat we zouden komen tot een gemeenschappelijke vertrouwensinfrastructuur voor drie domeinen: Overheid-Overheid, Overheid-Burger en Overheid-Bedrijfsleven, zodat individuele organisaties niet steeds zelf het wiel moeten uitvinden en er een gezamenlijk betrouwbaarheidsniveau t.a.v. vertrouwelijkheid en digitale identificatie zal ontstaan. Naar aanleiding van de discussie van vandaag is er duidelijk dat er een verschil van inzicht bestaat tussen Justitie en de Taskforce. [redacted] het gaat hier om het verschil tussen impliciet vertrouwen en expliciet vertrouwen. Voor de Taskforce is het geen probleem wanneer partijen van elkaars PKI (die nog niet aan het eindniveau voldoet) gebruik kunnen maken wanneer ze dat expliciet onderling afspreken. De Taskforce heeft er wel een probleem mee wanneer dit vertrouwen impliciet moet blijken uit deelname aan de gemeenschappelijke infrastructuur reeds voordat aan het eindniveau wordt voldaan: dat betekent namelijk een tijdelijk lager gemeenschappelijk niveau. [redacted] wij willen ook in dit stadium al het impliciete vertrouwen.

Na een korte discussie over de wijze waarop afspraken gemaakt kunnen worden vat de voorzitter de bevindingen van de workshop samen in een zestal punten:

1. PKI is een ontwikkeltraject.
2. Daarin zijn de organisatorische belangen, vanuit de bedrijfsprocessen dominant.
3. Gegeven de ontwikkelingen willen de deelnemers zich individueel ontwikkelen en migreren.
4. Daarbij onderkennen we in gezamenlijkheid dat er één eindsituatie is waar we allen naar streven. Deze eindsituatie is ook in ontwikkeling.
5. Afspraken moeten gemaakt worden over de mogelijkheid van compenserende maatregelen. Daarbij moet nog nader worden bepaald of deze afspraken impliciet of expliciet moeten zijn.
6. Kenniscentrum op gebied van PKI kan ons goed helpen.

Het BAC vraagt zich nog af of in deze punten nog wordt voorzien in een eenduidig geluid ter bevordering van een marktstandaard. De voorzitter geeft aan dat de gemeenschappelijke standaard richting geeft aan de marktstandaard. Het BAC benadrukt hierbij het belang van beïnvloeding van EU standaarden.

1. [REDACTED]
HEC

Deelnemers:

[REDACTED]

2. BAC
t.a.v. [REDACTED] 3
Postbus 9050
7300 GM Apeldoorn

(zelfde adres?)

4. Ministerie van Defensie 8
t.a.v. ing. [REDACTED] 5
DGE & F IV-pool
Postbus 20701
2500 ES Den Haag

+ DTO
(zelfde adres?)

6. Senter Den Haag 8
t.a.v. [REDACTED]
Postbus 30732
2500 GS DEN HAAG

[REDACTED]

7. Senter Zwolle 8
t.a.v. [REDACTED]
Postbus 10073
8000 GB ZWOLLE

2517-JS Den Haag

8. Ministerie van Justitie
[REDACTED]
Postbus 20301
2500 EH Den Haag

DJO KC 114.

9. Ministerie van Justitie 8
t.a.v. [REDACTED]
Postbus 20301
2500 EH Den Haag

[REDACTED]
Coldenhoeke laan 1

10. Ministerie van Verkeer en Waterstaat 8
t.a.v. [REDACTED]
Postbus 20901
2500 EX Den Haag

3185 RC Maasland

[REDACTED]

[REDACTED]

12. BZK/BPR [REDACTED]

13. ICTU/taskforce PKI [REDACTED]
Postbus 84011
2508 AA Den Haag

14. ICTU/taskforce PKI [REDACTED]
Postbus 84011
2508 AA Den Haag

15. ICTU/taskforce PKI [REDACTED]
Postbus 84011
2508 AA Den Haag

16. ICTU/taskforce PKI [REDACTED]
Postbus 84011
2508 AA Den Haag

[REDACTED]

17. BZK/DIOS [REDACTED]

18. [REDACTED]

Later per fax:
[REDACTED]



Datum
21 februari 2002

Ons kenmerk
DIOS/IC2002/58341

Onderdeel
Directie Informatiebeleid
Openbare Sector

Inlichtingen

T (070)
F (070)

Uw kenmerk

Blad
1 van 1

Aantal bijlagen

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

[Redacted]

Minuut

Van
Dir. IOS

Lijnparaaf

Onderwerp
Volmacht Europese aanbestedingsprocedure PKI-
diensten

Medeparaaf
CZW

[Redacted]

Afschrift aan
Archief

Kamer
H618

Afschrift aan

Kamer

Visie

Weer voorleggen

Datum

Geldig bezwaar
Begrotingsjaar

Begrotingsartikel

Bedrag
€

Budgetregel

Verzendgegevens
Uiterste verzenddatum
21 februari 2002

Aanwijzingen

- Aantekenen
- Per expresse
- Per koerier
- Per e-mail

- Per fax
- Internet
- Staatscourant

- Diplomail Aruba
- Diplomail Curaçao
- Diplomail St. Maarten

Bijzonderheden

Verzonden door
Naam

Verzenddatum

[Redacted]