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

Datum
29 november 1999

Ons kenmerk
DIOS/IC/U91707

Onderdeel
dgob/dios/i&c

Inlichtingen
[redacted]

Uw kenmerk

Blad
1 van 2

Aantal bijlagen
3

Bezoekadres
Schedeldoekshaven 200
2511 EZ Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

Aan de leden van de RWTI

Onderwerp
Instelling Taskforce Public Key Infrastructure

In het IB-beraad is op 21 oktober 1999 ambtelijke overeenstemming bereikt over het plan van aanpak voor een PKI taskforce (zie bijlage 1). Deze taskforce zal zich binnen een relatief korte periode belasten met het invoeren van een PKI infrastructuur die betrouwbare en vertrouwelijke elektronische communicatie mogelijk zal kunnen maken. Het IB-beraad adviseert mij om nu deze Taskforce in te stellen. Het advies is mede gebaseerd op twee rapporten *over beveiligde e-mail en Trusted Third Party diensten* voor de rijksoverheid (zie bijlage 2 en 3).

Voor elektronische dienstverlening is een betrouwbaar mechanisme nodig dat kan zorgen voor dezelfde waarborgen die op dit moment in de papieren wereld gelden. Bijvoorbeeld een elektronische aanvraag van een paspoort vraagt om de identiteitsvaststelling van de betrokkenen, de wilsverklaring dat er daadwerkelijk een paspoort wordt aangevraagd en de vertrouwelijkheid van de communicatie van de aanvrager met de uitgevende instantie. Daarvoor wordt gebruik gemaakt van cryptografische technieken. Een ontwikkeling van de laatste decennia is het zogenaamde Public/Private Key-mechanisme; de gebruiker heeft twee sleutels, een zogenaamde Private key die alleen hij kent en een Public key die aan iedereen bekend kan worden gemaakt. Door middel van een onomkeerbaar rekenproces kan hiermee authenticiteit (digitale handtekening) en vertrouwelijkheid gegarandeerd worden. Om de publieke sleutels te kunnen vinden is dan een autoriteit nodig die deze sleutels ergens openbaar beschikbaar stelt (anders zou men telkens de publieke

sleutel bij een communicerende partij op moeten halen). Daarvoor is dan een Public Key Infrastructure noodzakelijk.
Het betrouwbaar mechanisme is generiek; het kan zowel in de communicatie van de overheid met andere overheden, alsook in de communicatie met de burger en ook met het bedrijfsleven toegepast worden.
De in het besluit voorgestelde Taskforce PKI zal zich gaan buigen over het inrichten van een Public Key Infrastructure voor de communicatie van de overheid met deze partijen, en komen tot een ingevoerde PKI voor communicatie met de overheid in Nederland binnen een tijdsperiode van 3 jaar.
Deze infrastructuur zal dan de basis vormen voor een verbeterde externe en interne dienstverlening van de overheid. Toepassingen die gebruik kunnen maken van deze infrastructuur liggen op het gebied van aanvragen van diensten en het beschikbaar stellen van informatie, mogelijk maken van -elektronische- betrokkenheid van burgers bij het openbaar bestuur (elektronisch stemmen, referenda, consultaties etc), lastenverlichting voor het bedrijfsleven door het invoeren van uniforme regimes etc.

Ik ben voornemens om het advies van het IB-beraad over te nemen en de PKI Taskforce in te stellen.

DE MINISTER VOOR GROTE STEDEN- EN INTEGRATIEBELEID

R.H.L.M. van Boxtel

Bijlage 2

Beveiligde E-mail voor de Rijksoverheid

Communiceren in vertrouwen

EINDRAPPORT

Dit rapport werd geschreven in opdracht van de heer mr. [redacted] MPA van het Advies- en Coördinatiepunt Informatiebeveiliging door de heren [redacted] van M&I/STELVIO^{bv}, drs. [redacted] en dr. [redacted] van M&I/PARTNERS^{bv} en [redacted] van NLSign bv.

Inhoudsopgave

Managementsamenvatting

In dit rapport wordt verslag gedaan van een studie die is uitgevoerd door een consortium bestaande uit NLSign bv, M&I/PARTNERS en M&I/STELVIO, in samenwerking met het ACIB en met diverse vertegenwoordigers van onderdelen van de Rijksoverheid. De hoofdvraag van dit onderzoek luidt als volgt:

> *Wat moet er gebeuren om beveiligde e-mail in te voeren binnen onderdelen van de Rijksoverheid?*

Om deze hoofdvraag te beantwoorden worden achtereenvolgens de volgende deelvragen beantwoord:

1. *Wat is beveiligde e-mail?*
2. *Waarom wil men beveiligde e-mail binnen de Rijksoverheid?*
3. *Wat moet er op centraal niveau geregeld worden om de invoering van beveiligde e-mail binnen de Rijksoverheid succesvol te laten verlopen?*
4. *Welke opties zijn er bij de invoering van beveiligde e-mail?*
5. *Welke keuzemogelijkheden zijn er ten aanzien van bestuurlijke, organisatorische en technische aspecten van de invoering van beveiligde e-mail binnen de Rijksoverheid?*

Daarbij is de primaire invalshoek van dit onderzoek de inzet van beveiligde e-mail *binnen* de Rijksoverheid. Dat laat echter onverlet dat bij het opstellen van dit rapport voortdurend in het achterhoofd is gehouden dat de voorziening op den duur ook voor communicatie met derde partijen geschikt zou moeten kunnen zijn. De gekozen oplossing mag hierin geen belemmering vormen.

Wat is beveiligde e-mail?
Beveiliging van e-mail is nodig om communicatie via e-mail te laten voldoen aan eisen van betrouwbaarheid. De volgende betrouwbaarheidseisen (zoals geformuleerd in het Voorschrift Informatiebeveiliging Rijksdienst) zijn hier relevant:

- beschikbaarheid: de mate waarin een informatiesysteem in bedrijf is en de informatie beschikbaar is op het moment dat de organisatie deze nodig heeft;
- exclusiviteit: de mate waarin toegang tot een informatiesysteem, en kennisname van informatie, is beperkt tot een gedefinieerde groep van gerechtigden;
- integriteit: de mate waarin de informatie zonder fouten is.

In dit rapport beperkt de definitie van beveiligde e-mail zich tot de twee laatstgenoemde eisen namelijk exclusiviteit en integriteit. De beschikbaarheid van de infrastructurele componenten van een e-mail systeem valt buiten de scope van dit onderzoek. Derhalve is beveiligde e-mail in dit onderzoek, e-mail die voldoet aan de volgende beschrijving:

- de afzender van een bericht weet zeker dat alleen de ontvanger van het bericht in staat is het bericht te lezen (exclusiviteit) en wel in ongeschonden staat (integriteit);
- de ontvanger van een bericht weet zeker dat het bericht dat hij leest afkomstig is van degene die beweert het gestuurd te hebben, èn ongeschonden is (integriteit).

Bij de beveiliging van e-mail berichten is een belangrijk onderscheid te maken tussen encryptie enerzijds, en elektronische handtekeningen anderzijds.

- *Encryptie* kan in het kort omschreven worden als "het omzetten met behulp van een sleutel van tekst in een reeks onleesbare tekens die met een passende sleutel weer leesbaar gemaakt kunnen worden". Doel van encryptie is dus zeker te stellen dat het bericht alleen gelezen wordt door degene aan wie het gericht is (exclusiviteit);
- Een *elektronische handtekening* kan over het algemeen gebruikt worden om een waarmerk aan een document of bericht te hangen, bijvoorbeeld een waarmerk van echtheid of een tijdstempel. De ontvanger beschikt over de mogelijkheid om het waarmerk te controleren en zo bijvoorbeeld na te gaan of het bericht afkomt van degene die zegt het bericht gestuurd te hebben en of het bericht nog integer is en onderweg niet verminkt is geraakt (integriteit).

Waarom wil men beveiligde e-mail binnen de Rijksoverheid?
E-mail biedt de mogelijkheid om allerlei informatie (dus ook kwetsbare informatie) op een gemakkelijke wijze binnen en tussen organisaties te versturen. Om de voordelen die e-mail biedt op het gebied van een efficiënte en effectieve informatie-overdracht, optimaal te kunnen benutten, is voor de Rijksoverheid van groot belang dat deze informatie-overdracht wel betrouwbaar is. Dit betekent dat beveiliging van e-mail een belangrijk onderwerp is en moet zijn afgestemd op het gebruik dat van e-mail gemaakt wordt.

Daarbij is het van belang dat de Rijksoverheid initiatief neemt op dit terrein. De Rijksoverheid als geheel dient een aantal uitgangspunten te formuleren en bewaken om te voorkomen dat her en der losse initiatieven opkomen die niet voldoende samenhang vertonen om te komen tot een robuust kader voor elektronische overheidscommunicatie. De conclusie dat de Rijksoverheid iets moet doen, leidt vervolgens tot een aantal vragen: wat moet de overheid dan wel doen en welke opties en keuzes liggen hierbij voor? De volgende drie deelvragen hebben hier betrekking op.

Wat moet er op centraal niveau geregeld worden om de invoering van beveiligde e-mail binnen de Rijksoverheid succesvol te laten verlopen?
Deze vraag betreft een bestuurlijke eis ten aanzien van de invoering van beveiligde e-mail bij de Rijksoverheid: de vraag wat er op bestuurlijk niveau aan afstemming moet gebeuren. "Centraal" betekent hier niet dat per definitie bovendepartementale voorzieningen worden getroffen, maar wel dat een aantal zaken *gezamenlijk* geregeld wordt. Interdepartementale afstemming is cruciaal voor de succesvolle invoering van beveiligde e-mail binnen de Rijksoverheid. Deze interdepartementale afstemming dient vorm te krijgen op het hoogste bestuurlijke (en wellicht ook politieke) niveau en dient te worden gefaciliteerd door een nog vorm te geven coördinatie- en expertisecentrum. Binnen deze structuur dient allereerst een aantal overkoepelende kaders te worden vormgegeven en vastgesteld ten aanzien van de architectuur van beveiligde e-mail binnen de Rijksoverheid en de standaarden die hierbij ondersteund worden, de architect-rol. Vervolgens dient het coördinatie- en expertisecentrum vooral de rol van coach te vervullen bij de verschillende departementale invoeringstrajecten.

Cruciaal is derhalve, dat een overkoepelende architectuur wordt vastgesteld voor beveiligde e-mail binnen de Rijksoverheid. De hoofdlijnen van deze architectuur worden vastgesteld door middel van de beantwoording van de volgende deelvraag:

Welke opties zijn er bij de invoering van beveiligde e-mail?
De vraag naar de "opties" betreft in feite de architectuur voor beveiligde e-mail, het gezamenlijk plaatje dat de Rijksoverheid nastreeft bij de invoering van beveiligde e-mail. Deze architectuur betreft een geheel van gezamenlijke keuzes dat de grenzen en bedoelingen van de globale componenten van de beveiligde e-mail voorziening aangeeft. Deze architectuur omvat de volgende keuzes:

- de bestaande bevoegdhedenstructuur dient als uitgangspunt en dient te worden vertaald naar een elektronische omgeving;
  - beveiligde e-mail betreft de uitwisseling tussen functionarissen;
  - de bevoegdheden van de betreffende functionarissen worden vastgelegd en gegarandeerd in een overheidsbrede adressengids;
- er is sprake van end-to-end-beveiliging, beveiliging van berichten die plaatsvindt op applicatieniveau;
- er moet een keuze worden gemaakt ten aanzien van de ondersteunde betrouwbaarheidsniveaus: dient beveiligde e-mail ingezet te kunnen worden voor alle betrouwbaarheidsniveaus (tot staatsgeheim aan toe), of dient dat beperkt te worden?
- er dient een keuze gemaakt te worden voor een bepaalde vertrouwensstructuur: een structuur met TTP-diensten of een structuur met een web van vertrouwen;
- er dient een keuze gemaakt te worden ten aanzien van de uitgifte en het beheer van sleutels.

Hiermee zijn de keuzes op overkoepelend niveau geëxpliciteerd. Vervolgens is dan de vraag wat, naar aanleiding van deze keuzes, de belangrijkste bestuurlijke, organisatorische en technische keuzes zijn die gemaakt moeten worden bij de feitelijke invoering van beveiligde e-mail.

Welke keuzemogelijkheden zijn er ten aanzien van bestuurlijke, organisatorische en technische aspecten van de invoering van beveiligde e-mail binnen de Rijksoverheid?
Op bestuurlijk niveau zijn de belangrijkste keuzes die voorliggen, keuzes ten aanzien van:

- de reikwijdte van de implementatie;
- de vertrouwensstructuur;
- het genereren en distribueren van sleutels;
- de betrouwbaarheidsniveaus waarvoor beveiligde e-mail ingezet moet kunnen worden.

Op organisatorisch niveau liggen belangrijke keuzes voor ten aanzien van:

- installatie en beheer van software;
- opleiding van gebruikers;
- sleutelbeheer;
- organisatie van de aanmaak en distributie van sleutels.

Technisch, tenslotte, betreffen de keuzes de volgende onderwerpen:

- client software;
- voorzieningen voor sleutelbeheer;
- voorzieningen voor sleutel-distributie.

Hierbij dienen de bestuurlijke keuzes als vertrekpunt: de organisatorische en technische keuzes liggen veelal in het verlengde hiervan. Deze bestuurlijke keuzes leiden tot een tweetal "extreme" invoeringsscenario's:

- een "low profile"-scenario waarin de nadruk ligt op decentraal te maken keuzes en waarbij wordt uitgegaan van het "web van vertrouwen":
  - invoering van beveiligde e-mail per proces;
  - vertrouwen formaliseren door middel van een web van vertrouwen;
  - sleutels genereren gebeurt door gebruikers zelf;
  - er is een duidelijke beperking ten aanzien van het betrouwbaarheidsniveau waarvoor beveiligde e-mail inzetbaar is.
- een "high profile"-scenario waarin de nadruk ligt op interdepartementaal te maken keuzes, en waarin dus een aantal belangrijke voorzieningen op interdepartementaal niveau dient te worden getroffen:;
  - beveiligde e-mail wordt grootschalig, als algemene infrastructurele voorziening, geïmplementeerd,
  - vertrouwen wordt geformaliseerd door middel van TTP-diensten,
  - sleutels worden door de organisatie gegenereerd en gedistribueerd,
  - beveiligde e-mail dient inzetbaar te zijn voor alle binnen de Rijksoverheid onderscheiden betrouwbaarheidsniveaus.

Omdat er een grote diversiteit is in de stand van zaken ten aanzien van beveiligde e-mail binnen elk van de onderdelen van de Rijksoverheid en omdat beide scenario's een aantal voor- en nadelen hebben, wordt niet aanbevolen een harde keuze voor één van beide "extreme" scenario's te maken. Wel wordt aanbevolen op centraal niveau een gezamenlijk "eindplaatje" te definiëren, door middel van het uitwerken van de architectuur die hiervoor is beschreven.

De weg naar dit eindplaatje kent een aantal prioriteiten:

- hoewel binnen een organisatie begonnen kan worden met een structuur waarin vertrouwen geformaliseerd wordt in een web van vertrouwen en sleutels individueel worden aangemaakt, dient de doelstelling van een meer hiërarchische structuur (zowel TTP als centrale sleutel-distributie) hoge prioriteit te hebben;
- om als volwaardige vervanging van het papieren circuit te kunnen fungeren dient beveiligde e-mail ingezet te kunnen worden ter ondersteuning van zoveel mogelijk betrouwbaarheidsniveaus. De weg hier naartoe kan echter een geleidelijke zijn: in eerste instantie beperkt tot duidelijk afgebakende betrouwbaarheidsniveaus, met een zeer geleidelijke groei naar een inzetbaarheid voor andere niveaus;
- ook de weg naar een grootschalige implementatie is een zeer geleidelijke omdat de inzet van beveiligde e-mail altijd gerelateerd zal zijn aan concrete processen. Grootschalige implementatie is een groeitraject.

Om ervoor te zorgen dat elk van de decentrale invoeringstrajecten uiteindelijk wel naar dit gezamenlijk eindplaatje toewerkt, is een goede balans nodig tussen wat centraal aan kaders en voorwaarden wordt vastgesteld enerzijds, en de decentrale processen anderzijds.

De belangrijkste aanbevelingen die uit dit alles naar voren komen zijn de volgende:

1. Definieer een gezamenlijk "eindplaatje" waarin de keuzes uit architectuur zijn ingevuld waarin gekozen wordt voor:

a een elektronische vertaling van de huidige bevoegdheden-structuur in de vorm van een overheidsbrede adressengids;
b end-to-end beveiliging, oftewel beveiliging op applicatie-niveau;
c een hiërarchisch stelsel van vertrouwen, met een TTP-dienst en een centrale (oftewel gezamenlijke) sleutel-generatie en -distributie;
d een inzetbaarheid van beveiligde e-mail voor zoveel mogelijk betrouwbaarheidsniveaus;
e een grootschalige maar wel proces-gerelateerde implementatie.

2. Definieer groeiscenario's naar dit eindplaatje,
   a waarin de prioriteit wordt gelegd bij het bewerkstelligen van een hiërarchisch stelsel van vertrouwen en een centrale sleutel-generatie en -distributie;
   b en waarin ten aanzien van betrouwbaarheidsniveaus en grootschalige implementatie een geleidelijk groeimodel wordt gehanteerd.
3. Definieer in samenspraak met de betrokken organisatie-onderdelen het "instapniveau" van elk van de onderdelen in deze groeiscenario's.
4. Roep een centraal coördinatie- en expertisecentrum beveiligde e-mail in het leven dat de verschillende invoeringstrajecten begeleidt en de gezamenlijke doelstellingen bewaakt.
5. Zoek afstemming tussen wat bottom-up en top-down dient plaats te vinden:
   a stel de architectuur en daarmee het "eindplaatje" vast in het IB-beraad dat hiermee de strategische sturing voor zijn rekening neemt;
   b laat het coördinatie- en expertisecentrum fungeren als "coach" voor de invoeringstrajecten binnen de verschillende onderdelen van de Rijksoverheid.

1. Inleiding

Elektronisch communiceren is in opmars binnen de Rijksoverheid. De voornemens die de overheid ten aanzien van dit onderwerp heeft zijn onder andere weergegeven in het Actieprogramma Elektronische Overheid. Hierin wordt betoogd dat de opkomst van ICT (Informatie- en Communicatie-Technologie) in volle omvang de vier traditionele overheidsfuncties raakt: de ordenende, de sturende, de presterende en de verzorgende.

Het Actieprogramma concentreert zich op de presterende en verzorgende functies van de overheid, oftewel, de rol van de overheid als speler in het maatschappelijk proces. Ten aanzien van deze rol worden een drietal hoofdgebieden onderscheiden waarop het belang van ICT zich steeds meer doet gelden:

- een verbeterde interne bedrijfsvoering van de overheid;
- een betere publieke dienstverlening;
- een goede elektronische toegankelijkheid van de overheid.

Het rapport dat nu voor u ligt heeft primair betrekking op het eerste onderscheiden gebied waar ICT van belang is voor het functioneren van de overheid, een gebied dat ook randvoorwaardelijk is voor de andere twee: de interne bedrijfsvoering van de overheid. Mede hiervoor is de aanzet gemaakt om te komen tot een overheidsintranet. In het kader van dit overheidsintranet is nadrukkelijk gewezen op het belang van de mogelijkheid van beveiligde elektronische communicatie tussen medewerkers van de overheid - dit wordt in dit kader als een absolute "need to have"-applicatie beschouwd.

Ook het SG-beraad heeft zich concreet met het onderwerp van informatie-beveiliging met betrekking tot ICT bezig gehouden en het IB-beraad in september 1998 gevraagd een notitie op te stellen inzake beveiliging van het Internet. Door het IB-beraad zijn vier concrete acties opgestart:

- beveiligd end-to-end e-mailverkeer;
- omgaan met TTP's;
- overheidscommunicatie-protocol;
- gedragscode voor Internet-gebruik.

De eerste twee acties zijn voor het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB) van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aanleiding geweest een tweetal onderzoeken op te starten: een onderzoek met als doel te komen tot een architectuur voor beveiligde e-mail binnen (onderdelen van) de Rijksoverheid en een onderzoek met als doel te komen tot een architectuur voor Trusted Third Parties (TTP's) binnen de Rijksoverheid.

Beide onderzoeken zijn uitgevoerd in samenwerking met een consortium bestaande uit NLSign bv, M&I/PARTNERS en M&I/STELVIO en met diverse vertegenwoordigers van onderdelen van de Rijksoverheid. De beide onderzoeken hebben geleid tot een tweetal afzonderlijke maar wel samenhangende rapporten:

- het rapport "Vertrouwen in Communiceren" over TTP-diensten voor de Rijksoverheid;

- het voor u liggende rapport "Communiceren in Vertrouwen" over beveiligde e-mail binnen de Rijksoverheid.

De opdracht die ten grondslag lag aan dit onderzoek, was om een ontwerp uit te werken voor beveiligde elektronische berichtenuitwisseling binnen de Rijksoverheid, rekening houdend (niet in detail) met de bij de Rijksoverheid aanwezige verscheidenheid in voorzieningen.

1.1 Vraagstelling

De hoofdvraag van dit onderzoek luidt als volgt:

> *Wat moet er gebeuren om beveiligde e-mail in te voeren binnen onderdelen van de Rijksoverheid?*

Om deze hoofdvraag te beantwoorden, worden achtereenvolgens de volgende deelvragen beantwoord:

1. *Wat is beveiligde e-mail?*
2. *Waarom wil men beveiligde e-mail binnen de Rijksoverheid?*
3. *Wat moet er op centraal niveau geregeld worden om de invoering van beveiligde e-mail binnen de Rijksoverheid succesvol te laten verlopen?*
4. *Welke opties zijn er bij de invoering van beveiligde e-mail?*
5. *Welke keuzemogelijkheden zijn er ten aanzien van bestuurlijke, organisatorische en technische aspecten van de invoering van beveiligde e-mail binnen de Rijksoverheid?*

Met de achtereenvolgende beantwoording van deze vragen gaan we van een hoog abstractieniveau naar een steeds concreter niveau: eerst de afbakening van het onderzoeksterrein (het wat en waarom), vervolgens aangeven wat op centraal niveau geregeld moet worden en welke keuzes hierbij gemaakt moeten worden en tenslotte wat er binnen de verschillende onderdelen van de Rijksoverheid moet worden geregeld en welke keuzes er bij de concrete invoering van beveiligde e-mail binnen deze organisaties moeten worden gemaakt.

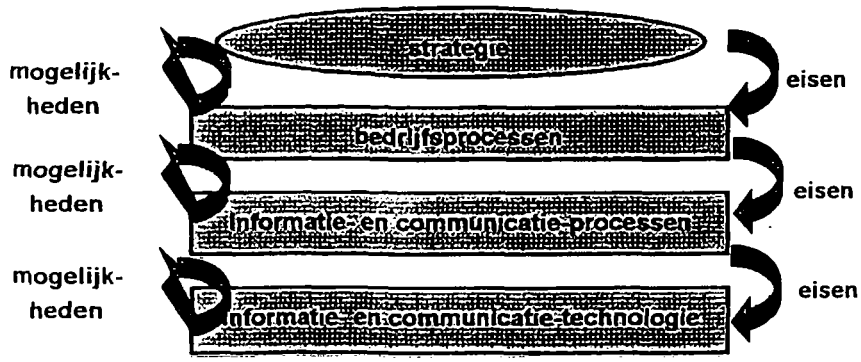
Daarmee vormt dit rapport een leidraad voor bestuurders die zich geconfronteerd zien met de noodzaak tot invoering van beveiligde e-mail, en die zich de volgende vragen stellen:
- Waaruit komt deze noodzaak voort? (hoofdstuk 2 en 3);
- Wat moet daarvoor op het hoogste bestuurlijke niveau geregeld worden? (hoofdstuk 4 en 5);
- Hoe geven we de invoering van beveiligde e-mail vervolgens vorm? (hoofdstuk 6).

1.2 Uitgangspunten

Alvorens de bovenstaande vragen te gaan beantwoorden, moet een aantal uitgangspunten van dit onderzoek duidelijk worden neergezet. Allereerst is de volgende afbakening van

het rapport essentieel: in eerste instantie beschouwt dit onderzoek de inzet van beveiligde e-mail *binnen* de Rijksoverheid.
De inzet van beveiligde e-mail in de interdepartementale communicatie is hier het primaire onderwerp. Dat laat echter onverlet dat bij het opstellen van dit rapport voortdurend in het achterhoofd is gehouden dat de voorziening op den duur ook voor communicatie met derde partijen geschikt zou moeten kunnen zijn. Dit betekent ook dat bij de feitelijke implementatie van beveiligde e-mail volgens de uitgangspunten die in dit rapport gepresenteerd worden, elk organisatie-onderdeel rekening zal moeten houden met deze mogelijke inzet van beveiligde e-mail voor communicatie met derden. De gekozen oplossing moet derhalve marktconform zijn en geen belemmering vormen voor de inzet van beveiligde e-mail in de communicatie met partijen buiten de Rijksoverheid. Dit wordt als een belangrijke randvoorwaarde beschouwd bij de invoering van beveiligde e-mail.

Het onderzoek richt zich op een analyse van de bestuurlijke, organisatorische en technische eisen die worden gesteld ten aanzien van de invoering van beveiligde e-mail binnen onderdelen van de Rijksoverheid. De benadering die daarbij gevolgd wordt is gelijk aan de benadering die in het parallel lopende traject betreffende TTP-diensten binnen de Rijksoverheid gevolgd wordt: primair wordt de analyse opgestart vanuit de diensten waaraan behoefte is, vanuit de processen waarin beveiligde e-mail kan worden ingezet. Tegelijkertijd wordt ook de techniek verkend en waar deze technische verkenning tegemoet komt aan de eisen vanuit de organisatie kan een oplossing liggen. Het volgende model geeft deze redeneerwijze ten aanzien van beveiligde e-mail weer:



Figuur 1.1. Interactie tussen organisatie en ICT (bron: [redacted], 1997)

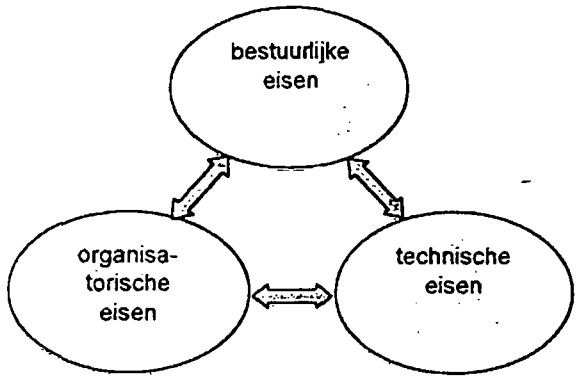
Dit model geeft twee redeneerwijzen weer ten aanzien van de onderlinge afstemming van organisatie en ICT:

1. Vanuit de organisatie-strategie wordt gekeken welke bedrijfsprocessen in een organisatie kunnen worden onderscheiden. Vervolgens wordt geanalyseerd welke eisen bepaalde kenmerken van deze bedrijfsprocessen stellen aan communicatieprocessen. Om aan deze eisen te voldoen, moeten communicatiemiddelen (bijvoorbeeld ICT-toepassingen) geselecteerd worden die hiermee overeenkomen.
2. In de tweede redeneerwijze staan de mogelijkheden die informatie- en communicatietechnologie biedt centraal. Hier wordt bekeken in hoeverre ten gevolge van de inzet van ICT veranderingen in de communicatieprocessen binnen en tussen organisaties optreden. Daarbij betekenen veranderingen in de communicatieprocessen uiteindelijk dat veranderingen in allerlei organisatorische processen kunnen optreden,

hetgeen uiteindelijk ook effecten kan hebben voor de strategische positie van de organisatie.

In dit onderzoek staat de eerste redeneerwijze centraal. Dat betekent dat wordt uitgegaan van bestaande processen en structuren en van de vervanging van bepaalde communicatiemiddelen door beveiligde e-mail (*substitutie*), om daarmee efficiënter en effectiever te kunnen communiceren. De tweede redeneerwijze is er een van *transformatie* van bestaande processen door de inzet van nieuwe technologie en dat is niet de invalshoek van dit onderzoek.

Hierbij vormen de *bestuurlijke eisen* de eisen die aan het hoogste bestuurlijke niveau in de Rijksoverheid gesteld worden: wat moeten zij doen om dit mogelijk te maken? Op grond hiervan worden bepaalde eisen gesteld aan verschillende departementen bij de invoering van beveiligde e-mail (*organisatorische eisen*), en op grond van deze organisatorische eisen worden weer bepaalde eisen gesteld aan de techniek die voor beveiligde e-mail gebruikt wordt (*technische eisen*). Anderzijds is het ook weer zo, dat bepaalde technische keuzen weer zekere eisen aan de organisatie stellen, en dat organisatorische keuzen weer hun weerslag hebben op de bestuurlijke aspecten. Globaal kan de samenhang tussen de verschillende soorten eisen als volgt weergegeven worden:



Figuur1.2. Samenhang tussen bestuurlijke, organisatorische en technische eisen

In de volgende hoofdstukken wordt de bovenstaande redeneerwijze gevolgd en uitgewerkt. Na in hoofdstuk twee duidelijk gemaakt te hebben wat beveiligde e-mail precies is komt in hoofdstuk drie het algemeen kader aan de orde waaruit de noodzaak tot de invoering van beveiligde e-mail voortkomt. In hoofdstuk vier worden de centrale keuzes behandeld die op interdepartementaal niveau gemaakt moeten worden, in hoofdstuk vijf vertaald naar een overkoepelende architectuur. Vervolgens komen de concrete bestuurlijke, organisatorische en technische keuzes aan de orde in hoofdstuk zes: de keuzes die gemaakt moeten worden bij de feitelijke invoering van beveiligde e-mail binnen de departementen. Uiteindelijk leidt dit alles tot een aantal conclusies en aanbevelingen in hoofdstuk zeven.

Tenslotte moet duidelijk zijn dat het onderzoek een sterke samenhang heeft met twee andere activiteiten die momenteel op het gebied van de overheidsinformatievoorziening worden uitgevoerd: het overheidsintranet, en Digitale Duurzaamheid.
Beveiligde e-mail is (zoals eerder gesteld) een "need to have"-applicatie in het Overheidsintranet. Digitale Duurzaamheid is van belang omdat een belangrijk vraagstuk

ten aanzien van betrouwbare overheidscommunicatie is, hoe omgegaan wordt met de archivering van beveiligde elektronische berichten en eventueel de bijbehorende sleutels.

Dit vraagstuk zal in dit rapport alleen zijdelings aan de orde komen - het is juist Digitale Duurzaamheid dat zich intensief hiermee bezig houdt. Naast de twee genoemde activiteiten is er nog een aantal projecten relevant (zoals de overheidswebsite en de overheidsadressengids), die in dit rapport zullen worden aangestipt waar dit van belang is.

2. Beveiligde e-mail

Alvorens in te gaan op de vraag wat de overheid nu precies moet met beveiligde e-mail is het noodzakelijk af te bakenen wat beveiligde e-mail eigenlijk is. In dit hoofdstuk wordt daarom achtereenvolgens besproken wat e-mail is, wat beveiliging van e-mail inhoudt en welke standaarden en producten er op dit gebied zijn. Daarmee wordt de eerste deelvraag beantwoord:

Wat is beveiligde e-mail?

2.1 E-mail als communicatiemiddel

Om enigszins zinvolle uitspraken te doen over het beveiligde gebruik van e-mail is het allereerst van belang om te bepalen wat e-mail is. Hier wordt de volgende definitie gehanteerd [redacted]:

> *E-mail is een medium door middel waarvan gebruikers op asynchrone wijze berichten kunnen uitwisselen tussen adresseerbare elektronische postbussen, gebruik makend van door telecommunicatie verbonden computers*

Een aantal elementen uit deze definitie verdient nadere toelichting. *Asynchrone* communicatie is uitgestelde communicatie, de verzending van de boodschap en de reactie hierop vinden op verschillende tijdstippen plaats waardoor communicatie onafhankelijk van tijd wordt. *Adresseerbare elektronische postbussen* zijn 'hokjes' in het computergeheugen, een e-mail applicatie deelt het geheugen van een computer op in aantal van zulke hokjes, die elk een eigen adres krijgen. Het systeem maakt gebruik van *door telecommunicatie verbonden computers* die communicatie tussen verschillende computers mogelijk maken, hierdoor wordt communicatie ook onafhankelijk van plaats.

Het gebruik van e-mail kan een aantal positieve effecten hebben voor organisaties ([redacted]):

- efficiënter kunnen werken dankzij e-mail: meer kunnen doen in minder tijd, sneller kunnen werken en taken efficiënter uitvoeren;
- efficiënter kunnen communiceren dankzij e-mail: communicatie wordt tijd- en plaats-onafhankelijk, men kan informatie efficiënter op de juiste plek krijgen en belangrijke contacten gemakkelijker bereiken;
- beter (effectiever) kunnen werken dankzij e-mail: een toename van de kwaliteit van de eigen werkzaamheden en van de informatie die men daarvoor nodig heeft;
- meer communicatie buiten de eigen organisatie: e-mail werkt een toename van externe communicatie in de hand;
- nieuwe contacten: in het verlengde van het vorige, is het door de laagdrempeligheid van e-mail ("een mailtje is zo verstuurd") en het grote reservoir aan mogelijke contacten op bijvoorbeeld het Internet, gemakkelijk nieuwe contacten op te doen.

- het ontstaan van een meer flexibele communicatiestructuur: e-mail blijkt minder formele communicatie in de hand te werken en direct contact te vergemakkelijken tussen personen die in de "formele" communicatiestructuur wellicht alleen indirect met elkaar te maken hebben.

Daarnaast kan ook een aantal minder positieve effecten van communicatie via e-mail onderscheiden worden:

- information overload: de bovengenoemde laagdrempeligheid van e-mail heeft ook een schaduwzijde, sommige gebruikers krijgen meer informatie per mail binnen dan ze kunnen afhandelen, en veel van die informatie blijkt ook nog eens irrelevant ("junk mail");
- sociale verarming: waar e-mail de telefoon en zelfs het face-to-face gesprek vervangt ontstaat de vrees voor een verarming van het sociale klimaat in de organisatie;
- oncontroleerbare informatiestromen: e-mail is, zoals hierboven ook al gezegd, een medium dat informele communicatie in de hand werkt. Dit kan als negatief neveneffect hebben dat communicatie die wel aan bepaalde formele eisen moet voldoen en die via e-mail wordt afgehandeld, niet meer aan de gestelde eisen voldoet. Dit heeft weer negatieve effecten op de processen in het kader waarvan de informatie wordt uitgewisseld. Deze formele eisen kunnen zowel te maken hebben met de deelnemers aan het communicatieproces (formele goedkeuringen, parafencircuit e.d.), als met de inhoud van het bericht.

Met name het laatste mogelijke negatieve effect van e-mail leidt tot problemen in (overheids)organisaties die te maken hebben met beveiliging. De algemene beveiligingsissues die met e-mail te maken hebben, worden in de volgende paragraaf besproken.

2.2 Beveiliging van e-mail

Bij communicatie via e-mail kunnen zich grosso modo de volgende problemen voordoen die met beveiliging te maken hebben:

1. Het bericht kan gelezen worden door iemand voor wie het niet bedoeld is.
2. De berichtinhoud kan gewijzigd worden.
3. Het bericht kan verloren gaan tijdens het transport, bij de verzendende partij of bij de ontvangende partij
4. Iemand kan een bericht sturen in naam van iemand anders (spoofing).
5. De verzender kan ten onrechte ontkennen het bericht gestuurd te hebben.
6. De ontvanger kan ten onrechte ontkennen een bericht ontvangen te hebben.
7. De ontvanger kan ten onrechte claimen een bericht ontvangen te hebben.
8. De verzender kan ten onrechte claimen een bericht gezonden te hebben.
9. Een bericht kan verkeerd afgeleverd of doorgestuurd worden.
10. Het transport kan (tijdelijk) uitvallen.

Het voorkomen van problemen die in de punten 5 t/m 8 in deze opsomming worden genoemd, wordt wel aangeduid met de term "non-repudiation", het dusdanig beveiligen van de voorziening dat ondubbelzinnig vast staat wie een bericht verstuurd heeft en wie het ontvangen heeft.

Om e-mail in te kunnen zetten voor een betrouwbare informatievoorziening, mogen de bovengenoemde problemen niet of in geringe mate voorkomen. Aan een betrouwbare informatievoorziening worden eisen gesteld die in het Voorschrift Informatievoorziening Rijksdienst (VIR, 1994) als volgt zijn geformuleerd:

- beschikbaarheid: de mate waarin een informatiesysteem in bedrijf is en de informatie beschikbaar is, op het moment dat de organisatie deze nodig heeft;
- exclusiviteit: de mate waarin toegang tot een informatiesysteem en kennisname van informatie, is beperkt tot een gedefinieerde groep van gerechtigden;
- integriteit: de mate waarin de informatie zonder fouten is.

In dit rapport beperkt de definitie van beveiligde e-mail zich tot de twee laatstgenoemde eisen: exclusiviteit en integriteit (inclusief "non-repudiation"). De beschikbaarheid van de infrastructurele componenten van een e-mail systeem valt buiten de scope van dit onderzoek. Derhalve is beveiligde e-mail in dit onderzoek, e-mail die voldoet aan de volgende beschrijving:

- de afzender van een bericht weet zeker dat alleen de ontvanger van het bericht in staat is het bericht te lezen (exclusiviteit) en wel in ongeschonden staat (integriteit) en
- de ontvanger van een bericht weet zeker dat het bericht dat hij leest afkomstig is van degene die beweert het gestuurd te hebben, en in ongeschonden staat is aangekomen (integriteit).

Over de beschikbaarheid van e-mail kan in het kader van de beveiliging nog wel het volgende gezegd worden: een bepaald niet denkbeeldig risico voor de beschikbaarheid van systemen en netwerken komt voort uit virussen. E-mail wordt vaak gebruikt om dergelijke virussen over te brengen. Dit is een belangrijk onderwerp maar een onderwerp dat samenhangt met algemeen informatiebeveiligings-beleid en niet specifiek met beveiliging van e-mail. Dit onderwerp wordt in dit rapport verder dan ook niet behandeld.

Bij de beveiliging van e-mail berichten is een belangrijk onderscheid te maken tussen encryptie enerzijds en elektronische handtekeningen anderzijds.

2.2.1 Encryptie

Encryptie kan in het kort omschreven worden als "het omzetten met behulp van een sleutel van tekst in een reeks onleesbare tekens die met een passende sleutel weer leesbaar gemaakt kunnen worden". Doel van encryptie is dus om zeker te stellen dat het bericht alleen gelezen wordt door degene aan wie het gericht is: het bewaren van de *exclusiviteit* van de overgedragen informatie dus. Hierbij wordt onderscheid gemaakt tussen symmetrische en asymmetrische encryptie.

Bij *symmetrische encryptie* beschikken verzender en ontvanger allebei over dezelfde sleutel. De sleutel waarmee encryptie wordt uitgevoerd is dezelfde sleutel als waarmee decryptie wordt uitgevoerd. Een bekend voorbeeld van een dergelijke vorm van encryptie is DES (Data Encryption Standard). Met iedereen met wie gecommuniceerd wordt is een zogenaamd "gedeeld geheim" nodig. Dit houdt in dat het aantal benodigde sleutels sterk toeneemt met het aantal deelnemers: waar vier deelnemers nog genoeg hebben aan zes sleutels, is voor acht deelnemers al een aantal van 28 sleutels nodig. Dit loopt snel op als gevolg van het feit dat het aantal benodigde sleutels een kwadratische functie is van het aantal deelnemers. Dit houdt in dat sleutelbeheer al gauw vrijwel onmogelijk wordt.

Bij *asymmetrische encryptie* wordt gebruik gemaakt van een sleutel*paar*. De verzender van een bericht versleutelt het bericht met één sleutel. De ontvanger ontcijfert het bericht met de bijpassende sleutel. Bij asymmetrische encryptie wordt één van de twee sleutels openbaar gemaakt (de publieke sleutel of public key). Dat is ongevaarlijk omdat de eigenschappen van de sleutels zo gekozen zijn dat het onmogelijk geacht wordt uit de publieke sleutel (public key) de geheime sleutel (secret key) te reconstrueren en andersom. Vanwege het publiceren van de publieke sleutel heet deze techniek ook wel "public key cryptography".
Omdat bij asymmetrische encryptie iedere deelnemer aan de communicatie over één publieke sleutel beschikt, is het mogelijk een persoon waarvan men de publieke sleutel heeft, een geheim bericht te sturen. Het nadeel van het onbeheersbare aantal sleutels wordt hier ondervangen: voor vier deelnemers zijn vier sleutelparen nodig, voor acht deelnemers acht sleutelparen, enzovoort.

Voor een gedetailleerde uitleg van encryptie wordt u verwezen naar Bijlage III, *Achtergrondinformatie Beveiligde E-mail en Digitale Handtekeningen*.

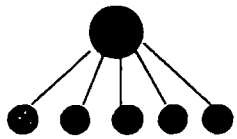
2.2.2 Elektronische handtekening
Een *elektronische handtekening* kan over het algemeen gebruikt worden om een waarmerk aan een document of bericht te hangen, bijvoorbeeld een waarmerk van echtheid of een tijdstempel. De ontvanger beschikt over de mogelijkheid om het waarmerk te controleren en zo bijvoorbeeld na te gaan of

- het bericht afkomt van degene die zegt het bericht gestuurd te hebben;
- het bericht nog integer is en onderweg niet verminkt is geraakt.

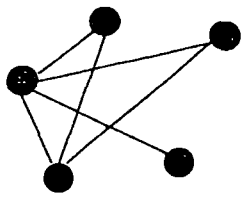
Het probleem "komt dit bericht wel van de persoon die beweert deze persoon te zijn" wordt echter als zodanig niet opgelost door een digitale handtekening. Dit komt omdat iedereen wel een digitale handtekening kan produceren en daar een naam in kan zetten. Daarom is het belangrijk te bepalen of zo'n digitale handtekening vertrouwd kan worden. Degene die de publieke sleutel gebruikt, of iemands digitale handtekening wil kunnen vertrouwen, dient een of andere manier te hebben om er zeker van te zijn dat die sleutel of handtekening ook echt van de persoon afkomstig is die zegt de sleutel uitgegeven te hebben. Ruwweg staan voor de realisatie van dat vertrouwen twee methodes ter beschikking: een hiërarchisch vertrouwen en een web van vertrouwen.

Bij *hiërarchisch vertrouwen* wordt het vertrouwen dat in een digitale handtekening wordt gesteld, ontleend aan een "hogere" autoriteit (een "Trusted Third Party"), die de handtekening van de persoon in kwestie voorzien heeft van de handtekening van de autoriteit. Een dagelijks voorbeeld daarvan kennen we allemaal: paspoort en rijbewijs zijn voorbeelden van documenten die iemands identiteit aantonen.

Bij het *"web van vertrouwen"* wordt het vertrouwen in iemands digitale identiteit gerealiseerd door het tekenen van elkaars publieke sleutel. Op die manier ontstaat een web van vertrouwen, omdat gebruikers het vertrouwen in elkaar formaliseren.



Hierarchisch vertrouwen



Web van vertrouwen

Het onderscheid tussen hiërarchisch en wederzijds vertrouwen wordt nader uitgewerkt in hoofdstuk 5. voor de begripsvorming in dit hoofdstuk volstaat de korte beschrijving die hierboven gegeven is.

Tenslotte is er nog een belangrijke recente ontwikkeling ten aanzien van de digitale handtekening: half mei 1999 kwam de Europese Commissie met een voorstel om tot een gemeenschappelijk juridisch kader voor digitale handtekeningen te komen. Bedoeling is een gemeenschappelijk methode te vinden om elektronische handtekeningen juridisch te erkennen. De Commissie beoogt hiermee te komen tot een situatie waarin elektronische handtekening juridisch op dezelfde manier behandeld worden als geschreven handtekeningen.

In deze paragraaf zijn wat algemene kenmerken van beveiligde e-mail genoemd. In Bijlage III, *Achtergrondinformatie Beveiligde E-mail en Digitale Handtekeningen,* staat een aanzienlijk meer gedetailleerde beschouwing over beveiligde e-mail. In de volgende paragraaf wordt beschreven welke producten er zijn op het gebied van beveiligde e-mail.

2.3 Mechanismen voor beveiligde e-mail

De twee beschikbare publieke mechanismen voor het versturen van secure e-mail zijn op dit moment S/MIME en PGP. Deze twee mechanismen verschillen fundamenteel van elkaar en wel in die mate dat betwijfeld wordt of er ooit één standaard voor beveiligde e-mail zal komen.
De meest in het oog lopende verschillen zijn:
- het gebruik van verschillende encryptie-algoritmen;
- het gebruik van verschillende vertrouwensmodellen.

De aanwezigheid van twee concurrerende standaarden waarbij de markt nog niet definitief heeft gekozen leidt licht tot een patstelling: "laten we nog maar niets doen, dan doen we het ook niet verkeerd". In de navolgende paragrafen wordt afzonderlijk ingegaan op standaarden, leveranciers en producten teneinde het veld overzichtelijker te maken.

Standaarden
Zoals al opgemerkt bestaan er twee open standaarden voor de realisatie van beveiligde e-mail. Die standaarden zijn:

- S/MIME, wat staat voor Secure MIME[1];
- OpenPGP, een publieke versie van PGP.

OpenPGP heeft zich tot nu toe aan exportbeperkingen weten te onttrekken. Aanvullende software (plug-ins) voor onder andere Microsoft en Netscape-producten worden kosteloos geleverd. Daar staat tegenover dat een hiërarchische infrastructuur voor vertrouwen, een PKI, (nog) niet aanwezig is. Open betekend niet alleen dat de specificatie van de standaarden publiek is, maar vooral dat de change-control van de standaarden voorbehouden is aan een standaardisatielichaam, in dit geval de IETF [2]. Op deze wijze wordt voorkomen dat eenzijdige wijziging van de standaard mogelijk is.

Leveranciers van PGP en S/MIME producten hebben daarnaast nog te maken met interoperabiliteitstesten die door het Internet Mail Consortium worden uitgevoerd en speciaal voor S/MIME heeft RSA labs een S/MIME testcentrum ingericht om de interoperabiliteit tussen producten van verschillende leveranciers te testen.
Voor S/MIME is de huidige standaard S/MIME versie 2. Deze standaard zal binnenkort vervangen worden door S/MIME versie 3, waarbij het gebruikelijk is dat de interoperabiliteit tussen diverse versies gewaarborgd blijft.

Leveranciers
Tot de leveranciers van S/MIME producten behoren de grote spelers op het gebied van E-mail en groupware voorzieningen zoals Microsoft, Novell en Netscape. Deze leveranciers hebben commitments afgegeven omtrent de implementatie van de S/MIME standaarden in hun producten en zijn ook zeer nauw betrokken bij de standaardisatie-activiteiten in de IETF.

Omdat voor gebruik buiten de VS en Canada exportbeperkingen gelden, worden in Nederland S/MIME versies afgeleverd met een relatief zwakke encryptie. De software is echter zodanig opgezet dat andere leveranciers, van buiten de VS, hierop kunnen inspelen door additionele software, zogenaamde plug-ins, te verkopen die wél de gewenste sterke encryptie biedt.

OpenPGP wordt tot nu toe door slechts één leverancier geleverd en wordt, zoals gezegd, niet gehinderd door exportbeperkingen. Daardoor kan de toegepaste encryptie sterk zijn en wordt OpenPGP ook beschouwd als een veiliger product. Dat is echter als zodanig niet zo, maar wordt uitsluitend door de exportbeperking veroorzaakt. OpenPGP lijdt echter wel aan de beperking dat de meeste leveranciers geen PGP inbouwen. Dat wordt echter gecompenseerd door de inspanning van de leverancier van OpenPGP die plug-ins voor de meest gebruikte e-mail software meelevert.

[1] MIME staat voor Multipurpose Internet Mail Extensions
[2] IETF staat voor Internet Engineering Task Force

Producten
In de productinventarisatie behorend bij dit onderzoek wordt uitgebreider op producten en de eisen aan producten ingegaan (zie Bijlage II, *Inventarisatie Marktproducten*). Hier kan gemeld worden dat alle grote leveranciers van E-mail en groupware producten S/MIME software hebben of hebben aangekondigd. Dit geldt bijvoorbeeld voor de combinatie Outlook98-Exchange server (Microsoft) voor Groupwise (Novell) en voor Netscape.

2.4 De relatie met de V-kaart

Aanvullend op de bovengenoemde ontwikkelingen rondom S/MIME en PGP is er ook een ontwikkeling die tot doel heeft staatsgeheime communicatie mogelijk te maken, de V-kaart. Deze kaart wordt onder andere in opdracht van het Ministerie van Defensie, het Ministerie van Buitenlandse Zaken, het Ministerie van Justitie en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontwikkeld door Philips Crypto bv. De beveiligingsfuncties zijn daarbij ondergebracht op een PC-insteekkaart en de gehele processing vindt ook op deze kaart plaats.

Met de V-kaart kan op dit moment geen e-mail versleuteld worden; wel kunnen documenten die met de V-kaart zijn versleuteld, meegezonden worden met e-mail. De kaart is bedoeld voor beveiligde communicatie binnen een afgebakend domein; ontwikkelingen die plaatsvinden maken het mogelijk de V-kaart ook in te zetten voor niet-gerubriceerde informatie en om de V-kaart te gebruiken voor e-mail. Zodra deze ontwikkelingen afgerond zijn, is het mogelijk de V-kaart rechtstreeks voor beveiligde e-mail in te zetten, waarbij de aard van de communicatie bepaalt of gebruik gemaakt wordt van de publieke mechanismen voor beveiliging danwel de V-kaart.

3. Waarom beveiligde e-mail?

De assumptie die aan de hoofdvraag van dit onderzoek ten grondslag ligt, is dat er gegronde redenen zijn voor de Rijksoverheid om beveiligde e-mail in te voeren. In dit hoofdstuk worden deze redenen naar voren gehaald, waarmee de volgende deelvraag beantwoord wordt:

Waarom wil men beveiligde e-mail binnen de Rijksoverheid?

In feite gaat het hier om een tweeledige vraag: allereerst moet worden duidelijk gemaakt welke waarde e-mail kan hebben voor onderdelen van de Rijksoverheid en vervolgens is de vraag waar de noodzaak voor beveiliging van deze voorziening uit voortkomt. Vervolgens dient zich dan de vraag aan, waarom het noodzakelijk zou zijn dat de Rijksoverheid activiteiten onderneemt ten aanzien van deze voorziening. Deze vragen worden achtereenvolgens in dit hoofdstuk behandeld.

3.1 ICT en overheids-informatievoorziening

In het Actieprogramma Elektronische Overheid wordt gesproken over de wens om met de inzet van ICT te komen tot een efficiëntere én effectievere overheidscommunicatie. Daarbij is het uitgangspunt dat de middelen waarvan de overheid gebruik maakt wel veranderen, maar dat de voorwaarden waaronder deze middelen worden ingezet (oftewel de eisen die vanuit de verschillende functies van de overheid gesteld worden aan de informatievoorziening) daarbij niet veranderen.

Het algemene kader waarbinnen de inzet van beveiligde e-mail bij onderdelen van de Rijksoverheid vorm dient te krijgen, draait dus vooral om de volgende zaken:

- de inzet van ICT in overheidsprocessen dient om de efficiëntie en effectiviteit van communicatie binnen de overheid verder te bevorderen;
- maar is geen doel op zich, en daarom betekent een inzet van andere middelen niet dat eisen ten aanzien van kwaliteit van dienstverlening, informatiebeveiliging en verantwoording ten aanzien van overheidshandelen worden aangepast. Oftewel, overheidscommunicatie via ICT moet aan dezelfde eisen voldoen waaraan overheidscommunicatie via andere media voldoet.

3.2 Waarom e-mail?

Het hiervoor geschetste bestuurlijk kader vormt de reden voor de Rijksoverheid om een nadere analyse te maken van de mogelijke inzet van e-mail. Zoals in hoofdstuk 2. is beargumenteerd, is e-mail een communicatiemiddel dat de efficiëntie en effectiviteit van (werkzaamheden binnen en tussen) organisaties positief kan beïnvloeden.

Vanuit de wens om ICT in te zetten in het kader van een efficiëntere en effectievere communicatie binnen de overheid is het beschouwen van e-mail als medium voor overheidscommunicatie dan ook logisch.

De feitelijke bijdrage die e-mail kan leveren aan efficiëntie en effectiviteit is afhankelijk van de concrete processen waarin het middel al dan niet kan worden ingezet. Voor dergelijke processen moet allereerst worden vastgesteld of e-mail wel een zinvol middel is om in te zetten. Om dat te beoordelen kunnen de processen worden gescoord op de volgende drie kenmerken:

- bereik: het fysieke bereik van een proces, het aantal personen of locaties dat erbij betrokken is, het gewenste interactieniveau tussen deze personen of locaties, etc;
- complexiteit: de mate waarin een proces duidelijk omschreven is, gestructureerd is, de mate waarin de informatiebehoefte duidelijk is te maken, de complexiteit van de uit te wisselen informatie, etc;
- tijdsafhankelijkheid: de mate waarin sprake is van bepaalde deadlines, verouderende bronnen, de mate waarin directe feedback noodzakelijk is.

Op basis van de scores van e-mail op deze kenmerken kan dan worden vastgesteld waar en in hoeverre e-mail daadwerkelijk een bijdrage kan leveren aan het bevorderen van de efficiëntie en effectiviteit van dit proces.

3.3 Waarom beveiliging?

Het vraagstuk van beveiliging van e-mail hangt samen met de eis dat de inzet van andere middelen voor overheidscommunicatie (in dit geval e-mail) dient te gebeuren onder minimaal gelijkblijvende voorwaarden van kwaliteit, beveiliging en verantwoording.

Ten aanzien van e-mail binnen de overheid hangt het vraagstuk van beveiliging samen met het feit dat een traditioneel informeel communicatiemiddel nu ook voor formele communicatie wordt ingezet. Van formele communicatie is sprake wanneer er regels (aantoonbaar) gevolgd moeten worden. Daarvan is sprake wanneer informatie een rol speelt in een proces waar rechtsgevolgen aan verbonden zijn, maar ook als het om interne regels binnen het Rijk gaat. Om van formele e-mail te kunnen spreken moeten tal van vraagstukken zijn opgelost (zie paragraaf 2.2): beschikbaarheid van systeem en informatie, autorisatie, authenticatie, identificatie, non-repudiation, behoud van integriteit, exclusiviteit.

Het Aktieprogramma Elektronische Overheid beschrijft het als volgt:

> ~~Bij elektronisch berichtenverkeer en dienstverlening is het van belang dat de~~ betrouwbaarheid van de informatie gewaarborgd is. De geautomatiseerde uitwisseling van gegevens biedt naast nieuwe kansen immers ook nieuwe risico's. Deze hebben onder meer betrekking op het waarborgen van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, berichten en transacties (informatiebeveiliging), maar ook op de mogelijkheid van het blijvend bewaren en het afleggen van verantwoording (digitale duurzaamheid). Organisaties moeten daarom kunnen beschikken over betrouwbare voorzieningen.

Dit vertaalt zich in bepaalde eisen aan concrete bedrijfsprocessen, die direct samenhangen met de beveiligingsvraagstukken ten aanzien van e-mail die in paragraaf 2.2 zijn beschreven. Het gaat hier om eisen als:

- de ene partij moet zeker weten wie de andere partij is (authenticiteit);
- informatie mag niet door onbevoegden worden gewijzigd of vernietigd, noch meermalen verzonden (integriteit);
- onbevoegden mogen de informatie niet lezen (vertrouwelijkheid ofwel exclusiviteit);
- verzending dan wel ontvangst kunnen niet worden ontkend (onweerlegbaarheid ofwel non-repudiation).

Alleen als de informatievoorziening aan deze eisen voldoet, kan de overheid als organisatie haar processen op basis van deze informatie correct uitvoeren.

3.4 Belang van initiatief van de Rijksoverheid

Het belang van de invoering van beveiligde e-mail binnen de Rijksoverheid kan nader geïllustreerd worden aan de hand van de situatie die zou ontstaan als de Rijksoverheid helemaal geen initiatief zou ondernemen op dit terrein.

Het is de afgelopen tijd wel duidelijk geworden dat de behoefte aan een dergelijke voorziening aanwezig is: er is nu al sprake van dat personen die daartoe een behoefte voelen, op de een of andere wijze beveiligd communiceren via e-mail. Als de Rijksoverheid geen initiatief in deze onderneemt, zullen dit soort bottom-up initiatieven de overhand krijgen, zonder dat er sprake is van een gezamenlijk overeengekomen kader dat voldoende waarborgen biedt om beveiligde e-mail daadwerkelijk te kunnen inzetten voor formele overheidscommunicatie. De bottom-up initiatieven zullen zich dan, situationeel afhankelijk als ze zijn, elk in een eigen richting ontwikkelen. Het wordt dan steeds moeilijker om infrastructurele voorzieningen te treffen die een dergelijk gezamenlijk kader mogelijk maken. Uiteindelijk leidt dit ertoe dat de bottom-up initiatieven niet leiden tot een situatie waarin de overheid een belangrijk deel van haar formele communicatie via e-mail kan afhandelen, een situatie waarin e-mail als volwaardige vervanging van het papieren circuit kan dienen.

Uiteindelijk komt de overheid dan te zitten met een aantal divergerende, elk voor bepaalde processen wel voldoende maar voor integrale overheidscommunicatie onvoldoende, initiatieven.

3.5 Conclusie

Concluderend kunnen we stellen dat de vraag "waarom beveiligde e-mail" wordt beantwoord aan de hand van algemene eisen die ten aanzien van informatievoorziening binnen de Rijksoverheid worden gehoord.

Het antwoord op "waarom e-mail?" heeft te maken met het streven naar een efficiëntere en effectievere overheid door middel van ICT.

E-mail biedt aanzienlijke mogelijkheden waar het gaat om het efficiënter en effectiever maken van communicatie binnen en tussen organisaties en zou daarom een grote bijdrage kunnen leveren aan het realiseren van dit streven.

Het antwoord op de vraag "waarom beveiliging" komt voort uit het feit dat de inzet van ICT (en dus van e-mail) slechts een middel is dat wordt ingezet onder minimaal gelijkblijvende eisen van kwaliteit, beveiliging en verantwoording als die nu gesteld worden aan de informatievoorziening. Dit vertaalt zich in een aantal eisen aan de informatievoorziening van de overheid, die elk doorwerken in de organisatie en techniek van beveiligde e-mail.

Tenslotte zit het belang van een initiatief van de Rijksoverheid in dit kader vooral in het feit dat de Rijksoverheid als geheel een aantal uitgangspunten moet formuleren en bewaken om te voorkomen dat her en der losse initiatieven opkomen die niet voldoende samenhang vertonen om te komen tot een robuust kader voor elektronische overheidscommunicatie.

4. Centraal en decentraal

In het vorige hoofdstuk is geconcludeerd dat het van belang is dat de Rijksoverheid initiatieven ontplooit ten aanzien van beveiligde e-mail, om te waarborgen dat er een gezamenlijk kader ontstaat voor elektronische overheidscommunicatie. Uitgangspunt bij de invoering van beveiligde e-mail binnen de Rijksoverheid is dat de verschillende onderdelen van de Rijksoverheid verantwoordelijk zijn voor de invoering binnen de eigen organisatie. Daarbij moet er echter wel een centraal referentiekader zijn waaraan de verschillende organisaties moeten voldoen om inderdaad te kunnen spreken van *beveiligde* e-mail. Dit houdt in dat op centraal niveau een aantal keuzes gemaakt moet worden. Hier komen we op de bestuurlijke eisen ten aanzien van beveiligde e-mail: de zaken die op centraal bestuurlijk niveau moeten worden geregeld. In dit hoofdstuk wordt duidelijk gemaakt op welke fronten zaken centraal geregeld moeten worden, waarmee de volgende deelvraag beantwoord wordt:

> *Wat moet er op centraal niveau geregeld worden om de invoering van beveiligde e-mail binnen de Rijksoverheid succesvol te laten verlopen?*

"Centraal" betekent hier overigens niet dat per definitie bovendepartementale voorzieningen worden getroffen maar wel dat een aantal zaken gezamenlijk geregeld wordt.

Hoofdstuk 4. concentreert zich op de vragen:
- wat moeten de onderwerpen zijn waarover interdepartementale afstemming plaatsvindt?
- wie moet er zorgdragen voor interdepartementale afstemming?
- hoe kan de interdepartementale afstemming, en de wisselwerking met de departementale invoeringspraktijk, het best georganiseerd worden?

In hoofdstuk 5. gaan we vervolgens in detail in op één van de onderwerpen waarover interdepartementale afstemming moet plaatsvinden: de architectuur voor beveiligde e-mail binnen de Rijksoverheid.

4.1 Interdepartementale afstemming

Het opstellen van een gezamenlijk kader voor beveiligde e-mail binnen de Rijksoverheid is per definitie een interdepartementaal gebeuren. Dit houdt in dat een aantal zaken interdepartementaal moet worden afgestemd. Dit is een belangrijke bestuurlijke eis ten aanzien van beveiligde e-mail: er moet op het hoogste niveau overeenstemming bereikt worden over een aantal uitgangspunten die voor alle departementen moeten gelden bij de invoering van beveiligde e-mail.

De "wat"-vraag betreft de onderwerpen waarover interdepartementaal afstemming moet plaatsvinden. Hier onderscheiden we de volgende onderwerpen:

- een overkoepelende "architectuur" voor beveiligde e-mail;
- standaarden voor uitwisseling en beveiliging;
- functies die centraal moeten worden georganiseerd.

Elk van deze elementen wordt in het vervolg van dit hoofdstuk nader uitgewerkt. Vervolgens dient zich dan de vraag aan wie deze afstemming moet bereiken en hoe de afstemming tussen "top down" (het interdepartementale deel) en "bottom up" (de invoeringstrajecten binnen de departementen) het best vormgegeven kan worden. Deze vragen worden in paragraaf 4.5 beantwoord.

4.2 Architectuur

Met een "architectuur" wordt in deze studie bedoeld: een geheel van keuzes op overkoepelend niveau dat de grenzen en bedoelingen van de globale componenten van de beveiligde e-mail voorziening aangeeft.

Het is van belang dat deze architectuur op overkoepelend niveau wordt vastgesteld en beheerd. Het gaat hier om een aantal fundamentele keuzes ten aanzien van beveiligde e-mail binnen de Rijksoverheid, waarvan individuele organisaties niet kunnen afwijken. In de architectuur worden keuzes vastgelegd ten aanzien van:
- het vertalen van de bestaande bevoegdhedenstructuur naar een elektronische omgeving;
- het niveau van "end-to-end" beveiliging van e-mail (berichten, netwerk, locaties, werkplek, et cetera);
- het betrouwbaarheidsniveau van berichten die via e-mail worden uitgewisseld;
- de wijze van formalisering van vertrouwen (wederzijds of hiërarchisch);
- verkrijging, verificatie en beheer van sleutels;
- relaties en verantwoordelijkheden van verschillende onderdelen van de technische architectuur.

Onderdelen van de Rijksoverheid die beveiligde e-mail willen uitwisselen met andere onderdelen, zullen zich moeten conformeren aan de keuzes die in de architectuur zijn vastgelegd. Deze architectuur wordt nader uitgewerkt in hoofdstuk 5.

4.3 Standaarden

In hoofdstuk 2. is een aantal standaarden op het gebied van beveiligde e-mail aan de orde geweest. Op centraal niveau moet een keuze gemaakt worden ten aanzien van deze standaarden: welke beveiligingsstandaard wordt gekozen? Dit houdt niet in dat daarmee ook een productkeuze wordt opgelegd, maar wel dat alleen producten gebruikt kunnen worden die gebruik maken van de gekozen beveiligingsstandaard.

Het is noodzakelijk een keuze te maken omtrent de beveiligingsstandaarden die gebruikt worden. Die keuze kan overigens zijn dat er van de beschikbare standaarden geen, één of allebei te gebruiken. Deze keuze kan gebaseerd zijn op de volgende overwegingen:
- is de beveiligingsstandaard veilig genoeg;

- is de beveiligingsstandaard toepasbaar in de nu gebruikte e-mail omgevingen;
- is de beveiligingsstandaard gebaseerd op de gewenste vertrouwensbasis (hiërarchisch danwel onderling);
- wat is de standaard waarmee personen en instellingen buiten de Rijksoverheid met de Rijksoverheid zal gaan communiceren;
- worden producten voor de beveiligingsstandaard door meer dan een leverancier geleverd, ofwel hoe reageert de markt op de aanwezigheid van twee beveiligingsstandaards.

Bij het kiezen van de beveiligingsstandaard zijn er drie mogelijkheden:
- er wordt geen keuze gemaakt;
- er wordt een standaard gekozen;
- er wordt een standaard gekozen die preferent is, dat wil zeggen dat de Rijksoverheid deze preferente standaard toepast en minimaal zorgt voor compatibiliteit met de andere standaard.

Het gevolg van geen keuze is dat beveiligde e-mail niet mogelijk zal zijn en dat enige wildgroei zal ontstaan bij die personen of afdelingen die beveiligde communicatie beslist nodig hebben (zie ook paragraaf 3.4). Als gekozen wordt voor één bepaalde standaard, met uitsluiting van andere, is de onderlinge communicatie binnen de Rijksoverheid verzekerd, maar bestaat de mogelijkheid dat de communicatie met partijen die gekozen hebben voor een andere oplossing gehinderd zal worden. Een keuze voor een preferente standaard, waarbij de tweede standaard wel geïmplementeerd wordt maar voor zelf geïnitieerde communicatie niet gebruikt wordt, betekent dat communicatie met iedereen mogelijk blijft. Wel is het zo dat het implementatietraject dan ingewikkelder zal zijn, wat betekent dat een afweging gemaakt moet worden tussen het bereik van de communicatie met beveiligde e-mail (beperkte groep of iedereen) en de inspanningen en kosten die gemoeid zijn met de implementatie. Bij deze afweging dient dan ook weer een rol te spelen dat de gekozen oplossing geen belemmering mag vormen voor communicatie met derde partijen.

4.4 Gezamenlijke functies

De invoering van beveiligde e-mail binnen de departementen is de verantwoordelijkheid van de afzonderlijke departementen. Wel moet er, zoals eerder betoogd, sprake zijn van een gezamenlijk kader waarbinnen deze departementale trajecten plaatsvinden. Om dat gezamenlijk kader te bewaken, is een zekere vorm van coördinatie nodig. Het overzicht over de verschillende trajecten moet bewaard blijven en er moet voor gezorgd worden dat bij deze departementale trajecten wel de gezamenlijke doelstellingen in het oog gehouden worden. Daarnaast zal er ook behoefte bestaan aan het delen van kennis, expertise en ervaringen met de invoering van beveiligde e-mail tussen de verschillende departementen. Zo wordt bevorderd dat elk departement een aantal dezelfde uitgangspunten hanteert bij de invoering van beveiligde e-mail en dat departementen kunnen profiteren van dezelfde kennis-voorraad, en van elkaars ervaringen.

De hierboven beschreven behoeften kunnen leiden tot het vormgeven van een tweetal gezamenlijke functies, die goed gecombineerd zouden kunnen worden in één organisatie:

- *coördinatiecentrum*: op centraal niveau kan een coördinatiecentrum worden ingericht, een interdepartementaal adviserend/coördinerend/faciliterend orgaan dat ondersteuning levert bij invoering, gebruik en beheer van beveiligde e-mail;
- *expertisecentrum:* het is zeer aan te bevelen een expertisecentrum voor implementaties van beveiligde e-mail in te richten. De centrale en departementale werkgroepen kunnen bij dit expertisecentrum terecht voor deskundig advies op beleids-, technologisch en juridisch terrein.

In hoofdstuk 2. is gesproken over het onderscheid tussen hiërarchisch vertrouwen en een web van vertrouwen. Indien gekozen wordt voor een systematiek van hiërarchisch vertrouwen, creëert dit weer een keuze voor het overkoepelende niveau. Hiërarchisch vertrouwen betekent, zoals in hoofdstuk 2. is aangegeven, dat gebruik gemaakt wordt van de diensten van een Trusted Third Party. Op het centrale niveau is een belangrijke vraag of dit een centrale overheids-TTP moet zijn. De afwegingen die bij deze laatste keuze gemaakt moeten worden, staan centraal in het rapport "Vertrouwen in Communiceren".

4.5 Organisatie

Ten aanzien van de "wie"-vraag is, gezien de onderwerpen waar het hier over gaat, van belang dat afstemming op hoog niveau plaatsvindt. Dan zijn er op het eerste gezicht twee mogelijkheden: interdepartementale afstemming kan plaatsvinden op het niveau van het IB-beraad (de ambtelijke top) of op het niveau van de Ministerraad (de politieke top). Omdat de invoering van beveiligde e-mail primair het functioneren van het ambtelijk apparaat raakt, lijkt het IB-beraad (dat overigens in de loop van 1999 overgaat in het "ICT-beraad") hier het aangewezen gremium.

Bij het realiseren van interdepartementale initiatieven komt de Rijksoverheid als concern altijd in aanraking met het feit dat de verschillende departementen nevengeschikt zijn: het ene Ministerie kan het andere niet dwingend iets opleggen. Dit betekent dat dergelijke initiatieven voor een belangrijk deel "bottom-up" tot stand moeten komen: elk Ministerie regelt de zaken binnen haar eigen verantwoordelijkheidsgebied, en vanuit die positie moet naar gezamenlijkheid worden toegewerkt.

De praktijk leert echter dat een dergelijke gezamenlijkheid niet tot stand komt als er niet ook "top-down" een aantal kaders worden vastgesteld. Dat onderstreept het belang van het interdepartementaal vaststellen van een aantal kaders waaraan de verschillende departementen zich hebben te houden bij de invoering van beveiligde e-mail binnen hun organisatie.

De afweging tussen wat top-down moet gebeuren en wat bottom-up, is geen gemakkelijke. Omdat het voor een coördinerend orgaan niet mogelijk is deze kaders dwingend aan andere onderdelen van de Rijksoverheid op te leggen, moet een juiste balans worden gezocht tussen top-down en bottom-up.

Bij de invoering van beveiligde e-mail binnen de Rijksoverheid zal de rol van het hiervoor beschreven coördinatie- en expertisecentrum vooral als "coach" te omschrijven zijn: de verschillende invoeringstrajecten zijn de verantwoordelijkheid van de departementen en

de activiteiten zullen zich vooral moeten richten op het faciliteren en ondersteunen van de verschillende invoeringstrajecten.

Er is echter ook een rol als "architect" weggelegd: ergens moeten centrale structuren worden opgesteld, moet de architectuur voor interdepartementale invoering en gebruik van beveiligde e-mail worden bewaakt. Deze architectuur wordt in het volgende hoofdstuk van dit rapport nader uitgewerkt. Pas als deze architectuur is gedefinieerd en is geaccepteerd op SG-niveau, kan de coach-rol van het coördinatie- en expertisecentrum worden ingevuld, pas als duidelijk is binnen welke gezamenlijke kaders de invoering van beveiligde e-mail dient plaats te vinden, kan met de feitelijke invoering binnen departementen begonnen worden. Dan wordt ook pas de ondersteunende en faciliterende rol relevant.

4.6 Conclusie

Conclusie is dat interdepartementale afstemming cruciaal is voor de succesvolle invoering van beveiligde e-mail binnen de Rijksoverheid. Deze interdepartementale afstemming dient vorm te krijgen op het hoogste bestuurlijke niveau. Binnen deze structuur dient allereerst een aantal gezamenlijke kaders te worden vormgegeven en vastgesteld ten aanzien van de architectuur van beveiligde e-mail binnen de Rijksoverheid en de standaarden die hierbij ondersteund worden, de architect-rol. Vervolgens dient het coördinatie- en expertisecentrum vooral de rol van coach te vervullen bij de verschillende departementale invoeringstrajecten.

Cruciaal is derhalve, dat een overkoepelende architectuur wordt vastgesteld voor beveiligde e-mail binnen de Rijksoverheid. In hoofdstuk 5. wordt deze architectuur in hoofdlijnen neergezet.

5. Naar een architectuur

In het vorige hoofdstuk is aangegeven welke interdepartementale afstemming noodzakelijk is om tot een Rijksoverheids-brede invoering van beveiligde e-mail te kunnen komen. Als cruciaal onderwerp waarover dergelijke afstemming moet worden bereikt, is een overkoepelende architectuur om te komen tot de invoering beveiligde e-mail binnen onderdelen van de Rijksoverheid aangewezen. Deze architectuur wordt in dit hoofdstuk in meer detail behandeld.

Met een "architectuur" wordt in deze studie bedoeld:

> een geheel van keuzes op overkoepelend niveau dat de grenzen en bedoelingen van de globale componenten van de beveiligde e-mail voorziening aangeeft.

In dit hoofdstuk worden de hoofdlijnen van deze architectuur geschetst. Dit gebeurt door aan te geven welke opties kunnen worden onderscheiden bij de invoering van beveiligde e-mail, welke keuzes er zijn bij de invulling van zo'n voorziening. Hiermee wordt de volgende deelvraag beantwoord:

> *Welke opties zijn er bij de invoering van beveiligde e-mail?*

Deze "opties" betreffen zowel bestuurlijke en organisatorische als technische keuzes.

5.1 Elektronische bevoegdhedenstructuur

Het uitgangspunt dat in dit rapport gehanteerd wordt bij de invoering van beveiligde e-mail is *substitutie*: een nieuw middel wordt ingezet binnen bestaande structuren en processen, zonder dat de kenmerken van en eisen aan deze structuren en processen fundamenteel veranderen.

Dat betekent allereerst dat de huidige bevoegdhedenstructuren binnen de overheid ongewijzigd blijven en dat e-mail binnen deze bevoegdhedenstructuren moet worden toegepast. Voor de architectuur voor beveiligde e-mail binnen de Rijksoverheid betekent dit een tweetal zaken:

- er moet een onderscheid mogelijk zijn tussen "functionarissen" en "personen";
- er moet een directory komen waarin voor elke functionaris te achterhalen is welke bevoegdheden deze heeft, waarin het certificaat is te vinden dat deze bevoegdheden bevestigt en waarin de geldigheid van dat certificaat gegarandeerd is.

Het onderscheid tussen persoon en functionaris kan gerealiseerd worden in de vorm van handtekeningen: indien een bericht is ondertekend met de handtekening van een functionaris, betreft dit een formeel bericht.

Bij informele communicatie kan het ook wel eens noodzakelijk zijn gebruik te maken van de beveiligde e-mail voorziening, en in feite zou de afzender dan een andere handtekening (een "persoonlijke" handtekening) moeten gebruiken.

Er zou ook gebruik gemaakt kunnen worden van een onderscheid tussen persoonlijke en functionele postbussen: informele berichten worden gestuurd aan de persoonlijke postbus, bijvoorbeeld "gerard.jansen@minbzk.nl". Formele communicatie betreft communicatie waarbij, zoals in hoofdstuk 3. is aangegeven, wel allerlei formele regels gevolgd moeten worden. Dergelijke berichten worden verstuurd naar de functionele postbus: "DGOB@minbzk.nl" (waar dezelfde persoon achter zit als achter het eerder genoemde adres): De vraag is echter in hoeverre dit daadwerkelijk iets toevoegt aan het gebruik van handtekeningen om de afzender als functionaris te kunnen identificeren.

Daarnaast is het, zoals gezegd, van belang dat deze bevoegdhedenstructuur ook traceerbaar en verifieerbaar is. Hier ligt een duidelijke koppeling met de overheidsadressengids waaraan in het kader van het Overheidsintranet gewerkt wordt. Deze overheidsadressengids fungeert in het kader van beveiligde e-mail als de overheidsbrede directory service, waarin voor elke functionaris binnen de Rijksoverheid (en op termijn mogelijk ook daarbuiten) te achterhalen moet zijn:

- wat zijn/haar e-mail adres is;
- wat zijn/haar (functionele dan wel persoonlijke) handtekening is;
- welke bevoegdheden gekoppeld zijn aan dit e-mail adres en deze handtekeningen;
- het certificaat dat deze bevoegdheden bevestigt;
- het certificaat dat de handtekening van deze functionaris verifieert;
- de geldigheid van deze certificaten.

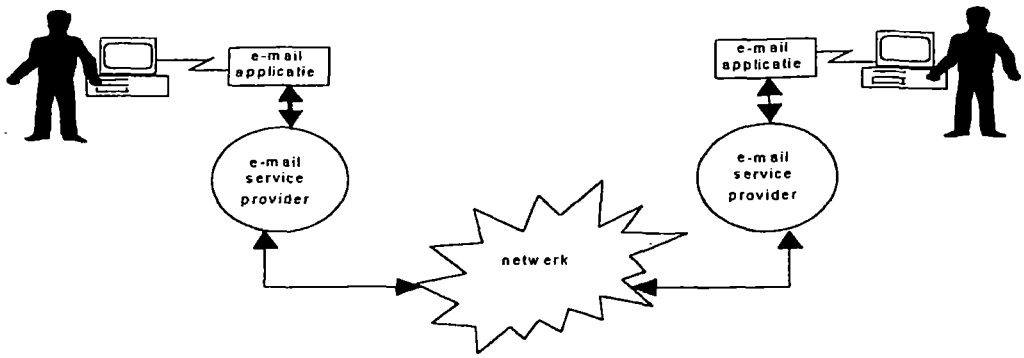
De overheidsadressengids krijgt daarmee een cruciale rol in het bewerkstelligen van betrouwbare elektronische communicatie binnen de overheid.

5.2 End-to-end beveiliging

De term "end-to-end beveiliging" wordt al snel gehanteerd als het om beveiligde e-mail gaat. Een belangrijke vraag is echter wat hier precies onder verstaan wordt en welke elementen van "end-to-end" daadwerkelijk thuishoren in een architectuur voor beveiligde e-mail.

Allereerst is het hier van belang "end-to-end" te onderscheiden van "point-to-point". Point-to-point beveiliging betreft beveiliging van verkeer tussen twee netwerk-aansluitpunten, terwijl het bij end-to-end beveiliging gaat om beveiliging tussen twee desktops - tussen twee gebruikers. Bij point-to-point beveiliging gaat het om beveiliging van netwerk-verkeer, maar dat is in feite niet het niveau waarop beveiligde e-mail zich afspeelt: daadwerkelijke beveiliging van e-mail verkeer vindt plaats op het applicatieniveau. Dit houdt in dat er ook geen sprake hoeft te zijn van een besloten e-mail service en infrastructuur, er kan gebruik gemaakt worden van generieke diensten op dit niveau. Beveiligingsvraagstukken op het niveau van de gebruiker en (de locatie van) diens PC zijn hier wel zeer relevant, maar vallen niet onder de beveiliging van de e-mail dienst zelf. Dit zijn vraagstukken die met name bij implementatie en beheer van deze dienst zeer relevant worden.

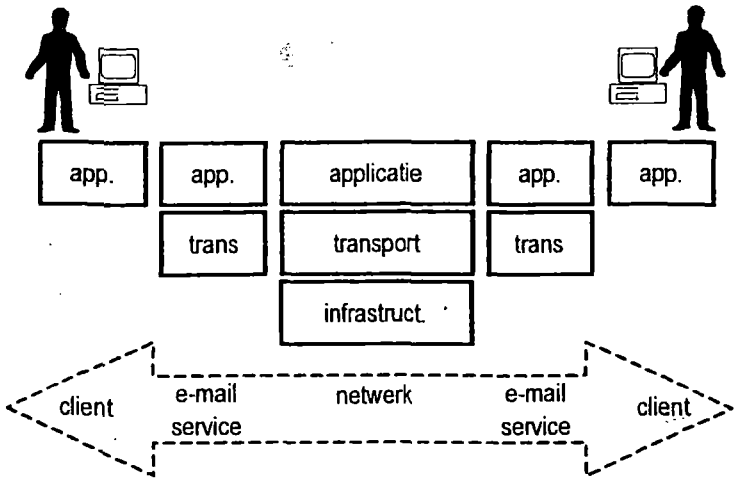
Om hierin meer helderheid te brengen, is het noodzakelijk het proces van e-mail uitwisseling nader te beschouwen. Het volgende model geeft dit proces weer:



Figuur 5.1. Schematische weergave e-mail uitwisseling

Een gebruiker maakt op zijn of haar PC, met behulp van de hierop actieve e-mail applicatie (de client) een bericht aan. Na dit bericht voltooid te hebben, stuurt de gebruiker het bericht naar de server die bij deze client hoort. Deze mailserver zoekt vervolgens connectie met de e-mail service provider (de transport-dienst), die met gebruikmaking van een fysieke netwerk-infrastructuur het bericht transporteert naar de service provider waarbij de beoogde ontvanger van het bericht is aangesloten. Daar komt het bericht dan vervolgens op de mailserver terecht, waar het (of direct, of nadat de ontvanger hiertoe zelf het initiatief heeft genomen) weer bij de client van de ontvanger terechtkomt en gelezen kan worden door de ontvanger.

In feite gaat het hier om verschillende "lagen" in het proces van communicatie:



Figuur 5.2. Lagen in e-mail uitwisseling

Op *applicatieniveau* gaat het om de communicatie tussen de verschillende componenten (clients en servers) van de applicatie. De *transportdienst* is de dienst die de berichten van de

mailbox van de verzender transporteert naar die van de ontvanger. De *infrastructuur* bestaat uit de kabels, routers en dergelijke die het fysieke netwerk vormen.

"End-to-end beveiliging" houdt hier in dat een verzender in de e-mail client een bericht schrijft, dit versleutelt en ondertekent en dat de ontvanger het versleutelde bericht van de verzender, vergezeld van diens elektronische handtekening, compleet en ongewijzigd in zijn of haar e-mail client kan lezen. Zoals eerder gezegd betekent dit dat beveiliging op *applicatieniveau* plaatsvindt: beveiliging heeft de vorm van versleuteling en ondertekening en betreft daarmee de communicatie tussen de beide clients. De transportdienst en de gebruikte netwerkinfrastructuur zijn niet noodzakelijkerwijs afgesloten, hiervoor kunnen algemeen toegankelijke voorzieningen gebruikt worden. Dit houdt in dat geen garanties kunnen worden afgegeven dat berichtenverkeer niet wordt afgetapt, maar het principe van versleuteling is nu juist dat derden de versleutelde berichten niet kunnen lezen. Overigens betekent dit niet dat met de leverancier van de infrastructuur (net als met die van de transportdienst) niet zeer stringente afspraken gemaakt moeten worden over beschikbaarheid en beveiliging.

De keuzes die hier gemaakt kunnen worden, komen voort uit het feit dat de beveiligde e-mail voorziening van de Rijksoverheid interdepartementaal is en op termijn moet kunnen worden uitgebouwd naar communicatie met externe partijen.

5.3 Betrouwbaarheidsniveaus van berichten

Een volgende keuze die in de architectuur gemaakt moet worden, is de keuze ten aanzien van het gewenste betrouwbaarheids- of beveiligingsniveau van berichten. Grosso modo worden de volgende betrouwbaarheidsniveaus onderscheiden (van "hoog" naar "laag"):

- gerubriceerde informatie;
  - staatsgeheim/zeer geheim;
  - staatsgeheim/geheim;
  - staatsgeheim/confidentieel;
- sensitieve informatie;
- openbare informatie.

Een belangrijke keuze die gemaakt moet worden, is of elk van deze niveaus wordt ondersteund door beveiligde e-mail, of dat beveiligde e-mail slechts tot een bepaald niveau mag worden ingezet. Op deze keuze wordt in hoofdstuk 6. nader ingegaan.

Wel dient daarbij rekening gehouden te worden met de volgende zaken:

- het technisch realiseren van meerdere betrouwbaarheids-niveaus heeft nogal wat voeten in de aarde;
- bij meerdere betrouwbaarheidsniveaus;
  - dient de organisatie volledig ingesteld te zijn op het werken met de verschillende betrouwbaarheidsniveaus;
  - dient het personeel zich zeer bewust te zijn van de verschillende betrouwbaarheidsniveaus;
- anderzijds is het zo dat, hoe meer betrouwbaarheidsniveaus ondersteund worden, hoe groter de inzetbaarheid van beveiligde e-mail is.

5.4 Hiërarchisch of wederzijds vertrouwen

Vertrouwen is essentieel voor vertrouwelijke communicatie, en ook in een elektronische communicatie-omgeving geldt dit, zoals in hoofdstuk twee is besproken. Wie iemands publieke sleutel wil gebruiken, of een digitale handtekening wil kunnen vertrouwen, dient een of andere manier te hebben om er zeker van te zijn dat die sleutel of handtekening ook echt van de persoon afkomstig is die zegt de sleutel uitgegeven te hebben. In hoofdstuk 2. is aangegeven dat er verschillende opties zijn om het vertrouwen tussen deelnemers aan een communicatieproces te formaliseren: hiërarchisch vertrouwen en een web van vertrouwen.

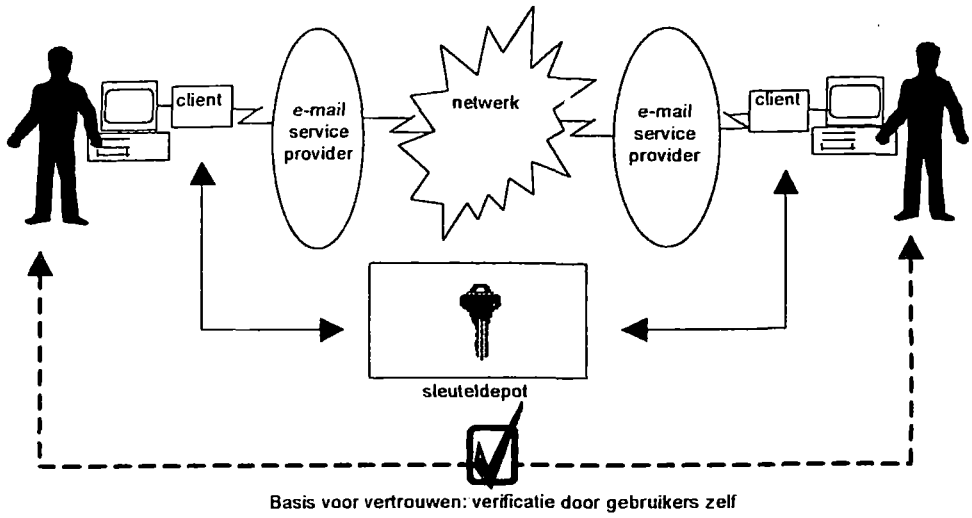
Bij *hiërarchisch vertrouwen* wordt het vertrouwen dat in een digitale handtekening wordt gesteld, ontleend aan een "hogere" autoriteit, een TTP die de handtekening van de persoon in kwestie voorzien heeft van de handtekening van de autoriteit. Deze autoriteit beheert de publieke sleutels van de verschillende partijen en dit houdt in dat deze sleutels ook gelijk geverifieerd zijn: de "trusted third party" is, zoals de naam al zegt, een vertrouwde partij en sleutels die hier worden opgeslagen en kunnen worden opgehaald zijn via een betrouwbare verificatieprocedure daar terechtgekomen.

Bij het *"web van vertrouwen"* wordt het vertrouwen in iemands digitale identiteit gerealiseerd door het tekenen van elkaars publieke sleutel. Op die manier ontstaat een web van vertrouwen, omdat gebruiker X bijvoorbeeld de sleutel van gebruiker Y op zich niet vertrouwt, maar weer wel als deze door gebruiker Z gesigneerd is. Gebruiker Z heeft ook X's sleutel getekend en X weet dat Z alleen iemands sleutel tekent als er Z er zeker van is dat die persoon ook degene is waarvoor hij zich uitgeeft. Bij dit web van vertrouwen kan de publieke sleutel op verschillende manieren verkregen worden:

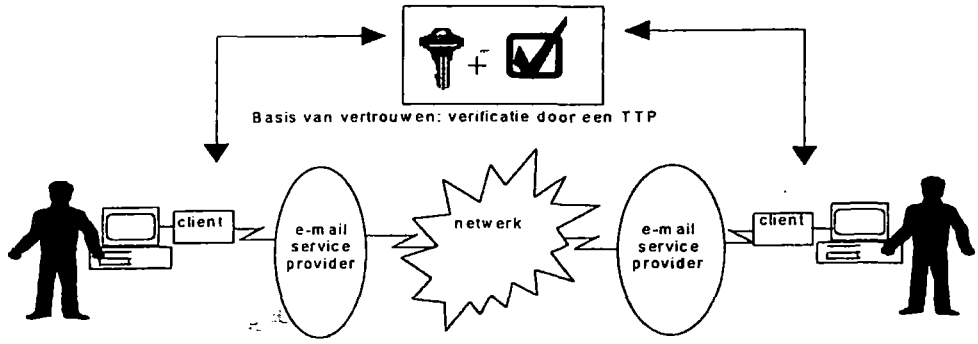
- Y stuurt X zijn of haar sleutel toe;
- X haalt de sleutel van Y op bij een "sleuteldepot", een server waarop iedereen zijn of haar publieke sleutel kan laten registreren.

In beide gevallen is er nog een aparte verificatieslag noodzakelijk: het "sleuteldepot" is niet omgeven met de betrouwbare verificatieprocedure die een TTP wel kent - in principe kan iedereen daar een publieke sleutel op laten slaan, zonder dat gecontroleerd wordt of deze sleutel daadwerkelijk van deze persoon is. Dat betekent dat via een ander communicatiekanaal (telefoon, fax, brief of een face-to-face ontmoeting) gecontroleerd moet worden of de sleutel die X ontvangen heeft wel echt de sleutel van Y is, of deze sleutel niet verlopen is, et cetera.

Onderstaande figuur geeft dit grafisch weer:



Figuur 5.3a. Verkrijging en verificatie van sleutels: wederzijds vertrouwen



Figuur 5.3b Verkrijging en verificatie van sleutels: hiërarchisch vertrouwen

Een belangrijke keuze die in de architectuur gemaakt moet worden is, zo mag uit het bovenstaande blijken, de keuze voor de vertrouwensstructuur. Op deze keuze en de consequenties ervan op zowel bestuurlijk, organisatorisch als technisch niveau, wordt in hoofdstuk 6. nader ingegaan.

5.5 Sleutelbeheer

Ten aanzien van sleutels is er een belangrijk onderscheid tussen handtekening (authenticatie, navolgbaarheid/onweerlegbaarheid, integriteit) en encryptie (exclusiviteit). Het is gebruikelijk dat voor het zetten van digitale handtekeningen (signing) een ander sleutelpaar gebruikt wordt dan voor het versleutelen van berichten. De reden hiervoor is dat een geheime sleutel voor ondertekening van berichten nooit gedeponeerd wordt. Dat is ook niet nodig, omdat van de inhoud altijd kennis genomen kan worden, hetzij doordat de boodschap nog leesbaar is (clear-signing), hetzij doordat de boodschap door middel van het publieke deel van het sleutelpaar ontcijferd kan worden (signing gebeurt met het geheime deel van een sleutelpaar). Het tekenen echter dient op geen enkele andere manier te kunnen gebeuren dan door de eigenaar.

Er moeten keuzes gemaakt worden ten aanzien van de uitgifte en het beheer van deze sleutels. Een eerste element hierbij is het bieden van de mogelijkheid iemands publieke sleutel op te halen teneinde hem versleutelde berichten te kunnen sturen. Vervolgens zijn twee elementen van belang ten aanzien van verificatie:

- het is van belang na te kunnen gaan of iemands sleutel nog wel geldig dan wel verlopen is;
- zeker zo belangrijk is het om na te kunnen gaan of iemand zijn sleutel heeft teruggetrokken.

Bij deze laatste twee elementen is weer een cruciale rol weggelegd voor de overheidsadressengids: daarin kunnen deze feiten worden nagegaan.

Daarbij is het, zoals gezegd, van belang gescheiden sleutels voor encryptie en handtekening te hanteren. Hierbij zijn twee elementen van belang: de mogelijkheid sleutels af te geven voor uitsluitend digitale handtekening en de mogelijkheid sleutels af te geven uitsluitend voor versleuteling. Op bestuurlijke, organisatorische en technische aspecten van sleutel-uitgifte en -beheer wordt in hoofdstuk 6. nader ingegaan.

5.6 Conclusie

De conclusie is dat architectuur voor beveiligde e-mail binnen de Rijksoverheid de volgende keuzes omvat:

- de bestaande bevoegdhedenstructuur dient als uitgangspunt en dient te worden vertaald naar een elektronische omgeving;
  - beveiligde e-mail betreft primair de uitwisseling tussen functionarissen;
  - de bevoegdheden van de betreffende functionarissen worden vastgelegd en gegarandeerd in een overheidsbrede adressengids;
- er is sprake van end-to-end-beveiliging, beveiliging van berichten die plaatsvindt op applicatieniveau;
- er moet een keuze worden gemaakt ten aanzien van de ondersteunde betrouwbaarheidsniveaus: dient beveiligde e-mail ingezet te kunnen worden voor alle betrouwbaarheidsniveaus (tot staatsgeheim aan toe), of dient dat beperkt te worden?
- er dient een keuze gemaakt te worden voor een bepaalde vertrouwensstructuur: een structuur met TTP-diensten, of een structuur met een web van vertrouwen;

- er dient een keuze gemaakt te worden ten aanzien van de uitgifte en het beheer van sleutels.

Hiermee zijn de keuzes die op centraal niveau moeten worden gemaakt ten aanzien van de invoering van beveiligde e-mail in de Rijksoverheid, geëxpliciteerd. Een tweetal keuzes is in dit hoofdstuk al gemaakt: de bestaande bevoegdhedenstructuur dient als uitgangspunt, en beveiliging vindt plaats op end-to-end niveau. De verdere keuzes ten aanzien van de inrichting van de beveiligde e-mail voorziening blijven hier echter vooralsnog open en worden in hoofdstuk 6. nader besproken. In hoofdstuk 6. wordt duidelijk wat, naar aanleiding van deze gezamenlijke keuzes, de belangrijkste bestuurlijke, organisatorische en technische keuzes zijn die gemaakt moeten worden bij de feitelijke invoering van beveiligde e-mail.

6. Bestuurlijke, organisatorische en technische keuzes

Op basis van de algemene uitgangspunten ten aanzien van beveiligde e-mail binnen de Rijksoverheid die in de vorige hoofdstukken zijn beschreven, kunnen de keuzes geëxpliciteerd worden die bij de invoering van beveiligde e-mail gemaakt kunnen worden. In dit hoofdstuk wordt de volgende vraag beantwoord:

> *Welke keuzemogelijkheden zijn er ten aanzien van bestuurlijke, organisatorische en technische aspecten van de invoering van beveiligde e-mail binnen de Rijksoverheid?*

Daarmee geeft dit hoofdstuk, voortbouwend op wat in hoofdstuk 5. hierover is gezegd, de fundamentele keuzes aan die gemaakt moeten worden, zowel interdepartementaal als departementaal, bij de invoering van beveiligde e-mail.

6.1 Bestuurlijke keuzes

De keuzes die op bestuurlijk niveau gemaakt moeten worden bij de invoering van beveiligde e-mail hebben te maken met de reikwijdte van de implementatie en met de organisatie van een aantal essentiële elementen van de architectuur die in het vorige hoofdstuk beschreven is.

6.1.1 Iedereen of bepaalde groepen?

Een eerste bestuurlijke keuze die gemaakt moet worden, betreft de reikwijdte van de invoering van beveiligde e-mail. Is het uitgangspunt dat iedereen over deze voorziening moet beschikken, of wordt per proces bekeken in hoeverre beveiligde e-mail van toegevoegde waarde is? In het laatste geval zou de voorziening dan alleen beschikbaar worden gesteld aan die functionarissen die betrokken zijn bij processen waarvan besloten is dat beveiligde e-mail daarin ingezet moet worden.

Er is natuurlijk ook een groeimodel mogelijk: beveiligde e-mail wordt allereerst dáár ingezet waar het een duidelijke meerwaarde in het proces heeft, en via die concrete inzet in processen groeit de voorziening (via een zogenaamde "olievlekwerking") geleidelijk uit tot een algemene voorziening.

Deze keuze heeft belangrijke consequenties voor:
- de kosten (het aantal clients dat moet worden gekocht en beheerd, het aantal gebruikers dat moet worden opgeleid);
- de organisatie van het beheer van de voorziening;
- de organisatie van gebruikersopleidingen;
- de hoeveelheid sleutels die aangemaakt en beheerd moet worden;
- de gekozen vertrouwensstructuur.

6.1.2 TTP of 1-op-1?

In de hoofdstukken 2 en 5 is besproken dat het vertrouwen tussen communicatiepartners op verschillende manieren geformaliseerd kan worden: enerzijds door gebruik te maken van TTP-diensten, anderzijds door het creëren van een web van vertrouwen. De keuze voor een vertrouwensstructuur is een belangrijke bestuurlijke afweging, die deels bepalend is voor de architectuur van beveiligde e-mail binnen de Rijksoverheid. Een keuze voor een TTP-structuur betekent dat er een duidelijke organisatorische structuur moet zijn voor het inbedden van de TTP-diensten, terwijl een keuze voor een web van vertrouwen betekent dat structuren gevonden moeten worden voor sleutelbeheer en -depots.

Deze keuze heeft ook wel een relatie met de vorige bestuurlijke keuze: bij een massale invoering van beveiligde e-mail wordt de situatie in het geval van een web van vertrouwen al gauw moeilijk beheersbaar in verband met het aantal sleutels, terwijl bij een kleinschalige invoering een TTP-structuur wellicht een wat zwaar middel is. Ook hier is een groeiscenario denkbaar: waar begonnen wordt met kleinschalige, procesgerelateerde invoering, kan een web van vertrouwen een afdoende manier zijn van het formaliseren van vertrouwen. Als dit relatief kleinschalige gebruik na verloop van tijd grootschaliger wordt, is op een bepaald moment in dit proces de overgang naar een structuur met TTP-diensten wenselijk.

Keuzes ten aanzien van de vertrouwensstructuur hebben belangrijke consequenties voor:

- de kosten: de kosten die samenhangen met de organisatie van TTP-diensten zijn in eerste instantie hoger, maar de beheerskosten kunnen bij een web van vertrouwen sterk toenemen als het aantal sleutels zeer groot wordt;
- het aantal te beheren sleutels, en dus de organisatie hiervan en de beheersinspanning die hiermee samenhangt;
- de mate waarin communicatie met de buitenwereld binnen deze structuur past.

6.1.3 Individueel of centraal sleutels genereren?

Een volgende bestuurlijke keuze die gemaakt moet worden, is de keuze voor de systematiek volgens welke sleutels worden aangemaakt. Kiest men voor een laagdrempelige systematiek van individuele sleutelgeneratie, of voor een systematiek waarin het genereren van sleutels een centraal belegde functie is? "Centraal" betekent hier weer niet per definitie dat er één instantie in het leven geroepen wordt die deze functie voor alle organisatie-onderdelen vervult, wel dat deze functie niet meer bij de gebruiker zelf komt te liggen. Het niveau waarop de functie dan wel geplaatst wordt (afdeling, departement, Rijksoverheid, vertrouwensdomein, et cetera) is dan verder een keuze die nog gemaakt moet worden. Het individueel genereren van sleutels is een systematiek die bijvoorbeeld in PGP wordt toegepast: elke gebruiker maakt zijn eigen sleutel en wachtwoord aan.

Ook deze keuze heeft weer een mogelijke relatie met de reikwijdte van de implementatie: bij een procesgerelateerde, redelijk kleinschalige invoering van beveiligde e-mail, kan het individueel genereren van sleutels (gezien de snelheid en laagdrempeligheid) de beste manier zijn, terwijl bij een massale invoering (gezien de beheersbaarheid en controle op de elektronische bevoegdhedenstructuur) het centraal genereren de voorkeur zal genieten. Opnieuw is er een groeiscenario denkbaar, waarin gaandeweg de uitbreiding van de toepassing van beveiligde e-mail wordt overgestapt van individueel gegenereerde sleutels naar een centraal belegde generatie-functie.

Keuzes ten aanzien van het genereren van sleutels hebben gevolgen voor:
- de laagdrempeligheid van het gebruik van de voorziening: de drempel voor het gebruik van de voorziening ligt lager als gebruikers zelf, op hun eigen desktop, sleutels kunnen aanmaken;
- de beheersbaarheid en controle: sleutels zijn essentieel voor het realiseren van beveiligde e-mail, en centrale sleutel-uitgifte geeft de organisatie een mechanisme om controle te houden over de bevoegdheden die worden toegekend, over het intrekken van sleutels, et cetera.

6.1.4 Verschillende betrouwbaarheidsniveaus?
Naast de vertrouwensstructuur en het sleutelbeheer is een derde belangrijk element van de architectuur die in hoofdstuk 5. is besproken, het element van de betrouwbaarheidsniveaus. Er worden verschillende betrouwbaarheidsniveaus van informatie onderscheiden en de vraag is of beveiligde e-mail in staat moet zijn elk van deze niveaus te ondersteunen. Oftewel, moet zowel sensitieve als staatsgeheime informatie via beveiligde e-mail kunnen worden verstuurd? Of wordt gekozen voor een "maximum" (bijvoorbeeld: wel sensitieve, maar geen gerubriceerde informatie)? Hierbij is van belang dat beveiligde e-mail is gedefinieerd als "end-to-end" beveiliging, oftewel, een beveiliging op applicatie-niveau.

In eerste instantie is het betrouwbaarheidsniveau afhankelijk van het proces waarin beveiligde e-mail wordt ingezet, maar andersom geredeneerd is de inzetbaarheid van beveiligde e-mail binnen een bepaald proces ook weer afhankelijk van het benodigde betrouwbaarheidsniveau. Hier moet dus een duidelijke keuze gemaakt worden, waarbij opnieuw een soort groeiscenario mogelijk is. Voor dit laatste zou dan gebruik gemaakt kunnen worden van de uitgangspunten van het "Multi Level Secure" principe dat bij het Ministerie van Defensie gehanteerd wordt: beveiligingsmechanismen moeten zich in principe zodanig kunnen ontwikkelen dat ze elk betrouwbaarheidsniveau aankunnen.

Keuzes ten aanzien van de betrouwbaarheidsniveaus hebben consequenties voor:
- de implementatie van de software: moet de gebruiker de mogelijkheid geboden worden zelf een betrouwbaarheidsniveau te kiezen, hoe wordt dit geïmplementeerd, et cetera?
- de inzetbaarheid van beveiligde e-mail: als er restricties zijn ten aanzien van de ondersteunde betrouwbaarheidsniveaus, betekent dit ook dat beveiligde e-mail in bepaalde processen niet ingezet zal kunnen worden.

6.2 Organisatorische keuzes

De organisatorische keuzes hangen samen met de bestuurlijke keuzes. Zo zal als gekozen wordt voor invoering voor iedereen de organisatie van de invoering anders verlopen dan wanneer alleen de deelnemers aan een beperkt aantal processen voorzien worden van beveiligde e-mail. De bestuurlijke keuzes hebben organisatorische gevolgen.

6.2.1 Software-installatie en versiebeheer

Als de bestuurlijke keuze voor de reikwijdte van de invoering is gemaakt (iedereen of bepaalde groepen) zal afhankelijk van die reikwijdte software en versiebeheer uiteenlopen van een grote tot een kleine operatie. De software-installatie zal daarbij onderverdeeld worden in client en servers, waarbij de client voorafgegaan wordt door de servers.
Deze upgrade van de e-mail infrastructuur op een departement kan noodzakelijk zijn omdat bijvoorbeeld de aanwezige softwareversie van de e-mail server niet overweg kan met certificaten. Maar ook een gebrekkige client kan uiteindelijk leiden tot een upgrade van het volledige e-mail systeem, omdat bijvoorbeeld een nieuwe client leidt tot de vervanging van de servers en de daarop aanwezige software. Soms kan ook uitsluitend de e-mail client vervangen worden als deze niet van de juiste aanvullende software ten behoeve van beveiligingsfuncties voorzien kan worden.

Zoals met andere gebruikersapplicaties gebeurt, zal ook bij het gebruik van beveiligde e-mail versie-beheer en ondersteuning een rol spelen.

Hoe groot de omvang van de operatie voor software-installatie is hangt derhalve af van de mate waarin beveiligde e-mail gebruikt gaat worden en van de mate waarin vernieuwingen in de infrastructuur noodzakelijk zijn. Voor versiebeheer en ondersteuning lijkt de meest voor de hand liggende keuze dit te integreren in reeds bestaande organisatorische eenheiden binnen departementen.

6.2.2 Opleiding van gebruikers en beheerders

Een belangrijk en vaak onderschat onderdeel van de invoering van een nieuwe ICT-voorziening is de opleiding van gebruikers en beheerders. Met name daar waar het gaat om het potentieel grootschalig gebruik van beveiligingfuncties en derhalve ook het foutieve gebruik ervan, is het van groot belang gebruikers te doordringen van de mogelijkheden en onmogelijkheden. Daarbij speelt de vraag *hoe* de voorziening gebruikt moet worden, maar waarschijnlijk in nog belangrijker mate de vraag *wanneer* de voorziening gebruikt moet worden.

Het hoeft geen betoog dat beheerders een grondiger en meer diepgaande opleiding behoeven dan gebruikers, teneinde de gewenste ondersteunende functies te kunnen vervullen.

Voor de invulling van de opleiding zal gekozen kunnen worden tussen uitbesteden of zelf doen. Daarnaast is het van belang dat nadat de opleiding van iedere betrokkene afgerond is, dit opleidingsonderdeel standaardvoorziening wordt bij de introductie van nieuw personeel.

6.2.3 Sleutelbeheer

In paragraaf 5.5 is al gewezen op het belang van sleutelbeheer voor het gebruik van beveiligde e-mail. Daarnaast verschijnt parallel aan dit rapport de studie "Vertrouwen in Communiceren" waarin op de problematiek van sleutelbeheer wordt ingegaan.

Wat georganiseerd moet worden is dat eenieder de publieke sleutels van een communicatiepartner bij de Rijksoverheid moet kunnen opzoeken. De ideale plaats daarvoor is een directory service, maar als deze (nog) afwezig is bestaat de mogelijkheid

hiervoor een eigen directory in te richten; een enkel software product biedt deze functie al op basis van de aanwezige directory die onderdeel van het betreffende e-mail pakket is.

De gemaakte keuze voor TTP of 1-op-1 vertrouwen beïnvloedt de inrichting van het sleutelbeheer nauwelijks, in beide gevallen is een instantie noodzakelijk die publieke sleutels beschikbaar maakt.

6.2.4 Aanmaak en distributie van sleutels

De schaal waarop de aanmaak en distributie van sleutels zal plaatsvinden wordt sterk beïnvloed door de keuze voor "iedereen of bepaalde groepen" en vanzelfsprekend door de keuze "centraal of individueel sleutels genereren".
Omdat sleutels voor integriteitsfuncties en sleutels voor vertrouwensfuncties verschillend dienen te zijn, zullen voor iedere deelnemer minstens twee sleutels aangemaakt moeten worden.

Als een departement besluit dat geen versleutelde berichten de organisatie mogen verlaten zonder dat zonodig daartoe bevoegde personen het bericht kunnen lezen, zal gezocht moeten worden naar software die daaraan voldoet. Als een departement besluit dat geen versleutelde berichten de organisatie mogen binnenkomen zonder dat zonodig daartoe bevoegde personen het bericht kunnen lezen, zal van elke medewerker de geheime encryptiesleutel toegankelijk moeten zijn voor de genoemde bevoegde personen.

6.3 Technische keuzes

De keuzes op zowel bestuurlijk als organisatorisch niveau hebben weer consequenties voor de keuzes die gemaakt worden op het niveau van de technische implementatie van beveiligde e-mail. Het betreft hier keuzes ten aanzien van zowel werkpleksoftware als centrale voorzieningen voor sleutelbeheer en -uitgifte.

6.3.1 clients

De e-mail client waarmee gewerkt wordt moet voldoen aan een aantal eisen; daarnaast zijn er wensen. Voor een uitgebreide opsomming wordt verwezen naar Bijlage II, *Inventarisatie Marktproducten*.

Een belangrijke eis ten aanzien van clients heeft te maken met het op correcte wijze kunnen omgaan met de gekozen vertrouwensfunctie (hiërarchisch danwel 1-op-1), een client dient bij voorkeur met beide mogelijkheden om te kunnen gaan, om een zo breed mogelijke communicatie binnen de Rijksoverheid, maar ook daarbuiten te kunnen bewerkstelligen. Het is namelijk een illusie te veronderstellen dat een keuze van de Rijksoverheid voor één van de twee mogelijkheden zou betekenen dat de communicerende partijen buiten de Rijksoverheid, die soms al beschikken over dergelijke voorzieningen, zich aan deze keuze zullen conformeren. Certificatie van de gebruikte versleutelings- en digitale handtekening-technieken in clients is van groot belang. Vastgesteld dient te worden wie de certificerende autoriteit voor deze technieken is, om op zodanige wijze de integriteit en de vertrouwelijkheid van de communicatie te waarborgen.

6.3.2 sleutelbeheer

De wijze waarop het sleutelbeheer ingericht wordt, hangt af van een aantal keuzes:

- wordt een key recovery service ingericht (mogelijkheid voor gebruiker zijn sleutel te herstellen nadat deze verloren is gegaan);
- wordt een key escrow service ingericht (sleutels toegankelijk voor daartoe bevoegde personen).

Als deze functies aanwezig zijn, is sleutelbeheer gecompliceerder omdat er meer stringente beveiligingseisen gesteld worden.

6.3.3 sleuteldistributie

Bij de sleuteldistributie zal veelal gebruik worden gemaakt van standaard aanwezige voorzieningen in de aanwezige e-mail omgeving. Zo kan bij de keuze voor hiërarchisch vertrouwen in een Microsoft omgeving gebruik gemaakt worden van de Microsoft-certificate server, maar gebruikmaking van andere services is evenzeer mogelijk. Belangrijk is dat de certificate server certificaten levert die voldoen aan de vigerende specificaties, zodat communicatie met andere partijen gegarandeerd is.

Als van een 1-op-1 vertrouwensmechanisme gebruik wordt gemaakt, zal de sleuteldistributie, bij centrale verschaffing van sleutels, geheel in eigen beheer opgezet moeten worden afhankelijk van de inrichting. Als bijvoorbeeld encryptiesleutels gegenereerd worden die automatisch de "firma-sleutel" meenemen bij elke encryptie (het doel hiervan is dat geen onleesbare boodschappen uitgestuurd worden) kunnen de sleutels alleen maar centraal uitgegeven worden.

Distributie van de publieke sleutels zal bij voorkeur plaatsvinden in een directory, waarin van alle gebruikers de publieke sleutel is opgeslagen. Aan de integriteit en de beschikbaarheid van een dergelijke directory worden hoge eisen gesteld.

6.4 Invoeringsscenario's

In de voorgaande paragrafen zijn de opties gepresenteerd ten aanzien van de bestuurlijke, organisatorische en technische aspecten van de invoering van beveiligde e-mail binnen de Rijksoverheid. In deze afsluitende paragraaf worden deze opties vertaald naar een aantal mogelijke scenario's voor deze invoering.

6.4.1 Low profile, high profile

Hierbij dienen de bestuurlijke keuzes als uitgangspunt, de organisatorische en technische keuzes liggen weer in het verlengde hiervan. In paragraaf 6.1 zijn ten aanzien van deze bestuurlijke keuzes de volgende dimensies onderscheiden:

Tabel 6.1. Bestuurlijke dimensies invoering beveiligde e-mail

	decentrale keuzes	**centrale keuzes**
reikwijdte invoering	proces-gerelateerd	algemene voorziening
vertrouwensstructuur	web van vertrouwen	TTP
sleutel-generatie	invididueel	Centraal (door de organisatie)
betrouwbaarheidsniveaus	één betrouwbaarheidsniveau	alle betrouwbaarheidsniveaus

In deze tabel is een onderscheid aangebracht tussen decentrale keuzes en centrale keuzes. De eerste betreffen een "low profile"-variant, waarin gekozen wordt voor een invoering

van beveiligde e-mail waarvoor op centraal niveau weinig geregeld hoeft te worden en waarbij de belangrijkste keuzes dus op decentraal niveau genomen kunnen worden.

Deze "low-profile"-variant heeft als kenmerken:

- de inzet van beveiligde e-mail is gerelateerd aan een concreet proces. De voorziening wordt alleen beschikbaar gesteld aan de deelnemers aan dit proces, er is geen sprake van een algemene infrastructurele voorziening. Besluiten rond de inzet van beveiligde e-mail worden dan gemaakt door diegenen die verantwoordelijk zijn voor dit proces;
- er wordt gebruik gemaakt van een "web van vertrouwen", van 1-op-1 verificatie van sleutels en handtekeningen. Er hoeft geen centrale voorziening (TTP) gebruikt te worden die het vertrouwen formaliseert, dus ook hier gaat het om een decentraal te nemen besluit;
- sleutels worden individueel aangemaakt: iedere deelnemer aan het proces maakt zijn eigen sleutel aan en plaatst deze op een server. Ook hier is dus geen centrale sleutel-uitgifte autoriteit of iets dergelijks nodig, ook hier gaat het om een keuze op decentraal niveau;
- er gelden duidelijke beperkingen ten aanzien van het betrouwbaarheidsniveau waarvoor beveiligde e-mail kan worden ingezet, bijvoorbeeld, wel sensitief, niet gerubriceerd. Deze keuze is natuurlijk ook weer afhankelijk van het concrete proces, maar anderzijds is de keuze voor een bepaald proces ook weer afhankelijk van keuzes die gemaakt worden ten aanzien van het ondersteunde betrouwbaarheidsniveau. In ieder geval gaat het ook hier om een decentraal te maken keuze: de verantwoordelijken voor het proces besluiten over deze betrouwbaarheidsniveaus.

De rechterkolom van tabel 6.1 bevat de keuzes die centraal gemaakt moeten worden: de "high profile" variant van het invoeringsscenario. Deze variant heeft als kenmerken:

- beveiligde e-mail wordt neergezet als infrastructurele voorziening van algemene aard. Voor iedere medewerker van de Rijksoverheid komt de voorziening in principe beschikbaar. Dit houdt in dat op interdepartementaal niveau besloten wordt tot grootschalige invoering. Ook wordt op dit niveau besloten hoe deze infrastructurele voorziening ingericht en ingevoerd gaat worden;
- er wordt gebruik gemaakt van een stelsel van "hiërarchisch vertrouwen", van TTP-diensten. Er dient dan ook een centrale voorziening (TTP) gebruikt te worden die het vertrouwen formaliseert en besluiten omtrent de inrichting en organisatie van deze TTP-diensten dienen op centraal niveau genomen te worden. In het rapport "Vertrouwen in Communiceren" wordt dit proces in detail uitgewerkt;
- sleutels worden centraal aangemaakt: er is een "centrale" autoriteit die hiervoor verantwoordelijk is (met alle nuances die eerder ten aanzien van de term "centraal" gemaakt zijn). Deze heeft een sterke relatie met de TTP - het ligt voor de hand de sleutel-distributie onder te brengen bij deze TTP. In ieder geval moeten ook hier een aantal keuzes op centraal niveau gemaakt worden;
- beveiligde e-mail moet voor alle betrouwbaarheidsniveaus kunnen worden ingezet. De infrastructurele voorziening wordt in dit scenario beschouwd als volwaardige vervanging voor het papieren traject, en dus dient de inzetbaarheid van deze voorziening maximaal te zijn. Dit houdt in dat op centraal niveau keuzes gemaakt moeten worden ten aanzien van de garanties die beveiligde e-mail biedt met

betrekking tot deze niveaus, de wijze waarop deze technisch gerealiseerd worden, de wijze waarop organisatie en gebruikers bewust gemaakt worden van het werken met verschillende betrouwbaarheidsniveaus et cetera.

6.4.2 De weg naar gezamenlijkheid

Gezien de complexiteit van de materie en de uiteenlopende situaties binnen de verschillende onderdelen van de Rijksoverheid, is het niet zinnig een harde keuze te maken tussen de twee hiervoor beschreven scenario's. Wel is het zinvol om op centraal niveau een gezamenlijk "eindplaatje" in zicht houden, waarbij sprake zal zijn van:

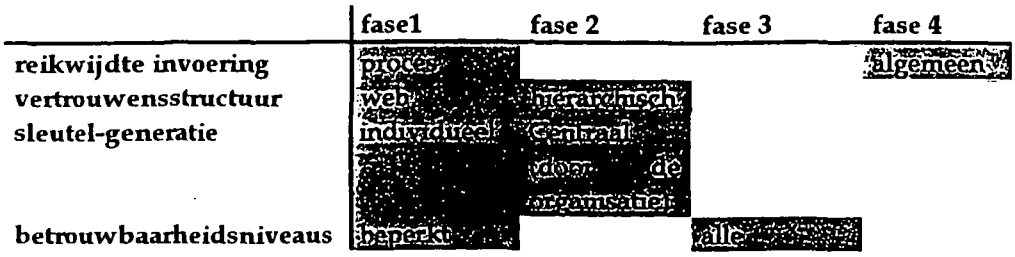
- grootschalige implementatie (als beveiligde e-mail inderdaad papier gaat vervangen, betekent dit dat het een breed geïmplementeerde voorziening moet worden);
- een hiërarchische vertrouwensstructuur: een TTP (een web van vertrouwen wordt bij die omvang onbeheersbaar) en centraal gegenereerde, gedistribueerde en beheerde sleutels (om beheer en controle over een dergelijke grootschalige voorziening optimaal te houden);
- verschillende betrouwbaarheidsniveaus (opnieuw, als beveiligde e-mail een reële vervanging van papier wordt, moeten niet alleen de laagste betrouwbaarheidsniveaus ondersteund worden).

Daarbij gelden verschillende prioriteiten ten aanzien van elk van de onderscheiden dimensies:

- hoewel gestreefd dient te worden naar een grootschalige implementatie, zal de inzet van beveiligde e-mail altijd gerelateerd moeten zijn aan concrete processen. De invalshoek zal dan ook primair die van proces-gerelateerde implementatie zijn, waarbij deze implementatie echter wel telkens het gezamenlijke eindplaatje als doel moet hebben. Grootschalige implementatie is duidelijk een groeitraject: naarmate beveiligde e-mail in meer processen wordt toegepast, ontstaat geleidelijk een steeds grootschaliger inzet van de voorziening;
- hoewel binnen zo'n proces gestart kan worden met een structuur waarin vertrouwen geformaliseerd wordt in een web van vertrouwen, en sleutels individueel worden aangemaakt, dient de doelstelling van een meer hiërarchische structuur (zowel TTP als centrale sleutel-distributie) hoge prioriteit te hebben. Als de "low profile" situatie lang voortduurt, kan een situatie ontstaan (met een grote hoeveelheid sleutels, die op vele verschillende plaatsen zijn uitgegeven en beheerd) waarin de overgang naar een meer centrale situatie een erg moeizame is. Aangeraden wordt dan ook, er naar te streven de overgang naar TTP en centrale sleutel-distributie hoge prioriteit te geven in het proces;
- ten aanzien van de betrouwbaarheidsniveaus geldt weer een soortgelijk groeimodel als voor de grootschalige implementatie. Op het gezamenlijk niveau moeten wel duidelijke kaders en voorwaarden gesteld worden waarbinnen beveiligde e-mail voor bepaalde betrouwbaarheidsniveaus gebruikt kan worden, maar het feitelijke traject naar deze situatie toe kan geleidelijk zijn. Oftewel, de inzet van beveiligde e-mail kan in eerste instantie beperkt blijven tot duidelijk afgebakende betrouwbaarheidsniveaus, met een zeer geleidelijke groei naar een inzetbaarheid voor andere niveaus. Voor een dergelijk traject kunnen de "Multi Level Secure"-uitgangspunten zoals die binnen Defensie gebruikt worden, als basis dienen.

Als we deze prioritering grafisch weergeven, ontstaat een plaatje als het onderstaande:

Tabel 6.2. Prioritering van dimensies



Oftewel, de eerste stap in de richting van het gezamenlijk eindplaatje wordt gezet door middel van een TTP en centrale sleuteldistributie[3]. Vervolgens wordt toe gegroeid naar een situatie waarin beveiligde e-mail voor alle betrouwbaarheidsniveaus kan worden ingezet, en via deze grootschalige inzetbaarheid uiteindelijk naar een situatie (via de inzet in steeds meer processen) waarin beveiligde e-mail een algemene infrastructurele voorziening voor de Rijksoverheid is.

Een dergelijk traject houdt in dat afstemming tussen het centrale niveau en het decentrale niveau essentieel is, dat een balans tussen wat top-down resp. bottom-up plaatsvindt gevonden moet worden. Hierover is in paragraaf 4.5 gesteld dat:

- de gezamenlijke kaders (de architectuur, het gezamenlijk eindplaatje) op SG-niveau zouden moeten worden vastgesteld en bewaakt (de strategische sturing);
- de decentrale invoeringstrajecten door een coördinatie- en expertisecentrum zodanig gecoached, gefaciliteerd en gecoördineerd zouden moeten worden dat ze elk deze gezamenlijke kaders als einddoel hanteren (de tactische sturing).

6.5 Samenvatting en conclusie

Op basis van het bovenstaande is de conclusie dat op bestuurlijk niveau de belangrijkste keuzes voorliggen ten aanzien van:

- de reikwijdte van de implementatie;
- de vertrouwensstructuur;
- het genereren en distribueren van sleutels;
- de betrouwbaarheidsniveaus waarvoor beveiligde e-mail ingezet moet kunnen worden.

Op organisatorisch niveau liggen belangrijke keuzes voor ten aanzien van:

- installatie en beheer van software;

[3] Met het in het leven roepen van een TTP-voorziening zijn de nodige inspanningen (en daarmee samenhangende kosten) gemoeid. In het rapport "Vertrouwen in Communiceren" wordt een eerste orde schatting gegeven van de omvang van deze inspanningen en kosten.

- opleiding van gebruikers;
- sleutelbeheer;
- organisatie van de aanmaak en distributie van sleutels.

Technisch, tenslotte, betreffen de keuzes de volgende onderwerpen:
- client software;
- voorzieningen voor sleutelbeheer,
- voorzieningen voor sleutel-distributie.

Hierbij dienen de bestuurlijke keuzes als vertrekpunt: de organisatorische en technische keuzes liggen veelal in het verlengde hiervan. Deze bestuurlijke keuzes leiden tot een tweetal "extreme" invoeringsscenario's:
- een "low profile"-scenario waarin de nadruk ligt op decentraal te maken keuzes, en waarin op centraal niveau zeer weinig geregeld hoeft te worden;
  - invoering van beveiligde e-mail per proces;
  - vertrouwen formaliseren door middel van een web van vertrouwen;
  - sleutels genereren gebeurt door gebruikers zelf;
- er is een duidelijke beperking ten aanzien van het betrouwbaarheidsniveau waarvoor beveiligde e-mail inzetbaar is;
- een "high profile"-scenario waarin de nadruk ligt centraal te maken keuzes, en waarin dus een aantal belangrijke voorzieningen op centraal niveau dient te worden getroffen;
- beveiligde e-mail wordt grootschalig, als algemene infrastructurele voorziening, geïmplementeerd;
- vertrouwen wordt geformaliseerd door middel van TTP-diensten;
- sleutels worden centraal gegenereerd en gedistribueerd;
- beveiligde e-mail dient inzetbaar te zijn voor alle binnen de Rijksoverheid onderscheiden betrouwbaarheidsniveaus.

Omdat er een grote diversiteit is in de stand van zaken ten aanzien van beveiligde e-mail binnen elk van de onderdelen van de Rijksoverheid, en omdat beide scenario's een aantal voor- en nadelen hebben, wordt niet aanbevolen een harde keuze voor één van beide "extreme" scenario's te maken. Wel wordt aanbevolen op centraal niveau een gezamenlijk "eindplaatje" te definiëren, door middel van het uitwerken van de architectuur die in het vorige hoofdstuk is beschreven.

De weg naar dit eindplaatje kent een aantal prioriteiten:
- hoewel begonnen kan worden met een structuur waarin vertrouwen geformaliseerd wordt in een web van vertrouwen, en sleutels individueel worden aangemaakt, dient de doelstelling van een meer hiërarchische structuur (zowel TTP als centrale sleutel-distributie) hoge prioriteit te hebben;
- om als volwaardige vervanging van het papieren circuit te kunnen fungeren, dient beveiligde e-mail ingezet te kunnen worden ter ondersteuning van zoveel mogelijk betrouwbaarheidsniveaus. De weg hier naartoe kan echter een geleidelijke zijn: in eerste instantie beperkt tot duidelijk afgebakende betrouwbaarheidsniveaus, met een zeer geleidelijke groei naar een inzetbaarheid voor andere niveaus. De "Multi Level Secure"-uitgangspunten van Defensie kunnen hier als basis dienen;
- ook de weg naar een grootschalige implementatie is een zeer geleidelijke, omdat de inzet van beveiligde e-mail altijd gerelateerd zal zijn aan concrete processen. Grootschalige implementatie is duidelijk een groeitraject: naarmate beveiligde e-mail in

meer processen wordt toegepast, ontstaat geleidelijk een steeds grootschaliger inzet van de voorziening.

Om ervoor te zorgen dat elk van de decentrale invoeringstrajecten uiteindelijk wel naar dit gezamenlijk eindplaatje toewerkt, is een goede balans nodig tussen wat gezamenlijk aan kaders en voorwaarden wordt vastgesteld enerzijds, en de decentrale processen anderzijds.

7. Conclusies en aanbevelingen

In dit rapport is de volgende vraag beantwoord:

> *Wat moet er gebeuren om beveiligde e-mail in te voeren binnen onderdelen van de Rijksoverheid?*

Op basis van de antwoorden op de deelvragen waarin deze onderzoeksvraag is opgedeeld, kan een aantal conclusies getrokken worden. Deze conclusies worden in dit afsluitende hoofdstuk gepresenteerd, gevolgd door een aantal concrete aanbevelingen van de opstellers van dit rapport aan het bestuurlijke niveau binnen de Rijksoverheid

7.1 Conclusies

Een eerste conclusie die getrokken kan worden, is dat beveiligde e-mail een essentiële voorziening kan vormen voor de Rijksoverheid, en dat initiatief van de overheid ten aanzien van deze voorziening gewenst is. E-mail kan in belangrijke mate bijdragen aan het optimaliseren van de efficiëntie en effectiviteit van overheidscommunicatie. Om optimaal te kunnen profiteren van deze bijdrage, moet e-mail ook ingezet kunnen worden in formele communicatie binnen de overheid, een communicatietraject dat nu nog voornamelijk op papier plaatsvindt. Om deze inzet van e-mail te kunnen realiseren is beveiliging van dit communicatiemiddel essentieel. Daarbij is het van belang dat de Rijksoverheid initiatief onderneemt op dit terrein. De Rijksoverheid als geheel dient een aantal uitgangspunten te formuleren en bewaken om te voorkomen dat her en der losse initiatieven opkomen die niet voldoende samenhang vertonen om te komen tot een robuust kader voor elektronische overheidscommunicatie.

Een tweede conclusie is dat, bij de invulling van een dergelijk overheidsinitiatief, interdepartementale afstemming cruciaal is. Deze interdepartementale afstemming dient vorm te krijgen op het hoogste niveau, en dient te worden geïnitieerd door een nog vorm te geven coördinatie- en expertisecentrum. Binnen deze structuur dient allereerst een aantal gezamenlijke kaders te worden vormgegeven en vastgesteld ten aanzien van de architectuur van beveiligde e-mail binnen de Rijksoverheid en de standaarden die hierbij ondersteund worden, de architect-rol. Vervolgens dient het coördinatie- en expertisecentrum vooral de rol van coach te vervullen bij de verschillende departementale invoeringstrajecten.

Een derde conclusie is dat de architectuur die op dit overkoepelende niveau moet worden vastgesteld, de volgende keuzes omvat:

- de bestaande bevoegdhedenstructuur dient als uitgangspunt, en dient te worden vertaald naar een elektronische omgeving;
- beveiligde e-mail betreft de uitwisseling tussen functionarissen;

de bevoegdheden van de betreffende functionarissen worden vastgelegd en gegarandeerd in een overheidsbrede adressengids;

- er is sprake van end-to-end-beveiliging, beveiliging van berichten die plaatsvindt op applicatieniveau;
- er moet een keuze gemaakt worden ten aanzien van de ondersteunde betrouwbaarheidsniveaus: dient beveiligde e-mail ingezet te kunnen worden voor alle betrouwbaarheidsniveaus (tot staatsgeheim aan toe), of dient dat beperkt te worden?
- er dient een keuze gemaakt te worden voor een bepaalde vertrouwensstructuur: een structuur met TTP-diensten, of een structuur met een web van vertrouwen;
- er dient een keuze gemaakt te worden ten aanzien van de uitgifte en het beheer van sleutels.

Een vierde conclusie is dat deze architectuur moet dienen als "eindplaatje" waarover overeenstemming bestaat tussen de verschillende onderdelen van de Rijksoverheid. De verschillende trajecten waarin beveiligde e-mail binnen deze onderdelen wordt ingevoerd, dienen dan ook deze architectuur als gezamenlijke doelstelling in het oog te houden.

Een vijfde conclusie is dat ten aanzien van de weg die moet worden afgelegd om te komen tot dit eindplaatje, grote verschillen bestaan tussen de verschillende organisatie-onderdelen. Tevens bestaat een duidelijk verschil in prioriteit tussen de verschillende elementen van het "eindplaatje":
- de hoogste prioriteit ligt bij het bewerkstelligen van een hiërarchisch stelsel van vertrouwen en een sleutel-generatie en -uitgifte door de organisatie
- ten aanzien van de reikwijdte van de implementatie en de te ondersteunen betrouwbaarheidsniveaus is de prioriteit aanzienlijk lager.

7.2 Aanbevelingen

Op basis van de antwoorden die in de voorgaande hoofdstukken van dit rapport zijn gegeven op de verschillende deelvragen, kan een aantal aanbevelingen worden gedaan met betrekking tot de invoering van beveiligde e-mail binnen de Rijksoverheid.

De belangrijkste aanbevelingen die uit dit alles naar voren komen, zijn de volgende:

1. Definieer een gezamenlijk "eindplaatje" waarin de keuzes uit architectuur zijn ingevuld, waarin gekozen wordt voor:
   a een elektronische vertaling van de huidige bevoegdheden-structuur in de vorm van een directory (overheidsadressengids);
   b end-to-end beveiliging, oftewel beveiliging op applicatie-niveau;
   c een hiërarchisch stelsel van vertrouwen, met een TTP-dienst, en een centrale sleutel-generatie en -distributie;
   d een inzetbaarheid van beveiligde e-mail voor zoveel mogelijk betrouwbaarheidsniveaus;
   e een grootschalige, maar wel proces-gerelateerde implementatie.

2. Definieer groeiscenario's naar dit eindplaatje,
   a waarin de prioriteit wordt gelegd bij het bewerkstelligen van een hiërarchisch stelsel van vertrouwen en sleutel-generatie en -distributie door de organisatie
   b en waarin ten aanzien van betrouwbaarheidsniveaus en grootschalige implementatie een geleidelijk groeimodel wordt gehanteerd.

3. Definieer in samenspraak met de betrokken organisatie-onderdelen, het "instapniveau" van elk van de onderdelen in deze groeiscenario's.

4. Roep een centraal coördinatie- en expertisecentrum beveiligde e-mail in het leven, dat de verschillende invoeringstrajecten begeleidt en de gezamenlijke doelstellingen bewaakt.

5. Zoek afstemming tussen wat bottom-up en top-down dient plaats te vinden:
   a stel de architectuur en daarmee het "eindplaatje" vast in het IB-beraad, dat hiermee de strategische sturing (de "architect"-rol) voor zijn rekening neemt;
   b laat het coördinatie- en expertisecentrum fungeren als "coach" voor de invoeringstrajecten binnen de verschillende onderdelen van de Rijksoverheid.

Bijlage I. Geraadpleegde documentatie

Actieprogramma Elektronische Overheid. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1998.

Bernstein, T, A. B. Bhimani, E. Schultz, C. A. Siegel. *Internet Security For Business.* New York: John Wiley & Sons, 1996.

Defensie E-mail Beveiligingsbeleid. Den Haag: Ministerie van Defensie, 1998.

Haalbaarheidsstudie Overheidsintr@net; Eindrapport. Den Haag: Het Expertise Centrum, 1998.

Handboek Informatiebeveiliging Rijksdienst 1995. Den Haag: Ministerie van Binnenlandse Zaken.

Handleiding A&K-Analyse. Den Haag: ACIB, juli 1996.

Hooff, B.J. van den. *Incorporating Electronic Mail; adoption, use and effects of electronic mail in organizations.* Amsterdam: Otto Cramwinckel Uitgever, 1997.

Informatiebeveiliging; Het IABB-procesmodel voor een gestructureerde aanpak. Utrecht: Stichting SURF, 1999. (http://www.surf.nl/iabb/iabb2.html)

Internet Security (Cursus-documentatie). Utrecht: SURFnet Expertise Centrum, 1998.

Naar een Verantwoorde Archivering van E-mail; Verslag van een symposium over de invoering, het gebruik en de archivering van e-mail in (overheids)organisaties. Den Haag: Rijksarchiefdienst, 1998.

Stikvoort, D.P. *Elektronische Post en Veiligheid.* SURFnetnieuws 19 augustus 1997. (http://nieuws.surfnet.nl/nieuws/snn-archief/achtergrond/jg97-98/04print.html)

Supporting Electronic Government: The Government of Canada Public Key Infrastructure. (http://www.cio-dpi.gc.ca/pki/Documents/Supp-Elec-Gvmt_eng.html)

Voorschrift Informatiebeveiliging Rijksdienst 1994. Den Haag: ACIB (http://www.minbzk.nl/acib/algemeen/TekstVIR.htm)

Bijlage II

Communiceren in vertrouwen.
Inventarisatie marktproducten beveiligde e-mail.

Versie 1.0

Dit rapport werd geschreven in opdracht van de heer [redacted] MPA van het Advies en coördinatiepunt informatiebeveiliging (ACIB) door de heer drs. [redacted] van M&I/STELVIO. Dit rapport maakt deel uit van een opdracht omtrent beveiligde e-mail" uitgevoerd door Nlsign, M&I/PARTNERS en M&I/STELVIO

8. Inleiding

Op 30 oktober 1998 is opdracht verschaft aan een consortium van NLsign bv, M&I/PARTNERS en M&I/STELVIO.

De doelstelling van beveiligde e-mail in het algemeen wordt in de opdracht als volgt geformuleerd:

"Een veilige manier te realiseren (met inachtneming van beschikbaarheid, vertrouwelijkheid en integriteit) waarop de rijksoverheid kan e-mailen met andere onderdelen van de rijksoverheid en waar mogelijk met partijen die betrokken zijn bij de processen van de ministeries (andere overheden, semi-overheidsinstanties en uitvoeringsorganen op afstand)".

9. Opdracht

De opdrachtformulering van het project beveiligde e-mail valt uiteen in drie delen:

1. *Bestuurlijke, organisatorische en technische eisen*
   Wat zijn de bestuurlijke, organisatorische en technische eisen die aan end-to-end beveiliging gesteld moet worden? Hierbij is het van belang aandacht te schenken aan vertrouwelijkheid, integriteit en beschikbaarheid van elektronisch verkeer en aan technische specificaties en de verschillende systemen waarmee gewerkt wordt. Hier moet onder andere de keuze gemaakt (kunnen) worden over het gewenste niveau van veiligheid en de categorieën informatie.
   Nader overleg met de opdrachtgever heeft tot de verduidelijking geleid dat de opdrachtgever in dit onderdeel een architectuurplan wenst te zien voor de voorbereiding van de roll-out. Het feitelijke Plan van Aanpak wordt door de opdrachtgever zelf uitgewerkt.

2. *Ontwerpen testsituatie en uitvoeren van een pilot*
   Ontwerp een testsituatie in de vorm van een pilot waarmee binnen de rijksoverheid op beperkte schaal (ongeveer 100 werkplekken met een looptijd van 3 maanden) end-to-end-beveiliging getest kan worden en waaruit goede inzichten kunnen worden verkregen voor de invoering op grote schaal.

3. *Inventarisatie producten*
   Maak een inventarisatie van producten die op de markt aanwezig zijn en die kunnen worden gebruikt met daarbij de voor- en nadelen van de verschillende producten.

Dit rapport gaat in op het derde onderdeel, de inventarisatie van producten is op de markt aanwezig voor het realiseren van end-to-end beveiliging.

10. Doel opdracht

Het doel van de opdracht is te komen tot:
- een overzicht van op de markt aanwezige producten;
- een (niet uitputtend) programma van eisen waaraan producten dienen te voldoen.

In het plan van aanpak wordt het programma van eisen nader gespecificeerd als:
- de technische kwaliteiten;
- de methode van beveiligde communicatie;
- het gemak waarmee de beveiligde communicatie door de gebruiker aangewend kan worden.

11. Afbakening

Het onderzoek beperkt zich tot producten die end-to-end beveiliging leveren. Hoewel de terminologie anders doet vermoeden, betekent dit dat het tussenliggende transport geheel onbeveiligd is/kan zijn en dat daaraan vanuit de productinventarisatie geen eisen worden gesteld.

End-to-end beveiliging betekent:

- dat de ontvanger(s) van een bericht er zeker van kan (kunnen) zijn dat het ontvangen bericht van de afzender afkomstig is (signing) en/of;
- verzender er zeker van kan zijn dat het verzonden bericht uitsluitend door de ontvanger(s) ontdaan kan worden van de versleuteling (encryption).

Het betekent derhalve niet:

- dat de afzender er zeker van kan zijn dat zijn of haar bericht de geadresseerde bereikt;
- dat de ontvanger er zeker van kan zijn dat alle berichten voor hem of haar bedoeld ook aangekomen zijn.

Erkend wordt dat een aantal problemen rondom e-mail niet in de applicatie opgelost kunnen worden, maar een betrouwbare transportlaag vereisen.

Een andere beperking is dat de eisen die in het Programma van Eisen genoemd worden uitsluitend betrekking zullen hebben op de producten en niet op het proces wat rondom de beveiliging dient plaats te vinden. Dit heeft tot gevolg dat bijvoorbeeld het "vaststellen van technische eisen waaraan versleuteling moet voldoen" hier wel genoemd wordt, maar geen rol moet spelen bij de beoordeling van de producten.

12. Werkwijze

De gevolgde werkwijze, zoals beschreven in de offerte, is:

- beperkte deskresearch naar verkrijgbare marktproducten;
- beoordeling marktproducten aan (technische) eisen.

Verder is een beperkt aantal producten getest om te zien in hoeverre deze voldeden aan in het Programma van Eisen genoemde aspecten.

13. Aspecten van onderzoek

In dit hoofdstuk wordt in algemene zin ingegaan op de elementen die een rol kunnen spelen bij de evaluatie van de producten.

Certificaties
Onderzocht is welke e-mail producten een certificatie hebben. Daarbij is gekeken of er e-mail producten voorhanden zijn die geëvalueerd zijn met gebruikmaking van TCSEC of CC (common criteria). Ook is onderzocht of
gebruikmakend van ITSEC nog e-mail producten gecertificeerd zijn; dit alles is niet het geval.
Er bestaat wel een certificatie voor S/MIME, waarbij marginaal onderzocht wordt of een product voldoet aan de S/MIME standaarden.

S/MIME en PGP
De twee beschikbare mechanismen voor het versturen van secure e-mail zijn op dit moment S/MIME en PGP. Deze twee mechanismen verschillen fundamenteel van elkaar en wel in die mate dat betwijfeld wordt of er ooit één standaard voor beveiligde e-mail zal komen. Wie dit gevecht gaat winnen is nog niet duidelijk.

PGP heeft zich aan exportbeperkingen voor sterke encryptie weten te onttrekken en aanvullende software (plug-ins) voor onder andere Microsoft en Netscape producten worden kosteloos geleverd. PGP heeft als nadeel dat een hiërarchische infrastructuur voor vertrouwen, een PKI, (nog) niet aanwezig is.

Grote marktspelers op het gebied van e-mail -Microsoft, Netscape en Novell (groupwise)- hebben zich aan S/MIME geconformeerd. Verder sluit S/MIME naadloos aan bij andere vormen van beveiligde communicatie zoals secure connection layer (SSL) voor Web-browsing. S/MIME is in de standaardsoftware edities voor de non-US markt voorzien van zwakke, eenvoudig te kraken, encryptie. Dit zal in de nieuwe S/MIME versie 3 niet veranderen. Voor de Rijksoverheid zal deze software, uitgerust met sterke encryptie, verkrijgbaar zijn.

Encryptie-schema
Volgens de huidige standaarden encryptie met een 128 bits symmetrische sleutel dient plaats te vinden. Belangrijk daarbij is dat de bescherming van de symmetrische sleutel door een asymmetrische sleutel plaatsvindt met een 1024 dan wel 2048 bits sleutel, bij voorkeur te kiezen door de gebruiker, zijn organisatie of beiden. Geaccepteerd veilige symmetrische encryptiemethodes zijn Triple-Des, Idea, Cast-128 en Elgamal.

Signing
Signing (het zetten van een digitale handtekening) vindt plaats door middel van versleuteling van een MAC, een Message Authentication Code. Een van de belangrijkste eigenschappen van een MAC is dat twee boodschappen die een zelfde MAC genereren (collisions) niet voorkomen. Juist op deze eigenschap is MD5 verdacht en wordt daarom in het algemeen SHA-1 gebruikt.

Clear vs opaque signing
Sommige S/MIME software waarmee een digitale handtekening wordt gezet, pakt handtekening én bericht samen nog een keer in. Het gegenereerde bericht is vervolgens niet meer leesbaar, tenzij de ontvanger ook over een S/MIME-client beschikt. Deze eigenschap maakt het onmogelijk berichten gelijktijdig naar meerdere ontvangers te sturen waarvan onduidelijk is of iedereen over de S/MIME functionaliteit beschikt. Clearsigning, waarbij het bericht leesbaar blijft en voorzien is van een apart bijgevoegde "handtekening", verdient daardoor de voorkeur.

Single-key vs dual-key
Het is gebruikelijk dat voor het zetten van digitale handtekeningen (signing) een ander sleutelpaar gebruikt wordt dan voor het versleutelen van berichten. De reden hiervoor is dat een geheime sleutel voor ondertekening van berichten nooit gedeponeerd wordt. Dat is ook niet nodig, omdat van de inhoud altijd kennis genomen kan worden hetzij doordat de boodschap nog leesbaar is (clear-signing), hetzij doordat de boodschap door middel van het publieke deel van het sleutelpaar ontcijferd kan worden (signing gebeurt met het geheime deel van een sleutelpaar). Het tekenen echter dient op geen enkele andere manier te kunnen gebeuren dan door de eigenaar en dit kan uitsluitend gewaarborgd worden door de sleutel (of de toegang tot de sleutel) niet te deponeren.

Het is echter denkbaar dat een bedrijfspolicy voorschrijft dat versleutelde berichten die ontvangen dan wel verzonden worden, altijd geopend kunnen worden door een functionaris van het bedrijf. In dat geval dienen de geheime encryptiesleutels van gebruikers gedeponeerd te zijn om naar de functionaris toegezonden berichten te kunnen ontcijferen.

14. Programma van Eisen

Het navolgende, niet uitputtende, Programma van Eisen valt uiteen in drie onderdelen. Achtereenvolgens wordt ingegaan op bestuurlijke eisen die aan beveiligde e-mail gesteld kunnen worden, vervolgens worden organisatorische aspecten behandeld en tenslotte volgt een opsomming van technische eisen. Deze volgorde stemt overeen met de gedachte uiteen gezet in het hoofddocument bij deze studie "vertrouwen in communiceren".

Telkens als zich in de beschrijving een eis voordoet, wordt hier een nummer geplaatst om een checklist te maken waaraan beschikbare producten getoetst kunnen worden

14.1Bestuurlijke eisen

Beschikbaarheid

De eis van beschikbaarheid wordt in het kader van het Programma van Eisen niet verder uitgewerkt; voor beveiligde e-mail gelden geen andere vereisten dan degene die al golden voor "gewone" e-mail. Daarnaast wordt erkend dat de eis van beschikbaarheid van de gehele keten niet in de e-mail client of server of beiden tegelijk op te lossen is.

Exclusiviteit

Aan de eis van exclusiviteit wordt invulling gegeven doordat een bericht dat voor een geadresseerde bestemd is, zodanig versleuteld wordt dat het niet leesbaar is als het in onbevoegde handen zou komen (B1). Dat een bericht als zodanig in onbevoegde handen kán komen wordt hiermee niet voorkomen, wél dat dan ook kennisname van de inhoud plaatsvindt. Dit heeft gevolgen voor de technische eisen aan de versleuteling. Denkbaar is dat een instantie binnen de Rijksoverheid (NBV ?) vaststelt welke technieken wel en niet geoorloofd zijn ter waarborging van de exclusiviteit vóórdat verregaande invoeringsmaatregelen worden genomen (B2).
De eis voor exclusiviteit kan echter gelijktijdig een eis van non-exclusiviteit met zich meebrengen. Zo kan een organisatie het ongewenst vinden als, met gebruikmaking van de publieke sleutels van de werknemers, versleutelde berichten naar de organisatie worden gestuurd (B3) die niet door een daartoe bevoegd persoon, niet zijnde de ontvanger van het bericht, geopend kunnen worden (B4). Evenzeer kan het ongewenst zijn dat versleutelde berichten de organisatie verlaten (B5) zonder dat een bevoegd persoon, anders dan de verzender, daarvan kennis kan nemen (B6).
Vandaar dat op bestuurlijk niveau vastgesteld dient te worden hoe met deze non-exclusiviteit wordt omgegaan (B7).

Integriteit

Aan de eis van Integriteit wordt invulling gegeven

1. doordat een bericht, bestemd voor een geadresseerde, zodanig gewaarmerkt wordt (B8), dat verwerking van het waarmerk bij de ontvanger zeker stelt dat het bericht (B8a) en de aanhangende documenten (B9b) onveranderd bij geadresseerde zijn aangekomen;
2. doordat het waarmerk voorzien wordt van een digitale handtekening van de verzender. Hiermee is gewaarborgd dat het bericht ook afkomstig is van de persoon die beweert het bericht gestuurd te hebben (B9 B9a). Daarvoor is dan wel een digitale handtekening vereist die op enigerlei manier voorzien is van een identiteitswaarborg of certificaat(B10) van een partij die daartoe bevoegd is (B11).

Denkbaar is dat een instantie binnen de Rijksoverheid (NBV ?) vaststelt welke technieken wel en niet geoorloofd zijn ter waarborging van de integriteit vóórdat verregaande invoeringsmaatregelen worden genomen.

14.2Organisatorische eisen

Sleutelbeheer

Er dient een organisatie te zijn die verantwoordelijk is voor het uitgeven en beheren van sleutels (O1). Een eerste element hierbij is het bieden van de mogelijkheid iemands publieke sleutel op te halen (O2) teneinde hem versleutelde berichten te kunnen sturen [4]. Verder is van belang na te kunnen gaan of iemands sleutel nog wel geldig dan wel verlopen is (O3). Zeker zo belangrijk is het om na te kunnen gaan of iemand zijn sleutel heeft teruggetrokken (O4, O5). Afhankelijk van wat de organisatie als bestuurlijk gewenst beschouwd, dienen er ook maatregelen getroffen te worden voor key-escrow (O6) en/of key-recovery (O6a).

Gescheiden sleutels

Gescheiden sleutels voor encryptie en voor signing zijn noodzakelijk (zie eerdere uitleg hieromtrent). Hierbij zijn twee elementen van belang: de mogelijkheid sleutels af te geven voor uitsluitend digitale handtekening (O7) en de mogelijkheid sleutels af te geven uitsluitend voor versleuteling (O8).

Hiërarchisch vertrouwen of web van vertrouwen

Een web van vertrouwen alleen schaalt niet, omdat uiteindelijk teveel wederzijdse trust relaties gelegd moeten worden. Welke techniek ook gekozen wordt, beide vereisen een hiërarchische benadering van vertrouwen (O9). Daarbij dient in acht te worden genomen dat voor hiërarchische S/MIME, specifieke producten bestaan. Dit is voor PGP niet het geval hoewel een dergelijk infrastructuur organisatorisch gezien niet complexer hoeft te zijn.
Vastgesteld dient te worden welke vormen van vertrouwen geoorloofd zijn (O10).

[4] Een demonstratie hiervan kan zelf uitgevoerd worden door te browsen naar https://digitalid.verisign.com/services/client/index.htm Vul vervolgens bij Search by name in: [redacted]. U vindt dan meerdere S/MIME-keys. Eén ervan is de preferred key en dat staat als zodanig aangegeven.
Een tweede mogelijkheid is te browsen naar http://www.nai.com/products/security/public_keys/lookup_key.asp
en daar in te vullen [redacted] U vindt dan twee PGP-keys; van 4-11-1994 en van 14-12-1998. Beide zijn bruikbaar.

Gecontroleerde uitgifte van certificaten

Vastgesteld moet worden:
- hoe in de organisatie certificaten uitgereikt worden (O11);
- welke identificatie noodzakelijk is (O12);
- hoe de certificaten en sleutels bewaard worden (O13).

Managen van Key Revocation List
Een mechanisme beschikbaar hebben om vast te stellen of sleutel die door iemand gebruikt wordt nog geldig is, is noodzakelijk (O14). Gebruikers dienen de mogelijkheid te krijgen hun sleutel te herroepen (O4), bijvoorbeeld omdat deze gecompromitteerd is geraakt.

Software versiebeheer

Software versiebeheer is noodzakelijk omdat gebleken is dat tussen sommige software versies aanzienlijke verschillen kunnen voorkomen (O15). In essentie wijkt dit niet af van software versiebeheer zoals nu al wordt toegepast voor applicaties.

14.3Technische eisen

Niveaus van beveiliging

Met deze eis wordt bedoeld dat meerdere gradaties van beveiliging uitgevoerd kunnen worden met gebruikmaking van dezelfde ICT- omgeving, zowel aan de gebruikers als aan de server kant (T1). Op dit moment ontbreekt een geldig classificatieschema voor beveiligde informatie. Daarom is de eis voor het niveau van beveiliging die op dit moment gehanteerd kan worden is uitsluitend aan of uit. Dat wil zeggen gebruikers zijn in staat:
- niet beveiligde (T2);
- gesigneerde (T3);
- versleutelde (T4);
- versleutelde en gesigneerde (T5).

berichten te versturen.
Verder moet het voor de gebruiker mogelijk zijn meerdere certificaten en sleutelcombinaties te gebruiken (T6) voor het geval speciale eisen aan certificaat of sleutel gesteld worden voor bijzondere vormen van communicatie, afhankelijk van het domein waarin gecommuniceerd wordt.

Implementatie E-mail RFC's
Te gebruiken producten dienen de Internetstandaarden met betrekking tot het gebruik van e-mail afdoende geïmplementeerd te hebben, met name voor wat betreft de S/MIME en PGP/MIME omgeving (T7)
Hiertoe wordt gerekend:
RFC822: format of header messages
RFC's 2045, 2046, 2047, 2048 en 2049 over MIME
RFC's 2311, 2312, 2313, 2314 en 2315 over S/MIME
RFC's 1991, 2015 en 2440 over PGP

Implementatie/plug-in S/MIME

De te gebruiken e-mail cliënt dient S/MIME zodanig geïmplementeerd te hebben dat het mogelijk is:

- meerdere certificaten te gebruiken (T8);
- verschillende certificaten te gebruiken voor encryptie en signing (T9);
- het beveiligingsniveau van de certificaten in te stellen (T10);
- gebruik te maken van een chipcard lezer voor opslag van de certificaten en sleutels (T11);
- berichten clear-signed te versturen (T12);
- certificaten in een standaardformaat te importeren en exporteren (T14);
- eventueel zelf te genereren certificaten te valideren bij een CA naar keuze (T15);
- na te gaan of de interoperabiliteit met andere S/MIME producten onderzocht is [5] (T16).

Als het een plug-in betreft zijn aanvullende eisen:

- dat het werken met de e-mail cliënt niet wezenlijk verandert (T13) [6].

Implementatie/plug-in voor PGP

De te gebruiken PGP plug-in moet voldoen aan de volgende eisen:

- verschillende sleutels voor signing en encryptie moeten gebruikt kunnen worden (T17);
- het gebruik van meerdere sleutels voor signing dient ondersteund te worden (T18);
- berichten moeten clear-signed verstuurd kunnen worden (T19);
- sleutels moeten geëxporteerd en geïmporteerd kunnen worden (T20).

Implementatie van beveiliging

Al eerder is betoogd dat er een noodzaak is om van gescheiden sleutels voor encryptie en signing gebruik te maken (T17)

De kwaliteit van het algorithme voor signing (T21) speelt een belangrijke rol als het gaat om:

- het vaststellen van de identiteit van de verzender;
- het vaststellen van de integriteit van de boodschap;
- Het te gebruiken algorithme dient door een nader te bepalen instantie gecertificeerd te zijn (T22).

De kwaliteit van het algorithme voor encryptie (T23) speelt een belangrijke rol in de realisatie van de vertrouwelijkheid.
Het te gebruiken algorithme dient door een nader te bepalen instantie gecertificeerd te zijn (T24).

Beveiliging van attachments
Attachments dienen op dezelfde manier beveiligd te zijn als andere body-parts. Dat betekent:

- dat de signing ook voor attachments moet gelden (T25);
- dat encryptie ook voor attachments uitgevoerd moet worden (T26);

Clear-signing
S/MIME is bij voorkeur zo geïmplementeerd dat gebruik gemaakt wordt van clear-signing (T27).
PGP is bij voorkeur zo geïmplementeerd dat gebruik gemaakt wordt van clear-signing (T28).

---

[5] S/MIME implementaties worden voor de correcte S/MIME werking gecertificeerd door RSA. Uitleg en laatste stand van zaken is te vinden op: http://www.rsa.com/smime/html/interop_center.html

[6] De achtergrond van deze opmerking is dat sommige S/MIME producten als een soort schil om het feitelijk e-mail programma heen werken; de gebruiker krijgt dan uiteindelijk een geheel andere gebruikersinterface voorgeschoteld dan daarvoor

15. Inventarisatie marktproducten

Afbakening
De inventarisatie van marktproducten is uitgevoerd door gebruik te maken van informatie verkregen van leveranciers en van bronnen op het Internet. Waar nodig is aanvullende informatie opgedaan bij relaties en/of leveranciers.

Producten marktpartijen

De volgende producten zijn geïdentificeerd als producten die een certificatie hebben verworven, in dit geval van het Mime-interoperability centre van RSA inc.

Fabrikant	Productnaam	Gecertificeerd in
Baltimore	MailSecure 1.0	6/97
Celo Communications	CeloCom Mail 1.5	11/98
Citibank	Global File Handler	12/98
Control Data	Cipher*Mail 1.5	12/98
Cyclone Software	Interchange Server 2.0	3/98
Entrust Technologies	Entrust Express 4.0	11/98
Frontier Technologies	e-Lock 2.0	02/98
Labcal Technologies	IsoShield/Mail	03/98
Microsoft	Outlook Express 4.0	7/97
Microsoft	Outlook 98 Beta 2	10/97
Mission Critical	Clavis 0.1b	02/98
Netscape	Communicator 4.01	6/97
NEL	Mahobin	6/97
OpenSoft	ExpressMail 2.0.2	7/97
PCSL	Stoplock NT Secure E-Mail 1.0	1/99
RSA	S/MAIL 1.0	6/97
Secude	authentemail 2.0.4C	11/98
SSE	TrustedMIME 1.0	6/97
Structured Arts	CertKit S/MIME 1.0	1/99
Worldtalk	WorldSecure Client	
Worldtalk	WorldSecure Server 3.0	5/98
XETI	JKIX Toolkit 1.0	7/98

Bovengenoemde certificatie is in vergelijking met het Programma van Eisen beperkt. De test bestaat uit het aanvragen van een certificaat en het verzenden van gesigneerde en versleutelde e-mail.
Andere aspecten die in het Programma van Eisen zijn genoemd komen in deze test niet aan bod.

Een ander onderzoek voegt nog enkele producten toe aan deze lijst, maar de interoperabiliteitstest zoals in de vorige tabel heeft niet plaatsgevonden.

Fabrikant	Productnaam	
Novell	Groupwise met Entrust	
LJL enterprises	Armormail	
Labcal technologies	ISOshield/Mail (Notes)	

15.1Beoordeling marktproducten aan Programma van Eisen

Voor de volledige beoordeling van marktproducten aan het Programma van Eisen zou een aparte studie, vergezeld van de ondersteuning een testlaboratorium noodzakelijk zijn, als van alle genoemde eisen die voor de beoordeling relevante onderdelen worden meegenomen.
De producten die van het S/MIME testcentrum gebruik maken en vermeld worden als werkend, voldoen niet altijd aan de aanvullend gestelde eisen. Met name de eis van clear-signing blijkt in de praktijk lastig te verwezenlijken voor een aantal producten. Vragen hieromtrent aan de respectievelijke fabrikanten worden niet beantwoord.
Omdat een feitelijke beoordeling van alle genoemde producten niet heeft plaatsgevonden, moet het Programma van Eisen gezien worden als een oriëntatie bij de keuze voor een definitief product.

15.2Beoordeling eisen voor relevantie productinventarisatie

In de onderstaande tabel zijn de eisen opgenomen zoals in eerdere paragrafen vermeld. Daarbij is elke eis omschreven, is aangegeven of deze eis relevant is in het kader van de productbeoordeling, is ruimte gelaten voor het toekennen van een gewicht aan de betreffende eis en is er ruimte voor opmerkingen.
De tabel is een gedeeltelijke voorzet voor de inrichting van een keuzeproces en niet het keuzeproces als zodanig.
De relevantie van de tabel behoeft op deze plaats enige nuancering, in die zin dat behalve de kwaliteit "beveiligde e-mail" er daarnaast nog een heleboel weegfactoren zijn waarom een e-mail pakket gebruikt wordt. Als illustratie moge dienen:

- de mate waarin het integreert met de desktop;
- de mate waarin een pakket als gebruiksvriendelijk wordt ervaren;
- beheerbaarheid;
- etcetera.

Eis	Omschrijving	Relevant	Gewicht	Opmerkingen
	Bestuurlijke eisen			
B1	versleuteld bericht mag niet onbevoegd gelezen worden, ook al valt de versleutelde versie in onbevoegde handen	Ja		
B2	aanwijzen instantie voor vaststellen kwaliteit versleuteling			
B3	de mogelijkheid versleutelde berichten te ontvangen	Ja		
B4	de mogelijkheid versleutelde ontvangen berichten te openen door een daartoe aangewezen persoon, niet zijnde de ontvanger	Nee		
B5	de mogelijkheid versleutelde berichten te verzenden	Ja		
B6	de mogelijkheid versleutelde verzonden berichten te openen door een daartoe bevoegd persoon, niet zijnde de verzender	Nee		
B7	vaststellen wenselijkheid/ procedures rondom B4 en B6			
B8	waarmerk van echtheid aan bericht koppelen	Ja		
B8a	waarmerk van echtheid kunnen bepalen voor bericht	Ja		
B8b	waarmerk van echtheid kunnen bepalen voor aanhangende documenten	Ja		
B9	waarborg van identiteit aan bericht koppelen	Ja		
B9b	waarborg van identiteit kunnen uitlezen	Ja		
B10	het kunnen uitgeven van identiteitswaarborgen	Nee		
B11	het hebben van een bevoegde partij die identiteitswaarborgen kan verschaffen	Nee		
	Organisatorische eisen			
O1	verantwoordelijke voor uitgifte en beheer sleutels	Nee		
O2	beschikbaarstelling publieke sleutels	Nee		
O3	controle door gebruiker op geldigheid van sleutel	Ja ?		
O4	de mogelijkheid een sleutel in te trekken (key revocation)	Ja ?		
O5	controle gebruiker op key revocation	Ja ?		
O6	mogelijkheid voor key escrow organiseren	Nee		
O6a	mogelijkheid voor key recovery organiseren	Nee		
O7	uitgifte separate sleutel voor digitale handtekening/ waarmerken integriteit van een bericht	Nee		

Eis	Omschrijving	Relevant	Gewicht	Opmerkingen
O8	uitgifte separate sleutel voor versleuteling van bericht	Nee		
O9	aanwezigheid hiërarchisch vertrouwen	Nee		
O10	vaststellen welk vertrouwen geoorloofd is	Nee		
O11	vaststellen hoe in de organisatie certificaten uitgereikt worden	Nee		
O12	vaststellen welke identificatie noodzakelijk is	Nee		
O13	vaststellen hoe de certificaten en sleutels bewaard worden	Nee		
O14	mechanisme beschikbaar voor key revocation	Nee		
O15	software versie beheer	Ja		
O16				
	Technische eisen			
T1	niveaus van beveiliging	Ja		
T2	onbeveiligde e-mail versturen	Ja		
T3	gesigneerde e-mail versturen	Ja		
T4	versleutelde e-mail versturen	Ja		
T5	versleutelde en gesigneerde e-mail versturen	Ja		
T6	meerdere sleutel en certificaten mogelijk	Ja		
T7	implementatie relevante Internet standaarden	Ja		
T8	gebruik meerdere certificaten mogelijk (wisselen)	Ja		
T9	verschillende certificaten voor versleuteling en digitale handtekening	Ja		
T10	instellen en wijzigen beveiligingsniveau certificaten	Ja		
T11	gebruik chipcard-technologie voor opslag sleutels	Ja		
T12	clear-signing van berichten	Ja		
T13	bij gebruik S/MIME plug-in verandert werken met client niet wezenlijk	Ja		
T14	certficaten kunnen geïmporteerd en geëxporteerd worden	Ja		
T15	zelf gegenereerde certificaten kunnen bij CA naar keuze gecertificeerd worden	Ja		
T16	interoperabiliteit S/MIME producten onderzocht	Ja		

Eis	Omschrijving	Relevant	Gewicht	Opmerkingen
T17	verschillende sleutels voor signing en encryptie	Ja		
T18	meerdere sleutels voor signing kunnen gebruiken	Ja		
T19	signing berichten is clear-signed	Ja		
T20	sleutel import en export is mogelijk	Ja		
T21	beoordeling kwaliteit signing algorithme	Ja		
T22	certificerende instantie voor signing	Nee		
T23	beoordeling kwaliteit algorithme voor encryptie	Ja		
T24	certificerende instantie voor encryptie	Nee		
T25	signing werkt voor attachments	Ja		
T26	encryptie werkt voor attachments	Ja		
T27	S/MIME signing is clear-signded	Ja		
T28	PGP signing is clear-signed	Ja		

16. Conclusie

Dit rapport vormt een eerste aanzet voor de selectie van een e-mail pakket voor beveiligde e-mail.
Beveiliging is echter één van de aspecten die in de beoordeling van e-mail producten een rol speelt. Daarnaast zijn elementen als gebruiksvriendelijkheid, integratie in een office-suite en beheerbaarheid belangrijke aspecten.
Deze inventarisatie moet daarom vooral gezien worden als een controle-lijst bij de keuze, waarbij de overwegingen om tot een bepaalde keuze te komen van groter belang zijn dan de keuze zelf.

Bijlage III

Achtergrondinformatie

beveiligde e-mail

en

digitale handtekeningen

[redacted]
M&I/STELVIO

27 mei 1999

17. Afbakening

Dit stuk is tot stand gekomen als achtergrondinformatie bij het project beveiligde e-mail, uitgevoerd door M&I/PARTNERS, M&I/STELVIO en NLsign voor het ACIB. Omdat gedurende het traject geconstateerd wordt dat het nuttig is als iedereen over gelijke achtergrondinformatie zou beschikken, is deze algemene uitleg geschreven. De onderwerpen die behandeld worden hebben betrekking op beveiligde e-mail; omdat daarin zaken als encryptie en digitale handtekeningen onvermijdelijk zijn, wordt ook daarop beperkt ingegaan.
Een belangrijk element van afbakening is "standaarden". In het gehele stuk wordt uitsluitend ingegaan op publiek verkrijgbare middelen om beveiliging middels computers te bewerkstelligen. Oplossingen die slechts voor een beperkte doelgroep beschikbaar zijn worden niet aangesneden.
Voor wie verder wil lezen en zich in de diverse onderwerpen wil verdiepen, wordt aan het eind verwezen naar redelijk toegankelijke standaardwerken.

18. Wat is beveiligde e-mail

18.1 Afbakening

Beveiligde e-mail is e-mail die voldoet aan een of meer van de volgende beschrijvingen:
1. de afzender van een bericht weet zeker dat alleen de ontvanger van het bericht in staat is het bericht te lezen en wel in ongeschonden staat en/of;
2. de ontvanger van een bericht weet zeker dat het bericht dat hij leest ongeschonden is én afkomstig is van degene die beweert het gestuurd te hebben.

Merk op dat hier niet gesproken wordt over gegarandeerde aflevering van berichten e.d. Het is op dit moment nog niet mogelijk te garanderen dat berichten aankomen. Het is wel mogelijk te vragen om een zogenaamd Read Receipt (bericht van lezen), het is ook mogelijk te verzoeken om een Delivery Notification (bericht van aflevering), maar of dit alles werkt is afhankelijk van de e-mail client dan wel het postkantoorprogramma (de MTA) dat de e-mail aflevert bij de gebruiker.

18.2 Bedreigingen

Bedreigingen in algemene zin die voor e-mail gelden zijn:
1. het bericht kan gelezen worden door iemand voor wie het niet bedoeld is;
2. de berichtinhoud kan gewijzigd worden;
3. het bericht kan verloren gaan tijdens het transport, bij de verzendende partij of bij de ontvangende partij;
4. iemand kan een bericht sturen in naam van iemand anders (spoofing);
5. de verzender kan ontkennen het bericht gestuurd te hebben;
6. de ontvanger kan ontkennen een bericht ontvangen te hebben;
7. de ontvanger kan claimen een bericht ontvangen te hebben;
8. de verzender kan claimen een bericht gezonden te hebben;
9. een bericht kan verkeerd afgeleverd of doorgestuurd worden;
10. het transport kan (tijdelijk) uitvallen.

Dergelijke bedreigingen voor e-mail vertonen, niet geheel toevallig, een grote analogie met bijvoorbeeld de bezorging van brieven of pakketten.

18.3 Maatregelen

Voor e-mail bestaat niet voor alle voorkomende bedreigingen een oplossing, althans als we ons beperken tot standaarden. De bedreigingen waar met beveiligde e-mail wat aan gedaan kan worden zijn:
- het bericht kan gelezen worden door iemand voor wie het niet bedoeld is;
- Deze bedreiging kan weggenomen worden als het bericht zodanig versleuteld wordt dat alleen degene voor wie het bericht bestemd is het bericht kan lezen. Op de precieze werking hiervan wordt nog ingegaan bij de paragraaf over encryptie;
- de berichtinhoud kan gewijzigd worden;

- Deze bedreiging als zodanig kan niet weggenomen worden; er kan echter wel voor gezorgd worden dat dit niet ongemerkt passeert door het plaatsen van een integriteitskenmerk in of bij de boodschap. Als de boodschap dan bij de geadresseerde aankomt en die beschikt over de juiste programmatuur, dan valt op dat de boodschap gewijzigd is. Op de exacte werking hiervan wordt nog nader ingegaan bij de paragraaf over de digitale handtekening;
- iemand kan een bericht sturen in naam van iemand anders (spoofing);
- Deze bedreiging kan als zodanig niet weggenomen worden; er kan echter wel voor gezorgd worden dat dit niet ongemerkt passeert, indien alleen berichten echt vertrouwd worden van personen en instanties die hun e-mail gesigneerd versturen;
- de verzender kan ontkennen het bericht gestuurd te hebben. Vaak wordt deze bedreiging als niet-bestaand geclaimd zodra van digitale handtekeningen gebruik wordt gemaakt. Net als echter bij getekende brieven een beroep gedaan kan worden op vervalsing van de handtekening, zo kan ook de elektronische handtekening vals zijn doordat;
- iemand even zijn PC onbeheerd achter heeft gelaten en een ander een bericht heeft gestuurd;
- iemand claimt een virus te hebben gehad dat er met zijn handtekening vandoor is (hier wordt slechts een verdedigend argument opgevoerd, niet een bestaande techniek);
- et cetera.

Zolang over de digitale handtekening geen jurisprudentie is, is het niet duidelijk hoe met de zojuist genoemde ontkenning van bericht zal worden omgegaan.

19. Wat is een TTP

19.1 Algemeen

Een Trusted Third Party (soms wordt ook de meer generieke term Public Key Infrastructure, PKI gebruikt) is een partij, die buiten de partijen staat die met elkaar communiceren, maar die door beide partijen wordt vertrouwd voor het genereren van bepaalde waarborgen.
Een dergelijke waarborg is bijvoorbeeld de identiteit van de communicerende partijen.
Een Trusted Third party kan de publieke sleutels tekenen van de communicerende partijen en zo de certificaten afgeven waarvan verderop in dit stuk sprake is.

19.2 Wat kan een TTP betekenen

Een TTP kan vele rollen aannemen. Een beperkt aantal wordt hier opgesomd:
1. Verschaffer van digitale identiteit aan personen middels certificaten.
2. Time-stamping, om vast te leggen bijvoorbeeld wanneer een digitaal document is afgegeven.
3. Digitale notariële functies.
4. etc.

19.3 Het gebruik van certificaten

Certificaten kunnen voor een aantal doeleinden gebruikt worden. Genoemd is al het waarborgen van identiteit, maar certificaten kunnen ook gebruikt worden om bijvoorbeeld Intranet-servers met clients te laten communiceren over een beveiligd (in dit geval vercijferd) pad. De laatste toepassing wordt van groot belang geacht bij het ontwikkelen van SET (secure electronic transactions).
In het kader van dit stuk zijn certificaten voornamelijk van belang om tussen communicerende partijen te waarborgen dat de verzender ook is wie hij/zij beweert te zijn. Voor een nadere detaillering wordt verwezen naar het hoofdstuk over vertrouwen..

20. Encryptie

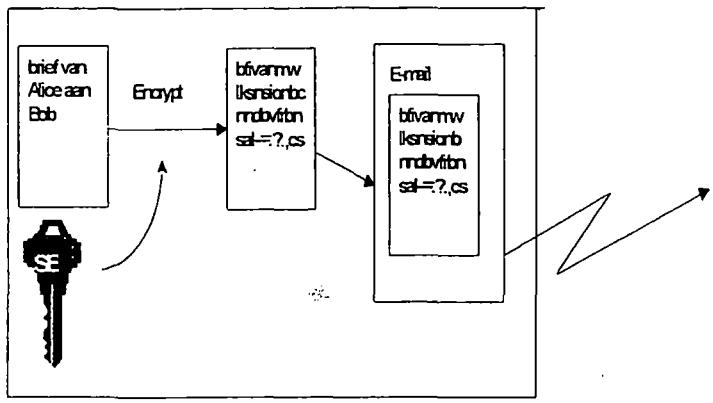
20.1 Algemeen

Encryptie kan in het kort omschreven worden als "het omzetten met behulp van een sleutel van tekst in een reeks onleesbare tekens die met een passende sleutel weer leesbaar gemaakt kunnen worden".
Een belangrijk onderscheid dat bij encryptie vaak wordt gemaakt is het onderscheid in symmetrische en asymmetrische encryptie.

20.2 Symmetrische encryptie

Bij symmetrische encryptie beschikken verzender en ontvanger allebei over dezelfde sleutel. De sleutel waarmee encryptie wordt uitgevoerd, is dezelfde sleutel als waarmee decryptie wordt uitgevoerd. Een bekend voorbeeld van een dergelijke vorm van encryptie is DES (Data Encryption Standard). Andere bekende symmetrische encryptie technieken zijn Triple-DES, RC2, IDEA en CAST-128.

In tekening ziet symmetrische encryptie er als volgt uit:



Met iedereen met wie gecommuniceerd wordt bestaat een zogenaamd "gedeeld geheim", de sessie sleutel SES. Het aantal benodigde sleutels is in de volgende tabel uitgezet tegen het aantal deelnemers.

deelnemers	2	4	8	16
sleutels	1	6	28	120

Hierin is goed zichtbaar dat het beheer van sleutels al snel onpraktisch wordt. Het aantal sleutels is een kwadratische functie van het aantal deelnemers. Als n het aantal deelnemers is, is het aantal benodigde sleutels n(n-1)/2.

20.3 Asymmetrische encryptie

Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De verzender van een bericht encrypt het bericht met één sleutel (de publieke sleutel). De ontvanger decrypt het bericht met de bijpassende sleutel (de geheime sleutel). Bij asymmetrische encryptie

wordt één van de twee sleutels openbaar gemaakt (de publieke sleutel of public key). Dat is ongevaarlijk, omdat de eigenschappen van de sleutels zo gekozen zijn dat het onmogelijk geacht wordt uit de publieke sleutel (public key) de geheime sleutel (secret key) te reconstrueren en andersom. Vanwege het publiceren van de geheime sleutel heet deze techniek ook wel "public key cryptography".
Omdat bij asymmetrische encryptie iedere deelnemer aan de communicatie over één publieke sleutel beschikt, is het mogelijk een persoon, waarvan men de publieke sleutel heeft een geheim bericht te sturen. Als we hier het aantal deelnemers uitzetten tegen de benodigde sleutelparen, zien we het volgende:

deelnemers	2	4	8	16
sleutelparen	2	4	8	16

Bekende voorbeelden van asymmetrische algorithmes zijn RSA, Diffie-Hellman en ElGamal.

21. Een vergelijking tussen symmetrische en asymmetrische encryptie

21.1 Algemeen

Hoewel het lijkt alsof asymmetrische encryptie voordelen heeft die voornamelijk te maken hebben met het sleutelbeheer, kleven er ook ernstige bezwaren aan. Zo is encryptie/decryptie die met behulp van een asymmerische sleutel wordt uitgevoerd vele malen trager dan encryptie/decryptie met een symmetrische sleutel. Dat mag voor een enkele, korte boodschap onbelangrijk lijken, maar in een productieproces telt dit wel degelijk mee. Om dat nadeel op te vangen worden asymmetrische sleutels meestal in combinatie met symmetrische sleutels gebruikt.

21.2 Hoe worden ze gebruikt

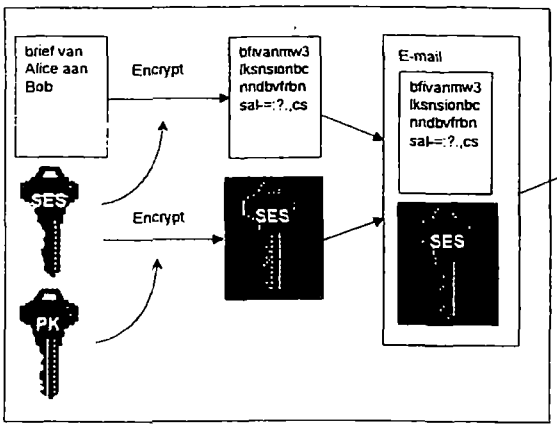
Omdat asymmetrische encryptie traag is, wordt bijna altijd een combinatie van symmetrische en asymmetrische encryptie gebruikt. We gebruiken hier het voorbeeld van Alice die Bob een bericht wil sturen. Dat werkt als volgt:

1. Alice beschikt over de publieke sleutel PK van het asymmetrische sleutelpaar van Bob. Zij gaat hem een boodschap sturen.
2. Alice genereert nu een symmetrische sleutel SES, die zij gebruikt om de te verzenden boodschap te encrypten.
3. de symmetrische sleutel wordt met de publieke sleutel van Bob encrypt.
4. Zowel vercijferde boodschap als vercijferde symmetrische sleutel worden verstuurd (gelijktijdig).

Nu komt de boodschap bij Bob aan.

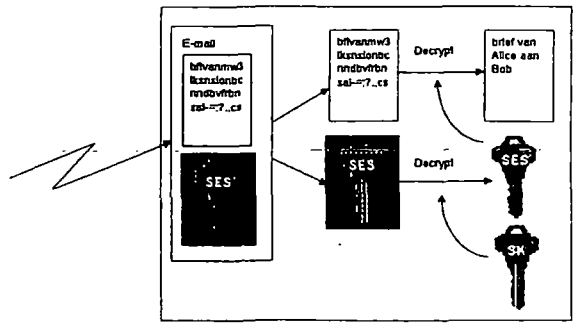
1. Bob splitst het bericht weer in vercijferde boodschap en vercijferde symmetrische sleutel
2. Bob gebruikt zijn geheime sleutel (SK) van het asymmetrische paar om de symmetrische sleutel te ontcijferen.
3. Met behulp van de symmetrische sleutel kan Bob nu de door Alice verstuurde boodschap ontcijferen.

Dat ziet er als volgt uit:



In het kort komt het proces neer op: asymmetrische encryptie wordt gebruikt om een zogenaamde symmetrische session key te beveiligen.

De symmetrische session-key zorgt dan voor de versleuteling van de feitelijke boodschap



Deze vorm van versturen van beveiligde berichten is echter niet zonder problemen.
We sommen er hier een paar op:

1. hoe weet Alice dat de sleutel die zij gebruikt echt van Bob is? Mogelijk heeft zij daarover apart contact met hem gehad en de zogenaamde vingerafdruk van de sleutel uitgewisseld, waardoor zij er zeker van is dat de sleutel van Bob is.
2. hoe weet Bob dat Alice de feitelijke verzender is van de boodschap. De boodschap is niet door Alice getekend, en dan nog: hoe zou Bob dan nog weten dat de digitale handtekening van Alice valide is.

Op beide problemen wordt nader ingegaan in het hoofdstuk over vertrouwen.

21.3Sleutellengte

Sleutellengte is belangrijk bij het versleutelen van berichten omdat de sleutellengte mede bepaalt hoe sterk of zwak een encryptie is. Sleutellengte heeft echter totaal verschillende betekenissen als het bij een symmetrische of asymmetrische encryptie gebruikt wordt. Een vergelijk tussen sleutellengtes ziet er bijvoorbeeld als volgt uit:

	aantal bits keylengte				
Symmetrische encryptie	56	64	80	112	128
Asymmetrische encryptie	384	512	768	1792	2304

(bron: Schneier, Applied Cryptography, second ed.)

Hier is duidelijk te zien dat voor dezelfde cryptografische sterkte bij asymmetrische encryptie een veel langere sleutel nodig is dan bij symmetrische encryptie. Overigens speelt de gebruikte encryptiemethodiek (het algorithme) ook nog een rol. Een sleutellengte van 1024 bij methode A heeft een andere betekenis dan bij methode B. Het best wordt dit geïllustreerd aan de hand van een methode die gekraakt is; daar helpt geen sleutel meer, hoe lang die ook is.

De tabel geeft ook aan hoe bij gecombineerd gebruik van een symmetrische en asymmetrische sleutel de keylengtes in evenwicht dienen te zijn. Zo heeft een asymmetrische sleutel van 2048 bits geen enkele betekenis als daarmee symmetrische keys van 56 bits verstuurd worden.

Een zogenaamde "brute force" aanval op de vercijferde tekst blijft namelijk een aanval op een 56-bits vercijferde tekst. Zo dient ook een 128-bits symmetrische key niet met een 384-bits asymmetrische key verstuurd te worden. De symmetrische key zelf is dan namelijk veel zwakker beschermd dan de tekst die met de symmetrische key beschermd wordt zodat het loont om een aanval op de asymmetrische key te doen.

22. Digitale handtekening

22.1 Algemeen

Een digitale handtekening kan in het algemeen gebruikt worden om een waarmerk aan een document of bericht te hangen. Dat kan een waarmerk van echtheid of een tijdstempel of iets dergelijks zijn. De ontvanger beschikt over de mogelijkheid om het waarmerk te controleren en zo bijvoorbeeld na te gaan of

- het bericht afkomt van degene die zegt het bericht gestuurd te hebben;
- het bericht nog integer is en onderweg niet verminkt is geraakt.

Het probleem "komt dit bericht wel van de persoon die beweert deze persoon te zijn" wordt echter als zodanig niet opgelost door een digitale handtekening. Dat komt, omdat iedereen wel een digitale handtekening kan produceren en daar een naam in kan zetten. Daarom is het belangrijk te bepalen of zo een digitale handtekening vertrouwd kan worden. In het hoofdstuk over vertrouwen wordt daar verder op ingegaan.

22.2 Methodes

Het zetten van een digitale handtekening gaat in het algemeen in een aantal stappen:
Eerst wordt van het te tekenen bericht of document een zogenaamde "hash" berekend. Een hash is een reeks tekens van een vaste lengte. De samenstelling (niet de lengte) van deze tekenreeks wordt beïnvloedt door de inhoud van het bericht of document. Vervolgens wordt iemands geheime sleutel (van een asymmetrisch sleutelpaar) gebruikt om de hash te encrypten. Deze versleutelde hash kan nu aan het document of het bericht "aangehangen" worden. Afhankelijk van de implementatie wordt ook nog de publieke sleutel van degene die het bericht heeft getekend meegestuurd; dat kan handig zijn voor de ontvanger, die hoeft dan niet op zoek naar de publieke sleutel.

22.3 Clear en opaque signing

Voor het tekenen van e-mail-berichten zijn twee methodes in gebruik en toegestaan; de voorkeursmethode heet clear-signing; daarbij wordt de handtekening achteraan een bericht toegevoegd (detached signature) en blijft het bericht zelf leesbaar. Dat biedt een groot voordeel als één bericht gelijktijdig naar ontvangers gestuurd wordt die wél en andere ontvangers die niet over de benodigde beschikken.
De tweede methode, opaque signing, pakt handtekening en bericht in in een file die uitsluitend voor clients leesbaar is die ook beschikken over de software om deze file te ontsleutelen. Deze methode heeft als voordeel dat de kans op verminking van het gesigneerd bericht kleiner is als er één of meerdere gateways in de transportweg zitten.

Het bericht zal echter bij opaque signing in het geheel niet gelezen kunnen worden door iemand die niet over de juiste software beschikt. Dat is een onbedoeld en ongewenst effect, omdat het doel van signing niet is het verbergen van de inhoud van het bericht.

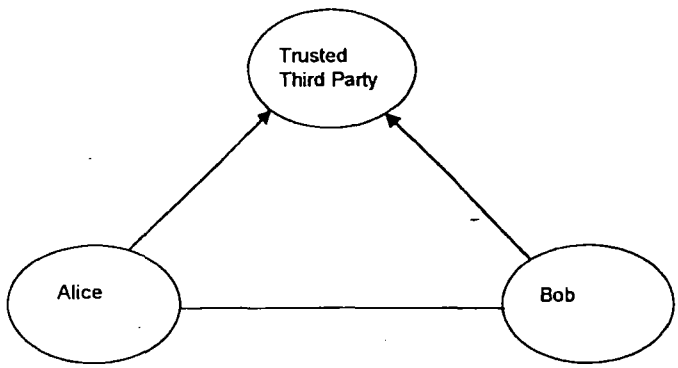
23. Vertrouwen

23.1 Algemeen

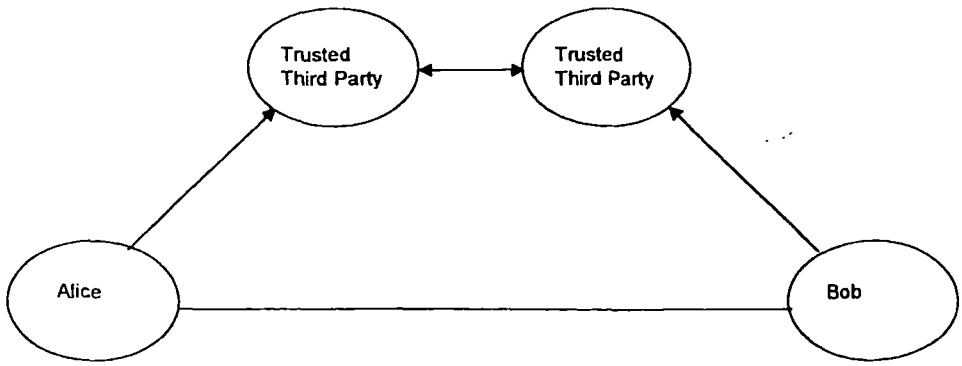
In een vorig hoofdstuk over digitale handtekening hebben we al gezien dat het niet voldoende is als een iemand een digitale handtekening produceert of als iemand zijn publieke sleutel publiceert. Degene die de publieke sleutel gebruikt of iemands digitale handtekening wil kunnen vertrouwen, dient een of andere manier te hebben om er zeker van te zijn dat die sleutel of handtekening ook echt van de persoon afkomstig is die zegt de sleutel uitgegeven te hebben.
Ruwweg staan voor de realisatie van dat vertrouwen twee methodes ter beschikking: een web van vertrouwen en hiërarchisch vertrouwen.

23.2 Hiërarchisch vertrouwen

Bij hiërarchisch vertrouwen wordt het vertrouwen dat in een digitale handtekening wordt gesteld, ontleend aan een "hogere" autoriteit, die de handtekening van de persoon in kwestie voorzien heeft van de handtekening van de autoriteit. Een dagelijks voorbeeld daarvan kennen we allemaal: paspoort en rijbewijs zijn voorbeelden van documenten die iemands identiteit aantonen. Het vertrouwen daarin wordt gewaarborgd doordat de overheid deze documenten afgeeft. Maar net als bij een paspoort of rijbewijs de mogelijkheid van misbruik bestaat, is dat bij gebruik van digitale handtekeningen ook niet helemaal uit te sluiten. Een afzender kan slordig met zijn handtekening omgaan en deze onvoldoende beveiligen, een virus kan speciaal ontworden zijn om de bescherming van de handtekening te doorbreken door een eventueel in te geven password op te vangen. Kortom, een gezonde dosis scepsis is ook bij gebruikmaking van digitale technieken wenselijk.



De hiërarchische vorm van vertrouwen kunnen we schematisch als volgt weergeven
Hier is Alice's digitale handtekening gewaarmerkt, gecertificeerd, door een Trusted third party.
Omdat Bob die TTP ook vertrouwt, vertrouwt hij daardoor ook berichten die van Alice afkomen voorzien van haar gecertificeerde handtekening.



23.4Wat zijn certificaten

Certificaten zijn, in de digitale wereld, de lakzegels die soms op documenten werden geplakt om de echtheid te waarborgen. Een certificaat waarborgt dat de digitale handtekening bij een bepaalde persoon hoort.
Alice's sleutel was in het voorbeeld van hiërarchische vertrouwen gecertificeerd door een CA[10], een "certificate authority", een (erkende) uitgever van certificaten.
In de praktijk gaat dat bijvoorbeeld als volgt:

1. Iemand besluit dat hij een certificaat nodig heeft om gesigneerde e-mail te kunnen versturen;
2. Hij genereert een sleutelpaar en stuurt de publieke sleutel naar de CA (dit gebeurt in het algemeen door de browser);
3. De CA tekent de sleutel en stuurt deze terug naar de afzender terwijl de CA gelijktijdig of eerder al maatregelen treft om zich te vergewissen van de identiteit van de aanvrager bijvoorbeeld:

- door de getekende sleutel aangetekend per floppy disk (in handen) te versturen of;
- door de aanvrager naar kantoor te laten komen met legitimatiebewijs of;
- door de aanvrager een e-mail te sturen met daarin de referentie waar het certificaat opgehaald kan worden;

4. de aanvrager;

- ontvangt de floppy disk van de postbode nadat hij zich gelegitimeerd heeft of;
- vervoegt zich bij het kantoor van de CA en neemt, na legitimatie, de floppy disk met zijn certificaat in ontvangst;
- ontvangt het e-mail bericht (dit is ook een vorm van identificatie) en haalt de publieke sleutel op.

5. De aanvrager kan nu het certificaat gebruiken om gesigneerde e-mail te versturen.

Welke techniek voor signing in e-mail toegepast wordt, wordt in het hoofdstuk "het praktische gebruik van encryptie en signing in e-mail" uiteengezet.

[10] Een CA is de authoriteit die in dit geval instaat voor de echtheid van de door haar verstrekte sleutel. Een CA beschikt minimaal ook over een Certification Policy waar degenen die de uitgereikte sleutels vertrouwd onder andere kan inzien welke waarborgen de CA biedt.

24. Het praktische gebruik van encryptie en signing in e-mail

24.1 Algemeen

In de vorige hoofdstukken zijn allerlei algemeenheden omtrent vercijferen en signeren van e-mail behandeld. Het wordt tijd eens te bezien hoe de hedendaagse standaarden en bijna standaarden die binnen e-mail gebruikt kunnen worden, omgaan met vercijfering en encryptie.
In het algemeen onderscheiden we twee methodes om beveiligde e-mail te realiseren: met S/MIME [12] en met (Open)PGP. De huidige versie van de S/MIME standaard is versie 2, aan versie 3 wordt gewerkt.
Bij het leggen van de laatste hand aan dit document (27 mei 1999) is S/MIME versie 3 nog niet af en nog niet gepubliceerd als RFC [13] hoewel dat een kwestie van weken is.
Een ieder die op dit moment beweert werkende S/MIME versie 3 implementaties te hebben dient met enig wantrouwen bekeken te worden omdat last minute veranderingen nog mogelijk zijn.

De elementen die van belang zijn bij de beoordeling van een techniek voor beveiligde e-mail zijn:
1. het hashing-algorithme: hoe wordt een "controle op echtheid" uitgevoerd;
2. het signeren: met welke techniek wordt de digitale handtekening gezet;
3. encryptie: wat wordt gebruikt om tekst om te zetten in versleutelde-tekst;
4. sessie: hoe wordt de symmetrische sleutel voor encryptie beschermd en geschikt gemaakt voor verzending.

24.2 Wat wordt gebruikt in S/MIME versie 2

Hashing: SHA-1 of MD5.
Signing: RSA met een 512 of 1024 bits lange sleutel
Encryptie: RC2 met een 40 bits sleutel (Europa) of 128 bits (US en Canada) danwel TripleDES (VS en Canada)
Sessie: RSA met 512 of 1024 bits sleutel

Opmerkingen
Een geheime sleutel van 40 bits lengte is volstrekt onvoldoende om vercijferde tekst te beschermen. Er zijn echter producten die als plug-in voor bijvoorbeeld Microsoft Exchange en Outlook leverbaar zijn, waarbij voor het vercijferen gebruik gemaakt wordt van TripleDES of RC2-128 bits.

---

[12] De afkorting staat voor Secure MIME. MIME is het mail-formaat dat het mogelijk maakt op eenvoudige manier gecompliceerde inhoud via e-mail te versturen, dus bijvoorbeeld tekstverwerkingsdocumenten inclusief opmaak. De toevoeging Secure betekent dat van een aanvullende standaard gebruik wordt gemaakt om de berichten te beveiligen.
[13] In het Internet is het gebruikelijk standaarden of voorgestelde standaarden te publiceren on der de titel RFC (Request For Comment)

25. Conclusie

De conclusie over het praktische gebruik is niet eenduidig. Aan de S/MIME v2 kant is 40 bits encryptie onvoldoende en 128 bits voldoende (maar niet beschikbaar voor iedereen). De infrastructuur rondom S/MIME met certificerende instanties is zich goed aan het ontwikkelen; aan de andere kant biedt PGP voldoende bescherming voor iedereen, maar schaalt het vertrouwensmodel niet. Het opzetten van een aparte vertrouwens infrastructuur voor PGP uitsluitend ten behoeve van e-mail naast een vertrouwensstructuur voor certificaat-georiënteerde toepassingen (wat veel breder is dan e-mail) lijkt nou ook niet direct voor de hand te liggen.
De markt is nog volop in beweging:

- OpenPGP is pas sinds enkele maanden een standaard;
- de afronding van S/MIME v3 vindt waarschijnlijk in het tweede kwartaal van 1999 plaats;
- OpenPGP zal in de volgende versies (er wordt niet verteld welke versie) met X.509 certificaten kunnen omgaan;
- Grote spelers op de markt zetten veel resources op S/MIME.

Hoe echter exportproblemen rondom S/MIME versie 3 opgelost zullen gaan worden, dat is nog geheel onduidelijk. Voor de overheid speelt dit echter geen rol omdat versies van de betreffende software met sterke encryptie eenvoudig te verkrijgen zullen zijn.

De berichten zien er voor iemand die geen S/MIME mail client heeft als volgt uit:

Bericht 1:

```
Return-Path: <[redacted]@Stelvio.nl>
X-Internal-ID: 36B83BEC000010CB
Received: from haddock (192.87.119.110) by passo.stelvio.nl (NPlex 2.0.108) for
smimetest@stelvio.nl; 22 Feb 1999 17:05:06 +0100
From: "[redacted]" <[redacted]@Stelvio.nl>
To: <smimetest@stelvio.nl>
Subject: deze boodschap is signed met Milsecure van Baltimore technologies
Date: Mon, 22 Feb 1999 17:06:44 +0100
Message-ID: <001b01be5e7d$57427a50$6e7757c0@haddock.molensloot.nl>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_001C_01BE5E85.B906E250"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook 8.5, Build 4.71.2173.0
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.3110.3

This is a multi-part message in MIME format.

------=_NextPart_000_001C_01BE5E85.B906E250
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_001C_01BE5E85.B906E250
Content-Type: application/x-pkcs7-mime;
    name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="smime.p7m"

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAaCAJIAEggFfQ29u
dGVudC1UeXBlOiBOZXh0L3BsYWluDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiBxdW90ZWQt
cHJpbnRhYmxlDQpDb250ZW50LURpc3Bvc2l0aW9uOiBpbmxpbmUNCg0KRGUgdGVrc3QgdmFuIGRl
emUgYm9vZHNjaGFwIGlzIG9wZ2VzdGVsZCBvbSBoZXQgdmVyc2NoaWwgdHVzc2VuPTIwDQpjbGVh
ciBlbiBvcGFxdWUgc2lnbmluZyB0ZSBpbGxlc3RyZXJlbi4gRGF0IGlzIHZvb3JhbCB2YW4gYmVs
YW5nDQphbHMgZWVuIGJlcmljaHQgZ2VsaWprdGlqZGlnIGdlc3R1dXJkIHdvcmR0IG5hYXIgcGVy
c29uZW4gZGllIHdlbA0KZW4gZGllIG5pZXQgb3ZlciBTL01JTUUgdm9vcnppZW5pbmdlbiBiZXNj
aGlra2VuAAAAAAAAoIIFkjCCAsUwggIuoAMCAQICBDbRe+cwDQYJKoZIhvcNAQEFBQAwgYsxCzAJ
MjIyMTU0NzAxWhcNMDAwMjIyMTU0NzAxWjCBizELMAkGA1UEBhMCTkwxFDASBgNVBAoUC00mSS9T
VEVMVklPMREwDwYDVQQLEwhkaXJlY3RpZTETMBEGA1UEAxMKQmVydCBTdGFsczEkMCIGCSqGSIb3
DQEJARYVQmVydC5TdGFsc0BTdGVsdmlvLm5sMRgwFgYDVQQUEw8rMzEgMzMgNDIyMCAzNDAwgZ8w
```