Technische beveiligingsstudie Encryptie

Technische beveiligingsstudie Encryptie

PI/DO
Platform Informatiebeveiliging
Werkgroep Encryptie

Figuur 0.1 Informatiebeveiligingspiramide

Uitgeverij LEMMA BV – Utrecht – 2002

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden auteur(s), redactie en uitgever geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

Ondanks de nodige nasporingen bleek het niet mogelijk van alle opgenomen illustraties de bezitter van het copyright te achterhalen. Eventuele rechthebbenden die niet voor deze uitgave zijn benaderd, worden verzocht zich met de uitgever in verbinding te stellen.

ISBN 90 5931 113 2
NUR 980

http://www.lemma.nl
infodesk@lemma.nl

Omslagontwerp en typografie: Twin Design BV, Culemborg

Voorwoord

Het Platform Informatiebeveiliging (PI) heeft als doel 'het bevorderen van de beveiliging van alle belangen betreffende gegevensverwerking, -opslag en -transport, alles in de ruimste zin van het woord'. Binnen deze doelstelling wordt het ontwikkelen van aanvaardbare richtlijnen voor de praktische inrichting van informatiebeveiliging als essentieel onderwerp gezien. Door het gezamenlijk opstellen van dergelijke richtlijnen kan worden gebruikgemaakt van praktijkervaringen, zodat een doeltreffende richtlijn ontstaat die ook uitvoerbaar is.

De PI-richtlijnen worden in werkgroepverband ontwikkeld onder auspiciën van een bestuurslid in de rol van projectleider. Deze ziet er onder meer op toe dat de PI-kwaliteitsrichtlijnen door de werkgroep worden gehandhaafd. De deelnemers van de werkgroepen zijn primair afkomstig uit de organisaties die aangesloten zijn bij PI, maar niet uitsluitend. Het betreft beveiligingsfunctionarissen en IT-auditors van uiteenlopende bedrijven en instellingen. Zij hebben allen gemeen dat zij in hun advies- en controlewerkzaamheden zeer hoge eisen moeten stellen aan organisaties in verband met de sterke automatiseringsgraad en de belangen die met de geautomatiseerde informatievoorziening zijn gemoeid. Door deze achtergrond vormen de deelnemers een representatieve afspiegeling van de aanwezige IT-beveiligingsexpertise in Nederland. Aldus kan aan de door hen ontwikkelde richtlijnen voldoende gezag worden verleend, hetgeen bevorderlijk is voor de acceptatie door het algemene en het IT-management.

De PI-beveiligingsrichtlijnen zijn primair bedoeld voor functionarissen die zijn belast met het implementeren van IT-systemen, zoals systeembeheerders en technische ontwerpers en bouwers.

Daarnaast zijn de richtlijnen van betekenis voor de volgende doelgroepen:

- IT-beveiligingsfunctionarissen (*security officers* en *administrators*). De IT-beveiligingsfunctie binnen een organisatie is verantwoordelijk voor het (doen) treffen van beveiligingsmaatregelen. De richtlijnen bieden hierbij ondersteuning;
- IT- en algemeen management. Het management is (eind)verantwoordelijk voor de informatiebeveiliging en geeft hieraan invulling door het (doen) analyseren van risico's en het bepalen van (globale) beveiligingsdoelstellingen. De beargumenteerde keuzen en de managementsamenvatting in de richtlijnen zijn hierbij een handvat;
- IT-auditors. De richtlijnen geven – gemotiveerd – de vereiste beveiligingsmaatregelen aan en de risico's, wanneer niet aan de vereisten is voldaan. Hierdoor kunnen de richtlijnen ook worden gehanteerd als toetsingsnorm bij IT-audits.

Aldus bieden de richtlijnen een handreiking aan beveiligingsfunctionarissen en het algemene en IT-management om een toereikende en evenwichtige beveiliging van de informatievoorziening te implementeren. Daarnaast bieden zij aan IT-auditors een basis voor de normstelling, die nodig is om de beveiliging van een IT-systeem te kunnen beoordelen.

Aan deze studie hebben de volgende personen en organisaties hun medewerking verleend:
Dr.ir. P.J.M. Veugen, TNO-FEL
M.W. Baurichter RE, KPMG Information Risk Management
Ir. A.W.J.M. Donkers, Le Reseau
Ir. B.M.P. Giesbers, Defensie Telematica Organisatie
Ing. T.G.A. van Rhee, EDP AUDIT POOL
Ing. J. van der Spek MSc, Verdonck, Klooster & Associates
Drs.ing. W.N.B. Tewarie RE, UWV, Accountantsdienst
Drs. S. Vos, Deloitte & Touche ERS
B. Bokhorst RE RA, Belastingdienst, Centrum voor ICT
Drs. G.J.C. van den Brink-Heikamp RE, zelfstandig gevestigd

Dank voor hun constructieve bijdragen in de reviewfase van de studie is verschuldigd aan:
A. Koot RE, Belastingdienst, Centrum voor ICT
G. Hulst, KPN Audit
W. van Eikenhorst, HBG NV

Inhoud

Inleiding

De integratie van automatisering met de bedrijfsprocessen en de complexiteit van automatiseringsoplossingen nemen steeds verder toe. Daarom dient er voortdurend aandacht te zijn voor zowel het vereiste niveau van informatiebeveiliging als de technische realisering hiervan. Ook gezien de ontwikkelingen op het gebied van wet- en regelgeving met betrekking tot informatiebeveiliging is deze aandacht noodzakelijk. Objectivering van het vereiste niveau van informatiebeveiliging en van de effectiviteit van gekozen technische oplossingen is voor veel organisaties een probleem, doordat slechts in beperkte mate standaarden voorhanden zijn. Beschikbare standaarden kennen ofwel een te beperkt werkingsgebied, of richten zich te veel op de organisatorische kant van de informatiebeveiliging. Door het gebrek aan deugdelijke standaarden zijn organisaties gedwongen zelf oplossingen te ontwikkelen en hierin veel energie te steken. De gevolgen zijn suboptimale oplossingen, verspilling doordat vele malen opnieuw het wiel moet worden uitgevonden en moeizame acceptatie door de afwezigheid van geobjectiveerde criteria.

Tegen deze achtergrond is het initiatief ontstaan om in werkgroepverband concrete, geobjectiveerde richtlijnen te ontwikkelen voor de inrichting respectievelijk de beoordeling van technische beveiligingsmaatregelen. Deze aanpak heeft de volgende voordelen:

– door uitwisseling van kennis, ervaring en inzicht ontstaat een belangrijk synergie-effect tussen de deelnemers; de deelnemers kunnen elkaar ondersteunen bij de keuze en implementatie van beveiligingsmaatregelen;
– met behulp van de ingebrachte kennis en inzichten kan worden gekomen tot de vaststelling van technische beveiligingsrichtlijnen die op een breed draagvlak kunnen rekenen;

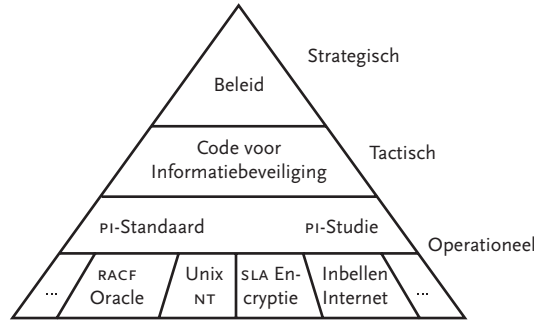
– toepassing van de opgestelde beveiligingsrichtlijnen leidt bij de betrokken organisaties tot een verhoging van de effectiviteit van de beveiliging.

De technische beveiligingsmaatregelen die in de richtlijnen worden beschreven, vormen een onderdeel van het gehele samenstel van beveiligingsmaatregelen om de kwaliteit van de geautomatiseerde informatievoorziening te waarborgen. Beveiligingsmaatregelen binnen deze bredere context zijn bijvoorbeeld beschreven in de publicatie 'Code voor Informatiebeveiliging, een Standaard voor Beleid en Implementatie[1]'. Deze Code, die vooral in het bedrijfsleven wordt gebruikt, richt zich in het bijzonder op het tactische niveau binnen organisaties en bestrijkt het gehele terrein van informatiebeveiliging. Door het abstractieniveau geeft de Code echter weinig concrete handvatten voor het implementeren van beveiligingsmaatregelen bij IT-systemen. Hetzelfde geldt voor het besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR)[2], dat voor de rijksoverheid van toepassing is.

De PI-richtlijnen kunnen dan ook worden beschouwd als een verdere uitwerking van de Code en de baselinebeveiliging van het besluit VIR en zijn vooral gericht op het operationele niveau binnen organisaties. Daarnaast kan nog een strategisch niveau worden onderkend, dat betrekking heeft op de eindverantwoordelijkheid voor informatiebeveiliging van het topmanagement. De samenhang tussen deze drie niveaus is schematisch weergegeven in figuur 1.

1 De Code voor Informatiebeveiliging is een uitgave van het Nederlands Normalisatie-instituut, mogelijk gemaakt door het ministerie van Economische Zaken in samenwerking met een groep toonaangevende bedrijven en organisaties in Nederland.

2 Het besluit Voorschrift Informatiebeveiliging Rijksdienst 1994 is uitgegeven door het ministerie van Binnenlandse Zaken in samenwerking met een begeleidingsgroep waarin alle ministeries en enkele toonaangevende organisaties waren vertegenwoordigd.



Figuur 1 Informatiebeveiligingspiramide

Aangezien over het tactische niveau van informatiebeveiliging en over de beleidsmatige en organisatorische maatregelen die op het strategische en tactische niveau moeten worden getroffen, al veel literatuur voorhanden is, wordt hierop in de PI-richtlijnen niet nader ingegaan. Het uitgangspunt van de PI-richtlijnen is dat op dit gebied voldaan is aan de Code voor Informatiebeveiliging en vergelijkbare standaarden. Dit houdt in dat er een beveiligingsbeleid is, dat er functiescheiding is tussen ontwikkeling en productie, enzovoort.

Bij de implementatie van een product of architectuur moet een evenwicht worden gevonden tussen risico's en daarmee samenhangend beveiligingsniveau, gebruikersgemak, invoerings- en beheerkosten en gevolgen voor de prestaties van het systeem. De richtlijnen bieden hierbij een praktische leidraad, doordat beargumenteerd wordt aangegeven waarom bepaalde keuzen zijn gemaakt. Door deze aanpak kunnen organisaties de vertaalslag maken naar hun eigen specifieke omstandigheden.

PI-beveiligingsrichtlijnen

De beveiligingsrichtlijnen die in PI-verband zijn en worden ontwikkeld, betreffen de technische maatregelen en voorzieningen die moeten worden getroffen ter waarborging van de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens die met een IT-systeem worden opgeslagen, verwerkt en/of getransporteerd.
De richtlijnen geven dus aan hoe de (beveiligings)functies van een IT-systeem die relevant zijn voor de genoemde kwaliteitsaspecten, moe-

ten worden ingesteld. Zij bevatten tevens aanwijzingen voor de organisatorische inbedding hiervan, maar primair gaat het om de techniek. Met de richtlijnen wordt vooral beoogd te bevorderen dat de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens in voldoende mate zijn gewaarborgd. Dat wil niet zeggen dan andere kwaliteitsaspecten, zoals efficiëntie (bedieningsgemak, performance, kostenbeheersing), uit het oog worden verloren. Juist door de inbreng vanuit de praktijk wordt gestreefd naar een optimaal evenwicht tussen beveiligingsniveau en praktische realiseerbaarheid. De richtlijnen vormen de neerslag van de gezamenlijke kennis, inzichten en praktische ervaringen van de werkgroep- en PI-leden.

De richtlijnen kunnen betrekking hebben op elke component van de IT-infrastructuur in de breedste zin van het woord (aangeduid als IT-systeem). De IT-infrastructuur betreft het geheel van apparatuur, besturings- en hulpprogrammatuur, faciliteiten voor data-, spraak- en videocommunicatie, alsmede de fysieke beveiligingsfaciliteiten van de geautomatiseerde informatievoorziening. Ook generieke toepassingen en diensten (zoals e-mail en file transfer) vallen onder dit begrip IT-systeem.

De beveiligingsrichtlijnen van PI vallen uiteen in twee categorieën:

1 *PI-standaarden*. PI-standaarden zijn technische implementatiehandleidingen voor concrete objecten (IT-producten), bijvoorbeeld een besturingssysteem van een bepaalde leverancier en een bepaalde versie;
2 *PI-studies*. PI-studies zijn technische beveiligingshandleidingen voor objecttypen, bijvoorbeeld een bepaalde categorie besturingssystemen, generieke IT-architecturen, bijvoorbeeld een *firewall*, internetverbinding of inbelfaciliteit, generieke diensten, bijvoorbeeld directory services en dergelijke.

Bij nieuwe versies van producten en bij nieuwe technologische of maatschappelijke ontwikkelingen bestaat er behoefte aan vroegtijdige risicoinschatting en standpuntbepaling met betrekking tot de invulling van beheer- en beveiligingsaspecten. In die gevallen zijn de richtlijnen meer het resultaat van een researchinspanning dan dat zij – zoals bij bestaande producten en architecturen – zijn gebaseerd op eigen praktische ervaring (*best practice*).

Het te bereiken beveiligingsniveau dient te zijn afgestemd op de waarde van het te beveiligen belang. Aangezien dit voor elke organisatie verschillend zal zijn, zijn de PI-richtlijnen primair gebaseerd op de beveiligingsmogelijkheden van het IT-systeem, dat wil zeggen op het optimaal benutten van de beveiligingsfaciliteiten die het biedt. Dit wordt het beginsel van goed huisvaderschap genoemd. Bij het opstellen van de richtlijnen wordt echter tevens nagegaan aan welk niveau het systeem redelijkerwijs zou moeten voldoen, gegeven de Code voor Informatiebeveiliging en andere gezaghebbende literatuur, de *state of the art* van de beveiligingstechniek, de gemeenschappelijke opvattingen van de werkgroepleden, enzovoort.

Uitgangspunten voor de studie encryptie

Uitgangspunt 1: het uitwerken van beleid voor het toepassen van encryptie valt buiten deze studie.

Encryptie van gegevens is binnen een organisatie een middel en geen doel. Voorzover gebruikers de keuze wordt gegeven om encryptie toe te passen dient binnen een organisatie een beleid te zijn vastgelegd waarin rechten en plichten van gebruikers zijn opgenomen in relatie tot de gegevens die binnen de organisatie worden gebruikt. Voor de juiste inrichting, het gebruik en de beheersing van encryptie is het noodzakelijk dat er reeds voor aanvang van een realisatietraject een beleid aanwezig is waarin de toepassing van cryptografische technieken kan worden ingebed. Een gegevensclassificatie maakt daarvan een belangrijk onderdeel uit. Aangezien deze studie zich richt op het operationele niveau, wordt ervan uitgegaan dat dit beleid is ingevuld.

Uitgangspunt 2: de invloed van specifieke regelgeving wordt in deze studie meegenomen.

Met name bij overheidsorganen kunnen wet- en regelgeving van invloed zijn op de maatregelen die getroffen moeten worden bij zowel vercijferde opslag als transport van gegevens. Om die reden wordt daarop in deze studie apart ingegaan.

Uitgangspunt 3: in deze studie wordt als extra kwaliteitsaspect tevens ingegaan op onweerlegbaarheid.

Naast de algemene kwaliteitsaspecten (vertrouwelijkheid, integriteit en beschikbaarheid) geldt dat door toepassing van encryptie nog een belangrijk kwaliteitsaspect, namelijk de onweerlegbaarheid, kan worden gerealiseerd. Onweerlegbaarheid wordt ook wel aangeduid als onloochenbaarheid of non-repudiation. Encryptie vervult bij de invulling van dit kwaliteitsaspect een essentiële rol.

Uitgangspunt 4: naast operationele beveiligingsnormering wordt in deze studie speciale aandacht besteed aan selectiecriteria voor de keuze van encryptietoepassingen.

Deze studie heeft niet de pretentie om voor het proces van totstandkoming van encryptietoepassingen beveiligingsnormen uit te werken. PI-studies en -standaarden richten zich namelijk op normering van de beveiligingsaspecten van de operationele bedrijfsvoering. Doordat encryptie-oplossingen vaak slechts een onderdeel uitmaken van de ingezette IT-middelen, is het de vraag of er in het proces van totstandkoming wel voldoende aandacht is geweest voor een goede selectie van encryptiemogelijkheden gezien de af te dekken risico's en bijvoorbeeld de vereiste beheerinspanningen. Gegeven de keuze van de encryptiemiddelen blijkt dat het niet mogelijk of zinvol is op generiek niveau, dat wil zeggen zonder diep in te gaan op specifieke producten, uitspraken te doen over beveiligingsinstellingen, die vragen om normering. Om die reden hebben wij extra aandacht besteed aan de keuzecriteria voor het inzetten van encryptiemiddelen.

Leeswijzer

In het eerste hoofdstuk is de managementsamenvatting opgenomen. In hoofdstuk 2 worden de basisbegrippen van encryptie beschreven die in de volgende hoofdstukken gebruikt worden. De selectiecriteria voor de toepassing van encryptie komen in hoofdstuk 3 aan de orde. Hoofdstuk 4 gaat over het gebruik van encryptie tijdens communicatie. Daarbij wordt ingegaan op het gebruik van encryptie in een drietal netwerklagen. Het gebruik van encryptie voor gegevensopslag wordt in hoofdstuk

5 toegelicht. Het beheer van encryptie, zowel tijdens communicatie als opslag, is het onderwerp van hoofdstuk 6. Het laatste hoofdstuk gaat in op de toekomstige ontwikkelingen rond encryptie.

1 Managementsamenvatting

Het is goed om te beseffen dat encryptie geen wondermiddel is, dat bijna alle beveiligingsproblemen kan oplossen. Het toepassen van encryptie kan net als andere beveiligingsmiddelen een bijdrage en in sommige situaties zelfs een essentiële bijdrage leveren aan het verhogen van het beveiligingsniveau. Het gaat hierbij dan om de aspecten vertrouwelijkheid, integriteit, beschikbaarheid en onweerlegbaarheid. Het gebruik van encryptie stelt echter zijn eisen aan de beheer- en gebruikersorganisatie en heeft ook gevolgen voor de werking van andere onderdelen van de IT-systemen. Vandaar dat het inzetten van encryptiemiddelen vraagt om een goed afgewogen keuze, waarbij recht wordt gedaan aan alle aspecten die bij deze keuze van toepassing zijn.
In deze studie worden richtlijnen beschreven voor het toepassen van encryptie in IT-systemen. Daarbij wordt ervan uitgegaan dat het beveiligingsbeleid van organisaties die deze richtlijnen willen gebruiken, hiervoor voldoende uitgangspunten verschaft. Met name de gegevensclassificatie zou hierop moeten inspelen.
Om encryptie effectief in een organisatie te kunnen toepassen is enige cryptografische kennis van zaken noodzakelijk. Met name het onderscheid tussen symmetrische en asymmetrische algoritmen is van belang om de gevolgen hiervan voor beheer en organisatie te kunnen inschatten. Hierop geven wij in deze studie een korte toelichting.

Bij PI-studies en -standaarden staat het streven centraal om een zo compleet mogelijke set basisnormen en -maatregelen uit te werken. De werkgroep heeft in dit geval extra aandacht besteed aan het positioneren van de encryptiemiddelen op de technische infrastructuur en het systematisch inventariseren van de impact die dit heeft voor beheer en beveiliging. Naast het leveren van een bijdrage aan de begripsvorming

omtrent de betekenis van encryptie, wordt daarmee ook een handvat aangereikt om bewuste keuzen te maken bij het inzetten van encryptiemiddelen.

In de studie wordt onderscheid gemaakt naar het gebruik van encryptie bij de opslag van gegevens en het gebruik van encryptie tijdens de communicatie. Deze twee methoden kunnen en worden in de praktijk naast elkaar toegepast, afhankelijk van de doelstellingen die men voor beveiliging nastreeft. Bij encryptie tijdens communicatie wordt een verdere onderverdeling gemaakt in drie verschillende lagen, te weten: applicatie-, netwerk- en datalinkniveau. Binnen deze lagen wordt ingegaan op de meest voorkomende standaarden en producten. Wij sluiten elk onderdeel af met een samenvattend overzicht in tabelvorm.

Voor het gebruik van encryptie bij de opslag van gegevens gaan wij in op de regelgeving die van invloed kan zijn op de toepassing van encryptie. Voor een goede positionering van de impact van encryptie hanteren wij een indeling naar: organisatie, gebruiker, applicatie en (besturings)systeem. Gaat het bij encryptie tijdens communicatie om invulling van de beveiligingsaspecten vertrouwelijkheid, integriteit en (in sommige gevallen) authenticatie en onweerlegbaarheid, bij encryptie tijdens de opslag wordt daarnaast ook ingegaan op het beschikbaarheidsaspect, omdat dit extra eisen stelt aan het beheer.

Het gebruik van encryptie en daarmee de effectiviteit van de hiermee te bereiken beveiliging staat en valt met een goed ingericht beheer van de *cryptografische sleutels*. Het sleutelbeheer wordt in deze studie uitgewerkt. De verschillende activiteiten, die bij dit beheer aan de orde zijn, worden toegelicht. Daarbij worden functiescheidingen aangegeven en krijgt bewustwording bij gebruikers een bijzonder accent.
In het algemeen zullen voor encryptie tijdens communicatie eerder *asymmetrische sleutels* gebruikt worden (voor authenticatiedoeleinden), en voor encryptie tijdens opslag *symmetrische sleutels* (in verband met de snelheid van verwerking). Hoewel de inrichting van het beheer van beide typen sleutels vergelijkbaar is, is er voor het beheer van asymmetrische sleutels een aantal extra activiteiten nodig. Dat geldt in nog sterkere mate voor het sleutelbeheer, als het organisatie- en serversleutels betreft.

Asymmetrische sleutels worden aan gebruikers meestal ter beschikking gesteld in de vorm van certificaten. Voor dit certificatenbeheer is een *Public Key Infrastructure* noodzakelijk. Vanwege het toenemend belang van dit onderwerp hebben wij hieraan een aparte sectie gewijd.

Het toepassen van encryptie wordt sterk bevorderd door de ontwikkelingen rond e-commerce. Daarbij tekenen zich duidelijke trends af op het gebied van te gebruiken toekomstige protocollen of diensten. Deze behandelen wij in het laatste hoofdstuk.

2 Basisbegrippen

2.1 Cryptografie

De geschiedenis zijn tal van geheime codes ontworpen, en diezelfde codes ook weer gekraakt. Met het behouden blijven van een code werd een oorlog gewonnen of verloren. Door het spel van het bedenken en breken van codes worden steeds betere en ingewikkeldere vercijferingen bedacht en vervolgens ook weer gekraakt.
De wetenschap van geheime communicatie, ook wel cryptografie geheten, is van oudsher een militaire wetenschap, bedoeld om communicatie geheim te houden voor de vijand. Zij gaat echter nu meer en meer een rol spelen in het leven van alledag. Het feit dat cryptografie is ontstaan vanuit de militaire toepassing heeft ertoe geleid dat veel belangrijke onderzoeken en uitvindingen (en de uitvinders ervan) op het gebied van cryptografie geheim waren en daardoor onbekend zijn gebleven of blijven.
Cryptologie is de studie van geheime communicatie en omvat cryptografie en cryptanalyse: de wetenschap om de cryptografie te kraken.

Doordat informatie een steeds waardevoller gebruiksgoed wordt, wordt ook het proces van het vercijferen van berichten, ook wel *encryptie* genoemd, steeds belangrijker. *Decryptie* is het tegenovergestelde van encryptie: het proces waarin de vercijferde tekst weer wordt omgezet in leesbare tekst.
Nu onze e-mails nog gemakkelijker onderschept kunnen worden dan mobiele telefoongesprekken en bovendien steeds meer zaken over het internet geregeld worden, komt onze privacy in gevaar. Dit effect wordt versterkt door de opkomst van web-winkels. Om bedrijven en hun klanten tegen deze inbreuk op hun privacy te beschermen, kan gebruik worden gemaakt van encryptie.

Hoewel in de zakenwereld de vraag naar cryptografie steeds groter wordt, brengt deze ontwikkeling ook veel zorgen met zich mee voor bijvoorbeeld de politie. Deze kan haar afluisterapparatuur niet meer gebruiken om de nationale veiligheid te waarborgen. Door in de wetgeving ook het gebruik van encryptie op te nemen, zoals bijvoorbeeld in de Europese richtlijn 99/93/EG, kan wellicht een compromis gevonden worden.

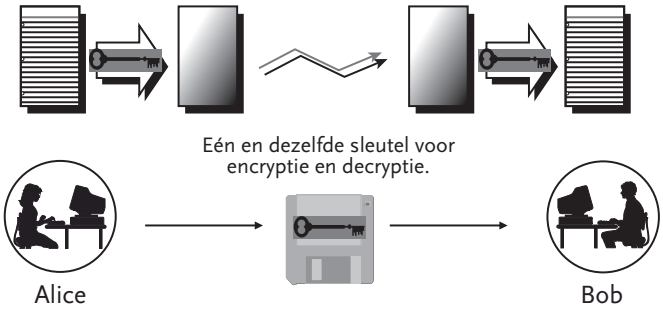
Waar men vroeger slechts letters gebruikte voor de oorspronkelijke tekst en voor de gecodeerde tekst, gebruikt men tegenwoordig computers en getallen. De gewone tekst vóór vercijfering heet nu *plain text,* en die na vercijfering heet *cipher text*.
Hoe wezenlijk het verschil tussen de tijd voor en na de invoering van de computer ook is, cryptografie maakt nog steeds gebruik van substitutie en transpositie. Hierbij worden elementen van de boodschap vervangen door andere elementen, of veranderen deze elementen van plaats of er wordt een combinatie van beide gebruikt. Bij cryptografie wordt gebruikgemaakt van een algoritme: een wiskundige functie of groep van regels die gebruikt wordt in het proces van data-encryptie en -decryptie.

2.2 Symmetrische en asymmetrische encryptie

De twee vormen waarin encryptie tegenwoordig gebruikt wordt, zijn symmetrische en asymmetrische encryptie. Symmetrische encryptie maakt gebruik van een enkelvoudig sleutelsysteem waarbij dezelfde geheime sleutel (*secret key*) wordt gebruikt voor encryptie en decryptie.
De meest bekende symmetrische encryptievormen zijn: DES, 3DES, RC2, RC4, RC5. Asymmetrische encryptie, ook wel public key encryptie of encryptie met een asymmetrisch algoritme genoemd, is een 'twee-sleutel'-systeem dat een complementair sleutelpaar gebruikt: een publieke sleutel en een privé-sleutel. De publieke sleutel wordt gebruikt om boodschappen te vercijferen bij verzenden en digitale handtekeningen te verifiëren bij ontvangst. De privé-sleutel gebruikt men om boodschappen te ontcijferen bij ontvangst en deze van een elektronische handtekening te voorzien bij het verzenden. Een voorbeeld van asymmetrische encryptie is RSA. Aan beide vormen van encryptie zijn voor- en nadelen verbonden die verderop in hoofdstuk 3 kort worden beschreven.

2.2.1 Symmetrische encryptie

Symmetrische encryptie werkt zoals aangegeven in figuur 2.1. Het symmetrische aspect heeft betrekking op de gelijkheid van encryptiesleutel en decryptiesleutel.



Figuur 2.1 Symmetrische encryptie

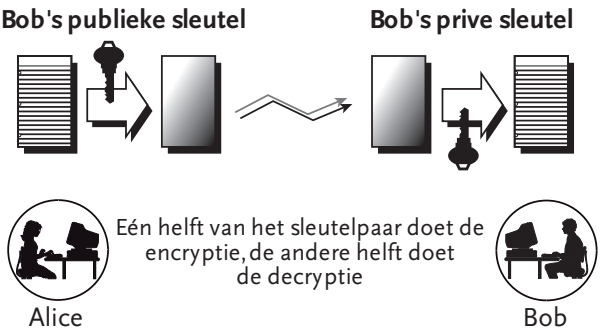
Een voorbeeld van symmetrische encryptie is DES (*Data Encryption Standard*). DES is ontwikkeld in de jaren zeventig door IBM en werd de standaard encryptiemethode voor de overheid van de Verenigde Staten in 1976. DES gebruikt een 56 bit key en ieder 56-bit getal kan worden gebruikt als sleutel; het algoritme is openbaar en dus gratis te gebruiken. DES is algemeen bekend in zowel hard- als softwareversies en is makkelijk te gebruiken, omdat ook de ontvanger het vaak al in gebruik heeft.
De DES-methode is enigszins achterhaad en wordt niet langer als veilig gezien. De opvolger, Triple DES, waarbij data drie keer worden vercijferd met twee of drie verschillende sleutels, wordt veel gebruikt in de financiële wereld.

In 1998 maakte de Electronic Frontier Foundation haar DES cracker project bekend. De EFF had dit project speciaal ontwikkeld en gefinancierd om DES te kunnen kraken. De overheid van de Verenigde Staten zocht daarna naar een nieuwe encryptiestandaard; de AES (Advanced

Encryption Standard). AES is een publiek algoritme bedoeld om de gevoelige overheidsinformatie van de Verenigde Staten te beschermen. Rijndael uit België is inmiddels door de overheid van de Verenigde Staten gekozen als nieuwe encryptiestandaard.

2.2.2 Asymmetrische encryptie

Bij asymmetrische encryptie worden twee sleutels gebruikt: één voor de encryptie, de andere voor de decryptie. De twee sleutels hebben een mathematisch verband. Dit betekent dat één sleutel geheim gehouden moet worden (zoals bij DES) maar dat de andere sleutel aan andere gebruikers beschikbaar kan worden gesteld. Hiermee kan iedereen iemand een vercijferde tekst versturen op basis van de publieke sleutel. De enige manier om de tekst weer leesbaar te maken is gebruik te maken van de privé-sleutel, welke uitsluitend bij de ontvangende partij bekend is.
Wanneer men als voorbeeld de twee partijen Alice en Bob neemt, werkt dit als volgt: als Alice een geheime tekst naar Bob wil sturen, gebruikt Alice de publieke sleutel van Bob voor de encryptie. Bob gebruikt zijn privé-sleutel voor de decryptie. Omgekeerd gebruikt Bob de publieke sleutel van Alice om vercijferde tekst naar Alice te sturen.



Figuur 2.2 Asymmetrische encryptie

Bij het gebruik van asymmetrische encryptie waarbij, in tegenstelling tot bovenstaand voorbeeld, de privé-sleutel wordt gebruikt om een bericht te vercijferen, en de publieke sleutel wordt gebruikt om hetzelfde bericht te ontcijferen, kan men ervan uitgaan dat alleen de verzender het bericht heeft kunnen schrijven. Dit maakt de zogenoemde digitale handtekening net zo waardevol als een handgeschreven handtekening. De rechtsgeldigheid van digitale handtekeningen wordt, in navolging op de Europese richtlijn 99/93/EG, binnenkort in de Nederlandse wetgeving opgenomen; in mei 2001 is daartoe een wetsvoorstel ingediend.

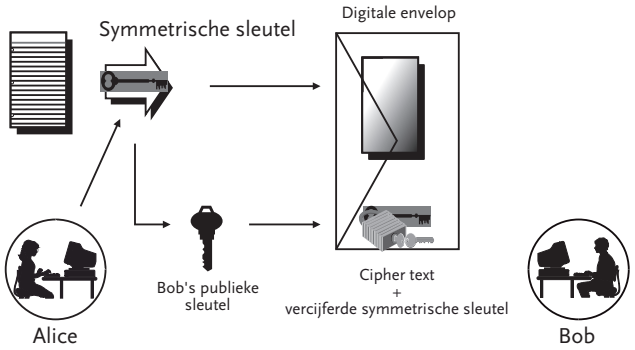
PKI en TTP

Een implementatie die gebruikmaakt van asymmetrische encryptie is PKI (*Public Key Infrastructure*): een publiek beschikbaar systeem om publieke sleutels op een veilige en voorspelbare manier te verkrijgen. De meest gebruikte toepassingen van PKI zijn: veilige e-mail, web-applicaties, *Virtual Private Network* (VPN), sleuteldistributie en e-commerce via webservers.
Whitfield Diffie en Martin Hellman hebben het concept van *Public Key cryptografie* als eerste ontdekt; Ron Rivest, Adi Shamir en Len Adleman ontwikkelden de eerste praktische *Public Key* toepassing. Dit systeem is, naar de uitvinders, RSA genoemd.
Het RSA algoritme is (vrijwel) onmogelijk te kraken, zeker wanneer de sleutellengte anno 2001 voldoende groot (1028 bits) wordt gekozen.

Voor een breed gebruik van publieke sleutels in een omgeving waar de gebruikers elkaar niet kennen, zoals bijvoorbeeld in de elektronische handel, moet men toegang hebben tot een algemeen vertrouwde instantie, een *Trusted Third Party*. Een *Trusted Third Party* (TTP) beheert databases van publieke sleutels in de vorm van certificaten. De certificaten worden opgeslagen nadat de identiteit van de gebruiker onomstotelijk is vastgesteld. De instantie die certificaten digitaal ondertekent en uitgeeft, wordt *Certification Authority* (CA) genoemd.
Meer informatie over PKI, TTP en CA vindt u in sectie 6.4.

2.2.3 Key wrapping

Door de complexiteit van het algoritme is asymmetrische encryptie traag in vergelijking tot symmetrische encryptie. Om die reden is het *key wrapping*-systeem geïntroduceerd, waarbij de grote hoeveelheden data met een symmetrische sessiesleutel (voor het begrip 'sessie' zie Bijlage A, sectie 2) worden vercijferd en uitsluitend de sessiesleutel volgens het asymmetrische principe wordt vercijferd. *Key wrapping* wordt ook wel hybride encryptie genoemd.
Het voorgaande maakt dat het systeem bij communicatie tussen meerdere personen zowel snel als eenvoudig te gebruiken is.



Figuur 2.3 Key wrapping

3 Criteria bij de selectie van encryptietoepassingen

Encryptie kan worden toegepast tijdens communicatie en/of bij opslag. Deze onderwerpen worden in respectievelijk hoofdstuk 4 en 5 behandeld. Vercijfering tijdens communicatie en vercijfering bij opslag kunnen elkaar in veel gevallen aanvullen en sluiten elkaar zeker niet uit.
De *vercijfering tijdens communicatie* heeft als doel de uitgewisselde gegevens te beschermen tegen manipulatie en afluisteren onderweg. Bovendien biedt het de mogelijkheid de communicerende partijen op een betrouwbare manier te authentiseren zodat de herkomst en de bestemming van de uitgewisselde gegevens gegarandeerd zijn.
De uitgewisselde gegevens komen vaak van een database of bestand op een systeem en worden na ontvangst meestal weer opgeslagen. Om ook daar de integriteit en vertrouwelijkheid van de gegevens te waarborgen is de *vercijfering van de opgeslagen gegevens* belangrijk.

Bij de keuze voor een encryptie-oplossing geldt een aantal algemene criteria. Daarnaast zijn er, afhankelijk van de toepassing voor opslag of communicatie, nog specifieke criteria te vermelden.

3.1 Algemene selectiecriteria

Algoritmen

Algoritmen (tezamen met de sleutels) realiseren de vercijfering van data. Het type algoritme (symmetrisch versus asymmetrisch) bepaalt enerzijds een deel van de functionaliteit (vercijfering bestemd voor bescherming van de vertrouwelijkheid of vercijfering bestemd voor authenticatie). Daarnaast bepaalt het algoritme zelf de mate van beveiliging (vertrouwelijkheid/authenticatie) van de data. In onderstaande tabel staan de voor- en nadelen van beide typen algoritmen.

Tabel 3.1 Algoritmen

	Symmetrische algoritmen	**Asymmetrische algoritmen**
Voordelen	– Snelle vercijfer- en ontcijfermethode door een relatief minder rekenintensieve methode en de mogelijkheid om relatief kleinere sleutels te gebruiken. – Veelal transparant voor gebruiker. Door gebruik van slechts één en dezelfde sleutel kan dit vaak in een applicatie worden geïntegreerd. – Relatief kleine sleutellengte is voldoende voor een hoge mate van veiligheid. – Relatief eenvoudig te realiseren in hardware (cryptobox).	– Bij een grote groep gebruikers of systemen blijft het beheer van de sleutels relatief eenvoudig, schaalbaar en beheersbaar. Het aantal benodigde sleutels is recht evenredig met het aantal gebruikers of systemen. Door het public key mechanisme kan de publieke sleutel aan derden worden verzonden zonder verlies van vertrouwelijkheid en authenticiteit. – Kan eveneens worden gebruikt voor het plaatsen en verifiëren van digitale handtekening. – Digitale handtekening krijgt snel een juridisch volwaardige status.
Nadelen	– Bij een grote populatie (gebruikers of systemen) is een relatief groot aantal verschillende sleutels nodig om een voldoende hoog betrouwbaarheidsniveau te behalen. (het aantal sleutels neemt kwadratisch toe met het aantal gebruikers of systemen) – Het beheer en de distributie van deze grote aantallen sleutels (zoals hierboven omschreven) wordt al snel zeer complex. – Door minder rekenintensieve vercijfering heeft een brute-force aanval sneller resultaat dan bij asymmetrische vercijfering.	– Rekenintensieve vercijfering (factor 1000 langzamer dan symmetrische vercijfering). – Extra maatregelen dienen te worden genomen om de authenticiteit van de eigenaar van de publieke sleutel vast te stellen. – Relatief grote sleutellengte noodzakelijk voor een hoge mate van veiligheid.

Van algoritmen die openbaar zijn en al vele malen zijn geëvalueerd, is bekend hoe betrouwbaar deze zijn; van algoritmen die geheim zijn, is dit vaak niet bekend. Deze laatste groep ongepubliceerde algoritmen kan natuurlijk veilig zijn, maar dat kan simpelweg niet worden gecontroleerd. Derhalve verdient het aanbeveling om encryptietoepassingen te selecteren die beschikken over algoritmen die openbaar zijn én die zich bewezen hebben als betrouwbaar.

Sleutellengte

De sleutellengte bepaalt in belangrijke mate de betrouwbaarheid van de vercijfering. Een algoritme met een door overheid en/of applicatie beperkte sleutellengte kan de betrouwbaarheid van de vercijfering (nadelig) beïnvloeden. In het algemeen geldt dat de inspanning die moet worden verricht om een sleutel te 'raden' (*brute force*), exponentieel groeit met de sleutellengte. Overigens moet er wat betreft de sleutellengte onderscheid worden gemaakt tussen de symmetrische en asymmetrische vercijfermethodes. Bij de symmetrische methodes kan de sleutellengte beduidend korter zijn (3DES bijvoorbeeld 168 bits) dan bij de asymmetrische methoden (RSA 2048 bits) om een vergelijkbare betrouwbaarheid te garanderen. De reden hiervoor ligt in de wiskundige basis van de asymmetrische methoden waarbij (zeer grote) priemgetallen moeten worden gebruikt of beschrijvingen van grote elliptische krommen.

Bij het bepalen van de gewenste sleutellengte speelt een aantal factoren een rol. In de meeste gevallen is de encryptie alleen te kraken door alle mogelijke sleutels uit te proberen. Dit vergt veel rekenkracht, die exponentieel toeneemt met de sleutellengte. Belangrijk bij de keuze van de meest geschikte sleutellengte is de verwachte levensduur van de encryptietoepassing. Als deze bijvoorbeeld vijf jaar mee moet gaan, dan zal ook over vijf jaar de benodigde rekenkracht nog steeds te groot moeten zijn om echt een risico te vormen. Zie ook hoofdstuk 6 over beheer en bijlage B over sleutellengte. Overigens zijn de schattingen van de levensduur van een bepaalde sleutellengte gebaseerd op de hiervoor genoemde *brute force* pogingen om de sleutel te bepalen. Bij een doorbraak in de techniek of nieuwe wiskundige mogelijkheden kan de gekozen sleutellengte eerder te kort blijken.

Naast deze ontwikkeling van de rekenkracht zijn de volgende factoren belangrijk bij een keuze van de gewenste sleutellengte:

- *Toepassing*: welk beveiligingsniveau dient voor de specifieke toepassing gehaald te worden?
- *Wetgeving*: welke maximum sleutellengte is door de nationale wetgeving toegestaan?
- *Performance*: bij welke sleutellengte (en welk algoritme) is de tijd benodigd voor encryptie/decryptie acceptabel? Ook kan hierbij de netwerkbelasting worden beschouwd.
- *Standaard*: welke sleutellengte wordt door leveranciers, klanten, overheid gehanteerd bij (soortgelijke) algoritmen?
- *Leveranciers*: welke lengte wordt door de leveranciers van de software ondersteund en geleverd? Is de leverancier betrouwbaar? Beschikt de leverancier over een goede supportorganisatie?
- *Literatuur*: welke lengte van sleutels wordt in de recente vakliteratuur omschreven als adequaat?

Flexibiliteit

De te selecteren encryptietoepassing dient veelal gedurende een langere tijd te worden gebruikt. Een toepassing die bij een nieuwe versie niet in staat blijkt te zijn informatie te ontcijferen die door een eerdere versie is vercijferd, leidt tot compatibiliteitsproblemen. Eveneens dient de encryptietoepassing de mogelijkheid te bieden om met verschillende sleutellengten te werken. Hierbij speelt ook een belangrijk beheeraspect een rol, namelijk het beheren van de sleutels. Als verschillende versies van een toepassing verschillende (soorten) sleutels vereisen, maakt dit het beheer extra gecompliceerd en is de kans op fouten groter dan bij eenduidige sleutels, die onafhankelijk zijn van de versie van de toepassing.
Een ander aspect van flexibiliteit komt neer op de hoeveelheid besturingssystemen en toepassingen die door een encryptietoepassing worden ondersteund. De beveiliging van informatie mag niet beperkt zijn tot een groep gebruikers die 'toevallig' met het juiste besturingssysteem of de juiste toepassing werken. De oplossing dient zo neutraal mogelijk te zijn voor wat betreft het besturingssysteem, de toepassing en (indien mogelijk) de leverancier. Alleen in het geval van een specifieke behoefte of een specifieke toepassing kan een maatwerkoplossing worden ingezet.

Integratie met andere applicaties

Encryptietoepassingen worden bijna altijd in combinatie met andere programmatuur gebruikt. Denk bijvoorbeeld aan bestaande kantoorautomatisering (tekstverwerkers, *office-suites*, e-mail applicaties, enzovoort). Een belangrijk evaluatiecriterium hierbij is de ondersteuning die encryptieapplicaties leveren aan bestaande softwareproducten. Gebruikers willen niet worden geconfronteerd met allerlei verschillende applicaties die naast elkaar moeten worden gebruikt.

Een zwaarwegend aspect bij het selecteren van encryptietoepassingen is derhalve integratie met kantoorautomatisering. Een ander aspect dat meeweegt bij een besluit tot invoering is dat de wederzijdse applicaties elkaar niet negatief beïnvloeden; dat wil zeggen dat het functioneren van encryptieapplicaties niet mag worden verstoord door overige applicaties en vice versa. Verstorende factoren voor het gebruik van encryptieapplicaties zijn bijvoorbeeld systeemondersteunende hulpmiddelen zoals 'disk defragmentatie programmatuur' en antivirus applicaties. Een antivirus applicatie geeft al snel een foutmelding bij vercijferde bestanden doordat deze onleesbaar zijn. Een defragmentation tool kan vercijferde bestanden gedurende zijn proces modificeren waardoor het vercijferde bestand niet meer kan worden ontcijferd en dus verloren is.
Een onderdeel van de selectieprocedure dient de inventarisatie van de huidige software te zijn en de beoordeling daarvan met betrekking tot eventueel te verwachten problemen. Veel van deze problemen kunnen pas definitief worden achterhaald door middel van het uitvoeren van tests met de encryptietoepassingen op de standaard computerconfiguratie. Dit is veelal alleen in een pilot project te onderzoeken, omdat dan daadwerkelijk alle componenten (hardware en software) bij elkaar komen en op elkaar dienen aan te sluiten.
Kies verder een applicatie die eenvoudig is te installeren.

Transparantie

Naast de integratie met bestaande programmatuur speelt de transparantie van de encryptie een belangrijke rol bij de acceptatie door gebruikers. Zie ook norm 5.5.1. in hoofdstuk 5. De gebruikers dienen met zo min mogelijk handelingen gebruik te kunnen maken van de encryptiemogelijkheden. Dit geldt niet alleen voor het daadwerkelijk vercijfer- en ont-

cijferproces, maar ook voor het beheer van de sleutels die daarbij gebruikt worden. De gebruiker moet op een eenvoudige en veilige manier zijn of haar sleutels kunnen beheren zonder extra inspanning. Belangrijk hierbij is het al dan niet locatieonafhankelijk zijn van de sleutels, met andere woorden: zijn de sleutels gekoppeld aan een specifiek werkstation of kan de gebruiker ze 'meenemen' en op een willekeurig werkstation gebruiken (bijvoorbeeld door toepassing van een *token* of een smartcard)?
Voor gebruikers kan de invoering van een encryptietoepassing betekenen dat zij met één of meer extra wachtwoorden te maken krijgen. Dit kan als attentiepunt voor de keuze van een bepaalde encryptietoepassing worden meegenomen.

Hulpmiddelen sleutelbeheer

Het adequaat beheren van sleutels is een omvangrijke klus, waarbij zich vele problemen kunnen voordoen. Encryptietoepassingen die meegeleverd worden met een geautomatiseerd pakket om essentiële beheertaken op het gebied van sleutels uit te voeren, hebben een duidelijk voordeel boven de toepassingen waarbij zo'n 'beheertool' ontbreekt. Hierbij is het belangrijk of deze sleutels (semi)centraal of decentraal kunnen worden beheerd. Ook de voorziening voor een zogenaamde *master key* (zie hoofdstuk 6 Beheer) om alsnog ontcijfering te kunnen plegen op gegevens, kan zeer nuttig zijn.
Vanzelfsprekend dienen de functionaliteit en beveiliging van deze beheerhulpmiddelen ook tijdens het selectieproces te worden beoordeeld.

Betrouwbaarheid en integriteit van de authenticatiemethode

Een belangrijk aspect van de te selecteren oplossing is de wijze waarop gebruikers worden geauthentiseerd om vervolgens de vercijferde gegevens te kunnen benaderen. Hieronder worden de meest gebruikte vormen genoemd:

Wachtwoord	gebruikers dienen in een apart scherm van de applicatie een juist wachtwoord in te voeren dat aan de privésleutel is gekoppeld;
Token	authenticatie vindt plaats door middel van een *hardware*

	based token (bijvoorbeeld PCMCIA-card of Smartcard) waarop zich vaak ook nog de privé- sleutel bevindt. Dit al dan niet in combinatie met een beveiliging door middel van een wachtwoord;
Biometrie	authenticatie vindt plaats op basis van persoonlijke kenmerken zoals iris, vingerafdruk en stemherkenning.

De mate van betrouwbaarheid en integriteit van de authenticatie hangt sterk samen met de toepassing. Een noodzakelijke voorwaarde is dat de authenticatie te integreren is in het systeem of de applicatie zonder in te boeten aan vertrouwelijkheid, integriteit of beschikbaarheid. Een organisatie kan op basis hiervan, als eerste stap in een selectietraject, bepalen aan welke criteria een toepassing absoluut dient te voldoen en welke criteria als 'nice to have' kunnen worden beschouwd.

3.2 Selectiecriteria voor encryptie tijdens communicatie

Naast de algemene uitgangspunten geldt bij encryptie voor communicatie een aantal specifieke uitgangspunten. Deze hebben te maken met uitwisselbaarheid en standaardisatie, zodat een goede en betrouwbare communicatie kan worden gegarandeerd.

Standaarden

Bij vercijfering van de communicatie is niet gegarandeerd dat aan beide kanten van de verbinding dezelfde versie van een product, of zelfs hetzelfde product wordt gebruikt. Onder deze condities is een goede en veilige communicatie alleen mogelijk als de gebruikte oplossingen en producten zich conformeren aan open standaarden. Dit zijn standaarden die door vele fabrikanten worden ondersteund en bewaakt worden door een onafhankelijke organisatie.

Als een organisatie kiest voor één fabrikant, dan is het mogelijk een fabrikantspecifieke oplossing als standaard te kiezen. Echter, in dit geval is er geen garantie voor een goede communicatie, omdat compatibiliteit met andere versies niet altijd afgedwongen kan worden. Bovendien is er

in deze situatie geen uitwijkmogelijkheid meer naar een andere oplossing. Een ander nadeel is dat veel fabrikanten hun methoden niet vrij geven waardoor de beveiliging niet door externe auditors kan worden getoetst.

Beheerinspanning

Alhoewel beheer ook een algemeen uitgangspunt is, levert encryptie tijdens communicatie extra beheerbelasting. Vaak wordt er bij de communicatie gebruikgemaakt van asymmetrische encryptie ten behoeve van authenticatie. Dit betekent in de praktijk dat er met certificaten wordt gewerkt die verspreid zijn over verschillende, soms veraf gelegen, systemen binnen de organisatie. Een veilig beheer van deze certificaten, op afstand, verdient extra aandacht bij de keuze van een oplossing.
Daarnaast is er de mogelijkheid dat gebruikers zelf certificaten moeten beheren ten behoeve van hun persoonlijke communicatie. Hierbij dient er extra aandacht te worden gegeven aan de back-up/restore van deze persoonlijke certificaten en aan het feit of de gebruiker hierbij aan een vaste werkplek wordt gekoppeld, omdat de certificaten zich daarop bevinden.

Het gebruik van encryptie in combinatie met een *firewall* kan leiden tot een aantal problemen. Afhankelijk van de manier waarop de encryptie wordt toegepast, kan een *firewall* in meer of mindere mate controle uitvoeren over het vercijferde verkeer.
Zo kan een *firewall* in het geval dat alleen de data vercijferd zijn, op basis van de IP-adressen en protocollen besluiten het verkeer door te laten of te blokkeren. Deze vorm van encryptie wordt in IPsec ook wel *transport mode* genoemd (zie hoofdstuk 4 paragraaf 4.3.2.4). Dit is immers, voor de *firewall* althans, normaal verkeer en dat kan via de gedefinieerde regels worden gefilterd. Uiteraard is het in dit geval niet mogelijk om content filtering te doen, de *firewall* is immers niet in staat de inhoud van het verkeer te beoordelen.

In het geval dat alle data, inclusief de IP-header, zijn vercijferd, kan een *firewall* alleen op basis van de IP informatie van het pakket dat om de vercijferde data heen zit, besluiten het verkeer al dan niet door te laten. Deze manier van vercijferen wordt binnen IPsec wel aangeduid met *tun-*

nel mode. Hierbij wordt een compleet IP-pakket, inclusief header, als vercijferde data meegegeven aan een ander IP-pakket. In dit geval is de *firewall* niet meer in staat om op basis van de oorspronkelijke IP-pakketten te filteren.

3.3 Selectiecriteria voor encryptie tijdens opslag

Ook voor encryptie tijdens de opslag gelden de algemene uitgangspunten. Daarnaast zijn er specifieke uitgangspunten die voor de vercijfering van opgeslagen gegevens gelden.

Toegang voor meer gebruikers

Bij de vercijfering van opgeslagen gegevens is het in veel gevallen noodzakelijk dat meer gebruikers, elk met hun eigen omgeving, toegang hebben tot deze gegevens. De gekozen oplossing dient dit te ondersteunen door elke gebruiker de juiste toegang te verlenen zonder de andere gebruikers te hinderen.

Multilevel toegang

In veel gevallen zijn er rollen gedefinieerd voor de toegang tot verschillende gegevens. Hierbij wordt er onderscheid gemaakt tussen het recht de gegevens te lezen en het recht de gegevens te wijzigen. De gebruikte oplossing dient deze rollen te ondersteunen. Daarnaast is het belangrijk dat de gekozen oplossing een gradatie kent in de vertrouwelijkheid van de vercijferde gegevens. Met andere woorden, afhankelijk van de rechten van de gebruiker dient hij of zij alleen toegang te krijgen tot de gegevens waarvoor hij of zij is geautoriseerd.

Beschikbaarheid

Bij uitval of beschadiging van systeemcomponenten of het gehele systeem dient de beveiliging van de opgeslagen gegevens niet in gevaar te komen. De gekozen oplossing dient te allen tijde een veilige situatie achter te laten.

Bovendien moet de gekozen oplossing bestand zijn tegen uitval van één of meer componenten en in staat zijn de vercijferde gegevens te herstellen.

Integriteit

De gekozen oplossing mag geen restanten van vercijferde gegevens onvercijferd achterlaten op het systeem (bijvoorbeeld in de *swap file* of prullenbak). Daarnaast dient de gekozen oplossing bestand te zijn tegen een fysieke inbraak op het systeem waar deze gegevens zijn opgeslagen.

Het gebruik van virussoftware in combinatie met encryptie tijdens de opslag kan tot problemen leiden. Sommige virusdetectie-software herkent de vercijferde bestanden niet en meldt in het ergste geval dat deze een virus bevatten. Ook is veel virusdetectie-software niet in staat zelf een vercijferd bestand te analyseren. Alleen bij applicatie transparante vercijfermethoden is reguliere virusdetectie-software in staat een bestand te controleren.

4 Encryptie tijdens communicatie

4.1 Inleiding

Dit hoofdstuk gaat in op de diverse specifieke aspecten van encryptie tijdens de communicatie tussen informatiesystemen. De vorm waarin dergelijke communicatie kan plaatsvinden, is sinds lange tijd gestandaardiseerd door middel van het internationaal geaccepteerde ISO-OSI-model. Aan de hand van de te onderscheiden lagen binnen het OSI-model wordt aandacht besteed aan de consequenties van het gebruik van encryptie in de desbetreffende lagen.
In paragraaf 4.2 wordt duidelijk gemaakt hoe de beveiliging gerealiseerd kan worden binnen het OSI-model. In eerste instantie wordt duidelijk gemaakt op welke locaties de encryptie gerealiseerd kan worden, waarna de gevolgen van de keuze voor een bepaalde locatie aan de hand van een aantal criteria worden behandeld. De paragraaf wordt afgesloten met een overzicht van de onderzochte beveiligingslocaties versus de onderkende besliscriteria voor het maken van een keuze.
In de laatste paragraaf wordt per beveiligingslocatie uitgebreider aandacht besteed aan de mogelijke beveiligingsprotocollen en -standaarden met bijbehorende voor- en nadelen.

4.2 Beveiliging binnen het OSI-model

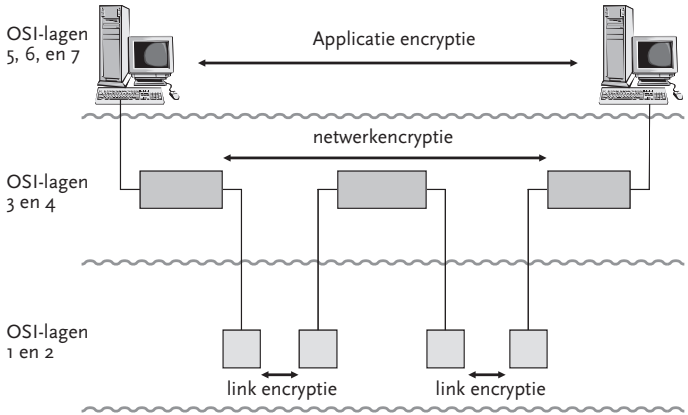
Door de *International Standardization Organization* (ISO) is het *Open Systems Interconnection* (OSI) model opgesteld. Het model bepaalt de standaard voor netwerken. Het OSI-model wordt helaas veelvuldig gezien als een netwerkarchitectuur welke geen toekomst heeft. De kracht van het OSI-model is echter dat het geen exacte invulling geeft van protocollen en

diensten, maar dat het een referentiemodel is dat als basis dient bij de implementatie van nieuwe diensten of netwerken. Door binnen deze studie gebruik te maken van het OSI-model is het dus mogelijk om een volledig overzicht te presenteren van de beveiligingsmogelijkheden van encryptie tijdens communicatie.
In bijlage A is enige achtergrondinformatie opgenomen over het OSI-model.

4.2.1 Mogelijke locaties van encryptie

Deze paragraaf schetst een mogelijke indeling die gemaakt kan worden ten aanzien van de locatie van de encryptie. Op basis van deze indeling wordt het hoofdstuk verder vormgegeven. Deze paragraaf volstaat met het beschrijven van de locatie van de encryptie en het aanstippen van de gevolgen hiervan.

Het is van belang om vast te stellen waar in de communicatieketen de maatregelen geïmplementeerd worden. De plaats van de beveiliging over de zeven OSI-lagen kan verdeeld worden in drie categorieën: applicatie-encryptie (applicatieniveau), netwerkencryptie (netwerkniveau) en



Figuur 4.1 Locatie van beveiliging door middel van encryptie in relatie tot het OSI-model

linkencryptie (datalinkniveau). Zie bijlage A voor een uitgebreide bespreking van het OSI-model.

Encryptie op applicatieniveau

Bij het toepassen van encryptie op applicatieniveau wordt de encryptie op de twee eindsystemen uitgevoerd. Het verzendende systeem vercijfert de data, waarna de data in vercijferde vorm ongewijzigd via het netwerk naar het ontvangende systeem worden gestuurd. De bestemming heeft een corresponderende sleutel en is zodoende in staat om de data te ontcijferen. De *end-to-end* encryptie verlost de gebruiker van de zorgen over de mate van beveiliging van netwerken en verbindingen die bij de communicatie worden gebruikt. Toch is er nog een zwakke plek aanwezig. Bij *end-to-end* encryptie worden namelijk alleen de applicatiedata vercijferd en niet de headerinformatie, omdat anders de pakketten in zijn geheel vercijferd zouden zijn en dus niet leesbaar voor de netwerkcomponenten, verantwoordelijk voor het doorsturen van de pakketten. Encryptie van deze verkeersinformatie zou dus problemen voor het afleveren van de pakketten veroorzaken. Hier staat echter weer tegenover dat *end-to-end* encryptie een zekere mate van authenticatie mogelijk maakt bij het gebruik van een asymmetrisch encryptiesysteem.

Veel beveiligingssystemen zijn gebaseerd op *end-to-end* encryptie. Denk bijvoorbeeld aan digitale handtekeningen en additionele softwaremodules speciaal bedoeld voor beveiliging. Ten behoeve van een succesvolle implementatie van een dergelijke beveiligingsapplicatie is het van belang dat alle communicerende partijen met de desbetreffende applicatie overweg kunnen en dat de organisatie rondom het noodzakelijke sleutelbeheer goed vormgegeven is.

Encryptie op applicatieniveau kan toegepast worden in combinatie met netwerkencryptie of linkencryptie om de geboden beveiliging op te voeren, Bijvoorbeeld om ook de transportdata in de headers veilig te stellen en/of te verbergen.

Encryptie op netwerkniveau[3]

Netwerkencryptie kent in principe nog maar een korte geschiedenis. De stormachtige ontwikkeling van internet, intranet en extranet, samen met de toenemende aandacht voor e-commerce toepassingen, heeft geleid tot de introductie van deze nieuwe locatie van de encryptiefunctionaliteit. Er is namelijk in toenemende mate behoefte aan private netwerken over het internet, de zogenaamde *Virtual Private Networks* (VPN's).

Bij het aanleggen van VPN's wordt gebruikgemaakt van een techniek die *tunneling* genoemd wordt. De datapakketten worden via een logische verbinding (*tunnel*) van het ene lokale netwerk via het internet naar het andere lokale netwerk gestuurd als ware het een directe (niet publiek toegankelijke) communicatieverbinding. Om een dergelijke *tunnel* tot stand te brengen worden de datapakketten bij het verlaten van het ene lokale netwerk verpakt in een internetpakket en (optioneel) beveiligd door encryptie ter bescherming van de exclusiviteit. Als de encryptie daadwerkelijk wordt toegepast, zal het ontvangende lokale netwerk het internetpakket ontcijferen en het oorspronkelijke datapakket uitpakken. Het belangrijkste voordeel van deze encryptiemethode zijn de lage kosten: internet is immers voor verbindingen op lange afstand aanmerkelijk goedkoper dan andere communicatiemedia zoals huurlijnen, telefoonlijnen of satellietverbindingen. Een ander voordeel is dat encryptie op netwerkniveau protocolonafhankelijk kan zijn. *Tunneling* is hiermee mogelijk over diverse verschillende protocollen, zodat bijvoorbeeld twee lokale Novell-netwerken via internet veilig op elkaar aangesloten kunnen worden.

Naast VPN's kunnen ook zogenaamde IP-encryptors worden gebruikt voor het opbouwen van een beveiligde *tunnel* op IP-niveau. Het verschil met een VPN-toepassing is dat een VPN over het algemeen extra functionaliteiten biedt zoals authenticatie en toegangscontrole.

3 Encryptie op netwerkniveau is gezien zijn oorsprong voornamelijk gebaseerd op het TCP/IP-protocol. Bij de behandeling van netwerkencryptie wordt dan ook het accent gelegd op dit protocol. Andere protocollen (zoals X.25) worden buiten beschouwing gelaten gezien de afnemende belangstelling hiervoor.

Encryptie op datalinkniveau

Bij deze vorm van beveiliging is de beveiliging op de onderste twee lagen van het OSI-model geregeld. Vandaar dat deze vorm van encryptie ook wel aangeduid wordt als linkencryptie. Het netwerk implementeert de benodigde functies om ervoor te zorgen dat het gewenste beveiligingsniveau wordt gerealiseerd. Alle data die verstuurd worden, dus ook alle protocolinformatie, is vercijferd. Dit houdt in dat bij alle tussenliggende netwerk-nodes (knooppunten) de data ontcijferd moeten worden opdat het adres van de ontvanger gelezen kan worden. De gegevens zijn dus bij elke node kwetsbaar. Bij publieke *packet switching* netwerken heeft de gebruiker dan ook geen controle op de door de node te verwerken data.

Linkencryptie wordt vooral gebruikt bij *Wide Area Networks* (WAN), bijvoorbeeld bij communicatie via het openbare telefoonnetwerk. Aan beide kanten van een telefoonlijn, gezien vanuit het openbare netwerk, wordt fysieke encryptie-apparatuur geplaatst. Deze apparatuur vercijfert alle data naar buiten en ontcijfert alles wat binnenkomt. De twee apparaten aan beide zijden van de lijnen vormen een team en bezitten dezelfde sleutels (bij symmetrische encryptie) of bij elkaar horende sleutelparen (bij asymmetrische encryptie). Sommige apparatuur is tot op zekere hoogte zelf in staat om het sleutelbeheer uit te voeren en kiest bijvoorbeeld periodiek automatisch een nieuwe sleutel. Bij dergelijke apparatuur is het verstandig om rekening te houden met de mogelijkheid van het doorsturen van niet-vercijferde informatie ingeval van het optreden en oplossen van storingen. Hierbij dient wel een procedure verzorgd te worden voor het voorkomen van het doorsturen van 'echte' gegevens en voor het registreren van elk individueel gebruik van deze *bypass*.

Lijnencryptie-apparatuur werkt op *point-to-point* niveau. De bescherming is van kracht op het communicatiekanaal tussen de encryptie-apparatuur en er vindt geen authenticatie ten behoeve van hoger liggende niveaus plaats.

4.2.2 Het kiezen van een encryptielocatie

Nu de indeling ten aanzien van encryptie tijdens communicatie geïntroduceerd is, is het van belang om een goede keuze tussen de locaties te

maken. Er is echter geen sprake van een eenvoudige keuze voor een bepaalde locatie: diverse omgevings- en beïnvloedingsfactoren zijn hierbij van belang. Daarom besteden we in deze paragraaf aandacht aan de voor- en nadelen per encryptielocatie, en wordt getracht enkele afwegingen te maken.

Encryptie op applicatieniveau

Een belangrijke eigenschap van encryptie op applicatieniveau is dat het hiermee mogelijk is de beveiliging toe te passen tot op het kleinste element: de informatie zelf. Tot op detailniveau kan bepaald worden welke informatie wel of niet beveiligd hoeft te worden.
Encryptie op applicatieniveau heeft als groot voordeel dat het mogelijk is beveiliging op *end-to-end-basis* te bewerkstelligen. Dit houdt in dat de informatie vanaf het moment van verzenden continu op een bepaalde wijze beveiligd is. De beveiliging maakt dat de te gebruiken applicaties niet afhankelijk zijn van het onderliggende netwerk en de gebruikte verbindingstechnieken. De gebruikers hoeven zich derhalve geen zorgen te maken over de veiligheid van het netwerk, omdat hun informatie zelf adequaat beveiligd is. Alleen de ontvangende partij voor wie de informatie bedoeld is, kan de informatie ontsluiten.

Ten behoeve van een succesvolle implementatie van een dergelijke beveiligingsapplicatie is het van belang dat alle communicerende partijen met de desbetreffende applicatie overweg kunnen en dat de organisatie rondom het noodzakelijke sleutelbeheer goed vormgegeven is. Dit is dan ook een groot nadeel van encryptie op applicatieniveau. Tussen de communicerende partijen dienen vergaande afspraken gemaakt te worden, opdat de informatie gedeeld kan worden. Een oplossing hiervoor kan gezocht worden in de *Public Key Infrastructure* (PKI), zie sectie 6.4.

Het bovenstaande impliceert dat encryptie op applicatieniveau de voorkeur heeft, als er niet met vele verschillende partijen gecommuniceerd dient te worden. Immers in dat geval is het mogelijk om snel afspraken te maken tussen de partijen. Als een handelsbedrijf bijvoorbeeld te maken heeft met tien verschillende leveranciers en twintig verschillende afnemers en met al deze partijen via datacommunicatie beveiligde verbindingen wil onderhouden, is de kans klein dat er één uniforme

afspraak gemaakt kan worden. Een oplossing voor dit probleem kan gevonden worden in een *Public Key Infrastructure* (PKI), zie sectie 6.4.
Een voordeel van encryptie op applicatieniveau is dat deze methode onafhankelijk is van de onderliggende netwerkstructuur. In het bovenstaand voorbeeld van de leverancier betekent dit dat er geen onderscheid in de communicatiemedia gemaakt hoeft te worden, wanneer een aantal partijen niet op beveiligde wijze wenst te communiceren terwijl andere dat wel graag wensen.

Een andere afweging om voor encryptie op applicatieniveau te kiezen is de grootte van de groep van gebruikers. Als een onderneming over vele gebruikers beschikt die op een beveiligde wijze informatie dienen te communiceren, dan zal het beheer over de te gebruiken applicaties behoorlijk veel werk met zich meebrengen. Maar ook het beheer over het noodzakelijke sleutelmateriaal zal in dit soort gevallen veel inspanningen vergen. Derhalve heeft beveiliging door middel van encryptie op applicatieniveau de voorkeur als het aantal gebruikers niet al te groot is.

Encryptie op netwerkniveau

Door middel van encryptie op netwerkniveau is het mogelijk om over publiek toegankelijke netwerken een logisch beveiligd communicatiekanaal op te zetten dat, zoals eerder reeds aangegeven, een *Virtual Private Network* (VPN) genoemd wordt. Naast applicatie-onafhankelijkheid heeft deze encryptielocatie het grote voordeel dat de kosten voor de verbindingen over grote afstanden laag zijn. Waar voorheen vaak relatief dure huurlijnen noodzakelijk waren, kan nu worden volstaan met een verbinding over bijvoorbeeld het internet.
Een ander voordeel dat met deze encryptielocatie bereikt wordt is de onafhankelijkheid van de onderliggende protocollen die binnen de netwerken en het tussenliggende medium toegepast worden. Hiermee is men in principe niet gebonden aan bepaalde leveranciers of netwerkcomponenten. Overigens blijkt in de praktijk dit laatste af en toe nog tegen te vallen; bij gebruik van IPsec (zie paragraaf 4.3.2.4) wordt vaak nog steeds aangeraden om componenten van één en dezelfde leverancier te gebruiken. Maar het is in ieder geval wel mogelijk om een *tunnel* te verwezenlijken over verschillende soorten netwerken.

Encryptie op netwerkniveau kent een nadeel dat voortvloeit uit het aspect compatibiliteit. Bij het toepassen van VPN's zal ervoor gezorgd moeten worden dat partijen die op deze wijze veilig willen communiceren gebruikmaken van dezelfde technologieën. Er dienen dan ook afspraken gemaakt te worden. Dit heeft te maken met de op dit moment onvoldoende aanwezige standaardisatie.
Vanwege het grote aanbod van producten, diensten en technieken wordt hier niet dieper ingegaan op specifiekere nadelen. Deze zijn namelijk altijd gerelateerd aan de desbetreffende technieken. Hiervoor verwijzen wij dan ook naar naar paragraaf 4.3.2, waarin een verdere technische uitdieping van deze encryptielocatie wordt gegeven.

Encryptie op datalinkniveau

Door middel van encryptie op datalinkniveau wordt zorg gedragen dat alle communicatie in vercijferde vorm verstuurd wordt. Het grote voordeel hiervan is dat aanvallen op het gebied van verkeersstroomanalyse niet succesvol zullen zijn. Verkeersstroomanalyse behelst de tactiek om waardevolle informatie te kunnen achterhalen op basis van de getransporteerde data (hoeveelheid, frequentie en grootte van de datapakketten). Een ander voordeel is de applicatie-onafhankelijkheid van deze techniek. Het grote nadeel van deze methode is dat hierdoor bij elke netwerknode de vercijferde informatie ontcijferd dient te worden, opdat het doorgestuurd kan worden.
Dit houdt dan ook in dat encryptie op datalinkniveau minder geschikt is voor publieke *packet switching* netwerken. Maar als gebruik wordt gemaakt van directe lijnverbindingen via een *circuit switching* netwerk (bijvoorbeeld het telefoonnetwerk), dan is deze beveiliging uitermate aan te raden.

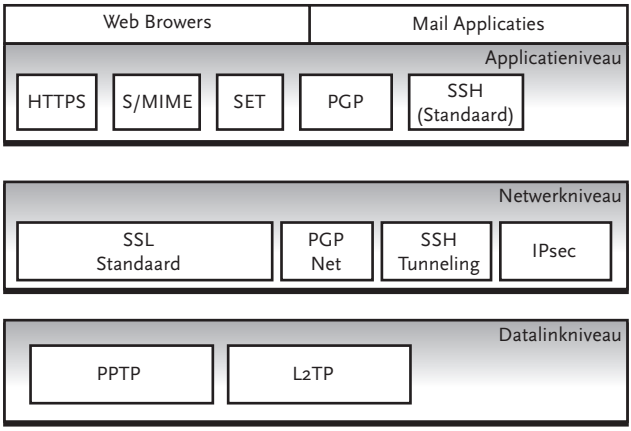
Bij encryptie op datalinkniveau is er, vanwege het feit dat de data tussen partijen volledig vercijferd worden, geen sprake van schaalbaarheid. Indien eenmaal besloten is om op deze wijze data te vercijferen is men daaraan 'veroordeeld'. Overigens hoeft dit niet dramatisch te zijn, omdat deze techniek transparant werkt voor de gebruikers.

4.2.3 *Overzicht locatie van de encryptie en besliscriteria*

In deze paragraaf wordt door middel van een matrix een verband gelegd tussen de onderzochte plaatsen waar encryptie kan plaatsvinden binnen het OSI-model en de mogelijke besliscriteria. Met de besliscriteria wordt enerzijds verwezen naar de binnen deze studie onderkende betrouwbaarheidsaspecten alsook aanvullende criteria die overkoepelend per locatie geldig zijn, ongeacht de gekozen technische invulling ervan. In tabel 4.1 is dan ook als aanvullend criterium 'snelheid' opgenomen, omdat per locatie een uitspraak gedaan kan worden over de snelheid. Zo is linkencryptie altijd sneller dan encryptie op applicatieniveau ongeacht de gekozen implementatie.

Tabel 4.1 De relatie tussen besliscriteria en de plaats van encryptie

Besliscriteria		**Plaats van encryptie**		
		linkencryptie	netwerk-encryptie	applicatie-encryptie
Authenticatie	node		+	
	gebruiker			+
Integriteit			+	+
Exclusiviteit		+	+	+
Onweer-legbaarheid	van ontvangst			+
	van verzending			+
Schaalbaarheid		--	+	++
Aantal gebruikers		++	+	+/-
Snelheid		++	+	+/-



Figuur 4.2 Standaarden gepositioneerd op een specifiek toepassingsniveau

4.3 Encryptieproducten en -standaarden gerelateerd aan de OSI-lagen

De huidige encryptiestandaarden en -producten zijn vaak applicaties en/of protocollen die een bepaalde encryptiefunctionaliteit op een specifieke OSI-laag bieden. Deze producten/standaarden bieden op zekere hoogte dezelfde beveiligingsmechanismen, maar verschillen in hun toepassingsbereik en hun plaats in de TCP/IP *protocol stack*.

De producten/standaarden worden in de praktijk ingedeeld op drie geclusterde niveaus, namelijk het applicatie-, het netwerk- en het linkniveau. In figuur 4.1 is al aangegeven welke OSI-lagen bij welk hoofdniveau behoren. In figuur 4.2 worden de producten op deze niveaus ingedeeld, waarna in de volgende paragrafen een korte beschrijving van de beveiligingsvoorziening (encryptie) per product/standaard wordt gegeven.

4.3.1 Applicatieniveau

Met de explosieve groei van het gebruik van e-mail, groeit de vraag naar authenticatie-, integriteits- en vertrouwelijkheidsservices. De twee be-

langrijkste oplossingen voor het beveiligen van e-mail zijn PGP *(Pretty Good Privacy)* en S/MIME *(Secure Multi-Purpose Internet Mail Extensions)*. Dit zijn applicaties die op basis van hun cryptografische functionaliteit op het applicatieniveau gepositioneerd worden. Andere applicaties en/of protocollen die ook op dit niveau thuishoren, zijn: HTTPS *(HyperText Transfer Protocol Secure)*, SET (*Secure Electronic Transactions)* en SSH *(Secure remote SHell*).

4.3.1.1 HTTPS

Communicatie van webverkeer tussen twee systemen op het internet verloopt volgens HTTP. HTTP biedt geen goede voorzieningen voor beveiliging: informatie wordt in HTTP onvercijferd over het netwerk verstuurd. Daarnaast zijn er geen goede faciliteiten voor client en server authenticatie. Client authenticatie is meestal gebaseerd op naam/wachtwoordcombinaties, op het IP-adres of de domeinnaam van de browser. Het risico van deze technieken is dat ze afgeluisterd en of gemanipuleerd kunnen worden. Door het ontbreken van server authenticatie kan de server zich niet aan de browser identificeren. Hierdoor kan de browser niet vaststellen of er al dan niet sprake is van een valide website.
Om deze problemen op te heffen wordt HTTP gecombineerd met *Secure Socket Layer* (SSL; zie ook paragraaf 4.3.2.1); men spreekt dan van HTTPS (HTTP *Secure*). Deze combinatie maakt encryptie van het datatransport en authenticatie van client en server mogelijk. Dit is een vereiste als het gaat om transport van vertrouwelijke gegevens over het internet.
Normaliter zal een browser een webserver benaderen via het HTTP-protocol. De URL (*Unified Resource Location*) begint dan met 'http://'. Wanneer een URL begint met 'https://', zal de client een verbinding met de server opbouwen via het HTTPS-protocol. HTTPS maakt op de server gebruik van een andere logische toegangspoort (433) dan HTTP (80). De meeste browsers geven in de statusbalk onder in het venster aan dat de huidige pagina via HTTPS verkregen is. Om dit aan te geven wordt een icoontje (sleutel, slot) gebruikt.

Voor- en nadelen

Een voordeel van HTTPS is dat het is te combineren met SSL, een de facto standaard die zowel door browsers als webservers goed wordt onder-

steund. Bovendien zijn geen aanpassingen vereist aan de inhoud van de webserver, waardoor een website zonder aanpassingen over kan gaan op een *secure* verbinding. Tevens zijn verschillende implementaties beschikbaar, zowel commercieel (*proprietary*) als publiek (*Open Source*). Ten slotte bestaat er de mogelijkheid tot integratie in een PKI-omgeving.
Een groot nadeel is dat de configuratie van een SSL-server complex is, door afhandeling van servercertificaten. De beveiliging staat of valt bovendien met de correcte beveiliging van het servercertificaat. Installatie en configuratie van clientcertificaten is complex, omdat browsers elk op hun eigen wijze certificaten aanmaken, opslaan en afhandelen. Een laatste complicerende factor is dat het laten verstrekken van vertrouwen in de identiteit van een server wordt gedelegeerd aan een derde partij.

Snel/langzaam

De snelheid van SSL is veelal geen bottleneck; de snelheid van het internet is vaak de beperkende factor.

Beheeraspecten

Beheer van SSL servers bestaat voor een groot deel uit het beheren van servercertificaten en de relatie met de CA (*Certification Authority*) en trustrelaties met andere onderdelen in de organisatie (of daarbuiten). Vooral het beheer van de privé-leutels van een certificaat bepaalt in sterke mate de betrouwbaarheid van deze certificaten.
Het beheer van clientcertificaten is zeer complex en vereist een TTP met bijbehorende procedures. Dit is vaak een te hoge drempel voor een organisatie.

4.3.1.2 S/MIME

S/MIME is een veilige methode om e-mail te verzenden en maakt onderdeel uit van de laatste versie browsers van Microsoft en Netscape. S/MIME is een verbetering van de beveiliging van het internet e-mail formaat standaard MIME. Hoewel S/MIME evenals PGP op IETF-standaards is terug te voeren, lijkt het waarschijnlijk dat S/MIME zal uitgroeien tot de industriestandaard voor commerciële en andere organisaties, terwijl PGP bij vele individuele gebruikers favoriet zal blijven voor beveiliging van persoonlijke e-mail.

S/MIME is een applicatieprotocol dat de vorm van vercijferde en digitaal ondertekende e-mail-berichten vastlegt en dat gebaseerd is op cryptografische standaarden zoals X.509 (een gestandaardiseerd formaat voor certifcaten, zie paragraaf 6.4.1.1). S/MIME gebruikt onder andere RSA als public key algoritme en RC2, DES en Triple DES als symmetrische algoritmen. Het volgt de syntax die in de *Public Key Cryptography Standard* (PKCS) is vastgelegd.

De functionaliteit die S/MIME biedt, lijkt erg veel op PGP. Beide bieden de mogelijkheid berichten te ondertekenen en/of te vercijferen.
Net als bij het PGP-model moeten S/MIME-beheerders en/of gebruikers elke client configureren met een lijst van vertrouwde sleutels en met 'certificaat *revoke*-lijsten' (zie paragraaf 6.4.1.4). De verantwoordelijkheid voor het onderhouden van de certificaten die nodig zijn om binnenkomende handtekeningen te verifiëren en om uitgaande berichten te vercijferen, is lokaal. De certificaten daarentegen, worden ondertekend door certificatie-autoriteiten.

Voor- en nadelen

Voordelen van S/MIME is dat het goed is te integreren in een PKI-omgeving; dit is zelfs een randvoorwaarde voor goed beheer van de certificaten. Bovendien is het een platform onafhankelijke standaard, die zowel ondertekening als vercijfering verzorgt.
Nadeel is dat S/MIME niet is te combineren met PGP, een andere standaard voor de uitwisseling van beveiligde e-mail. Bovendien kan in in grote organisaties het adequaat beheer van de certificaten een probleem worden.

Snel/langzaam

In de praktijk merkt de gebruiker een vertraging in het versturen en lezen van vercijferde e-mailberichten.

Beheeraspecten

Het beheer van een S/MIME-omgeving is vaak geïntegreerd in het beheer van een PKI-omgeving, omdat er veel met gebruikersgebonden certificaten wordt gewerkt.

4.3.1.3 SET

Naast SSL is er een andere standaard beschikbaar voor het veilig uitvoeren van financiële transacties over internet: SET (*Secure Electronic Transactions*). Deze standaard is ontwikkeld door een aantal banken en creditcardmaatschappijen in samenwerking met een aantal computerfabrikanten.
Het gebruik van SSL elimineert het risico van afluisteren onderweg. Echter, het risico dat vertrouwelijke informatie in verkeerde handen komt, wordt niet weggenomen. Vertrouwelijke informatie kan op een website in onvercijferde vorm verwerkt worden en al dan niet tijdelijk worden opgeslagen. Ook bestaat het risico dat de klant zaken doet met een onbetrouwbare aanbieder of omgekeerd. SSL v3 (de derde versie van het SSL-protocol) ondersteunt authenticatie van zowel de client als de server en vercijfering van de sessie (voor het begrip 'sessie' zie Bijlage A, sectie 2).
Het SET-protocol ondervangt de problemen met onvercijferde opslag en vervolgtransport van vertrouwelijke informatie (zoals creditcardnummers) en onbetrouwbare transactiepartners.

Bij een SET-transactie zijn vier partijen betrokken: de klant, de aanbieder, een betalingsgateway (een elektronische poort die het verkeer van informatiestromen regelt) en de creditcardmaatschappij. Het berichtenverkeer tussen de vier partijen is volledig vercijferd en wel op zo'n manier dat de anonimiteit van bestellingen en betalingen gewaarborgd is. Elke betrokken partij beschikt hiertoe over een certificaat voor authenticatie en sleuteluitwisseling. De klant beschikt over speciale *wallet software*, waarmee bestellingen geplaatst en betalingen uitgevoerd kunnen worden.
SET is een verzameling beveiligingsprotocollen en -formaten waarmee gebruikers de bestaande infrastructuur voor creditkaartbetalingen op een veilige manier op een open netwerk, zoals internet, kunnen gebruiken. Binnen deze protocollen worden cryptografische technieken (symmetrische- en asymmetrische sleutels) gecombineerd om de vertrouwelijkheid, integriteit en authenticiteit van de berichtenuitwisseling in SET te waarborgen.

Voor de uitwisseling van SET-berichten tussen de bij de SET-transactie betrokken partijen, is de inrichting van een *Public Key Infrastructure* (PKI)

noodzakelijk, omdat er binnen SET sprake is van certificaten en een *Certification Authority* (CA). In sectie 6.4 wordt een toelichting gegeven over PKI.

Voor- en nadelen

SET is weliswaar een krachtig en veilig systeem, maar het kent ook enkele nadelen. Ten eerste wordt het nog niet ondersteund door browsers. Daarnaast is ook SET kwetsbaar voor aanvallen waarbij de client wordt gekraakt. Tenslotte is SET nog niet algemeen geaccepteerd. Aanbieders en consumenten kijken de kat uit de boom: aanbieders wachten tot consumenten op grote schaal SET gaan gebruiken, terwijl consumenten wachten tot aanbieders op grotere schaal SET-betalingen mogelijk maken.

Snel/langzaam

De beveiliging in SET vergt veel processorcapaciteit voor cryptografische berekeningen en bandbreedte voor het uitwisselen van berichten met de diverse bij een SET-transactie betrokken partijen.

Beheeraspecten

Zowel de implementatie van de SET-standaard als het gebruik van SET is complex. De implementatie van een SET-omgeving vereist een uitgebreide PKI-omgeving. Het beheer van een SET-omgeving is geïntegreerd in het beheer van zo'n PKI-omgeving waarin er sprake is van een veelheid van certificaten en nationale- en internationale CA's (*Certification Authority*).

4.3.1.4 SSH

Evenals SSL is SSH opgezet op het bestaande TCP-protocol. SSH is in eerste instantie opgezet om de problemen rondom internet *unsecure remote access* op te lossen. Initieel stond SSH voor *Secure remote SHell*, een vervanging van RSH (*remote shell*) van Unix. Tegenwoordig is het meer als protocol bekend. In vergelijking met de RSH worden sommige taken door SSH vereenvoudigd. SSH stijgt in populariteit en is voor verschillende platformen geschikt gemaakt.
Tegenwoordig is SSH de de facto standaard voor een veilige remote verbinding tussen Unix systemen en Windows clients. Het is ook beschikbaar voor commerciële producten.

De eerste versie van SSH heeft enkele tekortkomingen en zal vervangen worden door SSH v2.0. De nieuwe versie SSH v2.0 is ontwikkeld om ook toekomstige PKI-omgevingen te faciliteren.
SSH (Unix Software) voorziet in een sterke authenticatie en een sterke encryptie. De symmetrische sleutel van het SSH protocol is 256 bits lang. Het is ook voorzien van een random generator die kan worden gebruikt om cryptografische sleutels te genereren.
Enkele cryptografische algoritmen die door SSH worden gebruikt, zijn: IDEA, DES, 3DES, RSA en AES. (in principe een open architectuur met betrekking tot algoritmen).

Voor- en nadelen

De voordelen van SSH zijn:
- het is beschikbaar voor verschillende platformen, zowel Unix als Windows. Een SSH-client is bijvoorbeeld ook beschikbaar voor een palmtop.
- het biedt een sterke authenticatie, vercijfering, datacompressie en een grafische interface voor *Secure File Transfer Protocol* (SFTP) in een Windows omgeving.
- SSH v2 biedt de mogelijkheid verschillende sessies te openen binnen dezelfde *secured channel* tussen twee computers.
- SSH v2 ondersteunt meerdere asymmetrische algoritmen.

De nadelen zijn:
- De kwaliteit van verschillende implementaties verschilt en leidt daardoor soms tot kwetsbaarheden.
- De interoperabiliteit tussen SSH v1 en SSH v2 is moeilijk.

Snel/langzaam

Het gebruik van compressie is te configureren. Afhankelijk van de omgeving waarin SSH wordt gebruikt, kan hier snelheidswinst behaald worden.

Beheeraspecten

Beheer van de SSH-server is centraal uit te voeren. Gebruikers zijn echter zelf verantwoordelijk voor hun eigen configuratie. Dit maakt het moeilijk centraal de gebruikers te beheren.

4.3.1.5 PGP

Door het wereldwijd toenemende gebruik van PGP (*Pretty Good Privacy*), is het uitgegroeid tot een feitelijke standaard. Naast commerciële implementaties zijn er ook *Open Source* implementaties beschikbaar.
Het programma PGP is beschikbaar voor Windows en Unix omgevingen. Het is de laatste jaren overvleugeld door de S/MIME techniek, die een internet standaard is en ondersteund wordt door de belangrijkste programma's op dit moment.

PGP maakt gebruik van zowel symmetrische als asymmetrische vercijfering. De data zelf worden vercijferd met een symmetrisch algoritme, bijvoorbeeld IDEA of 3DES. De sleutel die hiervoor wordt gebruikt, is random gegenereerd. Deze sleutel wordt ook wel de sessiesleutel genoemd.
De sessiesleutel zelf wordt met behulp van asymmetrische vercijfering vercijferd. Hierbij spelen de privé- en publieke sleutels van zowel de verzender als de ontvanger een rol, afhankelijk van het feit of de data alleen vercijferd, alleen ondertekend, of zowel vercijferd als ondertekend worden. De vercijferde sessiesleutel wordt in de header van het PGP-bericht meegestuurd.

Voor- en nadelen

De voordelen van PGP zijn:

- het biedt een vertrouwelijkheids- en authenticatieservice die voor toepassingen voor bestandsopslag kunnen worden gebruikt.
- PGP gebruikt goede cryptografische algoritmen die als bouwstenen beschikbaar zijn. Deze algoritmen zijn geïntegreerd tot universele toepassingen die onafhankelijk zijn van besturingssyteem en processor, en die zijn gebaseerd op een verzameling eenvoudig te gebruiken opdrachten.
- Het pakket en het document, met inbegrip van de broncode, is gratis via internet en bulletinboards verkrijgbaar; het wordt wel ondersteund door een (commercieel) bedrijf.
- De uitvoering van PGP bestaat uit vijf services: authenticatie, vertrouwelijkheid, compressie, e-mail compatibiliteit en segmentatie.
- het heeft een breed toepassingsbereik, van een gestandaardiseerd systeem voor het vercijferen van bestanden en berichten, tot indivi-

duele toepassingen voor het op een veilige wijze wereldwijd via internet en andere netwerken kunnen communiceren;
– het is noch ontwikkeld noch gecontroleerd door een overheidsinstantie of standaardorganisatie.

Het is dan ook niet vreemd dat PGP een forse groei doormaakt. Het is wereldwijd gratis beschikbaar in versies die op allerlei platformen draaien. Bovendien bestaan er commerciële versies voor gebruikers die een product met leveranciersondersteuning prefereren. Daarbij is het gebaseerd op algoritmen die uitgebreide publieke tests hebben overleefd en als maximaal betrouwbaar worden beschouwd.
Van belang is ook dat PGP als ondersteuning dient voor RSA, DSA en Diffie-Hellman als asymmetrische algoritmen en CAST-128, IDEA en 3DES als symmetrische algoritmen.

De nadelen zijn:
Het nadeel van PGP is dat het nooit een officiële internet standaard is geworden en dat het ook niet door alle populaire mailprogramma's ondersteund wordt. Veel besturingsystemen en e-mail applicaties zijn echter PGP-pluggable (door een kleine toevoeging aan de applicatie is PGP te gebruiken), zodat dit nadeel gedeeltelijk verdwijnt.

Snel/langzaam
In de praktijk merkt de gebruiker een vertraging in het versturen en lezen van vercijferde e-mailberichten.

Beheeraspecten
Bij gebruik van PGP bepaalt de gebruiker zelf de vertrouwensrelatie. Er is hierdoor sprake van vele één-op-één trusts die niet centraal kunnen worden beheerd.

4.3.1.6 Samenvattend overzicht

Tabel 4.2 geeft een samenvattend overzicht van de voornoemde producten/standaarden met betrekking tot de aspecten: mate van standaardisatie, beheerinspanning, organisatorische inspanning, technische impact, gebruikers impact en snelheid.

Tabel 4.2 Samenvattend overzicht

Applicatie aspecten	HTTPS	S/MIME	SET	PGP	SSH
Standaard (mate van standaar-disatie)	++	+/-	-	++	++ Standaarden niet compatible
Beheer-inspanning	Certificatie van cliënt	n.v.t.	Externe organisatie	n.v.t.	Centraal Service beheer
Organisa-torische inspanning	Certificatie leidt tot decentrale rollen; nieuwe functies	n.v.t.	Afhankelijk van de imple-mentatie	n.v.t.	Decentraal en centraal beheer (van sleutels)
Technische impact	Integratie met standaard browser (versiebeheer)	Integratie met standaar-disatie van mail cliënt	Koppeling externe of eigen appa-ratuur	Versiebeheer	Stand alone toepassing
Gebruikers impact	Afhankelijk van technische implementatie	– Zelf beheer sleutels t.b.v. eind-gebruikers – Authenticatie handelingen	– Eigen appa-ratuur en eigen software – Afhankelijk van imple-mentatie	– Zelf beheer sleutels t.b.v eindge-bruikers – Authenticatie handelingen	Zelf beheer van sleutels t.b.v. server
Snelheid	Zie SSL	Enig performance verlies	Grote overhead	Middelgrote overhead	Enig performance verlies

4.3.2 Netwerkniveau

De producten/standaarden die op netwerkniveau voorzieningen voor beveiliging bieden zijn:

– *Secure Socket Layer* (SSL),
– PGPnet,

– SSH *tunneling*,
– IP *security* (IPSec).

4.3.2.1 SSL

SSL is een protocol dat door applicaties kan worden gebruikt om een geauthentiseerde sessie op te zetten tussen een client en een server, cryptografische sleutels uit te wisselen en de sessie tussen de client en de server desgewenst te vercijferen.
SSL is een open protocol, ontwikkeld door Netscape Communications, voor betrouwbare toegang tot het internet en heeft zich ontwikkeld tot een de facto standaard. Als protocol bevindt SSL zich tussen de TCP/IP laag en de protocollen HTTP, FTP en SMTP.

De door SSL geboden faciliteiten zijn encryptie (vercijfering van de websessie), authenticatie van de webserver en, als de webserver dat wenst, authenticatie van de client. De technieken die hierbij worden gebruikt zijn gebouwd op concepten zoals asymmetrische cryptografie, certificaten en *Certification Authorities*. Binnen SSL wordt een random generator toegepast voor het genereren van de sessiesleutels.

Van SSL zijn twee versies in gebruik: SSL v2 en SSL v3. In SSL v3 zijn de authenticatiemogelijkheden uitgebreider dan in SSL v2. De belangrijkste browsers en webservers ondersteunen SSL v3, de meest actuele versie van SSL, die mede door de industrie is ontwikkeld.
De SSL v2 kende verschillende beperkingen op het gebied van cryptografische beveiliging (bijvoorbeeld het gebruik van voorspelbare sleutels, het gebruik van incorrecte certificaten, zwakke MAC-constructie) en functionaliteit. Nagenoeg alle tekortkomingen zijn in SSL v3 opgelost. De mogelijke opvolger van SSL is TLS (*Transport Layer Security*).
TLS is een standaardiseringsinitiatief van IETF *(Internet Engineering Task Force)* met als doel een internet-standaardversie van SSL te produceren. Het huidige ontwerp van TLS lijkt veel op SSL v3. Tussen de encryptiesuite (*een lijst van cryptografische algoritmen*) die onder SSL v3 en onder TLS beschikbaar is, bestaan kleine verschillen in de sleuteluitwisselingen en symmetrische encryptiealgoritmen. Een voorbeeld voor een dergelijk verschil is het ontbreken van de ondersteuning voor Fortezza (een smart card product voor encryptie) in TLS.

Bij de opbouw van een SSL-verbinding wisselen de client en de server eerst certificaten uit (X.509), met daarin publieke sleutels. Als de certificaten, na te zijn getoetst, worden geaccepteerd, wordt door de client random een aantal sleutels gegenereerd voor het vercijferen van de sessie en het berekenen van authenticatiecodes. Deze sessiesleutels worden door de client vercijferd met de publieke sleutel van de server en naar de server gestuurd. Vervolgens bepalen de client en de server in onderling overleg welke algoritmen ze gedurende die sessie zullen gebruiken. SSL ondersteunt onder meer RC4, DES en IDEA voor vercijfering en DSA voor digitale handtekening.

Voor- en nadelen

De voordelen van SSL zijn:

- SSL is onafhankelijk van de applicatie en infrastructuur. Het voordeel van SSL is dat het tot op het niveau van web-pagina geïmplementeerd kan worden. Het is dan niet langer noodzakelijk om SSL protectie op elke webserver of website te implementeren. De gebruikelijke benadering is om die pagina's met SSL te beschermen die vertrouwelijke en gevoelige informatie bevatten.
- SSL-enabled webclients en -servers kunnen interactief kiezen of een individuele connectie al dan niet beschermd moet zijn.

De nadelen zijn:

- Het gebruik van encryptiefaciliteiten in de transportlaag kan voor sommige applicaties problemen geven, omdat de cryptografische activiteiten door een protocol interface plaatsvinden en daardoor onopgemerkt blijven. Dit probleem wordt opgelost door SSL in de applicatie te integreren waardoor de applicaties de cryptografische activiteiten kunnen volgen.
- Servercertificaten geven de client zekerheid over de server, niet andersom. Zie ook de PI-studie met als onderwerp internet.
- In het kader van onweerlegbaarheid zijn in een SSL-omgeving extra maatregelen nodig. Overigens moet hierbij wel worden opgemerkt dat, omdat SSL zich op het netwerkniveau bevindt, het niet zonder meer een bijdrage aan de onweerlegbaarheid levert. Onweerlegbaarheid betreft immers transacties die op applicatieniveau worden afgehandeld.

Snel/langzaam

Het toepassen van encryptietechnieken binnen SSL introduceert een zekere overhead. Dit betekent dat bij gebruik van SSL er een toename is in de hoeveelheid getransporteerde data en daarmee ook een toename in het aantal datapakketjes. Deze toename in communicatie heeft een negatieve invloed op de performance bij datatransmissie tussen de server en browser.
SSL heeft ook de mogelijkheid tot compressie, maar deze optie is niet standaard ingeschakeld.

Beheeraspecten

Sleutelbeheer ten aanzien van een serversleutel. Zie ook paragraaf 4.3.1.1 over beheeraspecten HTTPS.

4.3.2.2 PGPNET

PGPNet is een VPN-oplossing die sterke banden heeft met het bekende PGP-product voor e-mail. Met behulp van PGPNet is het mogelijk om over een publiek en niet afgeschermd netwerk een beveiligde verbinding te maken tussen twee partijen. De verbinding tussen de partijen is vercijferd. Daarnaast maken de beide partijen gebruik van sterke authenticatie.
PGPNet is gebaseerd op de IPsec-standaard voor het opzetten en onderhouden van de VPN-verbinding tussen de twee partijen. PGPNet biedt hierbij de mogelijkheid om gebruik te maken van de PGP-sleutels van deze partijen voor identificatie en authenticatie.

Voor- en nadelen

De voordelen van PGPNet zijn:
- Hergebruik van de PGP-sleutels maakt het gebruik simpeler, een gebruiker hoeft minder sleutels te beheren.
- PGPNet is gebaseerd op de IPsec-standaard waardoor het mogelijk is om met andere partijen te communiceren die gebruikmaken van andere platformen en producten.

De nadelen zijn:

– PGPNet is op een beperkt aantal platformen beschikbaar en extra opties kunnen alleen gebruikt worden als er aan beide kanten van het VPN PGPNet wordt gebruikt.

Snel/langzaam

De snelheid van PGPNet is vergelijkbaar met IPsec-implementaties.

Beheeraspecten

Het beheer van een PGPNet-omgeving kan eenvoudiger zijn dan een gewone IPsec-omgeving, omdat de PGP-sleutels hergebruikt kunnen worden. Hierdoor is het sleutelbeheer eenvoudiger.

4.3.2.3 SSH Tunneling

Naast de 'gewone' interactieve terminal sessies kan SSH ook worden gebruikt om beveiligde communicatie tussen twee (niet noodzakelijk dezelfde) partijen tot stand te brengen. De twee communicerende SSH-programma's (client en server) bieden hiervoor de benodigde faciliteiten. De werking is hierbij als volgt.

De SSH-client creëert op de lokale machine één of meer netwerkpoorten waarmee een verbinding kan worden gemaakt. De beheerder van de *tunnel* bepaalt welke poorten dit precies zijn. Een gebruiker maakt verbinding met een van deze netwerkpoorten.

De data die over deze verbinding worden opgestuurd, wordt door de SSH client opgepakt en over de beveiligde verbinding naar de server gestuurd.

De server ontvangt deze data en stuurt deze vervolgens door naar een poort op zijn lokale machine, of een andere machine op het netwerk. Welke machine en poort dat precies zijn, wordt bepaald bij het opzetten van de *tunnel* door de beheerder van de SSH-*tunnel*.

Voor- en nadelen

Voordelen van SSH*Tunneling* zijn:

– Uitbreiding van een bestaande SSH-toepassing tot een VPN-toepassing is relatief eenvoudig.

– Het inrichten en het beheren van *tunnels* kan heel nauwkeurig worden gecontroleerd.

De nadelen zijn:
– *Tunneling* werkt alleen voor TCP-poorten en niet voor UDP of ICMP-poorten.
– De gebruiker die verbinding maakt met een *tunnelpoort* op de SSH client hoeft zich niet te authentiseren, maar lift mee op de identiteit van de beheerder van de SSH-*tunnel* (authenticatie op netwerkniveau).
– Het vrij kunnen opbouwen van een *tunnel* kan leiden tot een extra beveiligingsrisico bij een niet goed beveiligde client. De veiligheid van de *tunnel* is niet groter dan de veiligheid van de systemen aan weerszijden. Voor andere systemen is de *tunnel* transparant. Zij zien alleen de lokale services. Ongemerkt kunnen ze dus van onveilige diensten gebruikmaken en/of diensten aan een onveilige client leveren.

Snel/langzaam

Er kan indien gewenst gebruik worden gemaakt van compressie. Afhankelijk van de omgeving waarin SSH wordt gebruikt, kan hier snelheidwinst behaald worden.

Beheeraspecten

Voor het kunnen opzetten van SSH-*tunnel* heeft de beheerder rechten nodig op de systemen die het begin- en eindpunt van de *tunnel* vormen. Beheer van de SSH-server is centraal uit te voeren. Gebruikers zijn echter zelf verantwoordelijk voor hun eigen configuratie. Dit maakt het moeilijk centraal de gebruikers te beheren.

4.3.2.4 IPSEC

Een gangbare standaard voor encryptie op de netwerklaag is IPsec. IPsec is een standaard die door IETF ontwikkeld is om beveiliging aan een TCP/IP-netwerk toe te voegen. Het is een protocol waarmee een VPN (*Virtual Private Network*) kan worden opgezet. IPsec biedt een verzameling beveiligingsmaatregelen ten aanzien van integriteit, authenticatie, vertrouwelijkheid, sleutelbeheer en *tunneling* (LAN-to-LAN VPN).

Deze standaard wordt ondersteund door een groot aantal leveranciers en *Open Source* producten. Het biedt de mogelijkheid de communicatie te beveiligen die van een LAN via private en publieke WAN's (*Wide Area Networks*) en via het internet plaatsvindt. Voorbeelden hiervan zijn het realiseren van veilige kantoorverbindingen en veilige externe toegang via het internet.

Binnen IPsec wordt een oplossing gegeven voor encryptie en authenticatie op netwerkniveau door het gebruik van een aantal modes waaruit de gebruiker kan kiezen, zoals *transport mode* en *tunnel mode*. In *transport mode* vindt geen *tunneling* plaats, maar wordt alleen het gegevensveld van elk pakket vercijferd. Aan het pakket wordt een speciale header (zie figuur A.2) toegevoegd. Deze header bevat onder meer een *Security Parameter Index* (SPI). De SPI wordt gebruikt als index in een tabel die op elke router aanwezig is en waarin het encryptie algoritme en de sleutellengte zijn vastgelegd. In de *tunnel mode* wordt het gehele pakket vercijferd, waarna het wordt voorzien van een nieuwe IP-header. Ook hier wordt controle-informatie in een extra header opgenomen.
Binnen IPsec worden authenticatie en encryptie van elkaar gescheiden. Bij authenticatie wordt gebruikgemaakt van Authentication Headers, terwijl bij encryptie gebruik wordt gemaakt van *Encapsulated Security Payload* (ESP). De twee methoden kunnen, afhankelijk van de behoefte van de gebruiker, separaat of samen gebruikt worden.

Firewalls die gebruikmaken van IPsec, wisselen onderling symmetrische sessiesleutels uit, bijvoorbeeld door middel van een PKI.
Er zijn verschillende producten beschikbaar voor het betrouwbaar opzetten van encryptie op netwerkniveau. Daarnaast is er een *Open Source* product beschikbaar voor een aantal *Open Source* platformen (onder andere Linux).

Het IPsec protocol zal in de nabije toekomst een integraal deel gaan uitmaken van IP versie 6 (IPv6). Daarnaast is het nu al beschikbaar voor de huidige IP versie 4 (IPv4) netwerken. Vanwege de verschillen tussen IPv6 en IPv4 zijn er ook verschillen in de toepassing van IPsec, zoals de locatie van de extra toe te voegen beveiligingsinformatie binnen de pakketten en de verschillen in adressering. In het algemeen geldt dat IPv6 niet down-

ward compatible zal zijn met IPv4, en dus zal IPsec voor IPv6 ook niet compatible zijn met IPsec voor IPv4.

Voor- en nadelen

De voordelen van IPsec zijn:

- Het gebruik is transparant voor eindgebruikers en toepassingen;
- Het is een universele oplossing;
- Het bevat een filtermogelijkheid, zodat alleen geselecteerd verkeer de overhead van IPsec-verwerking hoeft te ondergaan;
- Er kunnen separate kenmerken voor verschillende communicatiepaden gehanteerd worden. Zo kunnen bepaalde communicatiepaden geauthentiseerd zijn, terwijl slechts enkele zijn vercijferd. Indien gewenst, is het ook mogelijk om *end-to-end* encryptie, met een unieke sleutel, tussen twee gescheiden delen toe te passen. Dit maakt IPsec flexibel;
- De implementatie van IPsec in een *firewall* of router levert een krachtige beveiliging, die op alle verkeer die deze grens passeert, kan worden toegepast;
- Indien nodig, kan IPsec individuele gebruikers veiligheid bieden. Dit is nuttig voor externe werkers en wanneer in verband met gevoelige toepassingen een veilig virtueel subnetwerk binnen een organisatie wordt opgezet.
- IPsec werkt onafhankelijk van de hoger gelegen applicaties. Deze applicaties behoeven geen verandering om gebruik te kunnen maken van de door IPsec geboden beveiliging.

De nadelen ervan zijn:

- IPsec definieert niet expliciet welk algoritme gehanteerd moet worden. Het maakt het mogelijk om afhankelijk van de situatie een algoritme te kiezen. Dit betekent dat IPsec even sterk of zwak is als de gekozen algoritmen en sleutels, inclusief het sleutelbeheer;
- Er zijn enkele, technisch geavanceerde, aanvallen op IPsec die een beveiliging in gevaar brengen.
- De interoperabiliteit van verschillende IPsec-implementaties laat met de huidige stand van zaken in de markt te wensen over.

Beheeraspecten

IPsec kent een open protocollenstructuur. Dat betekent dat de protocollen en algoritmen suite binnen IPsec veranderd kunnen worden, zonder dat hiervoor de IPsec-software hoeft te worden aangepast. Hierdoor is het mogelijk nieuwe procollen toe te voegen en verouderde te verwijderen. Dit maakt de implementatie van IPsec tegelijktijd flexibel en complex, mede door vele beveiligingingsopties.

4.3.2.5 Samenvattend overzicht

Tabel 4.3 geeft een samenvattend overzicht van de genoemde producten/standaarden met betrekking tot de aspecten: mate van standaardisatie, beheerinspanning, organisatorische inspanning, technische impact, beveiliging en gebruikersimpact.

4.3.3 Linkniveau

Er zijn verschillende standaarden/producten beschikbaar voor het betrouwbaar opzetten van encryptie op linkniveau. De protocollen die op linkniveau worden gepositioneerd, zijn PPTP (*Point to Point Tunneling Protocol*), L2F (*Layer2 Forwarding Protocol)* en L2TP *(Layer 2 Tunneling Protocol)*. De protocollen worden voornamelijk toegepast voor het construeren van VPN's. PPTP en L2TP hebben zelf geen voorzieningen voor encryptie en sleutelbeheer. In de huidige versie van L2TP wordt aanbevolen om hiervoor de voorzieningen van IPsec te gebruiken. Verwacht wordt dat in de toekomstige versie van PPTP ook zulke voorstellen gedaan zullen worden.
In de toekomst zullen PPTP en L2F vervangen worden door het L2TP protocol. In de volgende twee paragrafen zullen de protocollen PPTP en L2TP kort worden beschreven.

4.3.3.1 PPTP

PPTP is een protocol dat geschikt is voor zowel IP- als non-IP-omgevingen, zoals NETBEUI, IPX en AppleTalk. PPTP wordt ook ingezet voor Dial-in of client-to-LAN VPN's.

Tabel 4.3 Samenvattend overzicht

Netwerkniveau-aspecten	**SSL**	**PGPNet**	**SSH Tunneling**	**IPsec**
Standaard (Mate van Standaardisatie)	De facto standaard	+/-	+	+
Beheerinspanning	Afhankelijk van de gekozen features/ opties (sleutel-beheer voor certificaten)	n.v.t.	Decentrale configuratie en beheer	Sterk afhankelijk van de gekozen opties
Organisatorische inspanning	Introduceert centrale en decentrale rollen	n.v.t.	Decentraal beheer van sleutels	
Technische Impact	Is integraal onderdeel van meeste browsers onafhankelijk van de applicatie en infrastructuur	Versiebeheer	– SSH software benodigd aan de uiteinden van de tunnels – Eenvoudiger configuratie van de tussenliggende firewall mogelijk	– Verschillende protocollen voor sleutelbeheer Multi-point tunnels, gelijktijdig publieke en VPN-toegang tot internet – LAN-to-LAN tunneling – Intranets, extranets, remote access via tunneling
Beveiliging			Geen gebruikers-authenticatie	Geen gebruikers-authenticatie, packet authenticatie: AH header, packet encryptie: ESP header.
Gebruikers Impact	n.v.t.	– Eenvoudig sleutelbeheer – Zelfbeheer van sleutels door eindgebruikers		Transparant voor de gebruikers

Een PPTP VPN bestaat in het algemeen uit drie elementen: een netwerk access server, een PPTP-server, en een PPTP-client. De PPTP-server en -client worden geïnstalleerd onder verantwoordelijkheid van de desbetreffende organisatie, terwijl de netwerk access server aan de ISP (*Internet Service Provider*) kan worden uitbesteed. Wanneer een client voorzien wordt van PPTP-client software, is de organisatie ten aanzien van PPTP VPN niet afhankelijk van ondersteuning door een ISP. Wanneer een PPTP-server in een corporate site wordt gepositioneerd, fungeert de PPTP-server als een *security gateway*. Voor authenticatie kan gebruik worden gemaakt van verschillende protocollen waaronder RADIUS, CHAP (*Challenge Handshake Authentication Protocol)* en PAP *(Password Authentication Protocol)*.

Remote PPTP-clients worden op dezelfde wijze geauthentiseerd als bij PPP (*Point to Point Protocol*) waarbij sprake is van een dial-up verbinding tussen een RAS-client en een RAS-server (RAS staat voor *Remote Access System*). PAP en CHAP hebben geen sterke authenticatie. Er wordt slechts vertrouwd op een geheim wachtwoord dat opgeslagen is op zowel het remote- als op het lokale systeem. Bij een succesvolle aanval op één van de systemen kan gevoelige informatie uitlekken. Met behulp van CHAP- en PAP-authenticatie is het ook niet mogelijk verschillende netwerk toegangsprivileges aan verschillende gebruikers toe te kennen op een bepaald systeem. De set van privileges wordt namelijk toegekend aan een specifieke computer; iedereen die van die computer gebruikmaakt heeft dezelfde set privileges. Om privileges per computer per gebruiker toe te kennen, wordt gebruikgemaakt van het protocol RADIUS. RADIUS wordt ingezet voor zowel het beheer van *access rights* van gebruikers als voor het beheer van *security* informatie, zoals cryptografische sleutels.

Voor- en nadelen

De voordelen van PPTP zijn:

- Draait vanaf Windows NT, Windows 98-platformen.
- Voorziet in *end-to-end* en *node-to-node tunneling* (client to LAN *tunneling*).
- Maakt gebruik van bestaande Windows user domain voor authenticatie.
- Voorziet in multiprotocol mogelijkheden.
- Gebruikt RSA RC-4 encryptie.

Het heeft als nadelen:
– Het voorziet niet in data encryptie vanuit remote access servers;
– Het is sterk leverancier afhankelijk.

4.3.3.2 L2TP

Evenals PPTP is L2TP een protocol dat geschikt is voor zowel IP- als non-IP-omgevingen. Het maakt *tunneling* mogelijk via PPP, waardoor pakketjes van het type IP, IPX AppleTalk en NETBEUI via het internet vervoerd kunnen worden. L2TP wordt ook ingezet voor Dial-in of client-to-LAN VPS's.
L2TP kan worden gezien als een volgende generatie VPN-protocol, voornamelijk voor dial-in VPN's. Het combineert voorzieningen van de protocollen L2F (een *tunnelprotocol* dat Cisco als standaard heeft ingediend bij de IETF) en PPTP.

Er zijn twee componenten voor het creëren van een L2TP-*tunnel*: een LAC (L2TP *Access Concentrator*, het beginpunt van een L2TP-*tunnel*) en LNS (L2TP *Netwerk Server*, het eindpunt van een L2TP-*tunnel)* De LAC is gekoppeld aan bijvoorbeeld een *Public Switched Network* (PSTN) en zorgt voor de verbinding tussen de clients en de openbare netwerken (internet, *Frame Relay* en ATM Netwerk) (de zogeheten *remote site)*. De LNS bevindt zich tussen de openbare netwerken en de lokale netwerken (de zogeheten *central site* servers). Deze componenten geven ook de mogelijkheid om netwerkcongestie tegen te gaan.
Veel leveranciers hebben plannen om hun op PPTP gebaseerde producten geschikt te maken voor L2TP. L2TP biedt een aantal voordelen ten opzichte van PPTP, voornamelijk voor het afhandelen van multiple sessies over een *tunnel*. Er kunnen meerdere *tunnels* tussen LAC en LNS gecreëerd worden. Elke *tunnel* kan worden toegekend aan een specifieke gebruiker en/of aan gebruikersgroepen.
L2TP voorziet in een sterke veiligheid voor data, omdat het gebruikmaakt van ESP *(Encapsulated Security Payload* (encryptieservice)) van IPsec voor de vercijfering van pakketten.

Voor- en nadelen
Voordelen van L2TP zijn dat het PPTP en L2F combineert, en dat het IPsec voor encryptie gebruikt. Het heeft als nadeel dat het nog niet in veel producten is geïmplementeerd.

4.3.3.3 Samenvattend overzicht

Tabel 4.4 geeft een samenvattend overzicht van PPTP en L2TP met betrekking tot de aspecten: mate van standaardisatie, beheerinspanning, organisatorische inspanning, technische impact, beveiliging, gebruikersimpact en toepassing.

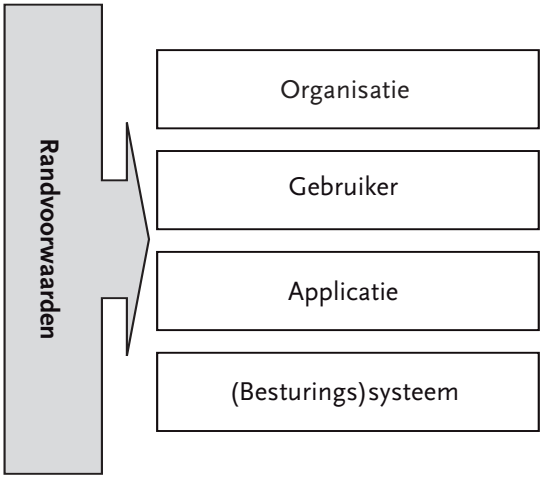
Tabel 4.4 Samenvattend overzicht

Link-encryptie aspecten	**PPTP**	**L2TP**
Standaard (Mate van standaardisatie)	Leveranciersafhankelijk	*(in ontwikkeling)*
Beheerinspanning	n.v.t.	n.v.t.
Organisatorische inspanning	Uitbesteding van PPTP functies aan een ISP (kostenreductie voor de organisatie)	n.v.t.
Technische Impact	– Geschikt voor multiprotocol omgevingen – Extra voorziening nodig voor de beveiligingsfuncties als encryptie en authenticatie – Single point to point tunnel, geen gelijktijdige internettoegang	– Geschikt voor multiprotocol omgevingen – Extra voorziening nodig voor beveiligingsfuncties als encryptie en authenticatie – Single point to point tunnel, geen gelijktijdige internettoegang
Beveiliging	– Geen gebruikers authenticatie – Packet authenticatie en encryptie in leverancierspecifieke implementaties – Geen sleutelbeheer	– Geen gebruikers authenticatie – Packet authenticatie en encryptie in leverancierspecifieke implementaties
Gebruikers Impact	n.v.t.	n.v.t.
Toepassing	Client to server, remote access via tunneling	Client to server, remote access via tunneling

5 Encryptie bij opslag

5.1 Inleiding

Dit hoofdstuk gaat in op de praktische vragen die een rol spelen bij opslag van data in een omgeving waar cryptografie wordt toegepast. Opslag van vercijferde gegevens blijkt, juist ten opzichte van een omgeving zonder vercijfering, in grote mate de complexiteit van een omgeving te bepalen. Deze complexiteit uit zich met name in het beheer van een dergelijke omgeving, maar evenzo in de maatregelen die op technisch en gebruikersniveau genomen moeten worden. Aan de beheeraspecten wijden we een apart hoofdstuk (hoofdstuk 6), maar in dit hoofdstuk over opslag ontkomen we niet aan de relatie met het beheer.



Figuur 5.1 Model voor encryptie bij opslag van gegevens

Voor encryptie bij opslag is een model te gebruiken analoog aan het in het vorige hoofdstuk gehanteerde OSI-model, zie ook figuur 5.1. Dit model is nodig om helderheid te behouden in de normen en maatregelen voor encryptie bij opslag. Het is namelijk niet voldoende om uitsluitend naar het technische niveau te kijken. We onderkennen vier niveaus of lagen waar encryptie van opgeslagen gegevens gevolgen heeft. Als eerste laag daarin bekijken we de *organisatorische aspecten* van opslag van vercijferde gegevens. Met name op dit niveau is sleutelbeheer van groot belang. Vervolgens 'dalen we af' naar de individuele *gebruiker*. Op deze laag speelt de impact van het gebruik van encryptie op de individuele gebruiker de hoofdrol. De volgende laag is die van de *applicatie* die door de gebruiker wordt gebruikt. Ook de te gebruiken applicaties voor encryptie van opgeslagen gegevens zullen aan specifieke eisen moeten voldoen. Tot slot belanden we op de technische laag: het *systeem*, bestaande uit de hardware en de besturingssoftware en de daaraan gekoppelde bedreigingen en maatregelen.

Het belang van deze lagen laat zich als volgt verklaren. Om voldoende aan de gestelde randvoorwaarden te kunnen voldoen, zal het geheel aan maatregelen over alle lagen in evenwicht moeten zijn. Immers, als de maatregelen op de hoogste drie niveaus goed zijn geregeld, maar aan het onderste niveau is weinig aandacht besteed, dan zal de kans op inbreuk op het geheel alsnog groot zijn. Het principe van 'de keten is zo sterk als de zwakste schakel' is hier van toepassing. In de praktijk blijkt vaak veel aandacht te zijn voor de technische lagen, maar wordt bijvoorbeeld de invloed van de gebruiker onderschat.
Dezelfde figuur wordt in dit hoofdstuk gebruikt als referentiekader voor de normen en maatregelen die van belang zijn bij encryptie van opgeslagen gegevens. Het hoofdstuk is dan ook als volgt opgebouwd. In de eerste paragraaf wordt een kader met randvoorwaarden geschetst aan de hand van de omgevingsfactoren. De volgende paragrafen gaan respectievelijk in op de organisatie, de gebruiker, de applicatie en het (besturings)systeem.

5.2 Randvoorwaarden

In deze paragraaf gaan we in op de randvoorwaarden die een rol spelen bij encryptie tijdens opslag van gegevens. Dit betreft de invloed van wetgeving op de te nemen maatregelen en de randvoorwaarden die vanuit organisatie-oogpunt worden gesteld aan beschikbaarheid, vertrouwelijkheid en integriteit van gegevens. Deze paragraaf heeft een beschrijvend karakter en heeft als doel het bieden van een achtergrond bij de later in dit hoofdstuk opgenomen basisnormen en -maatregelen.

5.2.1 Invloed wetgeving op de vercijfering van gegevens

Met het toepassen van vercijfering op opgeslagen gegevens wijzigt ook de relatie met de bestaande wetgeving. De wetgeving ijlt de technische ontwikkelingen achterna. De bestaande wetgeving dient dus opnieuw geïnterpreteerd te worden en in een enkel geval zelfs herzien te worden.

De belangrijkste wet- en regelgeving bestaat uit de Wet op Openbaarheid van Bestuur, de Wet op de Staatsgeheimen, de Archiefwet, de Wet op de Computer Criminaliteit, Exportcontrole en -restricties en de wetgeving omtrent rechtmatige toegang.

5.2.1.1 Wet op Openbaarheid van Bestuur

De Wet Openbaarheid van Bestuur (WOB) kent als doel het waarborgen van de controleerbaarheid van de overheid. Alle overheidsorganen vallen onder deze wetgeving. De WOB is niet volledig eenduidig. Ten aanzien van een aantal punten is men afhankelijk van jurisprudentie (uitspraken die gedaan zijn door een rechter aan de hand van een concreet geval).
Inhoudelijk bepaalt de wet dat iedereen, rechtens afdwingbaar, recht op informatie over een bestuurlijke aangelegenheid heeft, mits deze informatie is neergelegd in een document dat bij een overheidsorgaan berust. Daarnaast heeft de overheid de plicht om uit eigen beweging informatie te verschaffen over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodanig dat in het belang is van een goede en democratische bestuursvoering.

De wet kent een aantal uitzonderingen, waaronder:
- informatie die de eenheid van de Kroon in gevaar zouden kunnen brengen;
- informatie die de veiligheid van de Staat zou kunnen schaden;
- informatie die betrekking heeft op bedrijfs- of fabricagegegevens die in vertrouwen aan de overheid zijn meegedeeld.

Daarnaast kent de wet een aantal uitzonderingen indien het belang van de wet niet opweegt tegen de volgende belangen. Dit zijn onder andere:
- de betrekkingen van Nederland met andere staten en met internationale organisaties;
- opsporing en vervolging van strafbare feiten;
- de eerbiediging van de persoonlijke levenssfeer (Wet Bescherming Persoonsgegevens).

Voor een organisatie betekent dit dat documenten die onder deze wet vallen, gepubliceerd dienen te kunnen worden door het betreffende bestuursorgaan. In dit geval zal in principe de eigenaar van de gegevens ervoor zorg dragen dat de betreffende documenten onvercijferd worden gepubliceerd. Naast de directe toepassing van de Wet op Actuele Documenten, dient ook de Archiefwet (zie hieronder) in acht te worden genomen.

5.2.1.1 Wet op de Staatsgeheimen

Deze wet bevat nadere voorzieningen over de bescherming van staatsgeheimen. Een staatsgeheim is een gegeven, waarvan de geheimhouding door het belang van de Staat of zijn bondgenoten wordt geboden. In het algemeen kan gezegd worden dat het gegevens betreft, waarvan kennisneming door onbevoegden in meer of mindere mate schade aan de staatsveiligheid of andere gewichtige belangen van de Staat of van zijn bondgenoten kan veroorzaken. Staatsgeheimen kunnen worden onderverdeeld in de categorieën zeer geheim, geheim en confidentieel.
Hieruit kan worden afgeleid dat de toepassing van cryptografie voor staatsgeheime gegevens voldoet aan de eisen aan exclusiviteit, integriteit en beschikbaarheid. Dat betreft zowel verwerking, opslag als uitwisseling van de informatie.

5.2.1.3 Archiefwet

De Archiefwet 1995 en het Archiefbesluit 1995 (gepubliceerd in de Staatsbladen 1995, nrs. 276 en 277) zijn een instrument om de openbaarheid en het behoud van archieven te garanderen. De wet geeft het kader voor het beheer van binnen de organisatie gevormde gegevens. Voor een volledige toetsing wordt verwezen naar de originele wettekst.

5.2.1.4 Wet op de Computer Criminaliteit

De Wet Computercriminaliteit richt zich in feite uitsluitend op de strafbaarstelling van personen die zich schuldig maken aan computervredebreuk. Onder computervredebreuk wordt verstaan het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk. Beveiliging wordt in deze wet geformuleerd als voorwaarde voor strafbaarstelling en niet als eis. De wet vereist wel dat een zekere mate van beveiliging noodzakelijk is om strafbaarstelling mogelijk te maken. Met name de gedefinieerde niveaus 'minimaal beveiligingsniveau' en 'adequaat beveiligingsniveau' zijn van belang. In het eerste geval zijn uitsluitend minimale, maar daadwerkelijke maatregelen noodzakelijk. Strafbaarstelling is in dit geval mogelijk. Van adequaat beveiligingsniveau is sprake als er een evenwicht is tussen het te beveiligen belang en de mate waarin beveiligingsmaatregelen zijn aangebracht, in balans met de bedreigingen.
Op de toepassing van cryptografie heeft deze wet weinig invloed. Op grond van de overige eisen kan ook zonder cryptografie al snel worden voldaan aan het 'minimale beveiligingsniveau'.

5.2.1.5 Exportcontrole en -restricties

Encryptie dient te voldoen aan de vigerende wet- en regelgeving over de exportcontrole. Cryptografische producten van een bepaalde sterkte zijn onder exportcontrole gebracht op grond van het Wassenaar Arrangement.
Het Wassenaar Arrangement is bedoeld om bij te dragen tot de regionale en internationale beveiliging en stabiliteit door het promoten van transparantie en grotere verantwoordelijkheid in transport van conventi-

onele wapens en *dual-use* middelen en technieken; daarmee destabiliserende escalatie voorkomend. Onder *dual-use* wordt verstaan dat de middelen zowel voor militair als civiel gebruik toepasbaar zijn. Ook cryptografie valt onder deze regeling.
De beslissing voor het al of niet transporteren van zaken die onder het Wassenaar Arrangement vallen, is aan het betreffende land. Elk transport of weigering tot transport wordt geregistreerd binnen het Wassenaar Arrangement.

5.2.1.6 Rechtmatige Toegang (Law Enforcement)

Rechtmatige toegang (ook wel bekend als *Law Enforcement*) introduceert een extra probleem. In het voorgaande is met name aandacht besteed aan een enterprise-omgeving: de problematiek die zich voordoet bij het gebruik van encryptie binnen een organisatie. Rechtmatige toegang houdt in dat een persoon of organisatie op last van een gerechtelijk bevel aan een externe partij toegang dient te verlenen tot gespecificeerde informatie. Hiervoor dient geregeld te zijn dat een externe partij toegang kan krijgen tot de gebruikte sleutels zodanig dat de vercijferde informatie beschikbaar komt voor deze derde partij. In de praktijk komt dit neer op het archiveren van ieders privé-sleutel, waarbij deze slechts onder gecontroleerde omstandigheden toegankelijk is voor bevoegden.

5.2.2 Beschikbaarheid van vercijferde gegevens

Het vercijferen van gegevens heeft een grote impact op gebruikers en beheerders. Immers, het raakt veel situaties en handelingen waar gebruikers en beheerders aan gewend zijn geraakt. Deze paragraaf gaat in op deze nieuwe dimensie: op welke situaties en handelingen heeft deze vorm van beveiliging een verregaande invloed. In deze subparagraaf wordt gekozen voor de invalshoek 'beschikbaarheid van de gegevens'.

Levensduur gegevens (information life-cycle)
De levensduur van de gegevens krijgt een meer uitgesproken rol. In het verleden was het beheer van gegevens meer gericht op de exclusiviteit (vertrouwelijkheid) van de gegevens, de beschikbaarheid bij uitval van

systemen en het capaciteitsbeheer van de opslagmedia. Nu wordt de impact van de levensduur – de tijdsduur dat de gegevens zowel beschikbaar als vercijferd moeten zijn – groter. Immers, de gegevens worden met behulp van een bepaald algoritme en een bepaalde sleutel opgeslagen. De gegevens zullen gedurende de levensduur ontsloten moeten kunnen worden, ook na bijvoorbeeld een functiewijziging van de eigenaar. Daarnaast zullen in het algemeen de gegevens langer meegaan dan de gebruikte sleutel en wellicht ook langer dan het gebruikte algoritme. Het dient dan ook duidelijk te zijn welke stappen ondernomen moeten worden bij het vernieuwen van de sleutel of het algoritme. En uiteraard dient men te weten welke gevolgen dit heeft voor de technische, procedurele en organisatorische maatregelen.

Uitval van (besturings-)systeem

Uitval van het besturingssysteem kan gevolgen hebben voor het encryptiesysteem van de gebruiker. De ontcijferingssleutel van de gebruiker kan kwijtraken of corrupt raken, of er blijven onvercijferde restanten van gegevens achter. Het corrupt of beschadigd raken van de ontcijferingssleutel kan zich voordoen als deze is opgeslagen op een harde schijf. Bij uitval van het besturingssysteem kan de informatie op de harde schijf (zoals de ontcijferingssleutel) beschadigd worden. Alle gegevens die met deze sleutel ontcijferd dienen te worden, zijn daarmee ontoegankelijk geworden.

Het tweede beschreven geval is een risico bij het gebruik van bijvoorbeeld Windows besturingssoftware. Bij een onverwachte uitval van het (besturings-)systeem is het mogelijk dat bestanden of delen van bestanden in onvercijferde vorm achterblijven op het systeem. Denk daarbij aan tijdelijke directories of de Windows *swap file*.

Back-up en restore van beveiligde gegevens

Juist de bestaande back-up en restore procedures zijn voorbeelden van ingesleten handelingen die in een nieuw licht komen te staan bij toepassing van vercijfering van opgeslagen informatie. Het *maken* van back-ups vormt geen probleem aangezien er voor het back-up mechanisme geen verschil bestaat tussen vercijferde en niet vercijferde gegevens. Vercijferde gegevens kunnen zonder problemen een back-up procedure ondergaan.

Het uitvoeren van een restore-operatie kent wel een aanpassing. Het is vanzelfsprekend de bedoeling dat de gebruiker toegang heeft tot de herstelde gegevens. Wanneer in de periode tussen het maken van een back-up en het terughalen van een vercijferd bestand een wijziging heeft plaatsgevonden in het sleutelmateriaal van de gebruiker, vraagt dit om extra handelingen. Zo zal de eindgebruiker nog over zijn oude sleutel moeten beschikken om toegang te kunnen krijgen tot zijn gegevens. Hiermee dient rekening gehouden te worden bij het vernieuwen van sleutels.

Functiewijziging eigenaar

Als een werknemer het bedrijf verlaat of een andere functie gaat bekleden, zullen de gegevens waar hij of zij eigenaar van is, toegankelijk dienen te blijven voor bijvoorbeeld zijn opvolger, vervanger of meerdere. Deze gegevens zijn echter vercijferd. Om de gegevens alsnog te ontsluiten zijn dus aanvullende maatregelen nodig.

Compromittatie van de (privé) sleutel

Als de (privé) sleutel van een gebruiker gecompromitteerd raakt, is het van belang dat de gegevens die met deze sleutel ontcijferd kunnen worden, niet toegankelijk zijn voor onbevoegden, maar wel toegankelijk zijn voor de eigenaar van deze sleutel. Normaal gesproken zal de eigenaar de beschikking krijgen over een nieuw sleutelpaar. Dit proces kan relatief eenvoudig uitgevoerd worden. De uitdaging ligt bij de gegevens die in het verleden zijn opgeslagen en uitsluitend toegankelijk zijn met de gecompromitteerde sleutel. In het ergste geval is het niet mogelijk om met zekerheid vast te stellen dat de gecompromitteerde sleutel niet meer misbruikt kan worden. Het uitreiken van een nieuwe sleutel zal dan gepaard moeten gaan met het opnieuw vercijferen van de nog actuele gegevens. Juist in deze situatie doet zich het probleem voor dat aan de hand van de sleutel de daarmee vercijferde gegevens te vinden moeten zijn. Vaak zal de gebruiker voldoende zicht hebben op zijn actuele gegevens. Echter, bij oudere of gearchiveerde gegevens is dit minder duidelijk. Na het verkrijgen van de nieuwe sleutel zullen ook deze gegevens beschikbaar en toegankelijk moeten blijven.
Een mogelijkheid om deze problematiek te voorkomen, is om geen encryptie (!) te gebruiken. Hoewel dit in lijkt te gaan tegen de behoefte

om informatie te beveiligen, kan dit een bewuste keuze zijn. De bescherming van informatie dient in dit geval op een andere wijze geregeld te worden. Zo is het mogelijk om de aandacht meer te richten op fysieke en organisatorische beveiliging van de locatie waar de informatie is opgeslagen. Een andere optie is om juist meer correctieve maatregelen te treffen zodat de informatie hersteld kan worden.

Om compromittatie van de privé-sleutel te voorkomen, dient deze sleutel op een voldoende veilige wijze opgeslagen te worden. Op dit moment is een smartcard het meest geschikte medium. Vercijferde opslag in software op een harde schijf of diskette is een minder beveiligde omgeving vanwege een hogere kans op het breken van de softwarematige beveiliging. Niet elke smartcard is echter 'veilig genoeg'. Een smartcard dient bestand te zijn tegen de bekende aanvallen tegen smartcards. Dit zijn onder meer aanvallen waarbij de opbouw van het geheugen met een microscoop wordt geanalyseerd of waarbij de smartcard elektronisch onbevoegd wordt uitgelezen. Als de smartcard gebruikt wordt in combinatie met biometrie, dan dient de biometrische toepassing voldoende sterk te zijn. Zo dient het bijvoorbeeld niet mogelijk te zijn dat het gebruik van een cellofaan met vingerafdruk voldoende is om de authenticatie uit te voeren.

Delen van gegevens met een groep gebruikers

Ook het gebruik van gegevens door een beperkte groep gebruikers heeft een nauwe relatie met het gebruik van encryptie. Dit laat zich het makkelijkst illustreren met een voorbeeld. Indien een bestand in een vercijferde vorm wordt gepubliceerd voor tien personen, kan dit zonder problemen gebeuren. Als er echter een nieuwe gebruiker komt die ook toegang moet krijgen tot het bestand, ontstaat een nieuwe situatie. Het bestand zal ook voor deze persoon ontsloten moeten worden. Het is uiteraard ook in een groep van belang om de beveiliging van de informatie zeker te stellen als een lid van de groep de organisatie verlaat of als zijn of haar sleutel gecompromitteerd raakt. Voor dergelijke situaties zullen maatregelen getroffen moeten worden.

Overigens zal normaal gesproken de toegang tot een bestand gerealiseerd worden met behulp van toegangsrechten in plaats van met vercijfering. Toch is het denkbaar dat uitsluitend de eigenaar van gegevens de

toegang kan controleren in plaats van dat dit via een systeembeheerder loopt. In dergelijke gevallen doet dit type probleem zich voor.

5.2.3 Vertrouwelijkheid van opgeslagen gegevens

Vercijfering van gegevens heeft als doel het garanderen van de vertrouwelijkheid van deze gegevens. Alleen die personen die gerechtigd zijn tot het lezen van bepaalde informatie mogen daadwerkelijk toegang hebben tot deze informatie. Voor het realiseren van de vertrouwelijkheid (exclusiviteit) van opgeslagen informatie worden hulpmiddelen gebruikt. Deze hulpmiddelen zullen van voldoende kwaliteit moeten zijn om adequate vercijfering te kunnen garanderen. Dit komt tot uiting in eisen aan het gebruikte algoritme en de mogelijkheden om sleutels op te slaan.
Daarnaast is het voor de vertrouwelijkheidsaspecten bij het vercijferen van opgeslagen gegevens van groot belang om de risico's van de gebruikte technische hulpmiddelen te onderkennen en passende maatregelen te nemen. Het is immers niet zinvol om een zeer sterk algoritme te gebruiken voor vercijfering als de gebruikte hulpmiddelen een onvercijferde kopie van een bestand op de schijf achterlaten: de ketting is zo sterk als de zwakste schakel.

5.2.4 Integriteit van opgeslagen gegevens en authenticatie

Vanzelfsprekend is, naast de beschikbaarheid en vertrouwelijkheid van opgeslagen gegevens, ook de integriteit van deze gegevens van belang. Voor bepaalde bedrijfsgegevens zal een garantie vereist worden dat de gegevens niet gewijzigd kunnen worden. Daarnaast kan het in bepaalde toepassingen zo zijn dat meer dan alleen de integriteit van gegevens gewaarborgd dient te worden. We spreken dan van maatregelen die voorkomen dat personen achteraf kunnen ontkennen dat zij een bepaalde handeling hebben verricht (onweerlegbaarheid of *non-repudiation*). Andere maatregelen bieden een extra garantie tegen misbruik van de identiteit van een bepaald persoon. In de praktijk komt dit neer op het

garanderen van de koppeling tussen een document en de auteur daarvan, of van de koppeling tussen een document en een tijdsaanduiding.
Het garanderen van de integriteit van gegevens wordt gedaan met een berekening, uitgevoerd op de gegevens zodanig dat een kenmerk van deze gegevens ontstaat. De berekeningsmethode, het algoritme, dient zodanig opgebouwd te zijn dat verschillende gegevens tot verschillende kenmerken leiden. Vaak gaat deze toepassing samen met het plaatsen van een digitale handtekening op een bestand. Dit houdt in dat het kenmerk van de gegevens wordt gekoppeld met de privé-sleutel van de eigenaar van deze sleutel. De technische werking van deze functie is elders in deze studie beschreven.

Wanneer de bekrachtiging van de koppeling tussen een document en de auteur daarvan gewaarborgd dient te worden, kan vaak volstaan worden met een digitale handtekening. Dit is echter geen formele bekrachtiging, in specifieke toepassingen zal het gewenst zijn om deze koppeling te laten bekrachtigen door een derde partij. Deze functie is te vergelijken met de notaris in de 'gewone' wereld. De notaris bekrachtigt bijvoorbeeld een huisoverdracht met zijn handtekening en stempel. In het elektronische geval plaatst deze derde partij een digitale handtekening over de combinatie van gegevens en auteurshandtekening heen. De technische werking hiervan is hetzelfde als het plaatsen van een digitale handtekening.
De Europese wetgeving kent specifieke eisen voor het gebruik van een digitale handtekening, een handtekening die juridisch gelijkwaardig is met de handgeschreven handtekening. Eén van deze eisen is dat er gebruikgemaakt wordt van een smartcard voor opslag van de privé-sleutel. Daarbij wordt tevens vereist dat deze sleutel niet van de kaart af komt bij gebruik: berekeningen dienen dus op de smartcard plaats te vinden. Het gebruik van een smartcard biedt een sterkere beveiliging van de opgeslagen sleutel dan wanneer deze in een zogenaamde software wallet wordt opgeslagen, vercijferde opslag op bijvoorbeeld een harde schijf of diskette.

Tot slot kan het noodzakelijk zijn dat een tijdstempel op een document wordt gezet om formeel te bekrachtigen dat een document op een bepaald tijdstip is aangemaakt. Dit kan van toepassing zijn bij formele

contracten waarbij het moment van ingaan van belang is. In dit geval plaatst de derde partij een digitale handtekening over het totaal van het document en de tijdstempel.

5.2.5 Archivering van vercijferde gegevens

Deze subparagraaf gaat in op opslag van vercijferde gegevens voor archivering. We staan er even bij stil, omdat archivering opslag met een bijzonder karakter is, namelijk langdurige opslag. Deels vloeit deze paragraaf voort uit de voorgaande paragrafen.

Uit het Handboek EDP-auditing:

– *Juridisch archief*: dit is een bestand waarin (elektronische) berichten worden bewaard in de vorm waarin ze zijn verzonden. Bij jurisprudentie is het van belang dat het bewijs in ongewijzigde vorm aanwezig is. Dit houdt in dat vercijferde berichten hier ook in kunnen staan, inclusief de gegevens van de verzender en ontvanger. Dit type archief is bedoeld om de geldigheid van ontvangen berichten te kunnen aantonen. Om te kunnen voldoen aan de eisen voor een juridisch archief dient gewaarborgd te zijn dat in oorspronkelijke vorm opgeslagen bestanden toegankelijk blijven voor de tijd dat dit nodig is. Met andere woorden: de sleutels om toegang te krijgen tot deze bestanden dienen alle beschikbaar te zijn of beschikbaar gemaakt te kunnen worden.
– *Notarisarchief* (Administratief archief): in dit archief worden uitsluitend onvercijferde berichten opgeslagen. In dit geval is er dus geen relatie met het sleutelbeheer. Met behulp van afdoende procedurele, organisatorische en technische maatregelen (platformbeveiliging) dient de juistheid en volledigheid van het archief gewaarborgd te worden.

Zoals aangegeven kent alleen het juridisch archief implicaties in relatie tot encryptie. Dit laat zich toelichten met een voorbeeld. Stel dat een vercijferd en elektronisch getekend bestand (met asymmetrische encryptie) gedurende vijf jaar gearchiveerd moet worden en dat sleutels jaarlijks worden vervangen. Er dienen maatregelen getroffen te worden die

garanderen dat de informatie na de genoemde vijf jaar nog steeds ontcijferd kan worden.

5.3 Organisatie

Deze paragraaf gaat in op de organisatorische aspecten die een rol spelen bij encryptie van opgeslagen gegevens. Dit betreft de maatregelen die op organisatiebreed niveau genomen dienen te worden om encryptie te kunnen toepassen. In deze paragraaf ligt in het algemeen de nadruk op het sleutelbeheer en het beheer van de applicaties die worden gebruikt voor het toepassen van encryptie bij opslag. In hoofdstuk 6 wordt dieper ingegaan op het beheer en het sleutelbeheer in het bijzonder.

5.3.2 Basisnormen

1 Binnen een organisatie dient het duidelijk te zijn van welke gegevens op welke wijze de beschikbaarheid, vertrouwelijkheid en integriteit gegarandeerd dienen te worden.
2 (overheid) Vercijferde gegevens die onder de Wet op openbaarheid van bestuur vallen, dienen te allen tijde door de organisatie beschikbaar (leesbaar) te kunnen worden gesteld aan derden.
3 Vercijferde gegevens die van belang zijn voor de fiscus, dienen leesbaar beschikbaar gesteld te kunnen worden aan de fiscus indien daarom wordt gevraagd. Dit geldt uitsluitend in het geval dat de betreffende gegevens alleen in elektronische vorm beschikbaar zijn.
4 Op last van Rechtmatige Toegang (zie paragraaf 5.2.1.6) dienen vercijferde gegevens te allen tijde door de organisatie leesbaar beschikbaar gesteld te kunnen worden aan derden.
5 Vercijferde bedrijfsgegevens dienen leesbaar te zijn gedurende de door het bedrijfsproces vereiste periode. Dit geldt ook voor situaties zoals brand en personeelsverloop.
6 Vercijferde gegevens dienen in vercijferde vorm te worden gearchiveerd om een juridisch archief te creëren.
7 De mate van beveiliging van de vercijferde gegevens dient gedurende de vereiste beschikbaarheidstermijn gewaarborgd te zijn.

8 Een situatie waarbij een privé-sleutel van een gebruiker gecompromitteerd is, mag maximaal beperkte risico's opleveren voor beveiligde gegevens.
9 De handelingen om vercijferde gegevens te benaderen dienen vastgelegd te worden waarbij deze handelingen tot op de persoon herleidbaar zijn.

5.3.2 Basismaatregelen

De onderstaande maatregelen zijn gegroepeerd per basisnorm. Om de praktische haalbaarheid te garanderen, is aangegeven wanneer de maatregel aanvullend is. De overige maatregelen dienen wel ingevuld te worden om een afdoende beveiligingsniveau te behalen. Voor kleine organisaties zal de invulling met name pragmatisch zijn.

Ad 1

a Er is een overzicht van gegevens waarin is aangegeven op welke wijze deze vercijferd dienen te worden. Dit betreft de verantwoordelijke, de te volgen procedure en de beschikbare hulpmiddelen om de vercijfering uit te voeren.
b Er zijn procedures voor gebruikers voor het vercijferen van gegevens.
c Er is een procedure beschikbaar waarin sleutelvernieuwing en sleutelarchivering wordt beschreven.
d (aanvullende maatregel) Richt een team op dat zorg draagt voor periodieke controle van de wijze waarop gebruikers in de praktijk omgaan met de vercijfering van gegevens.

Ad 2, 3 en 4

a Er is een procedure beschreven waarin het op verzoek en op gecontroleerde wijze publiceren van vercijferde gegevens is beschreven. Deze procedure geldt uitstluitend voor de overheid.

Ad 2, 3, 4 en 5

a Eén of meerdere van onderstaande maatregelen zijn genomen:
  – Maak gebruik van functiegerelateerd sleutelmateriaal voor bedrijfskritische gegevens in plaats van persoonsgerelateerd

sleutelmateriaal waarbij de beschikbaarheid van het functiegerelateerde sleutelmateriaal te allen tijde gegarandeerd is.
  - Kies een applicatie die het gebruik van een *master key*, waarmee vercijferde gegevens te allen tijde ontcijferd kunnen worden, ondersteunt.
  - Archiveer alle uitgegeven privé-sleutels op een centrale plaats die goed is beveiligd tegen bedreigingen.

b Vercijferde gegevens worden volgens dezelfde beheerprocedures (zoals back-upprocedures) behandeld als normale gegevens.

Ad 6

a Er is een procedure voor de archivering van vercijferde gegevens.

b De bij de gearchiveerde vercijferde gegevens behorende sleutels en algoritmen worden ook gearchiveerd om de beschikbaarheid van de gegevens te waarborgen.

Ad 7

a Ten minste één van de onderstaande maatregelen is geïmplementeerd:
  - Vercijfer een vercijferd archief opnieuw, wanneer een nieuw algoritme en/of een nieuwe sleutellengte wordt gekozen voor vercijfering van gegevens.
  - Zorg voor een extra beveiliging van het archief met fysieke en procedurele maatregelen.

Ad 8

a Zorg voor voldoende compartimentering, zodat er verschillende ontcijfersleutels worden gebruikt voor verschillende typen gegevens danwel dat elke gebruiker een unieke ontcijfersleutel heeft.

Ad 9

a Er is ten minste één van onderstaande maatregelen gekozen:
  - Maak gebruik van persoonsgerelateerd sleutelmateriaal;
  - Maak gebruik van functiegerelateerd sleutelmateriaal waarbij eenduidig wordt vastgelegd welke persoon op welk moment van het functiegerelateerde sleutelmateriaal gebruik heeft gemaakt.

b Leg de door gebruikers uitgevoerde handelingen op een controleerbare wijze vast.

5.4 Gebruiker

Deze paragraaf beschrijft welke maatregelen een gebruiker dient te nemen om encryptie toe te kunnen passen bij opslag. Daarbij gaat het om de maatregelen die ervoor zorgen dat de door de gebruiker gewenste functionaliteit niet in gevaar komt, maar ook die ervoor zorgen dat een voldoende beveiligingsniveau wordt behaald. Immers, ondoordachte handelingen van een gebruiker kunnen de technische beveiliging van applicaties en systemen geheel tenietdoen. Een voorbeeld hiervan is de welbekende post-it met wachtwoord dat onder het toetsenbord van een PC is geplakt.

5.4.1 Basisnormen

1 De gebruiker dient zorgvuldig om te gaan met het vercijferen van gegevens.
2 De gebruiker dient zorgvuldig om te gaan met de te gebruiken applicaties voor vercijfering van gegevens.

5.4.2 Basismaatregelen

Ad 1

a De gebruiker beschikt over de benodigde hulpmiddelen en *tools* voor het vercijferen van gegevens.
b De gebruiker beschikt over de benodigde procedures voor het vercijferen van gegevens.
c De gebruiker heeft kennis van de procedures voor het vercijferen van gegevens.

Ad 2

a De gebruiker volgt opleidingen voor het gebruik van de vercijferapplicaties.
b De gebruiker beschikt over duidelijke handleidingen van de vercijferapplicaties.

5.5 Applicatie

In deze paragraaf wordt beschreven welke normen en maatregelen van toepassing zijn op het niveau van de door de gebruiker gebruikte applicatie. Dit betreft de infrastructuur die wordt gebruikt voor bijvoorbeeld vercijfering van een harde schijf. De eisen aan de applicatie komen voort vanuit de gedachte dat de applicatie enerzijds bestand dient te zijn tegen aanvallen en anderzijds de gebruiker niet noemenswaardig mag hinderen in de door hem gewenste functionaliteit. Immers, als het gebruik van een applicatie voor encryptie van opgeslagen gegevens niet voldoende gebruikersvriendelijk is, zal de verleiding voor de gebruiker groot zijn om de beveiliging te omzeilen.
De genoemde normen dienen gelezen te worden als algemene selectiecriteria (zie ook hoofdstuk 3) voor applicaties. De beschreven normen zijn niet bedoeld als normen om een specifieke applicatie in te richten. Daarvoor dient immers eerst een selectie gemaakt te worden voor een applicatie.

5.5.1 Basisnormen

1 De te gebruiken hulpmiddelen (*tools*, applicaties) dienen dusdanig transparant te zijn dat de gebruiker niet wordt gehinderd in zijn dagelijkse werkzaamheden. Anderzijds dienen de hulpmiddelen wel duidelijk de aanwezigheid en het gebruik van de aanwezige beveiligingsfuncties te tonen, zodat de gebruiker zich bewust is van deze beveiligingsfuncties. Zie ook hoofdstuk 3 bij selectiecriteria.
2 De te gebruiken hulpmiddelen (*tools*) dienen de mogelijkheid te bieden om gegevens vercijferd op te slaan zodanig dat deze gegevens voor een groep van meerdere (geautoriseerde) gebruikers toegankelijk zijn, en niet uitsluitend voor de eigenaar.
3 De te gebruiken hulpmiddelen voor de beveiliging van de gegevens die vallen onder de Wet op de Staatsgeheimen, dienen door de Nederlandse overheid geaccrediteerd te zijn voor de beoogde toepassing.

5.5.2 Basismaatregelen

De onderstaande maatregelen volgen direct uit bovenstaande normen. De maatregelen zijn selectiecriteria voor applicaties en dienen dan ook samen met de criteria uit hoofdstuk 3 gelezen te worden.

Ad 1

a Kies een applicatie waarbij bij een crash de gegevens nog steeds vercijferd zijn.

b Kies een applicatie die functioneert bij het gebruik van meerdere partities op de harde schijf.

Ad 2

a Kies een applicatie met een beproefd concept in grotere organisaties.

Ad 3

a Kies een applicatie die sterke authenticatie ondersteunt.

b Kies een applicatie die het gebruik van hardwarematige cryptomodules ondersteunt.

c (overheid) Kies een applicatie die toetsbaar is voor gebruik van gegevens die vallen onder de Wet op de staatsgeheimen.

d Kies een applicatie die het importeren van extern gegenereerde sleutels ondersteunt.

e Kies een applicatie die afdoende sterke algoritmen en lange sleutels ondersteunt (zoals op dit moment 3DES, CAST-128, Rijndael/AES, RSA).

f Kies een applicatie die vernieuwing van sleutels ondersteunt.

g Kies een applicatie waarbij tijdens gebruik alleen geopende bestanden zijn ontcijferd.

h Kies een applicatie waarbij het gebruik van tijdelijke geheugens (Windows *swap file*, Temporary Directory, enzovoort) niet aanwezig is of waarbij deze geheugens op een betrouwbare wijze geschoond worden.

5.6 (Besturings)systeem

Deze laatste paragraaf gaat in op de normen en maatregelen die gelden voor het systeem en besturingssysteem waarop de encryptieapplicaties

worden gebruikt. Daarbij dient opgemerkt te worden dat het haalbare beveiligingsniveau in sterke mate afhangt van de keuze voor het besturingssysteem (bijvoorbeeld Windows 95, Unix). Onderstaande normen en maatregelen kunnen gezien worden als algemeen geldig, maar beschreven vanuit de Windows-familie omdat deze systemen in de praktijk het meest voorkomen voor opslag van gegevens. In de betreffende PI-studies is uitgebreidere informatie beschikbaar over de beveiliging binnen verschillende besturingssystemen.

5.6.1 Basisnormen

1 Vercijferde gegevens mogen niet verminkt of openbaar worden na uitval van het besturingssysteem op het systeem waar ook de vercijferde gegevens zijn opgeslagen.
2 Vercijferde gegevens mogen niet verloren gaan bij uitval van kritische systeemcomponenten die gebruikt worden voor de opslag van gegevens.
3 Vercijferde gegevens dienen hersteld te kunnen worden na uitval van kritische systeemcomponenten die gebruikt worden voor de opslag van gegevens.
4 Na gebruik van vercijferde gegevens dienen geen onvercijferde restanten van deze gegevens meer aanwezig te zijn op het systeem. Deze gegevens zouden kunnen resteren in het virtuele geheugen dat besturingssystemen hanteren (Windows *swap file*, directory met tijdelijke bestanden, geheugen, Windows prullenbak) of door de wijze waarop bestanden worden gewist. Er zijn besturingssystemen zoals Windows, die uitsluitend de verwijzing naar het verwijderde bestand verwijderen, maar de daadwerkelijke gegevens zelf achterlaten.
5 Het besturingssysteem dient niet toe te staan dat vercijferde gegevens in vercijferde of onvercijferde vorm van het systeem afgehaald kunnen worden door het omzeilen van de aangebrachte beveiligingslaag met bijvoorbeeld een opstartdiskette.
6 Sleutelmateriaal dient technisch goed beschermd te zijn tegen bedreigingen zoals een zwak besturingssysteem.

5.6.2 Basismaatregelen

Ad 1

a Maak gebruik van een stabiel, beheerd besturingssysteem.
b Maak gebruik van standaard back-upapplicaties.

Ad 2

a Maak gebruik van standaard back-upapplicaties.

Ad 3

a Maak gebruik van standaard back-upapplicaties.

Ad 4

a Gebruik indien noodzakelijk na een risicoanalyse boven op het besturingssysteem applicaties die het virtuele geheugen (*swap file*, tijdelijke bestanden, prullenbak) wissen en overschrijven met betekenisloze informatie (*secure wipe*, *secure delete*, enzovoort).
b Gebruik smartcardreaders zonder cache of waarvan de cache automatisch geleegd wordt. Een cache is een stukje geheugen waarin de meest recente acties worden opgeslagen.
c Gebruik toetsenborden zonder cache.

Ad 5

a Maak gebruik van bootprotectie: bescherming van gegevens die worden gebruikt tijdens het opstarten van het systeem.
b Uitgefaseerde systemen en opslagmedia die vercijferde gegevens hebben bevat, dienen vernietigd te worden door fysieke vernietiging of demagnetisering.

Ad 6

a Gebruik een smartcard voor opslag van de privé-sleutel.
b Cryptografische berekeningen dienen zoveel mogelijk op een smartcard of ander hardware *crypto-device* te worden uitgevoerd.

6 Beheer

Organisaties die, op beperkte of op grote schaal, gebruik gaan maken van cryptografie zijn nadien niet gevrijwaard van additionele inspanningen. Immers, cryptografie is een relatief nieuw toe te passen techniek die eisen stelt aan andersoortige beheeraspecten zoals bijvoorbeeld sleutelbeheer en opslag van (vercijferde) informatie. Verder zijn er nog extra redenen te noemen waardoor beheer van cryptografie essentieel is. Eén van de doelen van cryptografie is het realiseren van exclusiviteit/vertrouwelijkheid van informatie. Dit doel kan zich bij het ontbreken van adequaat beheer of gebruik keren tegen de eigenaar van de data en uiteindelijk resulteren in het verlies van (de vertrouwelijkheid van) data.

Veel problemen kunnen worden voorkomen door een goed beheerproces in te richten. Dit hoofdstuk is gewijd aan de beschrijving van de beheeractiviteiten die bij cryptografie benodigd zijn. Hiertoe zijn de volgende beheeraspecten onderkend:
- activiteiten bij het sleutelbeheer (paragraaf 6.1);
- organisatie van het sleutelbeheer (paragraaf 6.2);
- bewustwording gebruikers (paragraaf 6.3);
- beheer van certificaten (paragraaf 6.4).

Het uitgangspunt bij deze beheeraspecten is dat ze onderdeel uit moeten maken van (en waar mogelijk dienen te worden geïntegreerd met) de reguliere beheerprocessen. Dit uitgangspunt wordt in de navolgende paragrafen niet verder uitgewerkt.
In dit hoofdstuk is ervoor gekozen asymmetrische sleutelparen te behandelen, terwijl het (voor het merendeel) evengoed symmetrische sleutels kan betreffen. Het uitgangspunt is dat sleutelbeheer voor asymmetrische en symmetrische toepassingen gelijk is, maar dat bij asymmetrisch sleutelbeheer additionele activiteiten benodigd zijn

(denk bijvoorbeeld aan de distributie van publieke sleutels).
Een specifieke oplossing voor het beheer van asymmetrische sleutelparen is het gebruik van certificaten in een *Public Key Infrastructure* (PKI). Door het toenemende gebruik van PKI, zoals bijvoorbeeld het gebruik van servercertificaten in het SSL-protocol, is hier een aparte paragraaf aan gewijd. De normen en maatregelen zoals die in de paragrafen 6.1 tot en met 6.3 genoemd worden, zijn tevens van toepassing op paragraaf 6.4.

6.1 Activiteiten bij het sleutelbeheer

De activiteiten die bij het sleutelbeheer worden onderscheiden, volgen de gehele levenscyclus van cryptografische sleutels. Dit houdt in dat hier aan de volgende zeven aspecten aandacht wordt geschonken:
- creëren en uitreiken van sleutels;
- bepalen van de levensduur van sleutels;
- opslaan van sleutels;
- distribueren (publiceren) van publieke sleutels;
- intrekken van sleutels;
- herstellen (*recovery*) van sleutels;
- controleren van de verrichte activiteiten.

Zoals al in de inleiding van dit hoofdstuk is opgemerkt ,zijn bovenstaande activiteiten niet zondermeer van toepassing op asymmetrisch en symmetrisch beheer. In onderstaande tabel is weergegeven wanneer een activiteit van toepassing is.

Tabel 6.1 Activiteiten bij sleutelbeheer

Activiteit	Symmetrisch beheer	Asymmetrisch beheer
Het creëren en uitreiken van sleutels	Ja	Ja
Het bepalen van de levensduur van sleutels	Ja	Ja
Het opslaan van sleutels	Ja	Ja
Het distribueren (publiceren) van publieke sleutels	Nee	Ja
Het intrekken van sleutels	Nee	Ja
Het herstellen (recovery) van sleutels	Ja	Ja
Het controleren van de verrichte activiteiten	Ja	Ja

6.1.1 Het creëren en uitreiken van sleutels

De eerste activiteiten betreffende het beheer van sleutels vinden plaats bij de creatie van deze cryptografische sleutels. Om te waarborgen dat niet te veel sleutelparen worden aangemaakt – met het gevaar dat 'zwevende' sleutels ontstaan die niet aan een enkele persoon gebonden zijn – dient een procedure te worden opgesteld waarin wordt geregeld dat iedere nieuwe medewerker, bijvoorbeeld bij indiensttreding, wordt voorzien van een privé en publiek sleutelpaar. Zo kan voor nieuwe medewerkers, conform de aanvraag van een netwerkaccount, een sleutelpaar worden aangevraagd en bij voorkeur vindt dit zelfs gelijktijdig plaats. De aanvraag van cryptografische sleutels dient door middel van een standaardformulier bij de beheerorganisatie te worden ingediend.
De beheerorganisatie dient vervolgens ervoor te zorgen dat dit sleutelpaar uniek wordt gegenereerd door de software. De desbetreffende beheerders dienen hiertoe als enigen over de logische toegangsautorisaties van deze software te beschikken. Het sleutelpaar wordt overgedragen aan de betreffende medewerker onder vaststelling van diens identiteit. Om te waarborgen (lees: af te dwingen) dat de privé-sleutel strikt persoonlijk blijft, dient de beheerorganisatie bij overdracht van de sleutels (op diskette, smartcard of ander opslagmedium) erop toe te zien dat de medewerker persoonlijk de sleutels in ontvangst neemt, hiervoor tekent, en onmiddellijk het tijdelijke wachtwoord op deze sleutel wijzigt. Indien dit van toepassing is, wordt dit door het systeem afgedwongen. De medewerker dient zich bij het in ontvangst nemen van de sleutels te legitimeren door middel van een officieel identiteitsbewijs en/of bedrijfsidentiteitkaart.
Eventuele kopieën van gegenereerde sleutels dienen, nadat deze voor behoud zijn opgeslagen (zie paragraaf 6.1.3), te worden verwijderd van de computer waarop ze zijn gecreëerd.

Een alternatief met betrekking tot het creëren van sleutels is de procedure waarbij een gebruiker zelf de mogelijkheid krijgt om de sleutel te creëren zonder tussenkomst van de beheerorganisatie. Hiervoor dient echter een betrouwbaar geautomatiseerd hulpmiddel beschikbaar te zijn. De aparte activiteit van opslag van gecreëerde sleutels (paragraaf 6.1.3) is in deze situatie niet adequaat te adresseren.

Aan het einde van het creatieproces dient de beheerorganisatie te beschikken over een (kopie) van het aanvraagformulier, met hierop:
- de originele aanvraag van netwerkaccount en sleutelpaar;
- de autorisatie van de aanvraag door de manager van de afdeling of Personeelszaken;
- de handtekening van de gebruiker die onder andere de sleutels in ontvangst heeft genomen.

Het originele formulier kan worden overgedragen aan een centrale afdeling, bijvoorbeeld personeelszaken, of retour worden gezonden aan de manager/aanvrager. De beheerorganisatie dient deze gegevens te bezitten, zodat achteraf geverifieerd kan worden dat de sleutelparen daadwerkelijk respectievelijk zijn aangevraagd, gegenereerd en uitgereikt.

6.1.2 Levensduur van sleutels

In sommige gevallen ondersteunen de software en sleutelparen de mogelijkheid de 'levensduur' te bepalen. Met levensduur wordt bedoeld de periode dat een sleutel als valide wordt beschouwd. Niet-valide sleutels kunnen nog wel worden aangewend om vercijferde berichten te ontcijferen, maar niet meer om berichten te vercijferen. Sleutels die nooit verlopen, hebben statistisch gezien een grotere kans om te worden gekraakt dan sleutels die periodiek worden vervangen. Bovendien is de impact van een sleutel waarvan de vertrouwelijkheid niet meer kan worden gewaarborgd én waarvan de levensduur oneindig is vele malen groter dan bij een sleutel die slechts een jaar geldig blijft. Echter, vele organisatorische en praktische problemen duiken op bij sleutels die periodiek dienen te worden vervangen.
Zo dient de beheerorganisatie bij de creatie van de sleutelparen te noteren wanneer de sleutelparen verlopen en dus nieuwe sleutels dienen te worden aangemaakt. Let op, de 'oude' sleutels dienen evengoed te worden bewaard om de mogelijkheid te behouden teksten te ontcijferen. Een ander potentieel probleem is de afnemende overzichtelijkheid door de vele verlopen sleutels; vercijferde teksten dienen herleidbaar te zijn naar de originele sleutels. Dit herleiden wordt moeilijker naarmate er meerdere (verlopen) sleutelparen per gebruiker bestaan.

In bijvoorbeeld *Pretty Good Privacy* is een optie aanwezig die gebruikers de mogelijkheid biedt om sleutelparen van zogenaamde *subkeys* te voorzien. Een sleutelpaar bestaat dan uit een *master key* en een bepaald aantal *subkeys*. Deze *subkeys* krijgen een verloopdatum aangegeven waarna automatisch de volgende *subkey* valide wordt en kan worden gebruikt. Bij uitgifte van de privé- en publieke sleutel beschikt zowel de houder/gebruiker als de zender over valide sleutels die automatisch verlopen en worden vervangen. Hiermee wordt een groot deel van de problematiek rond het periodiek vervangen van sleutels voorkomen.

Zoals gezegd kan de levensduur van sleutelparen bijdragen om de vertrouwelijkheid van deze sleutelparen te waarborgen. Echter, de vertrouwelijkheid van sleutels kan relatief gemakkelijk worden doorbroken door andere bedreigingen op werkstations zoals:
- Kwaadaardige software (zoals *trojans* en *keyboard loggers*) die het wachtwoord afvangt en de privé-sleutel kan kopiëren;
- Zwakke implementatie van wachtwoordbeleid waardoor gebruikers over langere tijd hetzelfde wachtwoord kunnen gebruiken en dus een grotere kans lopen dat het wachtwoord van een privé-sleutel wordt gekraakt.

De aandacht dient dus ook op andere aspecten te worden gevestigd om de vertrouwelijkheid van sleutels te blijven waarborgen.

6.1.3 Opslag van sleutels

Sleutels die door de beheerorganisatie zijn gegenereerd, dienen altijd te worden opgeslagen. Redenen hiervoor zijn:
- Gebruikers kunnen sleutels kwijt raken (bijvoorbeeld verlies of diefstal van laptop, smartcard, enzovoort);
- Gebruikers die uit dienst treden kunnen vercijferde data achterlaten (in geval van slechte overdrachtsprocedure zijn deze data niet meer toegankelijk voor de organisatie);
- Sleutels kunnen fysiek beschadigd raken (bijvoorbeeld door bad sectors op een harddisk).

Aan de opslag van sleutels moet een aantal voorwaarden worden gesteld:

Opslag en identificatie

De sleutels dienen in een database te worden opgeslagen en wel op dusdanige wijze dat in de toekomst op basis van één of meerdere zoekvariabelen de juiste sleutel kan worden geselecteerd. De volgende van onderstaande variabelen kunnen hiervoor bijvoorbeeld worden gebruikt:

- personeelsnummer;
- datum creatie van sleutel;
- serienummer computer;
- datum indiensttreding personeelslid.

Vanzelfsprekend kan de benaming van de sleutel zelf ook bijdragen aan een (juiste) identificatie van de te zoeken sleutel.

Beschikbaarheid

De database met sleutels dient dagelijks te worden veilig gesteld door middel van back-ups en/of een dagelijkse replicatie naar een andere database. Verder kunnen technische maatregelen zoals *disc-mirroring* ook uitkomst bieden teneinde de beschikbaarheid van de database te waarborgen.

Logische beveiliging

Toegang tot de database en tot de computer zelf dient door middel van stringente logische toegangsbeveiliging te worden beperkt tot geautoriseerde medewerkers van de beheerorganisatie. Op het niveau van het besturingssysteem dienen ook stringente beveiligingsmaatregelen te zijn geïmplementeerd. Bovendien verdient het de voorkeur de computer als een *stand-alone* configuratie op te nemen, zodat inbraakpogingen via het netwerk niet mogelijk zijn.

Wanneer ervoor wordt gekozen de computer (waarop de database met sleutelparen is geïnstalleerd) te verbinden met het netwerk, verdient het de voorkeur de database zelf te vercijferen. In deze situatie is het beheer van de sleutel behorende bij de vercijferde database essentieel en dit dient dan ook met uiterste zorg te worden uitgevoerd.

Fysieke beveiliging
De computer (alsmede de bijbehorende back-ups en replicatie computer) dient fysiek te zijn afgeschermd van ongeautoriseerde medewerkers.

Ten slotte dient te worden opgemerkt dat in deze paragraaf de maatregelen voor opslag zijn beschreven die noodzakelijk worden geacht, zodat private en *public keys* beschikbaar blijven bij optredende incidenten. Echter, voor regulier gebruik dienen ook maatregelen te zijn getroffen om bijvoorbeeld de opslag van *public keys* op een centrale server of X.500 directory structuur te waarborgen. De maatregelen genoemd in deze paragraaf kunnen hiervoor tevens het richtsnoer vormen.

6.1.4 Publicatie van (publieke) sleutels

Het gebruik van asymmetrische vercijfering vraagt om publicatie van publieke sleutels, zodat gebruikers hierover kunnen beschikken indien dit gewenst is. Dit is in eerste instantie een handeling die niet van nature wordt uitgevoerd. Men is immers gewend aan het geheim houden van encryptiesleutels. Het publiceren van publieke sleutels kan globaal op twee verschillende wijzen worden uitgevoerd:

1 volgens het *pull-principe*;
2 volgens het *push-principe*.

Het *pull-principe* houdt in dat diegene die de publieke sleutel nodig heeft, hierom vraagt. We lichten dit toe met een voorbeeld. Als een persoon, Alice, een vercijferd bericht wil verzenden aan een ander, Bob, dan heeft zij Bob's publieke sleutel nodig. In dit geval zal zij contact opnemen met Bob en hem vragen om zijn publieke sleutel. Deze kan dan op een willekeurige wijze aan Alice gestuurd worden, elektronisch of via een ander medium (bijvoorbeeld met de post).
Deze aanpak wordt veelal gevolgd op het internet en is ook toepasbaar in kleinere organisaties.

Het *push-principe* werkt als volgt. Elke publieke sleutel wordt op een centrale, algemeen toegankelijke plek opgeslagen. Iedereen die toegang heeft tot deze plek, heeft toegang tot alle daar opgeslagen publieke sleu-

tels. Op dit moment wordt dit praktisch ingevuld met het gebruik van een X.500 directory structuur. Deze aanpak wordt in de praktijk voornamelijk binnen grote organisaties uitgevoerd.
De wijze waarop de integriteit wordt gegarandeerd van deze publiek toegankelijke gegevens en de koppeling van de persoon (of functionaris) aan de publieke sleutel, is onderwerp van een paragraaf 6.4, die gaat over PKI.

6.1.5 Intrekken van sleutels

Een soortgelijke activiteit als het publiceren van sleutels is het tegenovergestelde hiervan, namelijk het intrekken van sleutels. Zodra een medewerker bijvoorbeeld uit dienst treedt, zou in principe het gebruik van zijn privé-sleutel (die gekoppeld is aan een organisatienaam) niet meer mogelijk moeten zijn. Ook in het geval dat de vertrouwelijkheid van een privé-sleutel wordt geschonden, dient deze sleutel te worden ingetrokken.

Voornamelijk de volgende situaties kunnen aanleiding zijn tot het intrekken van sleutels:

1 Een medewerker treedt uit dienst. Personeelszaken (PZ) waarschuwt conform afspraak een functionaris die belast is met het intrekken van sleutels.
2 Een gebruiker geeft aan dat zijn privé-sleutel waarschijnlijk gecompromitteerd is. Dit dient door middel van een formulier (ondertekend) door de gebruiker kenbaar te worden gemaakt.

Hierboven is het functionele proces beschreven. Vanzelfsprekend dient dit technisch realiseerbaar te zijn. Een techniek die bij PKI-toepassingen wordt gebruikt, is de *Certificate Revocation List* (CRL). Hiermee kunnen (ongeldige of gecompromitteerde) certificaten worden ingetrokken. Meer hierover is opgenomen in paragraaf 6.4.1.4.

Als een organisatie of een cryptografische toepassing niet beschikt over een mogelijkheid om sleutels actief in te trekken, bijvoorbeeld door middel van een CRL, dan dient naar andere mogelijkheden te worden

gezocht. Zenders waarmee gecommuniceerd wordt, kunnen bijvoorbeeld actief worden benaderd en op de hoogte worden gesteld van de ontstane situatie. Het moge duidelijk zijn dat dit laatste een chaotisch en inefficiënt proces is.

6.1.6 Herstellen (recovery) van sleutels

Als een gebruiker het wachtwoord van zijn privé-sleutel vergeet of wanneer een medewerker onverwachts de organisatie verlaat en men weet het wachtwoord van deze medewerker (zoals het hoort) niet, dan dient er een voorziening te bestaan waarmee de beheerorganisatie de sleutel kan wijzigen of herleiden.
Hiertoe bestaan meerdere technieken, waarvan er hier twee worden besproken. Bij deze technieken zijn twee soorten sleutels van belang: de persoonlijke sleutelparen en de herstelsleutels (*recovery keys*).
De *persoonlijke sleutelparen* zijn de sleutels die centraal in deze studie staan, de sleutels waarmee gebruikers data kunnen vercijferen. De *herstelsleutels* kunnen alleen worden gebruikt om de wachtwoorden op persoonlijke sleutelparen te herstellen c.q. te 'resetten'. Let wel, het gebruik van de herstelsleutels is niet mogelijk, wanneer de persoonlijke sleutelparen niet voorhanden zijn.
Hieronder wordt een procedure besproken die kan worden toegepast als er geen specifieke hersteltechniek voorhanden is.

Hersteltechniek door middel van een master recovery key

Bij deze techniek kan het wachtwoord op een sleutel die de gebruiker heeft verloren, door middel van een zogenaamde *master key* (moedersleutel) worden gereset naar een standaard of dynamisch gegenereerd wachtwoord. Vervolgens heeft de gebruiker met behulp van dit wachtwoord weer toegang tot de sleutel.
De beheerorganisatie dient het unieke sleutelpaar te hebben opgeslagen ingeval dat de gebruiker niet meer de fysieke beschikking heeft over de sleutel. Doordat deze *master key* op ieder sleutelpaar van toepassing is, heeft de beheerorganisatie geen additionele informatie nodig. Het moge duidelijk zijn wat de impact is op de informatiebeveiliging bij verlies van deze *master key*.

Hersteltechniek door middel van een individual recovery key

Bij deze techniek beschikt ieder sleutelpaar over een unieke herstelsleutel (*individual recovery key)* waarmee het wachtwoord op de bijbehorende sleutel kan worden gereset.
De beheerorganisatie dient het unieke sleutelpaar te hebben opgeslagen in het geval dat de gebruiker niet meer de beschikking heeft over de sleutels. De beheerorganisatie dient een duidelijke en betrouwbare administratie te voeren van de uitgegeven sleutelparen en de bijbehorende unieke herstelsleutel, zodat een succesvolle herstelactie kan worden uitgevoerd.

Geen specifieke hersteltechniek

Bovenstaande hersteltechnieken komen vaak voor, maar ook bestaan er toepassingen waarbij dit niet het geval is. In zulke gevallen dient ieder sleutelpaar derhalve te worden opgeslagen (zie 6.1.3) en te worden voorzien van een standaard wachtwoord of van een wachtwoord dat achteraf kan worden herleid. Bij verlies van het wachtwoord haalt de beheerorganisatie de oude kopie van de sleutel van de back-up waarvan dus het oude originele wachtwoord nog bekend is. Ook hierbij dient de beheerorganisatie een zeer betrouwbare administratie te voeren.
Analoog aan de ondersteunde hersteltechniek dient de beheerorganisatie de opslag van haar sleutels in te richten.

Herstel van de sleutels zelf is een activiteit die door de gebruiker persoonlijk en schriftelijk dient te worden aangevraagd. Aangezien dit proces de vertrouwelijkheid van de sleutels (en daarmee de vertrouwelijkheid van de informatie) kan doorbreken, dient dit proces met uiterste zorg te worden uitgevoerd. De beheerder dient daarom evenals bij de eerste uitgifte de identiteit van de gebruiker vast te stellen. Een apart formulier dient inzicht te geven in:

- de aanvraag tot *recovery* van een sleutel door de gebruiker, voorzien van zijn/haar handtekening;
- de reden van de aanvraag (verlies, corruptie, verlies wachtwoord);
- de naam van de beheerder die de *recovery* uitvoert.

Dit formulier dient opvraagbaar te zijn voor een controlerend orgaan binnen de organisatie (zie ook paragraaf 6.1.7) en de volledigheid van

deze *recovery*formulieren dient achteraf vastgesteld te kunnen worden door volgnummers of vastlegging in een (geautomatiseerd) register.
Essentieel is om de (*master*) *recovery key* na uitvoering van de *recovery* te verwijderen van het station waarop de activiteiten hebben plaatsgevonden. Eveneens dient de gebruiker het standaard wachtwoord te wijzigen.

6.1.7 Controleren

De beheeractiviteiten van sleutels zijn van dermate belang, dat hierop structureel en onafhankelijk controle dient plaats te vinden. De controle dient in elk geval te omvatten:

- Acties die blijken uit de logging van de sleuteldatabase (kopiëren, verwijderen, enzovoort) vergelijken met de formulieren waarop de beheeractiviteiten zijn aangetekend.
- Het aantal ontvangen uitgifteformulieren vergelijken met het aantal sleutels dat zich in de database bevindt (zie paragraaf over opslag).
- Constateren uit de vastleggingen en de eigen waarneming dat de vereiste functiescheidingen worden gehandhaafd.
- Constateren uit de vastleggingen dat de vastgestelde deelactiviteiten op juiste wijze worden doorlopen.
- Vaststellen dat de gebruikte formulieren volledig en juist worden ingevuld.

6.1.8 Normen en maatregelen

Basisnormen

1 Per gebruiker dient slechts één (actief) sleutelpaar te bestaan. Tevens dient ieder sleutelpaar uniek identificeerbaar/herleidbaar te zijn naar de gebruiker.
2 Een centrale vertrouwde organisatie dient belast en verantwoordelijk te zijn voor de creatie, uitgifte en inname van sleutels.
3 De verantwoordelijke afdeling dient het sleutelpaar persoonlijk aan de rechtmatige gebruiker over te dragen. Deze overdracht dient tegen kwijting plaats te vinden.
4 De beschikbaarheid van sleutelparen dient te zijn gewaarborgd. Dit

geldt voor zowel actieve als verlopen sleutelparen en voor sleutels van medewerkers in dienst en van medewerkers die reeds uit dienst zijn getreden.

5 De logische en fysieke toegangsbeveiliging van de opgeslagen sleutelparen dient adequaat te worden gewaarborgd.

6 De beheerorganisatie dient te allen tijde *technisch* de mogelijkheid te hebben om verloren sleutels te vervangen (*recovery*).

7 Vervanging (*recovery*) van sleutelparen door de beheerorganisatie dient slechts na schriftelijke aanvraag van de gebruiker en/of aangewezen verantwoordelijke functionaris plaats te vinden.

8 Een audit trail van de uitgevoerde vervangingen van sleutels dient aanwezig te zijn.

9 De vertrouwelijkheid en integriteit van sleutelparen (aanwezig op werkstations en/of virtuele smartcards van de gebruikers) dient te worden gewaarborgd.

10 De levensduur van sleutelparen dient eindigend te zijn, de levensduur dient met een vaste periodiciteit, bijvoorbeeld één jaar, te worden verlengd.

11 Incidenten met betrekking tot cryptografie dienen onderdeel uit te maken van trendanalyse, evaluatiebeleid en maatregelen.

12 Op de uitgevoerde beheerhandelingen dient specifiek controle te worden uitgeoefend.

Basismaatregelen

Ad 1

- Creëer de sleutels van medewerkers bij specifieke situaties (bijvoorbeeld indiensttreding).
- Verifieer periodiek het aantal uitgegeven sleutels met het aantal voor cryptografie geselecteerde medewerkers.
- Verifieer periodiek of voor ieder verlopen sleutelpaar van een medewerker een actief sleutelpaar is aangemaakt of stel vast dat de betrokken medewerker uit dienst is getreden.
- Creëer een eenduidige naamconventie voor benaming van de sleutels, bijvoorbeeld personeelsnummer, naam gebruikers en/of e-mailadres gebruiker.

Ad 2

– Sluit een *Service Level Agreement* (SLA) af met een organisatie waarin duidelijk de verwachte diensten, plichten en verantwoordelijkheden voor beide partijen (gebruikersorganisatie en beheerorganisatie) worden vastgelegd.

Ad 3

– Laat gebruikers persoonlijk tekenen voor ontvangst van sleutels op daarvoor bestemde formulieren.
– Identificeer de gebruikers met behulp van een geaccepteerd identificatiemiddel (zoals paspoort, rijbewijs, *Corporate Identity Card*).

Ad 4

– Richt een afzonderlijke database in waarin alle beschikbare sleutels worden opgeslagen.
– Richt technische en procedurele maatregelen in zodat verwijdering en wijziging van sleutels in de database niet mogelijk is.
– Reguliere maatregelen (redundante middelen, back-ups, uitwijk) teneinde de beschikbaarheid van deze database te waarborgen, moeten strikt worden nageleefd.

Ad 5

– Ieder sleutelpaar dient van een persoonlijk wachtwoord te worden voorzien.
– De sleutels dienen op een plaats te staan welke is beveiligd door middel van een wachtwoord.
– Diskettes en andere media met een sleutel dienen opgeslagen te zijn in een kluis.

Ad 6

– Richt een computer in met gemirrorde disks of andere beschikbaarheidsbevorderende maatregelen en plaats hierop de database met sleutels.
– Bewaar een *master key* (of andersoortige *recovery key*) op een plek die te allen tijde toegankelijk is (bijvoorbeeld een diskette, smartcard in een kluis) voor hiertoe geautoriseerde medewerkers.

Ad 7

- Gebruik een aanvraagformulier voor *recovery* van sleutels voorzien van gebruikersnaam, personeelsnummer en handtekening door de houder van de sleutels.
- Identificeer de gebruiker met behulp van een geaccepteerd identificatiemiddel (zoals paspoort, rijbewijs, *Corporate Identity Card*).
- Stel vast dat een (van de beheerorganisatie gescheiden) functionaris op dit formulier toestemming heeft verleend aan de beheerorganisatie om tot *recovery* over te gaan.
- De functionaris van de beheerorganisatie dient op het formulier aan te geven wanneer *recovery* is uitgevoerd.

Ad 8

- Zorg dat de *recovery*formulieren van een volgnummer zijn voorzien of registreer deze formulieren in een register, zodat de volledigheid achteraf is vast te stellen.

Ad 9

- Installeer een antivirus programma en voorzie deze regelmatig van de laatste virus databases.
- Beveilig toegang tot de sleutel door middel van wachtwoorden en bij voorkeur in combinatie met *tokens*.

Ad 10

- Creëer sleutels met een eindigende geldigheidsduur van bijvoorbeeld één jaar.
- Na elk jaar dient er automatisch een nieuwe sleutel te worden gegenereerd en de oude dient te worden verwijderd.

Ad 11

- In het proces van incidentenregistratie dient een code te worden gebruikt die problemen met cryptografie classificeert. De oorzaak van ieder incident/probleem dient te worden nagegaan en te worden geëvalueerd op de noodzaak tot aanpassing van beleid en/of maatregelen.

Ad 12
- Controleren logging van de sleuteldatabase.
- Ontvangen uitgifteformulieren moet in aantal gelijk zijn aan het aantal sleutels in database.
- Handhaving functiescheidingen.
- Volgen vastgestelde procedures.
- Juist en volledig invullen formulieren.

6.2 Organisatie van het sleutelbeheer

Zoals in voorgaande paragraaf reeds naar voren is gekomen, worden door de introductie van cryptografie aan een organisatie andere en aanvullende eisen aan de desbetreffende beheerorganisatie gesteld.
In de vorige paragraaf zijn de beheeractiviteiten inclusief de controle op een rijtje gezet. Om tot een goede uitvoering van het beheer te komen, dient er een centrale beheerorganisatie te zijn, waarbinnen de volgende activiteiten door verschillende functionarissen dienen te worden uitgevoerd:
- creëren en uitreiken van sleutels en het bepalen van de levensduur;
- opslaan en publiceren van sleutels;
- intrekken van sleutels;
- herstellen (*recovery*) van sleutels;
- controleren van de voorgaande beheeractiviteiten.

Het doel van deze scheiding is om beheerders nooit in staat te stellen meerdere activiteiten autonoom uit te voeren. Het risico zou immers kunnen optreden dat beheerders ongeautoriseerd sleutels aanmaken of resetten. De functiescheiding dient verankerd te worden door het zodanig inrichten van het beheerproces dat afgeronde activiteiten en het resultaat daarvan, de aangemaakte sleutels bijvoorbeeld, formeel worden overgedragen aan de 'volgende' beheerder. Bij deze overdracht moet een formulier worden gebruikt voor beëindiging van verantwoordelijkheden, waarbij décharge (kwijting) wordt verleend.
Controle op deze scheiding dient te waarborgen dat de functiescheiding instant is en blijft.

Bij creatie, uitgifte en/of *recovery* van sleutels met grote impact zouden als vereiste altijd meerdere personen aanwezig moeten zijn, die volgens het vierhandenprincipe activiteiten kunnen verrichten. Men kan hierbij denken aan sleutels die voor het uitvoeren van transacties worden gebruikt of sleutels die voor een organisatie als geheel moeten gelden. Tevens zou de onafhankelijke controleur ook aanwezig moeten zijn voor het doen van eigen waarnemingen (direct toezicht).
Gezien het feit dat de meest gevoelige beheerhandelingen meestal slechts met een lage frequentie zullen plaatsvinden, is het argument van inefficiëntie hier niet van toepassing.

Basisnormen

1 Er dient voldoende functiescheiding aanwezig te zijn binnen de centrale beheerorganisatie.
2 De belangrijkste beheeractiviteiten, ten behoeve van sleutels met grote of organisatiebrede impact, dienen door meerdere functionarissen (vierhandenprincipe) te worden uitgevoerd.

Basismaatregelen

Ad 1

– De verschillende hoofdactiviteiten (creatie, uitgifte, herstel van sleutels, controle) moeten worden uitgevoerd door verschillende medewerkers binnen een organisatie.
– Bij voorkeur dient een functionaris die niet behoort tot de uitvoerende beheerorganisatie, belast te zijn met controle op juistheid en integriteit van het proces en hierover te rapporteren aan het management.
– Bovenstaande hoofdactiviteiten dienen eveneens in de logische beveiliging (rechten op systeem en in database) en fysieke beveiliging (toegang tot servers, kluis, enzovoort) van middelen die ter ondersteuning van het cryptografisch proces aanwezig zijn, te worden geïmplementeerd.

Ad 2

Het vierhandenprincipe en enveloppenprocedure dient te worden toegepast bij beheeractiviteiten ten behoeve van sleutels met grote of organisatiebrede impact.

6.3 Bewustwording gebruikers

Naast eisen aan de inrichting van het beheer zijn ook eisen te stellen aan het gebruik, dat wil zeggen aan de uit te voeren (beheer)activiteiten door gebruikers. Immers, de gebruiker is onderdeel van de keten van handelingen, die uiteindelijk de doelstellingen van het inzetten van encryptiemiddelen mede bepalen.
Gebruikers van cryptografische toepassingen dienen allereerst te begrijpen welk doel wordt nagestreefd met het gebruik van encryptie. Dit is noodzakelijk aangezien medewerkers zelf geen direct profijt zien of inzien van het gebruik van cryptografie. Beveiliging van gegevens is immers niet zozeer een doel van individuele medewerkers, maar meer van de organisatie.
Eveneens dient de werking van de gebruikte software en hulpmiddelen (en in het algemeen de werking van cryptografie) te worden toegelicht. Gebruikers moeten begrijpen waarom een privé-sleutel geheim dient te worden gehouden en waarom een publieke sleutel wel mag worden rondgezonden.
Ten slotte dienen gebruikers bewust te worden gemaakt van risico's die de effectiviteit van cryptografie kunnen verstoren: bijvoorbeeld het (onbewust) importeren van *trojans* en virussen door het uitvoeren van toegezonden programmatuur.
Kortom, het succes van cryptografie is ook in grote mate afhankelijk van het eigenlijke gebruik door medewerkers. Een organisatie dient dan ook voldoende aandacht te schenken aan de voorlichting en opleiding van gebruikers.

Basisnormen

1 Gebruikers dienen bekend te zijn met en bewust te zijn van de betekenis van het gebruik van cryptografie. Dit mede om draagkracht voor het gebruik van cryptografie te creëren.
2 Gebruikers dienen snel en adequaat te reageren op een situatie waarbij zijn of haar privé-sleutel is gecompromitteerd.
3 Gebruiker dienen zorgvuldig om te gaan met zijn privé-sleutel zodat compromittatie wordt voorkomen.

Basismaatregelen

Ad 1

- Bij de introductie van nieuwe medewerkers dient voldoende aandacht aan de betekenis en het gebruik van cryptografie te worden besteed, inclusief aan de potentiële risico's van cryptografie die uiteindelijk een nadelig effect kunnen hebben op de effectiviteit ervan.
- Ter handhaving van de awareness dient regelmatig in voorlichting en in opleidingen te worden ingegaan op het gebruik en de risico's van de cryptografische toepassingen.
- Directie/managementteam onderkent en ondersteunt het belang van encryptie en draagt dit uit.
- Gebruikers nemen deel aan een *security awareness program* (bewustwordingsprogramma).

Ad 2

- De gebruiker beschikt over procedures waarin de vereiste handelwijze is beschreven bij compromittatie van zijn of haar privé-sleutel.

Ad 3

- Maak de gebruiker bewust van het belang van zijn privé-sleutel bij het *security awareness program*.
- De gebruiker wordt aangesproken op onzorgvuldige behandeling van zijn privé-sleutel. Een voorbeeld hiervan is, bij gebruik van een smartcard voor opslag van de privé-sleutel, dat de gebruiker deze smartcard onbeheerd op zijn werkplek of daarbuiten achterlaat. Dit dient dan ook gecontroleerd te worden bij melding van het verlies van de smartcard.

6.4 Het beheer van certificaten

De vorige secties gingen over het beheer van cryptografische sleutels in het algemeen. Een veel toegepaste oplossing voor het beheer van asymmetrische sleutels is het gebruik van certificaten. Een *Public Key Infrastructure* (PKI) is dan een middel om die certificaten te organiseren en beheren. Een PKI maakt het mogelijk om partijen, zowel binnen één organisatie als partijen die niet van tevoren contractueel met elkaar zijn

verbonden, op een betrouwbare manier elektronisch met elkaar te laten communiceren. Belangrijke aspecten hierbij zijn dat partijen elkaar kunnen identificeren en authentiseren en dat desgewenst de uitgewisselde informatie kan worden vercijferd.
Hoewel in de voorgaande paragrafen voornamelijk van de situatie van persoonlijke cryptografische sleutels is uitgegaan, is het beheer van niet-persoonlijke sleutels zoals organisatie- en servercertificaten in feite gelijksoortig. Een groot verschil tussen de beheeractiviteiten betreft de frequentie van de toegepaste beheerprocedures. Een servercertificaat zal met een vaste periodiciteit worden vervangen en aangemaakt, terwijl de creatie en vervanging van persoonlijke certificaten dagelijks plaatsvinden.

Het belang van een organisatie- of servercertificaat is echter aanzienlijk. Er dient dan ook extra toezicht op de bewaring en het gebruik van dit soort certificaten te worden uitgevoerd. De volgende beheerprocedures dienen, in aanvulling op de eerder beschreven beheerprocedures, als basisnormen in de organisatie te worden ingebed:

- Een functionaris uit de organisatie wordt aangewezen als (functioneel) eigenaar van het certificaat en heeft beslissingsbevoegdheid over het gebruik;
- Opslag van het certificaat dient gescheiden plaats te vinden van reguliere certificaten/sleutels;
- Fysieke beveiligingsmaatregelen dienen stringenter te zijn dan de vereiste maatregelen voor reguliere certificaten/sleutels.

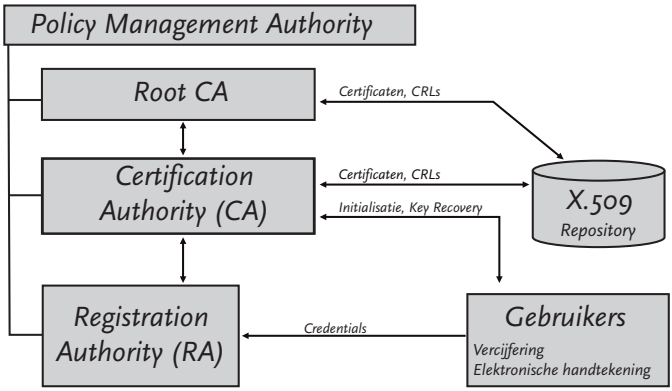
Verder dient opgemerkt te worden, dat indien een bedrijf onvoldoende kennis in huis heeft over PKI en ook geen belang heeft om deze kennis in huis te halen, kan worden besloten om een PKI te outsourcen. Diverse partijen in de markt bieden de mogelijkheid om 'PKI-diensten' in de vorm van een zogenaamde *managed* PKI te leveren.

Het principe van PKI wordt in deze paragraaf verder toegelicht.

6.4.1 Onderdelen van een PKI

Een PKI bestaat uit de volgende (organisatorische) onderdelen:
- Certificaten (X.509);
- *Certification Authority* (CA);
- *Registration Authority* (RA);
- Gebruikers;
- *Certificate Revocation List* (CRL);
- Een *Policy Management Authority* (optioneel).

Een samenhang van deze onderdelen is weergegeven in figuur 6.1.



Figuur 6.1 Schematische voorstelling PKI

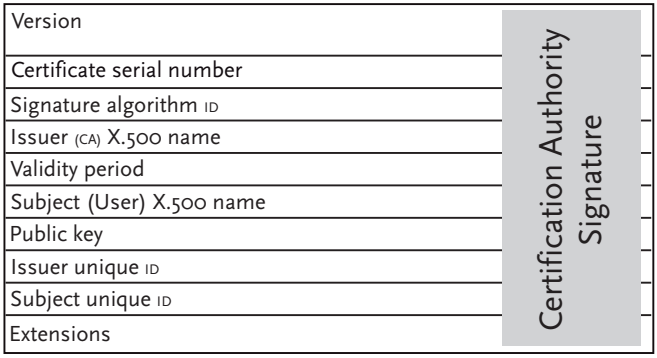
Verder zijn de volgende aspecten van belang bij de implementatie van een PKI: *Certificate Policy* (CP), *Certificate Practice Statement* (CPS) en het gebruik van sleutelparen.

In de volgende subparagrafen worden deze onderdelen en aspecten verder uitgewerkt.

6.4.1.1 Certificaten

Een certificaat is een elektronisch document waarin de identiteit van een partij (persoon) is vastgelegd. Minimaal worden in een certificaat de

naam van de gebruiker, zijn publieke sleutel, de naam van de certificaatuitgever en de geldigheidsduur van het certificaat opgenomen. Deze gegevens worden gegarandeerd door de uitgever door middel van een digitale handtekening van de uitgever. Meestal wordt gebruikgemaakt van de X.509 standaard voor het vastleggen van gegevens in een certificaat. Een voorbeeld van een dergelijk certificaat is gegeven in figuur 6.2 Inhoud X.509 V3 certificaat.



Figuur 6.2 Inhoud X.509 V3 certificaat

Naast het versie- en serienummer wordt in het certificaat aangegeven welk algoritme wordt gebruikt (*signature algorithm* ID). Verder wordt de (X.500) naam van de uitgever (*Certification Authority*) vermeld evenals de geldigheidsduur van het certificaat en de naam van de gebruiker. De publieke sleutel van de gebruiker is opgenomen in het certificaat en bovendien is zowel van de uitgever als de gebruiker een uniek ID vastgelegd.

Het laatste veld geeft aan dat er nog extensies kunnen worden ingevuld, bijvoorbeeld over het toepassingsgebied van het certificaat. Omdat dit veld optioneel is en vrij kan worden ingevuld vormt dit meteen het grootste knelpunt van het X.509 versie 3 certificaat. Doordat verschillende partijen hier verschillende informatie invullen, wordt de uitwisseling van certificaten bemoeilijkt. Daarom wordt aangeraden hier zo weinig mogelijk informatie in te vullen.

Er zijn drie soorten certificaten te onderscheiden die elk een verschillend niveau van betrouwbaarheid hebben, namelijk class 1, class 2 respectievelijk class 3 certificaten.
Class 1 certificaten worden uitgegeven aan individuele gebruikers, waarbij uitsluitend is aangegeven dat een bepaald door de gebruiker opgegeven e-mailadres bij deze gebruiker hoort. Er vindt geen check plaats of dit correct is. Class 1 certificaten hebben daarom een laag betrouwbaarheidsniveau.
Class 2 certificaten worden eveneens aan individuele gebruikers uitgegeven. Hierbij wordt onder andere gecheckt of de door de gebruiker opgegeven adresgegevens correct zijn. Per CA wordt deze check verschillend uitgevoerd: de check kan automatisch worden uitgevoerd door de CA, maar de check kan ook worden uitgevoerd door de gebruiker zich te laten identificeren bij een RA. Afhankelijk van de manier waarop de controle van de identiteit van de gebruiker plaatsvindt, hebben class 2 certificaten een hogere graad van betrouwbaarheid.
Class 3 certificaten worden zowel aan individuele gebruikers als aan organisaties uitgegeven. Hierbij vindt altijd een check aan de hand van een identiteitsbewijs plaats. Deze certificaten hebben een hoge graad van betrouwbaarheid, maar zijn als gevolg van de arbeidsintensieve checkprocedure ook duurder dan de beide andere soorten certificaten.

De certificaten worden opgeslagen in een database. Meestal wordt hierbij gebruikgemaakt van een X.500 Directory. Zie verder bijlage C (directory services en LDAP van de studie uit de reeks S*tandaarden en studies in informatiebeveiliging*) die handelt over Netwerken.

De uitgever van certificaten is de zogenaamde *Certification Authority* (CA).

6.4.1.2 *Certification Authority* (CA)

Een *Certification Authority* draagt zorg voor de ondertekening en uitgifte van certificaten. Ondertekening van een certificaat door een onafhankelijke instantie is nodig als bewijs van de echtheid van het certificaat. De onafhankelijke instantie kan een eigen organisatie-onderdeel zijn, bijvoorbeeld bij een interne PKI, maar meestal is dit een externe, vertrouwde partij, ook wel *Trusted Third Party* (TTP) genoemd.

De CA ondertekent de certificaten met de privé-sleutel van de CA. Hierdoor kunnen alle gebruikers die beschikken over de publieke sleutel van de CA, de certificaten verifiëren. De privé-sleutel van de CA dient bij voorkeur off-line te worden bewaard om compromittatie van deze privé-sleutel te voorkomen. Compromittatie van deze sleutel brengt namelijk met zich mee dat geen enkel certificaat van deze CA meer te vertrouwen is. Dit kan verstrekkende gevolgen hebben, zoals het vervangen van alle uitgegeven certificaten.
Het is een verantwoordelijkheid van de CA om de identiteit van de (nieuwe) gebruiker te controleren voordat certificaten worden uitgegeven. Over het algemeen wordt deze controle uitbesteed aan de *Registration Authority* (RA). Daarbij kunnen meerdere RA's van dezelfde organisatie aangesloten zijn op één CA.

6.4.1.3 *Registration Authority* (RA)

De *Registration Authority* (RA) draagt zorg voor het aanbieden van gegevens (credentials) van gebruikers aan de CA ten behoeve van het uitgeven van (nieuwe) certificaten door de CA. De RA is daarbij verantwoordelijk voor het vaststellen van de identiteit van de gebruiker (authenticatie). De RA ondertekent de certificaten niet en geeft ook geen certificaten uit, dit is een taak voor de CA. Dit betekent dat er een vertrouwensrelatie moet zijn tussen de RA en de CA. Ook moet worden voorkomen dat de door de RA aangeboden gegevens onderweg kunnen worden gemanipuleerd. Het aanbieden van de gegevens aan de CA gaat, mits het aanbieden van deze gegevens elektronisch gebeurt, daarom vergezeld van een digitale handtekening van de RA.

6.4.1.4 *Certificate Revocation List* (CRL)

Een *Certificate Revocation List* (CRL) is een lijst (bestand) met (voor de verstrijkdatum) ongeldig verklaarde certificaten die door de uitgevende CA wordt bijgehouden. Een certificaat kan ongeldig worden verklaard als bijvoorbeeld een gebruiker de organisatie heeft verlaten of, als er gebruik wordt gemaakt van een pincode, deze pincode vergeten is. Ook wordt een certificaat ongeldig verklaard als de privé-sleutel gecompromitteerd is.

Het is van belang dat deze lijst, bij voorkeur real-time, via *Online Certificate Status Protocol* (OCSP), zoveel mogelijk up-to-date gehouden wordt en on-line checking kan plaatsvinden. In de praktijk wordt meestal één keer per 24 uur een nieuwe CRL gegenereerd.
Niet elk systeem of applicatie ondersteunt automatisch het checken van de CRL. Soms moeten hiervoor aparte afspraken worden gemaakt met de CA.

6.4.1.5 *Gebruikers*

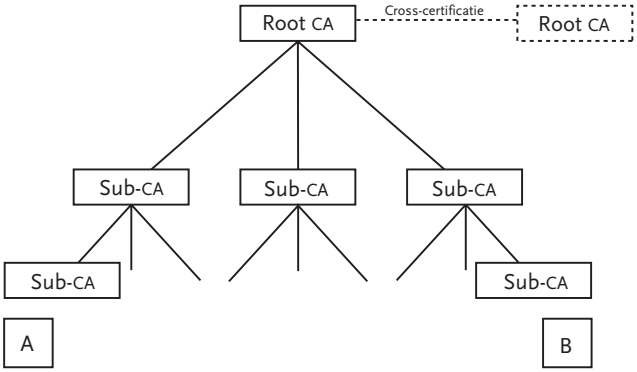
Een gebruiker dient een aanvraag voor het verkrijgen van een certificaat in bij de RA. Hiertoe dient hij zich, afhankelijk van het soort certificaat dat wordt aangevraagd, te identificeren met een geldig identiteitsbewijs. Bij deze aanvraag geeft de gebruiker tevens aan voor welke toepassing het certificaat wordt aangevraagd, bijvoorbeeld voor het zetten van digitale handtekingen, het vercijferen van informatie, enzovoort. De gebruiker wordt geacht kennis te nemen van de *Certificate Policy* van de CA.

6.4.2 Uitwisselen van certificaatgegevens

Onder de root-CA (*issuer*) worden verschillende groepen gebruikers gevormd die veilig met elkaar kunnen communiceren, zie figuur 6.3. Als gebruiker A wil communiceren met gebruiker B, dan wordt via de verschillende certificaten van de sub-CA's, de root-CA enzovoort de publieke sleutel van gebruiker B verkregen. Dit wordt ook wel een certificatie-pad genoemd. Een certificatie-pad is dus, logisch gezien, een ononderbroken keten van vertrouwde punten tussen twee gebruikers om elkaar te authentiseren. Vanwege de *hiërarchie* zijn de *Certificate Policies* (CP's) en *Certificate Practice Statements* (CPS'n) van alle CA's op elkaar afgestemd.

Als twee verschillende CA's gebruik willen maken van elkaars certificaten, dan kan dit door *cross-certificatie*. Dit is in figuur 6.3 met stippellijnen aangegeven. Allereerst dient er een vertrouwensrelatie tussen beide CA's te bestaan. Vervolgens moeten de *Certificate Policies* (CP's) en *Certificate Practice Statements* (CPS'n) op elkaar worden afgestemd. Dit is het meest complexe deel van de cross-certificatie. Als de ene CA namelijk

een hoger veiligheidsniveau hanteert voor de uitgifte van certificaten dan de andere CA, kan de certificaat-informatie niet zonder meer worden uitgewisseld. Zou dit wel gebeuren, dan zou dit een inbreuk op het veiligheidsniveau van de CA met het hoogste veiligheidsniveau als gevolg hebben.
Als de CP's en de CPS'n op elkaar zijn afgestemd, dan hebben de CA's een vertrouwensrelatie en kunnen certificaatgegevens tussen twee verschillende CA's worden uitgewisseld.
Hierbij moeten er natuurlijk wel afspraken worden gemaakt over de te gebruiken algoritmen.



Figuur 6.3 Hiërarchische X.500 structuur voor de uitwisseling van certificaatgegevens

6.4.3 Gebruik sleutelparen

Bij een PKI wordt gebruikgemaakt van asymmetrische sleutels zoals besproken in hoofdstuk 2.

Er wordt een onderscheid gemaakt in *one-key pair* en *two-key pair* systemen. Bij *one-key pair* systemen wordt hetzelfde sleutelpaar gebruikt voor zowel het zetten van de handtekening onder een bericht en het verifiëren hiervan als voor het vercijferen en ontcijferen van de inhoud van een bericht. Een nadeel van het *one-key pair* systeem is dat key back-up en *recovery* niet eenvoudig is. Immers, de privé-sleutel voor het zetten van

handtekeningen mag uitsluitend beschikbaar zijn voor de eigenaar zelf, om misbruik te voorkomen.
Een *two-key pair* systeem kent dit nadeel niet. Bij dit systeem worden twee afzonderlijke sleutelparen gebruikt voor het zetten van de handtekening onder een bericht en het verifiëren hiervan en voor het vercijferen en ontcijferen van de berichtinhoud. De gebruiker moet hierbij zelf zorg dragen voor een back-up van de privé-sleutel voor het zetten van zijn handtekening. Een kopie van de sleutels voor het vercijferen en ontcijferen van de berichtinhoud kan eventueel door een onafhankelijke derde, een zogenaamde *Trusted Third Party,* worden opgeslagen ten behoeve van sleutelherstel.

6.4.4 Juridische aspecten van een CA

De juridische aspecten van een CA, zoals leveringsvoorwaarden, aansprakelijkheid en toepassingsgebied staan aangegeven in het *Certificate Practice Statement* (CPS) en de *Certificate Policy* (CP) van de CA.

Certificate Policy (CP)

In de *Certificate Policy* staat aangegeven voor welke toepassing(en) een certificaat bedoeld is.
Een formele definitie van de ITU X.509 Recommendation is:

A named set of certificate policy rules relating to the use of a certificate and the certified public key, recognized by both the issuer and the user of the certificate. A certificate policy relates to a class of activity across a community of distributed systems which has a common security requirement, e.g. electronic data interchange (EDI) for trading of goods within a given price range.

Per toepassing kunnen zodoende verschillende voorwaarden voor het gebruik van het certificaat gelden, ook als het certificaat door dezelfde partij is uitgegeven.

***Certificate Practice Statement* (CPS)**

Een *Certificate Practice Statement* geeft aan onder welke algemene condities en op welke wijze de CA certificaten uitgeeft. In het CPS is opgenomen tot hoe ver de verplichtingen en aansprakelijkheid van een CA gaan. Ook kan in de CPS opgenomen zijn wat de verplichtingen van een gebruiker en van de RA zijn. Verder is uit de CPS af te leiden hoe hoog het betrouwbaarheidsniveau van de CA in relatie met de verschillende classes van certificaten is.

Het is daarom voor een gebruiker noodzakelijk om kennis te nemen van de CPS om te weten wat hij van de CA kan verwachten (en wat niet).

Verder wordt een CPS vaak gebruikt als deel van een contract tussen twee verschillende CA's.

Zowel de CP's als de CPS'n kunnen onder toezicht staan van een zogenaamde *Policy Management Authority* (PMA). Deze PMA bepaalt het beleid ten aanzien van het kwaliteitsniveau van de certificaten en de voorwaarden waaronder certificaten worden uitgegeven.

6.4.5 Applicaties

De volgende applicaties zouden gebruik kunnen maken van een PKI om betrouwbare communicatie mogelijk te maken:

- *E-mail:* De meest bekende applicatie die gebruik kan maken van een PKI is e-mail. De identiteit van de verzender kan hierbij aan de ontvangerzijde worden geverifieerd en bovendien kan de berichtinhoud worden vercijferd.
- *Webserver verkeer:* Bescherming van het webserver verkeer vindt plaats door gebruikmaking van SSL: authenticatie van de webserver en vercijfering van het verkeer.
- *VPN's:* In omgevingen waar grote aantallen VPN's worden toegepast, kan gebruik worden gemaakt van een PKI om het sleutelbeheer van deze VPN's efficiënt uit te kunnen voeren.
- *Access control: Single Sign-on* op basis van een PKI. Hierbij is sprake van eenmalige authenticatie met behulp van een PKI, waarna een gebruiker is geautoriseerd voor toegang tot diverse applicaties.

Bijlage 1

Overzicht relatie Code voor Informatiebeveiliging met Basisnormen Beveiliging en Beheer ICT-infrastructuur

Toelichting: voor het ontwikkelen van een compleet beveiligingsnormenstelsel voor een exploitatieorganisatie van een serviceprovider (intern binnen een concern dan wel als zelfstandig bedrijf) zullen ook een meer algemene beveiligingsonderwerpen aan de orde moeten komen, die niet tot de reikwijdte van deze PI-studie behoren. Normen die uitsluitend betrekking hebben op het beleid op concernniveau, bedrijfsvoering in de klant- of gebruikersorganisatie of op het ontwikkelen van informatiesystemen zijn, hier niet aangekruist.

Code voor informatiebeveiliging		BBBI ICT-infra	BBBI beheer	Overige processen
3	**Beveiligingsbeleid**			
3.1	Informatiebeveiligingsbeleid			
3.1.1	Beleidsdocument voor informatiebeveiliging			
3.1.2	Beoordeling en evaluatie			
4	**Beveiligingsorganisatie**			
4.1	De infrastructuur van informatiebeveiliging			
4.1.1	Stuurgroep voor informatiebeveiliging			
4.1.2	Coördinatie van informatiebeveiliging			
4.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging			X
4.1.4	Autorisatieproces voor ICT-voorzieningen	3.1.2	4.9 INC	X
4.1.5	Specialistisch advies over informatiebeveiliging		4.9 INC	
4.1.6	Samenwerking tussen organisaties		4.9 INC	
4.1.7	Onafhankelijke beoordeling van informatiebeveiliging			X
4.2	Beveiliging van toegang door derden			
4.2.1	Identificeren van risico's van toegang door derden			X
4.2.2	Beveiligingsvoorwaarden in contracten met derden		4.13 Sup	

Code voor informatiebeveiliging		BBBI ICT-infra	BBBI beheer	Overige processen
4.3	Uitbesteding			
4.3.1	Beveiligingsvoorwaarden in uitbestedings contracten		4.13 Sup	
5	**Classificatie en beheer van bedrijfsmiddelen**			
5.1	Verantwoording voor bedrijfsmiddelen			
5.1.1	Overzicht van bedrijfsmiddelen			X
5.2	Classificatie van informatie			
5.2.1	Richtlijnen voor het classificeren		4.4 SeM	X
5.2.2	Labelen en verwerken van gegevens			
6	**Beveiligingseisen ten aanzien van personeel**			
6.1	Beveiligingseisen in de functieomschrijving en bij het aannemen van personeel			
6.1.1	Beveiligingseisen in de functieomschrijving			X
6.1.2	Screening en personeelsbeleid			X
6.1.3	Geheimhoudingsverklaring			X
6.1.4	Arbeidsvoorwaarden			X
6.2	Training voor gebruikers			
6.2.1	Opleiding en training voor informatiebeveiliging			X
6.3	Reageren op beveiligingsincidenten en storingen			
6.3.1	Het rapporteren van beveiligingsincidenten			X
6.3.2	Het rapporteren van zwakke plekken in de beveiliging			X
6.3.3	Het rapporteren van onvolkomenheden in de programmatuur			X
6.3.4	Lering trekken uit incidenten			X
6.3.5	Disciplinaire maatregelen			X
7	**Fysieke beveiliging en beveiliging van de omgeving**			
7.1	Beveiligde ruimten			
7.1.1	Fysieke beveiliging van de omgeving			X
7.1.2	Fysieke toegangsbeveiliging			X
7.1.3	Beveiliging van kantoren, ruimten en voorzieningen			X
7.1.4	Werken in beveiligde ruimten		4.12 Oper	
7.1.5	Afzonderlijke ruimten voor laden en lossen van goederen		4.12 Oper	X

Code voor informatiebeveiliging	BBBI ICT-infra	BBBI beheer	Overige processen
7.2 Beveiliging van apparatuur			
7.2.1 Het plaatsen en beveiligen van apparatuur		4.12 Oper	X
7.2.2 Stroomvoorziening	3.1.2	4.12 Oper	X
7.2.3 Beveiliging van kabels			X
7.2.4 Onderhoud van apparatuur			X
7.2.5 Beveiliging van apparatuur buiten de organisatie			X
7.2.6 Veilig afvoeren en hergebruiken van apparatuur		4.12 Oper	
7.3 Algemene beveiligingsmaatregelen			
7.3.1 Clear desk en clear screen policy	3.4		X
7.3.2 Het verwijderen van bedrijfseigendommen		4.12 Oper	X
8 Beheer van communicatie – en bedienings-processen			
8.1 Bedieningsprocedures en verantwoordelijkheden			
8.1.1 Schriftelijke bedieningsprocedures		4.12 Oper	
8.1.2 Het beheer van wijzigingen		4.10 CHG	
8.1.3 Procedures voor het behandelen van incidenten		4.9 INC	
8.1.4 Functiescheiding		4.1 Inr	
8.1.5 Scheiding van voorzieningen voor ontwikkeling en productie	3.1.1	4.1 Inr	
8.1.6 Extern beheer van voorzieningen		4.1 Inr, 4.10 CHG	
8.2 Systeemplanning en -acceptatie			
8.2.1 Capaciteitsplanning		4.4 Cap	
8.2.2 Acceptatie van systemen		4.10 CHG	
8.3 Bescherming tegen kwaadaardige programmatuur			
8.3.1 Controle op kwaadaardige programmatuur	3.1.2	4.4 SeM, 4.9 INC, 4.10 CHG, ICT-infra	X
8.4 Huisregels			
8.4.1 Reservekopieën maken (back-ups)		4.12 Oper	
8.4.2 Bijhouden van een logboek		4.12 Oper	
8.4.3 Storingen opnemen in een logboek		4.12 Oper	
8.5 Netwerkbeheer			
8.5.1 Maatregelen voor netwerken		4.12 Oper	

Code voor informatiebeveiliging	BBBI ICT-infra	BBBI beheer	Overige processen
8.6 Behandeling en beveiliging van computermedia			
8.6.1 Beheer van verwijderbare computermedia		4.12 Oper	
8.6.2 Afvoer van media		4.12 Oper	X
8.6.3 Procedures voor de behandeling van gegevens			X
8.6.4 Beveiliging van systeemdocumentatie			X
8.7 Uitwisseling van gegevens en programmatuur			
8.7.1 Overeenkomsten over het uitwisselen van gegevens en programmatuur			X
8.7.2 Beveiliging van media tijdens transport		4.12 Oper	X
8.7.3 Beveiliging van elektronische handel (e-commerce)			
8.7.4 Beveiliging van elektronische post (e-mail)			
8.7.4.1 Beveiligingsrisico's			
8.7.4.2 Beleid ten aanzien van elektronische post			
8.7.5 Beveiliging van elektronische kantoorsystemen			X
8.7.6 Publiek toegankelijke systemen			X
8.7.7 Andere vormen van gegevensuitwisseling			X
9 Toegangsbeveiliging			
9.1 Zakelijke eisen ten aanzien van toegangsbeveiliging			
9.1.1 Beleid ten aanzien van toegangsbeveiliging		4.4 SeM	X
9.2 Management van toegangsrechten/ autorisatiebeheer			
9.2.1 Registratie van gebruikers			X
9.2.2 Beheer van speciale bevoegdheden			X
9.2.3 Beheer van gebruikerswachtwoorden			X
9.2.4 Controle op toegangsrechten			X
9.3 Verantwoordelijkheden van gebruikers			
9.3.1 Gebruik van wachtwoorden			X
9.3.2 Onbeheerde gebruikersapparatuur			X
9.4 Toegangsbeveiliging voor netwerken			
9.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten		4.4 SeM	
9.4.2 Verplichte route	2.5		
9.4.3 Authenticatie van gebruikers bij externe verbindingen	2.3		
9.4.4 Node-verificatie	3.3		

Code voor informatiebeveiliging	BBBI ICT-infra	BBBI beheer	Overige processen
9.4.5 Beveiliging van diagnosepoorten op afstand		4.12 Oper	
9.4.6 Scheiding in netwerken	3.5		
9.4.7 Beheer van netwerkverbindingen	3.5		
9.4.8 Beheer van netwerkroutering	3.5		
9.4.9 Beveiliging van netwerkdiensten		4.13 Sup	
9.5 Toegangsbeveiliging voor besturingssystemen			
9.5.1 Automatische identificatie van werkstations	3.4		
9.5.2 Aanlogprocedures voor werkstations	3.4		
9.5.3 Gebruikersidentificatie en -authenticatie			X
9.5.4 Wachtwoordsysteem	3.7		
9.5.5 Gebruik van systeemhulpmiddelen	3.1.3 3.8.2		
	3.10		X
9.5.6 Stil alarm ter bescherming van gebruikers			X
9.5.7 Time-out voor werkstations	3.4		
9.5.8 Beperking van verbindingstijd	3.6		
9.6 Toegangsbeveiliging voor toepassingen			
9.6.1 Beperking van toegang tot informatie			X
9.6.2 Isolatie van gevoelige systemen			X
9.7 Bewaking van toegang tot en gebruik van systemen			
9.7.1 Vastleggen van beveiligingsrelevante activiteiten ('event-logging')	3.10		
9.7.2 Bewaking van systeemgebruik			X
9.7.3 Synchronisatie van systeemklokken	3.1.2	4.12 Oper	
9.8 Mobiele computers en telewerken			
9.8.1 Mobiele computers	3.4		X
9.8.2 Telewerken			X
10 Ontwikkeling en onderhoud van systemen			
10.1 Beveiligingseisen voor systemen			
10.1.1 Analyse en specificatie van beveiligingseisen			
10.2 Beveiliging in toepassingssystemen			
10.2.1 Validatie van invoergegevens			
10.2.2 Validatie van de interne gegevensverwerking			
10.2.3 Authenticatie van berichten			
10.2.4 Validatie van uitvoergegevens			

Code voor informatiebeveiliging	BBBI ICT-infra	BBBI beheer	Overige processen
10.3 Cryptografische beveiliging			
10.3.1 Beleid ten aanzien van het gebruik van cryptografische beveiliging			
10.3.2 Versleuteling (encryptie)			
10.3.3 Digitale handtekeningen			
10.3.4 Onweerlegbaarheid			
10.3.5 Sleutelbeheer			
10.4 Beveiliging van systeembestanden			
10.4.1 Controle op operationele programmatuur		4.11 Rel	
10.4.2 Beveiliging van testgegevens		4.12 Oper	
10.4.3 Toegangsbeveiliging voor bibliotheken met bronprogramma's		4.11 Rel	
10.5 Beveiliging bij ontwikkel – en ondersteuningsprocessen			
10.5.1 Procedures voor het beheer van wijzigingen		4.11 Rel, 4.10 CHG	
10.5.2 Technische controle op wijzigingen in het besturingssysteem		4.10 CHG	
10.5.3 Restricties op wijzigingen in programmatuurpakketten	3.1.2		
10.5.4 Geheime communicatiekanalen en Trojaanse paarden		4.13 Sup	
10.5.5 Uitbestede ontwikkeling van programmatuur			
11 Continuïteitsbeleid			
11.1 Aspecten van continuïteitsbeleid			
11.1.1 Het proces van continuïteitsplanning		4.5 ISCM	X
11.1.2 Bedrijfscontinuïteit en analyse van mogelijke gevolgen			X
11.1.3 Het schrijven en invoeren van continuïteitsplannen		4.5 ISCM	X
11.1.4 Structuur voor continuïteitsplannen		4.5 ISCM	X
11.1.5 Testen, bijwerken en evalueren van continuïteitsplannen		4.5 ISCM	X

Code voor informatiebeveiliging	BBBI ICT-infra	BBBI beheer	Overige processen
12 Naleving			
12.1 Naleving van de wettelijke voorschriften			
12.1.1 Specificatie van de van toepassing zijnde wetgeving			
12.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)		4.4 SeM, 4.11 Rel	X
12.1.3 Beveiliging van bedrijfsdocumenten		4.4 SeM, 4.12 Oper	X
12.1.4 Bescherming van persoonlijke informatie			X
12.1.5 Voorkomen van misbruik van ICT-voorzieningen			X
12.1.6 Voorschriften ten aanzien van het gebruik van cryptografische middelen			X
12.1.7 Verzamelen van bewijsmateriaal			X
12.2 Beoordeling van de naleving van het veiligheids-beleid de technische vereisten			
12.2.1 Naleving van het beveiligingsbeleid		4.1 Inr	X
12.2.2 Controle op naleving van technische normen			X
12.3 Overwegingen ten aanzien van systeemaudits			
12.3.1 Beveiligingsmaatregelen voor systeemaudits			X
12.3.2 Beveiliging van hulpmiddelen voor systeemaudits		4.12 Oper	X

Bijlage 2

Overzicht relatie CobiT met Basisnormen Beveiliging en Beheer ICT-infrastructuur

Toelichting: de aangegeven relatie tussen CobiT en de basisnormen van deze PI-studie betekenen niet dat de control objectives van CobiT per onderscheiden aandachtsgebied volledig zijn overgenomen. De relatie kan bijvoorbeeld slechts betrekking hebben op één control objective. De andere objectives hebben niet specifiek betrekking op een exploitatieorganisatie.

CobiT	Basisnormen Beveiliging en Beheer ICT-infrastructuur
Planning & Organisatie	
PO1 Define a strategic information technology Plan	
PO2 Define the Information Architecture	
PO3 Determine Technological Direction	
PO4 Define the ICT Organisation and Relationships	4.1 Inrichting processen
PO5 Manage the ICT Investment	
PO6 Communicate Management Aims and Direction	4.6 Security Management
PO7 Manage Human Resources	
PO8 Ensure Compliance with External Requirements	
PO9 Assess Risks	
PO10 Manage Projects	
PO11 Manage Quality	
Acquisiction & Implementation	
AI1 Identify Automated Solutions	
AI2 Acquire and Maintain Application Software	
AI3 Acquire and Maintain Technology Infrastructure	
AI4 Develop and Maintain Procedures	
AI5 Install and Accredit Systems	
AI6 Manage Changes	4.11 Change Management

CobiT		Basisnormen Beveiliging en Beheer ICT-infrastructuur
Delivery & Support		
DS1	Define and Manage Service Levels	4.2 Service Level Management
DS2	Manage Third-Party Services	4.14 Supply Management
DS3	Manage Performance and Capacity	4.4 Capacity Management
DS4	Ensure Continuous Service	4.5 ICT Service Continuity Management 4.3 Availability Management
DS5	Ensure Systems Security	4.1 Inrichting, 4,6 Sec.Mgt, 4.9 Incident, 4.13 Operations, 3 ICT-infrastructuur
DS6	Identify and Allocate Costs	
DS7	Educate and Train Users	
DS8	Assist and Advise Customers	4.8. ServiceDesk, 4.9 Incident Management,
DS9	Manage the Configuration	4.7 Configuration Management; 4.12 Release Management
DS10	Manage Problemen and Incidents	4.8 ServiceDesk, 4.9 Incident Management, 4.10 Problem Management
DS11	Manage Data	4.13 Operations, 4.12 Release Mgt, 3 ICT-infrastructuur
DS12	Manage Facilities	3. ICT-infrastructuur
DS13	Manage Operations	4.13 Operations
Monitoring		
M1	Monitor the Processes	4.1 Inrichting processen
M2	Assess Internal Control Adequacy	4.1 Inrichting processen
M3	Obtain Independent Assurance	4.14 Supply Management
M4	Provide for Independent Audit	

Bijlage 3

Begrippen

ICT-Service: het geheel van toepassingen, TIS-componenten, servicedocumentatie en -handleidingen, die tot een afzonderlijke dienstverlening leidt en waarvoor een SLA kan worden afgesloten.

ICT-component: elke verschijningsvorm van apparatuur, systeem- en toepassingsprogrammatuur en bijbehorende gegevensbestanden.

TIS-component: elke verschijningsvorm van apparatuur en systeemprogrammatuur inclusief bijbehorende systeembestanden (TIS = Technische InfraStructuur).

Configuratie Item: elke (logische) verschijningsvorm van een ICT-component of ICT-service alsmede documentaties hieromtrent, die te onderscheiden zijn in verband met het beheer van de ICT-infrastructuur.

ICT-infrastructuur: het geheel van ICT-componenten.

Systeemprogrammatuur: besturingssystemen die kunnen bestaan uit: (netwerk)operating systems, databasemanagement systems, transactieprocessing monitors, utilities en ondersteunende standaardprogrammatuur voor het technisch, operationeel of beveiligingsbeheer van ICT-componenten.

Domein: de logische verzameling van clients en servers met hetzelfde beveiligingsniveau, die via een netwerkinfrastructuur zonder enige beperking contact met elkaar kunnen opnemen en gegevens(pakketten) kunnen uitwisselen. Domeinen communiceren met elkaar via filterende netwerkkoppelingen.

Clients: werkstation, Portable PC, handheld of andere mobiele eindgebruikerapparatuur;
– client Operating System met bijbehorende systeembestanden;
– toepassingsprogrammatuur met bijbehorende gegevensbestanden.

Servers: Alle servers, mini's en mainframes die door één of meer clients worden benaderd:
– gateways en beheerstations;
– systeemprogrammatuur met bijbehorende systeembestanden;
– toepassingsprogrammatuur met bijbehorende gegevensbestanden.

Netwerkinfrastructuur: Netwerkverkeer, protocollen:
– routers, bridges en soortgelijke actieve netwerkcomponenten;
– bekabeling en badgasten;
– netwerkaansluitpunten.

Filterende netwerkkoppeling: een deel van de ICT-infrastructuur, dat de koppeling verzorgt tussen twee domeinen met een verschillend beveiligingsniveau door op enigerlei wijze het onderling verkeer te beperken.

Bijlage H - Literatuuroverzicht

Boeken en artikelen

"802.11b Wired Equivalent Privacy (WEP) Security", Wireless Ethernet Compatibility Alliance, 19 februari 2001

"Applied Cryptography protocols, algorithms, and source code in C", second edition, Bruce Schneier, Wiley, 1996

'Basismethoden cryptografie', J. van der Lubbe, 1e druk, Delftse Uitgevers Maatschappij, 1994

"*Bestuurlijke informatieverzorging deel 1, algemene grondslagen"*, 4e druk tweede oplage, Starreveld, Mare, Joëls, 1997
Building and Managing Virtual Private Netwrork, Dave Kosiur,1998, Wiley Computer Publishing, ISBN: 0-471-29526-4

'Code, de wedloop tussen makers en brekers van geheime codes en cijferschrift', S. Singh, De Arbeiderspers, 1999 (origineel: *'The code book'*, Simon Singh, London 1999).

'Computernetwerken en datacommunicatie, hoofdlijnen en praktijk', R. Matthijssen, J. Truijens, H. Doorenspleet, 5e druk, Academic service, 1997

Consultatiedocument PKI Overheid, Taskforce PKI Overheid, 26 april 2001.

Crypto Law Survey, B. Koops

Cryptografie en ICT, Theorie en praktijk, S. El Aoufi, ISBN 90 395 1759 2, Academic Service, 2001.

'*Cryptografie in de praktijk'*, G. Damen, R. Goossens, A. Hofman, E. Verheul, L. de Vries, Ten Hagen en Stam, 2000

'Defending your digital assets', Randall K. Nichols, Daniel J Ryan en Julie J.C.H. Ryan, (NewYork 2000).

Elektronisch verrichten van Rechtshandelingen, MDW Rapport, maart 1998.

Encryption and strong Authentication for Electric Commerce, Helsinki University of technology,

'Get SET for secure electronic transactions', Compact, jubileumuitgave 25 jaar, Ir. R. de Wolf

'Handboek Informatiebeveiliging', Gemeente Amsterdam, 1994

Het Handboek voor Inernet- & Intranettechnologie, Jereon Vanheste, 2000, Addison-Wesley, ISBN: 90-430-0227-5

'*Informatie en telecommunicatie'*, H. Pijnappels, Wolters-Noordhoff, 1987

'Informatiebeveiliging onder controle', P. Overbeek, E. Roos Lindgreen, M. Spruit, Prentice Hall, 2000

"Intercepting Mobile Communications: The Insecurity of 802.11", draft, Nikita Borisov en David Wagner (UC Berkeley) en Ian Goldberg (Zero-Knowledge Systems)

'Internet, intranet en beveiliging: het technische kader', P. van Dam, G. Hulst, H. van Hulst, H. Luiijf, M. Spruit, Ten Hagen en Stam, 1998

Internet Cryptography, Richard E. Smith, 1997, Addison-Wesley, ISBN: 0-201-92480-3

Layer Two Tunneling Protocol, White Paper:, Lucent Technologies

'Netwerkbeveiliging en cryptografie, beginselen en praktijk', W. Stallings, Academic service, 2000

Network-Layer Encryption, white paper : Cisco IOS software Fearture

Ontwerp Regeling geordende en toegankelijke staat archiefbescheiden 2000, Versie 2000-01-14, CONCEPT.

"Opzet Key Management organisatie – NVB-handleiding voor Key Management", Nederlandse Vereniging van Banken (NVB), april 1998

'Quantum-sleutel-kwantum', A. van Leeuwen, Artikel uit c't 2000, nummer 3

'Secure Data Networking', M. Pursers, Artech House, 1993

"Selecting Cryptographic Key Sizes", Arjen K. Lenstra, Eric R. Verheul, 24 november 1999

"Sleutelen aan Versleutelen, organisatorische aspecten rond cryptografie", M. W. Baurichter, Compact, ten Hagen Stam, Amsterdam, 1999

'Virtual Private Networks', de EDP Auditor, nummer 4, 1998, Arjan Vos.

Wet Computer Criminaliteit, Staatsblad 1993, 33.

Wet Openbaarheid van bestuur, MP10 – 002, 1994.

'Wide area networks en Datanet 1', Samson Bedrijfsinformatie, 1991

Overzicht urls

URL	**Omschrijving**
http://www.nist.gov/	NIST (National Institute of Standards and Technology) Standaarden met betrekking tot cryptografische algoritmen en veilige opslag van cryptografisch materiaal.
http://csrc.nist.gov/encryption/aes	NIST, publicatie over AES
http://www.counterpane.com	Counterpane Internet Security

	Informatieve site met veel publicaties van Bruce Schneier
http://www.cert.org/	Informatieve site met meldingen over vulnerabilities, incidenten en oplossingen
http://www.crypto.com	Matt Blaze's crypto resource on the web. Nieuws, artikelen en links mbt cryptografie
http://www.cryptosavvy.com	Informatie over sleutellengte
http://www.secg.org/	SECG: Standards for Efficient Cryptography Group
http://www.ict.etsi.org/eessi/EESSI-homepage.htm	Standaarden voor digitale handtekeningen van EESSI
http://www.ietf.org	IETF: Internet Engineering Task Force Standaarden voor Internet omgeving
http://www.openssh.org/	Open Source versie van SSH
http://www.openssl.org/	Open source toolkit voor SSL
http://www.cdt.org/crypto/risks98/	The risks of "Key Recovery", "Key-Escrow" and "Trusted Third-Party" Encryption.
http://www.commoncriteria.org/	Common Criteria Evaluatiecriteria voor de beveiliging van ICT componenten.
http://www.itsec.gov.uk/	ITSEC Evaluatiecriteria voor de beveiliging van ICT componenten.
http://www.pkiforum.org/	Internationale non-profit multi-vendor alliantie met als doel de acceptatie en het gebruik van PKIS en op PKI gebaseerde producten en services te versnellen.
http://www.bsi-global.com/ http://www.c-cure.org/	Code of Practice – BS7799
http://wwwpkioverheid.nl/	Gebruik van een PKI voor de Nederlandse overheid
http://www.icsa.net/	ICSA: International Computer Security Agency. Certificatie van beveiligingsproducten. Recentelijk overgenomen door Truesecure Corporation:

	http://www.truesecure.com/
http://www.wapforum.org/	WAP-Forum Forum ter bevordering van de ontwikkeling, standaardisatie en publicatie van WAP specificaties.
http://www.rsasecurity.com/rsalabs/	RSA algoritme en PKCS